texas
crime
prevention
institute

54058

SOUTHWEST TEXAS STATE UNIVERSITY

# DATA ANALYSIS

DATA ANALYSIS COURSE
FOR CRIME PREVENTION
OFFICERS AND ANALYSTS

SPONSORED BY:

CRIMINAL JUSTICE DIVISION
OFFICE OF THE GOVERNOR
STATE OF TEXAS

# DATA ANALYSIS COURSE FOR
# CRIME PREVEVTION OFFICERS AND ANALYSTS

prepared for the

TEXAS CRIME PREVENTION INSTITUTE
SOUTHWEST TEXAS STATE UNIVERSITY
SAN MARCOS, TEXAS

by

Dr. James Poirot
Mathematics Department
Southwest Texas State University

Lt. James Rand
Department Of Public Safety
Sunnyvale, California

G.K. Maenius
Texas Crime Prevention Institute
Southwest Texas State University

# ACKNOWLEDGEMENTS

The development of the Data Analysis School for Crime Prevention Officers and Analysts could not have been undertaken without the aid and assistance of several individuals.

First, we would like to acknowledge those persons responsible for developing the material for this text: Dr. James Poirot, Mathematics Department, Southwest Texas State University, whose expertise in the field of computer science contributed to a substantial protion of this book and Lt. James Rand, Sunnyvale Department of Public Safety, Sunnyvale, California, whose knowledge and input in the area of crime data analysis was invaluable.

The Texas Crime Prevention Institute wishes to extend its appreciation to Sterling Swift Publishing Company for usage of parts of Computer Science for the Teacher included in Chapters V, VII and VIII. Appreciation is also expressed to IBM Corporation and Sperry-Univac Corporation for many of the photographs contained within this text.

Finally, the Texas Crime Prevention Institute would like to extend its appreciation to Bronwynn Berish, Geraldine Caldwell, James Poirot, and Peter A. Stone for usage of parts of Specialized Data School for Crime Prevention Officers: 1975, in developing Chapters I and IV of this manual.

# FOREWARD

Crime data analysis is a set of processes consisting of data collection, data collation, data analysis, interpretation, program implementation and program evaluation. All of these functions are undertaken in order to predict criminal trends for the purpose of reducing crime in a cost-effective manner.

Whether the crime prevention analysis function is accomplished by a civilian analyst or a law enforcement officer, the individual is faced with not only implementing a relatively new concept within a traditional environment, but also must be capable of the possible dealing with individuals ranging from the city manager to local citizenry. The analyst must be aware of the potential help and support he may receive and likewise give to his constituency. Chapter I, "Implementing a New Concept in a Traditional System" and Chapter II "Objectives in Crime Analysis" are designed to acquaint the analyst with some of the possible tasks facing him.

Since the analyst is concerned so deeply with the analysis of criminal data, it is logical then, that one studies the most powerful data storage and data manipulation device available, the electronic computer. The computer, over the past twenty years, has had a tremendous impact on law enforcement agencies. Functions ranging from simple data storage and retrieval to sophisticated statistical analysis of this data can be easily and quickly accomplished by use of the computer. Criminal records, judicial information, traffic control, and police deployment are only a few of the many uses for which a computer can be employed. It is imperative then, that everyone associated with data analysis in the law enforcement area, be familiar with the operation and application of the computer.

As stated above, three of the primary duties of the analyst are to collect, collate, and analyze criminal data. Chapters III and IV covering "The Use and Misuse of Statistics" and "Records" provide valuable information for accomplishing these duties.

In order to effectively use the electronic computer, one must understand the operation and configuration of a complete computer system. Chapter V covers these topics, while Chapter VI reviews many of the law enforcement applications of the computer. The Dallas Criminal Justice Information System is studied in detail.

The computer is known for its problem solving ability. Thus, Chapter VII on "Flowcharting" is included. Even though flowcharting is an aid in computer programming, it can be used most effectively in any problem solving situation, whether or not the problem is to be solved on a computer.

Chapter VIII covers one of the simple computer languages, BASIC. This language is generally available on all computer systems so that the analyst could quite easily be writing his own computer programs.

Chapter IX covers the "Privacy Act" while Chapter X discusses "Computer Security". These two topics are of particular interest to analyst because of the recent development relating to criminal information security. Chapter XI is included giving examples of "Computer Crimes" so that analysts might be increasingly aware of the problems in this fast growing crime area.

## TABLE OF CONTENTS

# CHAPTER I

## IMPLEMENTING A NEW CONCEPT IN A TRADITIONAL SYSTEM

Whether the crime prevention analysis function be accomplished by a civilian analyst, a law enforcement officer, or a person responsible for crime analysis on a regional basis, the individual(s) are faced with not only implementing a relatively new concept within a traditional environment, but with functioning within both a formal and informal structure. The multiple facets of the public with whom the analyst must deal, depending on his particular job description, may include city managers, chiefs, sworn officers, ranking officers, citizenry, and other individuals of like responsibility as his own. The analyst must be aware of the potential help and support he may receive and likewise give to his constituency.

In many areas the position of crime prevention analyst has either never existed before or is relatively new. Conversely the law enforcement agency itself has existed in basically the same form for several decades. Bearing this in mind, an analyst entering an agency must realize that he will be dealing with people having years of experience in understanding and dealing with crime trends, analysis of these trends, and techniques for the prevention of crime although this sometimes is only "gut feeling" which may or may not have ever been formalized. The analyst can therefore draw a wealth of information from the constituency he is serving.

"Red flags" should go up in the mind of any analyst (because they will in the minds of his peers) that approaches the subject of crime analysis with the attitude that through crime analysis he alone can solve the crime problem. Think twice before making a statement like the following: "If you do such and such, I guarantee your problems will be solved".

An analyst is not a soothsayer and cannot say that by subtracting B from A you unequivocally will get C when dealing with crime data. The analyst can be studying the data, by considering an many variables as possible, and by drawing on the experience of others, present the facts gleaned from the data and suggest realistic possibilities to be considered for solution.

## Communication

As suggested before, communication must be open in order to receive the information needed for analysis and also to present the information prepared by the analyst. A helpful hint to remember is that communication, whether formal or informal, will necessarily be structured differently dependent upon the makeup for the group with whom you are communicating.

For instance, if you are talking to a more advanced group, you may want to discuss in terms of "detailed statistical analysis" mentioning the different types of statistical methods you used in your evaluation. However, if you wanted to present the same information to a group composed of persons functioning primarily in the area of enforcement the more sophisticated approach using statistical terminology may result in a "turn-off". Don't talk down to anyone, but do not try to talk over their heads either.

When communication is kept open, the analyst stands to gain as much help from his peer group as he provided them.

## Understanding the Organizational Structure

Before the analyst can affect a functional analysis unit and before there can be successful communication within the total orgainzation, he must understand the Organizational Structure of the agency with whom he will be working.

The first step towards accomplishing this may necessarily be to sit down with a copy of a formal organizational chart of the agency to determine the structural hierarchy. Because of the structural likeliness to a military organization existent within law enforcement agencies, an understanding of the chain of command is important to an analyst's success. A sworn officer functioning in this position won't have the difficulty in recognizing the chain of command that a civilian or possibly regional planner may have. The analyst, new to the law enforcement environment, will find that by understanding the orgainzational structure, he will know where he can find the data he wants for his informational needs and, who to approach to get this data. In a law enforcement agency, the shortest distance between two points is not necessarily a straight line.

Once the crime prevention analyst is established, and gains some insight into the people around him, he may find the existence of a more informal organizational structure. In this type environment, the analyst can often times accomplish a perceived goal in a more informal way, (i.e. oral communication through informal talks) by communicating directly with the individual most familiar with the information the analyst needs. He may also find that in the informal organization a wealth of information may become available to him that would be virtually unobtainable from strict compliance to a formal organizational structure. The analyst will with time and insight learn to discern the most reliable information sources.

Helpful hints:

1) Know the people you work with.
2) Allow them to know you.
3) Be thorough in your evaluation of any given problem.
4) Be open to suggestions from peers on all levels. (i.e. listen)
5) Be able to substantiate any conclusions you draw.

## Impact of Crime Analysis

Crime analysis means many different things to different people. To the line officer it means where things are happening, when they are happening, and with some insight, tells him why they are happening.

To the line supervisor who spends most of his time tied to a desk, crime analysis gives him concise information as to what is happening around him, by the week, month or year. Line supervisors can and do use crime analysis data in the evaluation of their personnel.

Administrative staff use crime data consistently to evaluate their position now, relative to goals and objectives previously set for any particular time frame. Crime data shows the chief administrator much more than just who fell victim to what type of crime. With the correct information the chief administrator can set policy, modify existing policy and talk knowingly about the crime profile in the community.

City planners, city managers, city councils, in fact all city departments can and do use crime data for a variety of purposes. The city manager may use it to judge in part the effectiveness of the police chief. City councils use the data to evaluate both the city manager and the police chief. Planners use crime data information in planning future development of the community. Parks and recreation people use crime data in setting up programs to counter delinquency. Budget hearings sometimes bear heavily on crime analysis facts and figures.

You should get some idea from the above, that the work you do in analyzing crime in your community from the police standpoint goes far beyond the reaches of the department. Realize that fact and do not ever forget it. Always do the best job possible with the material available. Make your reports accurate, neat, and interesting. Be careful about interjecting your personal preferences into any statistical report. Lastly, always save every scrap of paper you use for figuring your answers. It is not infrequent for someone to ask where or how you got these figures, and it goes a long way in establishing your credibility if you can produce the back-up data immediately, rather than having to refigure the entire report.

Suggested Readings

Managerial Psychology - Harold J. Leairtt

Organization for the Public Service - John D. Millett

Games People Play - Eric Berne

# CHAPTER II

## OBJECTIVES IN CRIME ANALYSIS

### Why?

When asked, "What is Crime Analysis", the usual answer is that it is "the study of crime". This answer is correct, but it fails to answer the question in depth, or give any definitive meaning to the answer. In the space available here, an attempt will be made to probe the answer or answers available to the question and give some real meaning to them.

Why does one study crime? What should any department allocate valuable manpower resources to study what has already happened? You may be asked that very question yourself one day soon and the answer you give may well be the basis used by management to justify establishing or abolishing the position of the crime analyst.

There are many answers available to the question, all of which have a degree of correctness, but only one of which is the most correct.

Do we study crime in order to determine our department's position in the hierarchical pecking order as established by the FBI for cities of the lowest crime rate? Certainly statistical results of efforts expended is a useful tool, but it is not the reason crime is studied.

Is crime analysis used to justify budget requests for manpower and equipment? Yes, that is frequently done. It is known as scare tactics in the trade, but it again is not the reason crime is studied.

Is crime studied in order to define the communities' crime problem? Certainly this is a by-product of crime analysis but it is not the primary reason for the analysis of crime.

The list of what can be done with the results of crime analysis is only as limited as the imagination of the user of the results, and the ability of the analyst. But what is the real purpose, the number one reason for the studying of crime data?

It is suggested very simply in this text that, the real reason for crime analysis, and the only one that will stand alone on merit is "to aid in the apprehension of criminals and assist in the prevention of crime." Everything else done with the results of crime analysis is secondary to this goal. Anything less than meeting this noble objective reflects an abject failure, either on the part of the analyst or on the part of the administration in putting to use the results.

If the reader is in agreement with the "Why" of crime analysis, the next step in the sequence would seem to be "what" is done with crime analysis data. If the primary objective is agreed with, then the answer is one of relative simplicity. Get the information to line personnel in a manner and in a time frame that will assist them in their task. This principle should never be forgotten, for no matter what the results, the analyst realized for his efforts, all is for naught unless relevant information is put to use where it belongs.

A glance at Chapter I, Impact of Crime Analysis, alludes to many uses of crime data, but all of these possible uses are effected by its primary one--helping the line patrol officer be more effective in the performance of his duty. The answer then to the "What" of crime analysis is the "compilation and messaging of raw data presented to line patrol officers in an effort to improve their actions toward the suppression of crime".

At this point, it would be fair to ask, "Is the objective of crime analysis strictly or solely directed at the line patrol officer?" The answer is, certainly not, but the belief is that everything else resulting from the analysis of crime is a by-product of what is thought to be its primary objective. Again, the subsection on the Impact of Crime Analysis in Chapter I, delineates many administrative uses of crime analysis data.

The last topic to be addressed in this section is "How" do we realize the primary objective of crime analysis? Again, emphasis must be directed toward the thought that how the data is used by line patrol officers is only limited by the imagination of the analyst and the reception of line patrol officers. To give a few ideas is all space allows for here, but the below should be a starting point.

1. High Target Areas - The crime analyst should readily be

able to provide patrol with information (graphic display) delineating high crime areas by type of crime. Residential burglary, commercial burglary, auto theft are but to name a few.

For the officer in the small department, pin maps (several) are an adequate method of presenting this information.

2. Trend Analysis - The projection of future crime patterns based on previous statistical data is extremely valuable to the patrol supervisor in the allocation of his manpower resources. This information is best presented in monthly, quarterly, and yearly reports. The crime analyst should bear in mind the fact that with trend analysis you must constantly update your figures. Your predictions for the next year, by month, will vary somewhat as new data is assimilated into your statistical base.

3. M. O. Factor Analysis - By studying the modus operandi of known criminals it is possible to connect an unsolved crime with a known offender with a high degree of success. This is one area where the officer in the field provides the raw data to the analyst by the taking of complete, accurate reports. In order for the analyst to use the report, the officer in the field must record not only what he feels relevant, but every observable fact at the crime scene.

## Establishing the Position

Possibly one of the most difficult tasks in modern day police work is getting a new or improved operation started. A great many senior police officials still believe that the old way is good enough. After all, it worked for the last fifty years. Why should it not work for the next fifty?

The statistical analysis of crime and its many associated factors is still a relatively new concept in many areas. However, to listen to old line chiefs talk, they have been doing it for years. They can tell you how many crimes of what type occurred during most statistical periods. They can, for the most part tell you how many cases were cleared by arrest, cleared by any other means and what percentage of crimes went unsolved. This is, infact, a part of crime analysis but only a scratch of the surface.

One selling point for crime analysis is that it is not new, but merely an improvement on what has been done in the past. True, crime analysis is an indepth study of the problem, one which may offer several solutions to any given problem, and one which leaves very few unanswered questions.

It is suggested here that one of the surest ways to convince someone of the usefullness of crime analysis is by demonstrations. As alluded to in previous sections and as will be further defined in subsequent sections, the means of analyzing crime data and crime trends is limited solely by the imagination of the analyst. Charts, graphs, overlays, showing comparative analysis, trend analysis, localized problems etc., are but a few ideas. Topics for analysis are almost beyond numerical limitations.

Thinking for a moment of only an offender's race, sex, age, socio-economic status, educational status, city of residence, county of residence, criminal history, employment status are but a few factors which can be statistically interrelated to draw a composite of the average burglar, rapist, robber or in more general terms, the average arrestee. That information alone can be used by at least a dozen city agencies.

Demonstrating the need for information is an easy task. It has been found through experience that the informational appetite of the community, the department, city hall, detectives, patrol, etc., is insatiable. The problem for the crime analyst is in knowing what information is available, who can use it, and getting it to them in a timely, accurate and usable format.

Knowing what information others will want or need is also a task that falls to the crime analyst, for many people being unfamiliar with what is available do not know what to ask for. The best advice is to give a full work-up the first time, and let the recipient decide what he can use and what he wants in the future.

You may have to sell the idea of crime analysis within your own department. In order to do that you are going to have to know the why, what, and how of crime analysis. Perhaps paramount to that even is believing in what you do and doing it well.

A very uncomfortable position for the crime analyst, after everyone gets his number, is deciding on priorities and who to say no to.

Get your foot in the door with a good job, in a small project, and rest assured that the door will soon swing open, for nothing begets results like results themselves.

# CHAPTER III

## THE USE AND MISUSE OF STATISTICS

The crime analyst will be primarily interested in performing four major functions related to crime data:

| | |
|---|---|
| (1) collection | (3) analysis, and |
| (2) organization | (4) interpretation. |

The accomplishment of these four functions is a science generally referred to as <u>Statistics</u>. Statistics does not then refer to large complicated formulas or technical sounding names and terminology. So often use of terms like "regression analysis", "correlation coefficients", "analysis of variance" turn people off simply because they do not understand their meanings. They, therefore, assume statistics is too complicated and, therefore, worthless. We will then start our discussion of statistics with a warning - do not try to impress people with terminology and formulas. Remember that these formulas, etc., fit into only one of the four functions of statistics, analysis, and, even though these formulas are important and necessary at times, you should use analysis techniques that are easily explainable and helpful to accomplish the fourth function of statistics, interpretation.

The first two functions of statistics, collection and organization of data, is accomplished by a well organized reporting scheme as discussed in previous sections. The fourth function, interpretation of crime data, will be discussed later. In this section we will concentrate on some simple techniques of statistical analysis.

## Data and Sampling

Before data is to be analyzed, the way it was collected and organized must be studied. For example, if you are to analyze the frequency of burglaries, you should make certain the data on burglaries has been accurately filed. Moreover, if for instance you want the average number of burglaries per month, you would not take only the data from the month of November and December. Two major errors would be made.

First, the data is not *independent* and representative. Burglaries are generally more frequent during these months. Also, the *sample* taken is too small. The weight one can place upon statistical estimates is directly related to the independence of data and sample size. It would be quite simple to "prove" that average daily rainfall for Texas is .5 inches if I only measured the rainfall in San Marcos during the first week of May.

One should make certain that the data is accurate and representative before performing analysis and should remember that small data samples can be most misleading. Sample sizes should always be represented so that the proper significance can be placed on the results.

## Averages

Before using the term "average" one should remember that there are different types of averages, and each type may lead to a different interpretation of the data. The mean or arithmetic average is generally most familiar and used most often. The mean salary of a group of individuals is simply the sum of all salaries divided by the total number of individuals.

The median of a set of data is that point on a scale of measurement where an equal number of cases are on each side of it--half are above and below the median. For example, the median of the numbers 10,8,8,7,6,5,5,5,0 is 6 since 4 numbers are larger and 4 smaller.

The mode is that measurement or piece of data that repeats most often. For the example above, 5 is the mode since it repeats most often.

An analyst should use that "average" which is most meaningful for the data being considered. For example, assume data on value of property stolen is given as in Table 1. Out of 15 items stolen the arithmetic average of $6,243.33 gives a fair idea of the total value stolen, but not a good idea of the types of items. Perhaps the median of 300 or the mode of 10 would better communicate the desired meaning.

TABLE 1

| Item | Value of Item in Collars | |
|---|---|---|
| 1 | 50,000 | |
| 2 | 40,000 | 6243.33=MEAN |
| 3 | 1,000 | |
| 4 | 700 | |
| 5 | 500 | |
| 6 | 500 | |
| 7 | 400 | |
| 8 | 300 | MEDIAN |
| 9 | 100 | |
| 10 | 100 | |
| 11 | 10 | MODE |
| 12 | 10 | |
| 13 | 10 | |
| 14 | 10 | |
| 15 | 10 | |

## Graphing*

The term graphic display means anything that is intended to be observed visually, and is not limited solely to graphs. It is a well known fact that people are more prone to respond favorably to well done graphics than to extracting the same information from several pages of documents. The old addage that one picture is worth ten thousand words is most applicable to police work today. Administrators have literally reams of paper to read each day, and they certainly do not want any more. A crime analyst can work this fact to his advantage by presenting his findings graphically rather than in long boring reports that perhaps will never be read anyway. If a crime analyst knows how to make an effective graphic it's going to get more attention than a written report. Presented below are several different types of graphs that can be used for different situations. Remember that black on white graphs are as boring as a rainy day; use color to advantage.

In graphing in two dimension, there are always two variables under consideration. For example, a monthly burglary rate is shown in Figure 3.1, where one variable (<u>independent</u>), the months of the year, are in increasing order while the other variable, the number of burglaries in the month, dependent on which month is being considered. The histogram generally uses the upper and lower limits of an interval and the entire interval is plotted on the graph.

*Acknowledgement is given to Davis Publishing Company, Santa Cruz, California for use of some of the following copyrighted material.

Keep in mind that any visual aid is used only as a means of analysis and does not interpret the data. Interpretation must be accomplished by someone familiar enough with the data to determine if the results are significant. Figure 3.1 can be used in conjunction with our discussion on complete data samples. Let's assume that we consider the sample size large enough to make estimates of burglary trends. If one considers only the months of January - May, one might predict a fantastic decrease in burglaries. This, of course, is imcomplete data samples, since the summer and holiday (December) months are typically bad as far as occurrences of burglaries are concerned.

A polygon is a graphic method which uses points to represent frequencies, with lines connecting these points. Figure 3.2 is Figure 3.1 redrawn as a polygon.

One final expample of how figures, say polygons, can be drawn to be somewhat misleading is shown in Figures 3.3 and 3.4. Assume Figure 3.3 is a graph of the monthly expenditures for crime prevention during the past year. While the expenditures have increased, relatively, this increase was small. Figure 3.4 represents the same data, but notice that the scale has changed significantly, implying a fantastic increase in expenditures. Care should be taken when constructing graphs, and when interpreting them, to make sure the graph is not misleading.

Correlation

Correlation is a measure of the relationship occurring between two variables. The simplest type of correlation study is graphical linear correlation. Two variables, say truancy

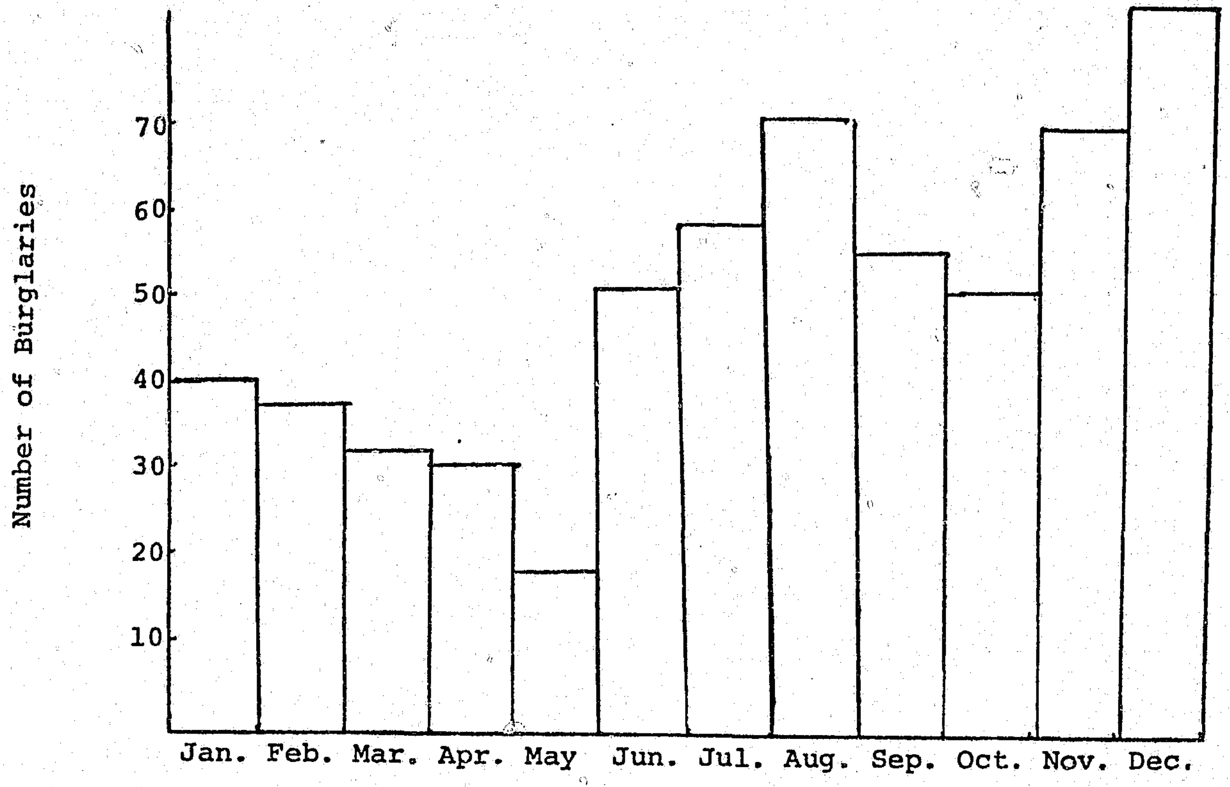


Figure 3.1

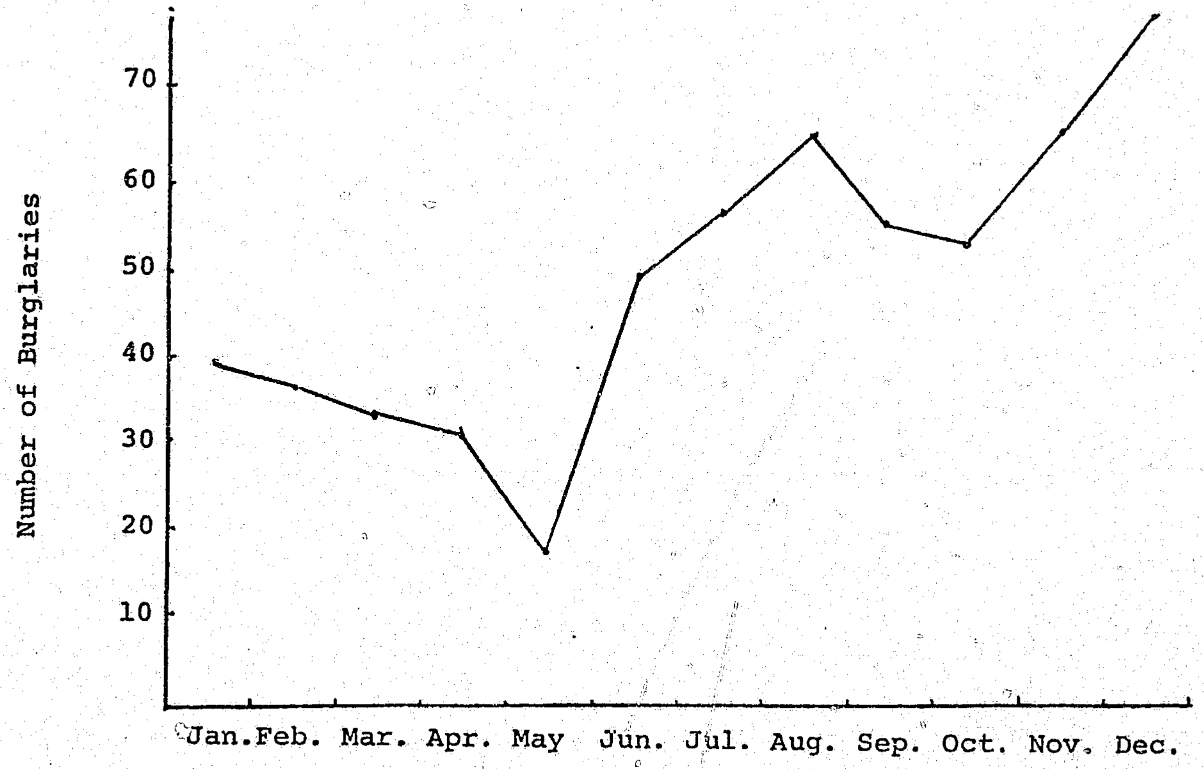


Figure 3.2

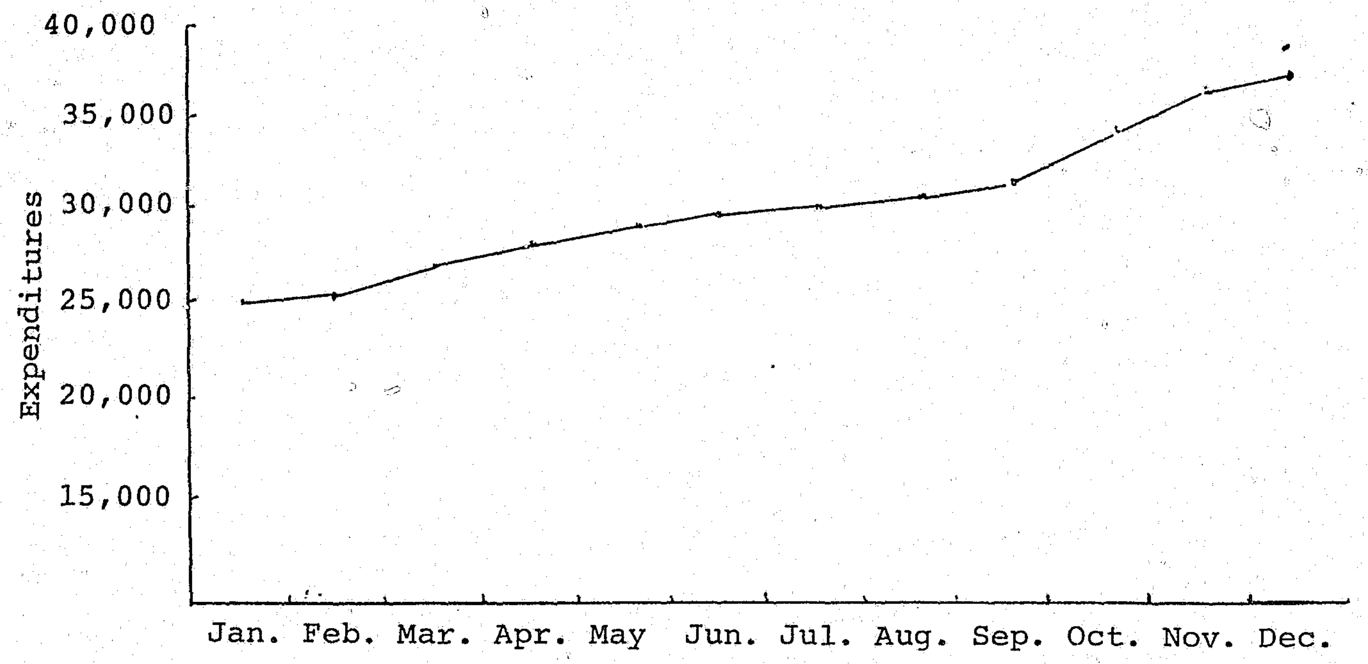


Figure 3.3

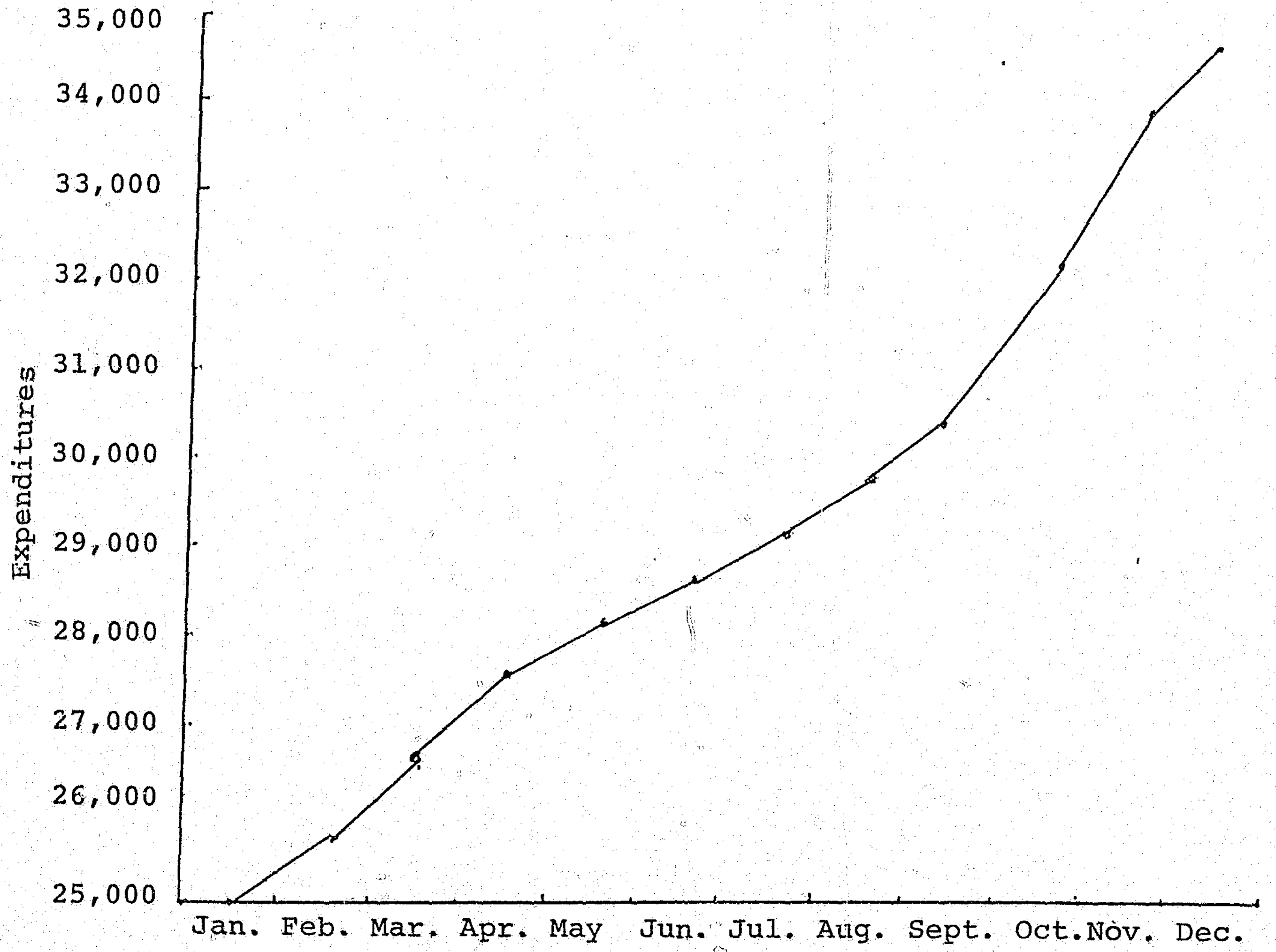


Figure 3.4

and number of burglaries are plotted on a graph so that the number of truancies is in increasing order. (Measurements are graphed then according to say weekly truancies and weekly burglaries.) Figure 3.5 draws this graph. Notice that as truancies increase, so do burglaries. We, therefore, say there is a correlation, and since the data appears to be on a straight line, there is linear correlation.

If the plot appears to have no relationship, or if the straight line is a horizontal one, no correlation is present. See Figure 3.6.

Figure 3.7 shows a correlation such that as one variable increases, the other decreases. This is referred to as negative correlation since the straight line has a negative slope. Figure 3.5 was an example of positive slope or positive correlation.

A general equation of a line is given by $y= mx+b$ where $x$ and $y$ are the variables, and $m$ is the slope. The values $m$ and $b$ may be computed for any sample of data so that the straight line can be computed. The reader is referred to texts in the bibliography or any introductory statistics book for these formulas.

Keep in mind that correlation <u>does</u> <u>not</u> necessarily imply that one of the variables causes or even affects the other. For example, one might examine the correlation between temperature and number of petty thefts. It might appear that as temperature goes up, so does petty theft. They are, therefore, related. However, one certainly cannot assume that the rise in temperature causes the rise in thefts. Instead, it could be the fact that school is not in session during the summer months that explains the increase. In other words, the correlation between two variables may be caused by a third variable. Care should therefore be taken on interpreting correlation graphs, although their uses are of extreme importance.

Questions to Ask

As a matter of summary, we end this section with three questions which should be asked whenever performing analysis, or reviewing someone else's results and conclusions.

1. How reliable is the data?

   Make sure the data was acquired and reported accurately and independently. Make sure there is no built in bias. For example, was data collected only in one area, say, to make someone "look" good? Finally, make sure the sample size was large enough to perform a reasonable analysis.

2. What is the best way to present the data?

   Remember that many people will be interested in your data and many may aid in the process of interpreting

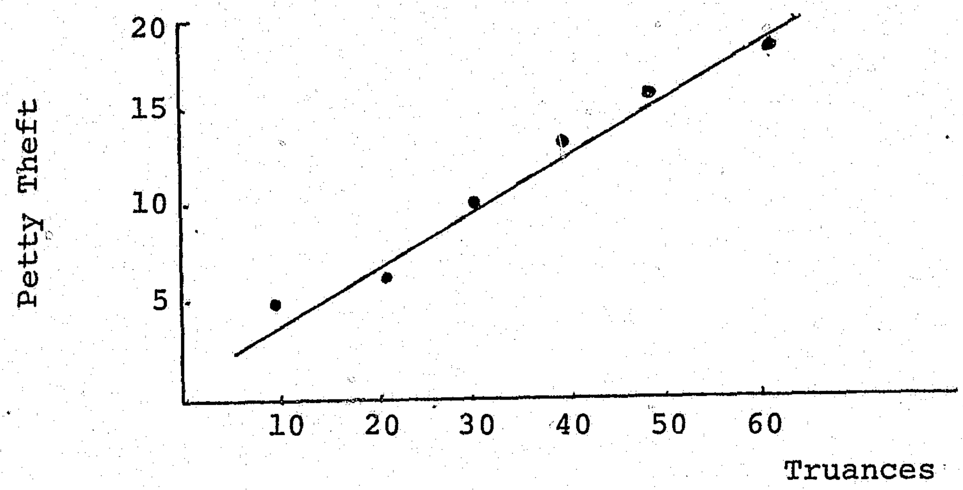


Figure 3.5

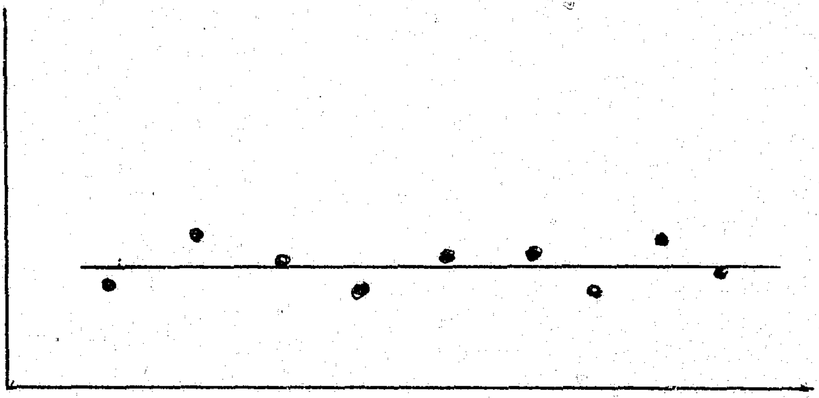


Figure 3.6

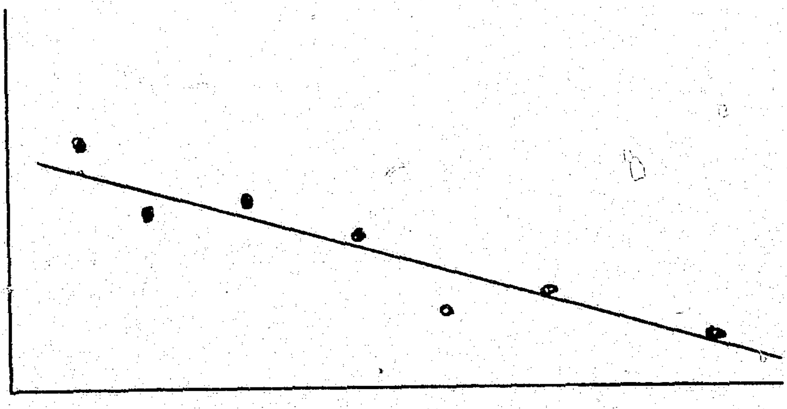


Figure 3.7

your data. Thus, choose the presentation technique which best fits your audience and which best represents your data.

Remember that your mode of presentation may greatly affect interpretation as was demonstrated in Figures 3.3 and 3.4.

3. Does the result make sense?

Always remember that the fourth function of statistics is interpretation and that ultimately some conclusions will be reached. Make sure that the results are reasonable! If they are not, perhaps one of the four steps of collection, organization, analysis and interpretation of the data had a flaw which led to the unrealistic results.

# BIBLIOGRAPHY

Huff, Darrell. How to Lie With Statistics. New York: Norton & Co., 1954.

Ingram, John A. Introductory Statistics. Menlo Park, California: Cummings Publishing, 1974.

Lindgren, Bernard W. Basic Ideas of Statistics. New York: MacMillan Publishing, 1975.

McCauley, R. Paul. Crime Analysis. Louisville, Kentucky: The National Crime Prevention Institute

# LAW ENFORCEMENT RECORDS

## Analysis and Management

Management of a police department is similar in many respects to management of any of the larger business enterprises in the community. There is one significant difference, however. The police "business" is one that directly involves the liberty and safety of every person served by the police organization.

Information is what allows any law enforcement agency to function. However, each agency must evaluate its own needs and how best to meet these needs face-to-face. The mere filing of records, whether required by statute or not, without summarizing and analyzing, serves very little purpose other than spending money and consuming space. Keeping reports of information is only useful if they serve to provide answers to problems and guides to programs of action. In my opinion, an effective law enforcement record system should do something in terms of administrative and operational management by providing the optimum of information. This empowers an agency with the ability to provide the best law enforcement service to its community. How information is put to use in most cases serves as the yardstick which measures the effectiveness of that agency and its administration.

Information, through reports, in many law enforcement agencies, is a one-way street. The reporting process flows in and little, if any, usable information is returned to the officer on the street to assist him in the performance of his duties. With the volume of reports generated daily by all divisions of a medium to large size law enforcement agency, requirements for the rapid processing, analyzing, and retrieving needed information is of paramount importance.

A thorough examination of the overall aims, goals, and objectives of the law enforcement agency is a prerequisite to any efficient and effective records system.

By study and analysis of proper police records the police department will have in its files the basic data concerning crime, traffic, and delinquency that are necessary for an intelligent plan of attack. Based on the statistical data that can be produced by a records division, the Chief of Police (Chief of Operations, etc.) will be in a position to focus the work of the police department when and where it yields the greatest immediate results. Records data will not give the solution to the crime problem. It will isolate factors concerning it so that an intelligent <u>departmental plan</u> of attack can be formulated. There must be developed a records and accounting system to show if the departmental operational plan of attack is producing results. Large departments need mechanical compiling and analyzing machinery to do this work.

It is impossible to do it by hand soon enough, and without errors creeping into the work. Small departments use hand sorting of index cards.

To derive the optimum of needed and essential information from law enforcement records the analysis and study process should include: (1) having a thorough knowledge of what information the records system should produce for the department's needs; (2) extensive use of flow charts; (3) starting from the end result in what is desired from the records system and work towards the beginning. This process eliminates the costly and time consuming trial and error method; (4) consider all the legal requirements imposed upon the department; (5) consider all interagency needs and requirements; and (6) always evaluate your budget and manpower resources.

The President's Commission on Law Enforcement and Administration of Justice noted that:

> Many departments resist change, fail to determine shortcomings of existing practice and procedures through research and analysis, and are reluctant to experiment with alternative methods of solving problems. The police service must encourage, indeed put a premium on, innovation, research and analysis, self-criticism and experimentation.

Who gathers the bulk of information from the field in any law enforcement agency? Without the field officers' reports there would not be any information available to other divisions within an agency. If this occurred, obviously the reviewing, analyzing, and summarizing of information would not be possible. "Police reporting has become one of the most significant processes in modern police operations."

The need for standardized and clearly defined written reporting procedures is essential to the overall administrative and operational conduct of any police department. Besides their being a permanent record of activity, reports form the basis of many administrative decisions.

> They provide a basis for budget planning and distribution of funds within the department. They are the basis for long-range planning of future needs. Reports can be used to point up needs in training in specific areas within the department.
>
> Unless police agencies have a well-defined reporting policy for incidents of both criminal and noncriminal nature, they will be unable to assess accurately the extent of criminal activity in their jurisdictions, and will also find themselves ill-equipped to take effective measures against it.
>
> Moreover, inconsistent reporting procedures contribute to a lack of confidence in police; persons may well assume that certain kinds of behavior are tolerated in one section of the community but not in another.
>
> Every policeman should be thoroughly familiar with agency policy specifying the conditions under which police reports are to be taken. Such policies should require that all relevant criminal information be reported, and should discourage procedures that permit the failure to take a report.

Well designed and utilized field reports are essential to any records system and especially to one that is computerized.

All of the forms used by a law enforcement agency should be designed to meet more than one need if possible. They should be practical, standardized, relatively easy to read and prepare, as well as allowing for statistical analysis summaries. Many law enforcement agencies have already placed great emphasis on their record systems and forms utilized in the collection of information. It is recommended that a review of other agencies methods be carefully examined and understood prior to any final decisions. In addition to that previously stated, the following should always be considered in forms design and development:

1. Odd-ball size forms creates an unnecessary expense upon the agency's budget when purchasing printed forms and filing cabinets, etc.

2. The forms designer should consider future conversion to automation when preparing a form. This eliminates costly and time consuming modification or complete re-design at a later date.

3. Use the "paste-up" method. This is when one cuts out the best of everybody else's law enforcement forms and pastes them on a piece of paper the size they want their form to be. Through this method a department can create its own forms tailor-made to meet their specific needs.

4. Consultants may be necessary as they can provide a different perspective not previously taken into consideration. However, don't overlook the talents of the people within your own departments and their experience and knowledge of that agency's operations.

Once the aims, goals, and objectives of a law enforcement agency have been set forth, the methods and procedures to achieve them must be made known to all employees. It now becomes the responsibility of the records unit to provide summarized information necessary for administrative and operational decisions. However,

> The capability of a police records staff to provide timely, accurate, and complete information to administrative and operational components of the department depends primarily upon the quality of information originally provided by its contributors. In order to insure maximum usefulness of collected information, the records element must organize the information into logical groupings that allow for the system to provide or receive information randomly and without undue inconvenience or delay.
>
> All information to be gathered, processed, stored, and disseminated falls within several major categories. It should be arranged in logical, prescribed ways to form files of retrievable data. The major categories include:
>
> 1. FIELD OPERATIONS PRIMARY DATA:
>
>    a. Case reports and related materials
>
>    b. Statements and depositions
>
>    c. Investigative notes, sketches, and similar items

d. Evidence and property - identification information

e. Photographs, fingerprints, and other supportive documents or records

2. FIELD OPERATIONS SECONDARY DATA:

a. Field interview information

b. Traffic and other violation citation data

c. Miscellaneous information required by or for field personnel

3. FIELD OPERATIONS SUPPORTIVE DATA:

a. Criminal history records

b. Modus operandi information

c. Criminal specialties file

d. Personal identification data

e. Wanted persons information

4. COMPLAINT AND DISPATCH DATA:

a. Time, date, location and other information concerning incidents reported.

b. Advisory information of immediate procedural importance to responding officers received from complaints, such as descriptions of suspects and escape routes.

c. Information concerning officers assigned, case report numbers, and other case work-load data.

d. Radio and teletype messages and other inter or intra-agency information sent and received.

5. ADMINISTRATIVE DATA:

   a. Comprehensive periodic reports, summaries and tabulations

   b. Case-load data on personnel and assignments

   c. Informational notices and bulletins

6. INTERNAL CONTROL DATA:

   a. Longs and registers

   b. Report review and control files

   c. Indices and cross reference data

   d. Other information required to process reports, records, and other data.

To provide field and staff elements with information concerning the incidence of crime and traffic conditions, and important personnel and other data, the records element should provide both consolidated and comprehensive, daily, monthly, and annual statistical reports, special analysis of certain types of incidents, and detailed breakdowns of both statistical and analytical data. This information should be given to designated departmental elements and city and other officials or offices.

Law enforcement records should meet or exceed minimum standards as prescribed by law, department policy, inter-agency requirements, Uniform Crime Reporting, and the needs of that community.

To insure that a law enforcement agency has the needed information, their records system should meet the following minimum standards:

1. A permanent written record is made of each crime as soon as the complaint is received. All reports of crime and attempted crimes are included, regardless of the value of property involved.

2. Staff, or headquarters, control exists over the receipt of complaints. This is to insure that each is promptly recorded, properly classified, and subsequently counted.

3. An investigative report is made in each case. It shows fully the details of the offense as alleged and as disclosed by the police investigation. Each case is closely followed to see that reports are made promptly.

4. All reports are checked to see that the crime class conforms to the uniform classification of offenses.

5. The offense reports on crimes cleared by arrest or by exceptional means are so noted.

6. Arrest records are complete, special care being taken to show the final results of the charge.

7. Records are centralized; records and statistical reports are closely supervised by the chief administrative officer; periodic inspections are made to see that the rules and regulations of the local agency on records and reports are strictly followed.

8. Statistical reports meet the Uniform Crime Reporting standards and regulations.

A suitable records system contains and can provide the following:

1. Information useful in the investigation of crimes.

2. Identification of persons and property.

3. Investigation reports (of crimes, offenses,and other matters of concern to the police) when classified, indexed, and filed.

4. Register assignments can provide a check on accomplishments so that (1) errors may be traced, (2) inadvertent oversight and willful neglect detected, and (3) successful performance assured.

5. Provide a basis for reviewing work, thus helping supervisory officers in their day to day operations by revealing deficient or improper handling of cases.

6. Show whether officers were correctly dispatched to the scene of criminal operations.

7. The progress of investigation.

8. Failure to follow up on investigations or otherwise correctly dispose of police business are revealed.

9. Prevention of the individual policeman from conducting an investigation or discontinuing it in violation of departmental policy and sound police practice.

10. Enable the police department to disprove charges of improper police action by providing prompt and complete answers to specific allegations and inquiries from the administrative head of the city, citizens, etc.

11. Records and summary reports will give a picture of present conditions and problems faced by the department, of the work of individual employees, activities of units, etc., in dealing with these problems.

12. Reveal significant changes in criminal and other activities requiring police attention.

13. Prompt analysis of police records guide the police official in meeting unusual needs.

    a. The first step in solving a problem is to diagnose it. Facts concerning the character, location, time, circumstances of crime and incidents requiring police action can be found.

    b. Possible to determine engineering, education and enforcement needs pertaining to traffic.

    c. Locate and identify police hazards, isolate the locations requiring attention.

14. Assistance in the development of police strategy and in making various follow-through procedures.

15. The success of programs launched to lower crime and accident rates can be ascertained by record analysis.

16. Provide measuring sticks or indices to appraise police efficiency and accomplishment.

17. Effectiveness of police policies and procedures, and the results of changes in methods of operation may be appraised.

18. Information for public dissemination is made readily available through a suitable record system.

19. Supplying information useful in preparing and supporting budget estimates.

    a. Assist in managing the department's fiscal affairs.

    b. Accurate payrolls compiled.

    c. Competing with the programs of other city departments for public funds can be justified.

As a law enforcement information system increases in size and volume, the need for some form of automated system becomes necessary for the effective management and control of that information. Should an agency have need for automating its records system, the following should be given careful and serious consideration.

An operating law enforcement system should be established to serve: "(1) daily operations, (2) investigative analysis, (3) management analysis, and (4) program formation."

It should be emphasized that the use of automated data processing is a management tool. The computer is by no means the answer to every law enforcement agency. The quality, integrity, and accuracy of computerized information is only as good as those human beings who write the data collection reports, key punch the information, and program the computer to print the needed information in usable form. Once high standards have been established, the rapid retrieval of information becomes almost commonplace. Decisions in a law enforcement agency have to be made rapidly.

Automation provides this capability; not subject to vacations, regular days off, and coffee breaks, but operating rapidly, accurately, and efficiently to provide indicators and guidance in decision making. It is impossible to do it by hand soon enough, and without errors creeping into the work.

> Automated information systems make it easier to collect, process, and communicate data; but they cannot be expected to exercise responsible judgment. Any tool that facilitates the collection and organization of data in a complicated and changing fact situation is a significant aid to judgment. Of course, computers are useful in assembling the facts on which to base a decision. Computers can provide no substitute for the process of judgment based on experience. The electronic revolution offers the creative police administrator and field officer greater scope, as it makes available more data, assembled more rapidly, from a wider geographic range of sources, and more easily combined and recombined.

A law enforcement information system, while safeguarding the rights to privacy of individuals, can effectively provide important indicators to other local, state and federal agencies performance of their responsibilities.

> Success in protecting society is not measured by the length of time it takes the police to respond to a crime scene, by the number of arrests they make, or by the number of arrestees successfully prosecuted or sentenced. Rather, success or failure is determined by the degree to which society is free of crime and disorder.
>
> This is but another way of saying that no element of the criminal justice system completely discharges its responsibility simply by achieving its own immediate objective. It must cooperate effectively with the system's other elements. This requires an effort on the part of each element to communicate with the other elements, which is sometimes difficult because of legal and administrative separation of powers and responsibilities.

A law enforcement information system, properly administered, can serve many needs; from the chief or sheriff, the prosecutor, the crime analyst, and the criminal justice planners to name a few. However, one fact remains very clear. It is this:

> No one program alone can deal effectively with crime and delinquency. The home, the school, the church, the welfare agency, the clinic, the police, the court, the probation department, the correctional institution, the parole agency, and all the other agencies and institutions that are interested in crime and delinquency must work together as a team through coordinating councils or through some similar coordinating device in a concentrated attack on these problems. But the teamwork cannot be completed without public support. This support must be given in the form of interest in community affairs, participation in community programs, law observance, insistence on wholesome community conditions, and abundant opportunity for young people, respect for law enforcement and effective court procedures, demand for an adequate number of well-qualified police officers, judges, probation officers, welfare workers, institutional employees, and parole officers, and a willingness to pay for programs that can deal effectively with social problems.

# BIBLIOGRAPHY

## Books

Adams, Thomas F. Law Enforcement-An Introduction to the Police Role in the Community. New Jersey: Prentice-Hall, Inc., 1968.

Authors Unknown. Administration and Use of Police Records. (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11. (Note: this is an unpublished course outlines).

Caldwell, Robert G. Criminology, 2nd Ed., New York: The Ronald Press Co., 1965.

Dienstein, William. How to Write a Narrative Investigation Report. Springfield: Charles C. Thomas, 1964.

Eastman, George D. and Eastman, Esther M. Municipal Police Administration. Washington: International City Management Assn. 1969.

Gammage, Allen A. Basic Police Report Writing. Illinois: Charles C. Thomas, 1970.

Kelly, Clarence M. Uniform Crime Reporting Handbook. District of Columbia: Federal Bureau of Investigation, 1974.

Parsa, John H. "An Automated Police Information System for a Small Town." Diss. Texas Tech University, 1972.

Whisenand, Paul M. and Tamaru, Tug T. Automated Police Information Systems. New York: John Wiley and Sons, Inc., 1970.

## Public Documents

National Advisory Commission on Criminal Justice Standards and Goals Task Force on Police. US. Government Printing Office, 1973.

Task Force Report: The Police, Washington: U. S. Government Printing Office, 1967.

## Footnote Page

## Chapter IV

## Law Enforcement Records

Berish, Caldwell, Poirot, and Stone, Specialized Data School for Crime Prevention Officers:1975, Texas Crime Prevention Institute, San Marcos, 1975. pp 9-23.

P. 1, pa 1: Thomas F. Adams, Law Enforcement - An Introduction to the Police Role in the Community, (New Jersey: Prentice - Hall, Inc.,1968) p. 238.

P. 2, pa 3: Authors unknown, Administration and Use of Police Records (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11 (Note: This is an unpublished course outline.)

P. 3, pa 3: Task Force Report: The Police (Washington: U. S. Government Printing Office, 1967), p.44.

P. 3, pa 4: Allen A. Gammage, Basic Police Report Writing, (Illinois: Charles C. Thomas, 1970), p. 5.

P. 4, pa 3: William Dienstein, How to Write a Narrative Investigation Report, (Springfield: Charles C. Thomas, 1964) p. 3.

P. 4, pa 4-6: National Advisory Commission of Criminal Justice Standards and Goals Task Force on Police, (U. S. Government Printing Office, 1973)p. 571.

P. 8, #6d: Eastman, George D. and Eastman, Ester M., Municipal Police Administration (District of Columbia: International City Management Association, 1969)pp 252-253.

P. 8, pa 3 Ibid, p 266.

P. 9, # 8: Kelley, Clarence M., Uniform Crime Reporting Handbook (District of Columbia: Federal Bureau of Investigation, 1974) p. 3.

P.11,#19c: Authors unknown, Administration and Use of Police Records (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11 (Note: this is an unpublished course outline).

P.11, pa 2: John H. Parsa, "An Automated Police Information System for a Small Town", Diss. Texas Tech University, 1972,p.8.

P.12, pa 3: Paul M. Whisenand and Tug T. Tamaru, Automated Police Information Systems, (New York: John Wiley and Sons, Inc., 1970) pp. 198-199.

P.13, pa 2: National Advisory Commission of Criminal Justice Standards and Goals, Police (Washington: U. S. Government Printing Office, 1973), p. 70.

P.13, pa 4: Robert G. Caldwell, Criminology, 2nd Ed., (New York: The Ronald Press Co., 1965) p. 724.

# CHAPTER V

# COMPUTER DEVELOPMENT AND ORGANIZATION

## Introduction

It is difficult to find an individual in our country today who is not directly or indirectly influenced by the electronic computer. Obvious daily computer usage is found in payroll checks, utility bills and department store check-out stands. In law enforcement agencies alone, we find computers being implemented for a variety of applications, ranging from traffic control to data analysis and report generation. The effect the computer has had on society has been fantastic, and yet misunderstandings and even fear of the computer are prevalent in this same society. The majority of these fears are generated by ignorance of the computer and its operation. In turn this ignorance has been caused for the most part by the rapid development and widespread usage of the computer during the past 25 years.

The majority of this country's population was educated prior to the introduction of computer related curriculum in our school systems. It therefore behooves many of us to undertake computer education independently or outside of the formal education process. The knowledge of a science which is so influential in our society today and one which will most probably increase in importance and usage is imperative.

We start our study of the computer with a brief historical survey of computer development. Knowing the rapidity at which computer science has developed should help us to understand "computer problems" which for the most part can be considered to be caused by "growing pains".

## Historical Survey

Man has always strived to make his work "easier". Mathematical computations surely trace back to the stone age when cave men might have traded one spear for one club plus five smooth stones. The first device used for computation is generally believed to be the abacus, produced about 3000 B.C. by the Chinese. The abacus is simply a device made up of beads on sticks or wires and is still being used in computations today.

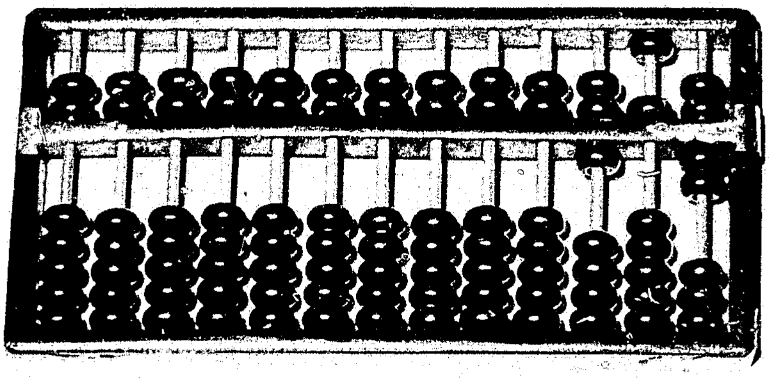


Figure 5.1 Abacus

We must go all the way to the 17th century before we have a significant improvement over the abacus. In 1642 a French mathematitian by the name of Blaise Pascal invented the first mechanical adding machine and in 1694 a man by the name of Leibnitz produced a machine which could also multiply. These machines were certainly a far cry from our present day calculators.

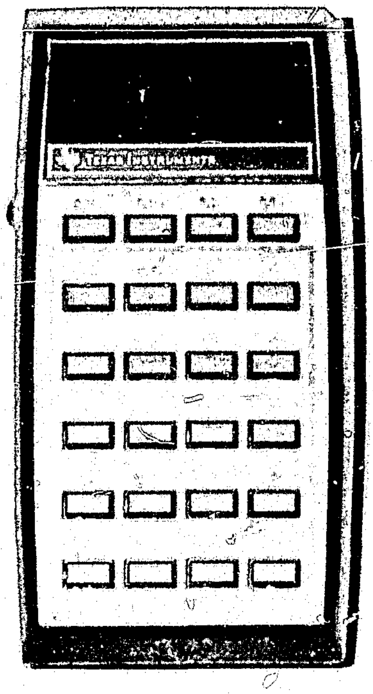


Figure 5.2 Modern electronic calculator

In 1812, Charles Babbage at the age of 20, started work on his difference engine and analytical engine which were to be the prototype of modern electronic computers containing memory units, punched card input and printed output. Unfortunately, the technology available in the 19th century could not adequately perform the necessary operations for Babbage's machines to be functional. It would take another 130 years before electronics could be employed to implement the ideas Babbage had.

In 1890 a man by the name of Hollerith devised a scheme to facilitate the tabulation of the 1890 census. His basic concept, using the holes in a particular card to activate a series of electrical counters, is still widely used whenever punched cards or tapes appear. The general notion of calling such cards "IBM" cards is well-founded, sinch Hollerith later sold his interest to a predecessor of the International Business Machines Corporation.

We now must skip all the way to 1944 when IBM produced the Mark I, the first large-scale automatic calculating machine. The Mark I still was not a "computer" as we know it, for it had both electronic and mechanic parts.

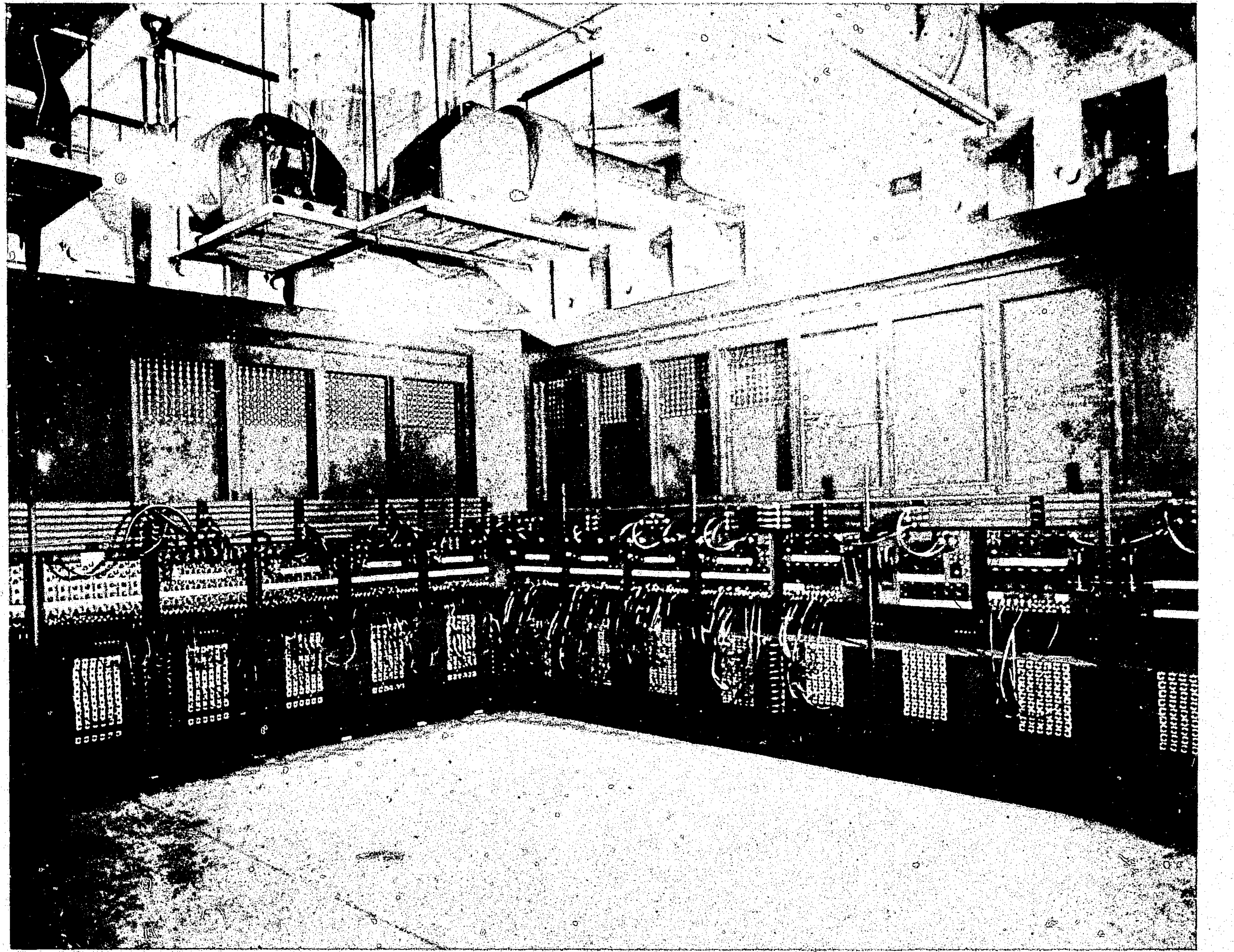


Figure 5.3. The ENIAC, the first electronic computer.

World War II and the corresponding government paperwork and scientific research initiated extensive research which finally led to the production of the ENIAC (Electronic Numeric Integrator and Calculator) the first electronic computer. In 1946 Eckert and Mauchly at the University of Pennsylvania are credited with the production of ENIAC which operated with the help of 18,000 vacuum tubes. The big selling point for ENIAC was that it could accomplish "300 days of work in one day". It did have one major disadvantage though - it could not store its programs. Thus the EDSAC (Electronic Delay Storage Automatic Calculator) was produced in 1949.

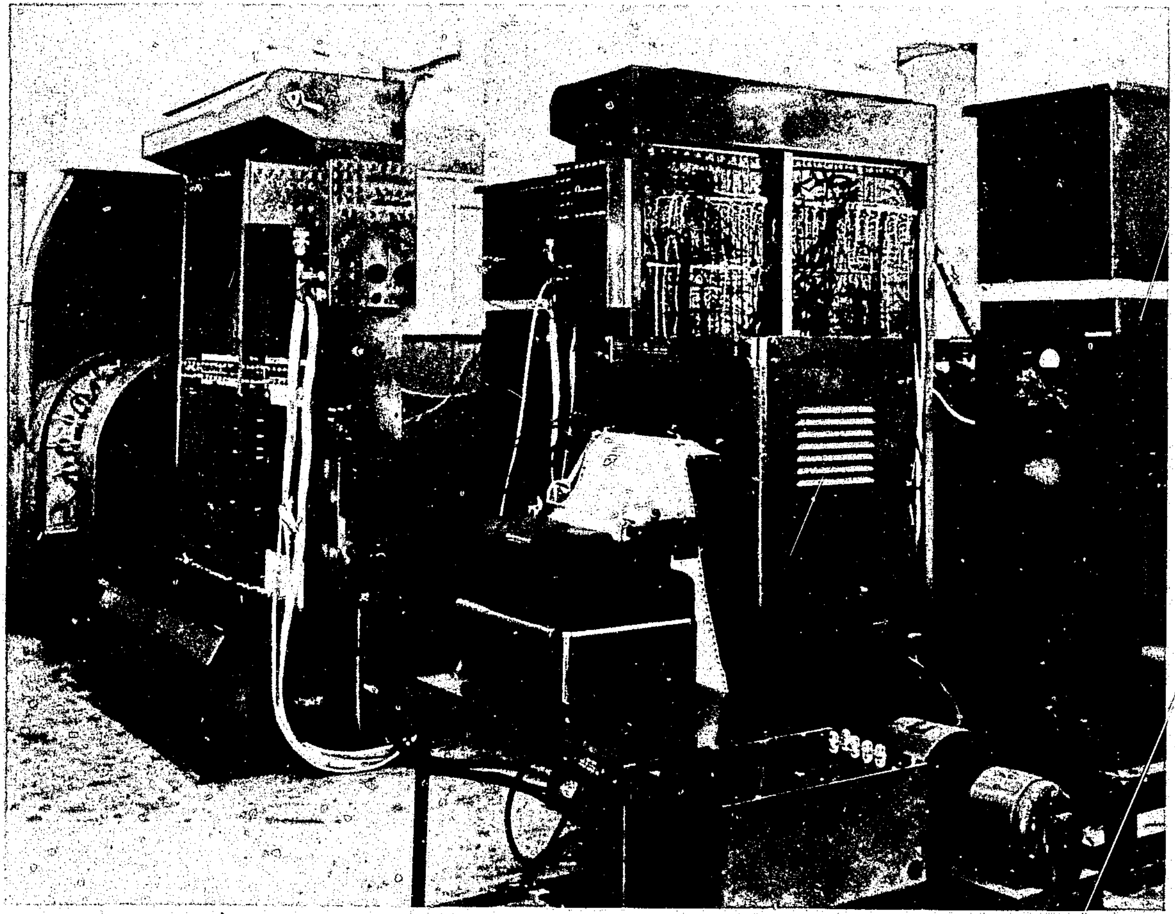


Figure 5.4. One of the first commercially available computers.

The ENIAC marked the start of the first generation of computers of those computers built with vacuum tubes. It wasn't until 1951 however, that a computer was commercially available, the UNIVAC (Universal Automatic Computer). The UNIVAC was considered by most to be the best until 1956 when IBM took over the lead with their IBM 705. Until that time, IBM had dealt primarily in business machines. Even though they entered the computer race later than some, the experienced and widespread marketing force helped them become and now maintain IBM as the "biggest" computer firm.

The First Generation computers built with vacuum tubes and relays were necessarily large, cumbersome, slow, and heat-producing, A major breakthrough, important to all phases of the electronic industry, was the development in 1947 at Bell Laboratories of the transistor. In 1959, the transistor was implemented in computer design, opening the era of the Second Generation computer.

In 1965 most computer firms went to chemical means to fabricate numerous transistors and associated components on small chips of a semiconducting material such as silicon. These chips are referred to as Integrated Circuits (ICs) and are characteristic of the Third Generation computers. Most computer systems now in operation are Third Generation, although some claim to now be in the Fourth or Fifth generation. No clear cut accomplishment however, has characterized a Fourth Generation computer.

The reduced size and power requirements of the IC have led to extreme miniaturization, as witnessed by the processes of medium- and large-scale integration. The physical proximity is such that very little time elapses while electrical currents travel between components. In addition, the time required for a transistor to change states, "on" to "off" or back, is so brief that times on the order of a few nanoseconds are now typical (one nanosecond = $1 \times 10^{-9}$ second, the time required for light to travel a distance of 29.978 centimeters or approximately $2.99776 \times 10^{10}$ centimeters per second or 186,272 miles per second). This transistion time enables incredible speeds of calculation, storage, retrieval, and manipulation, with relatively small physical size and minimal power requirements. Were it to be built with vacuum tubes and relays, a computer with the proposed capabilities of the IBM 370 series would require a large building for housing, more electricity than a small town, and would be slower than a pocket calculator in the hands of an experienced operator. As it is, this very powerful multipurpose computer can be housed in a moderately-sized room, and draws no more current than a large air-conditioning system.

After about 1964, most accomplishments and developments in the computer field are found to be improvements, modifications, or refinements of earlier discoveries. Improvements in speed, accuracy, adaptability, and compactness have allowed the advent of the "minicomputer," a physically small computer with internal storage capactiy of some 4K to 16K bytes, with access to additional peripheral storage up to perhaps 15 megabytes. The "microcomputer" is a single IC CPU with tremendous potential as a "built'in" processor for limited-size applications.

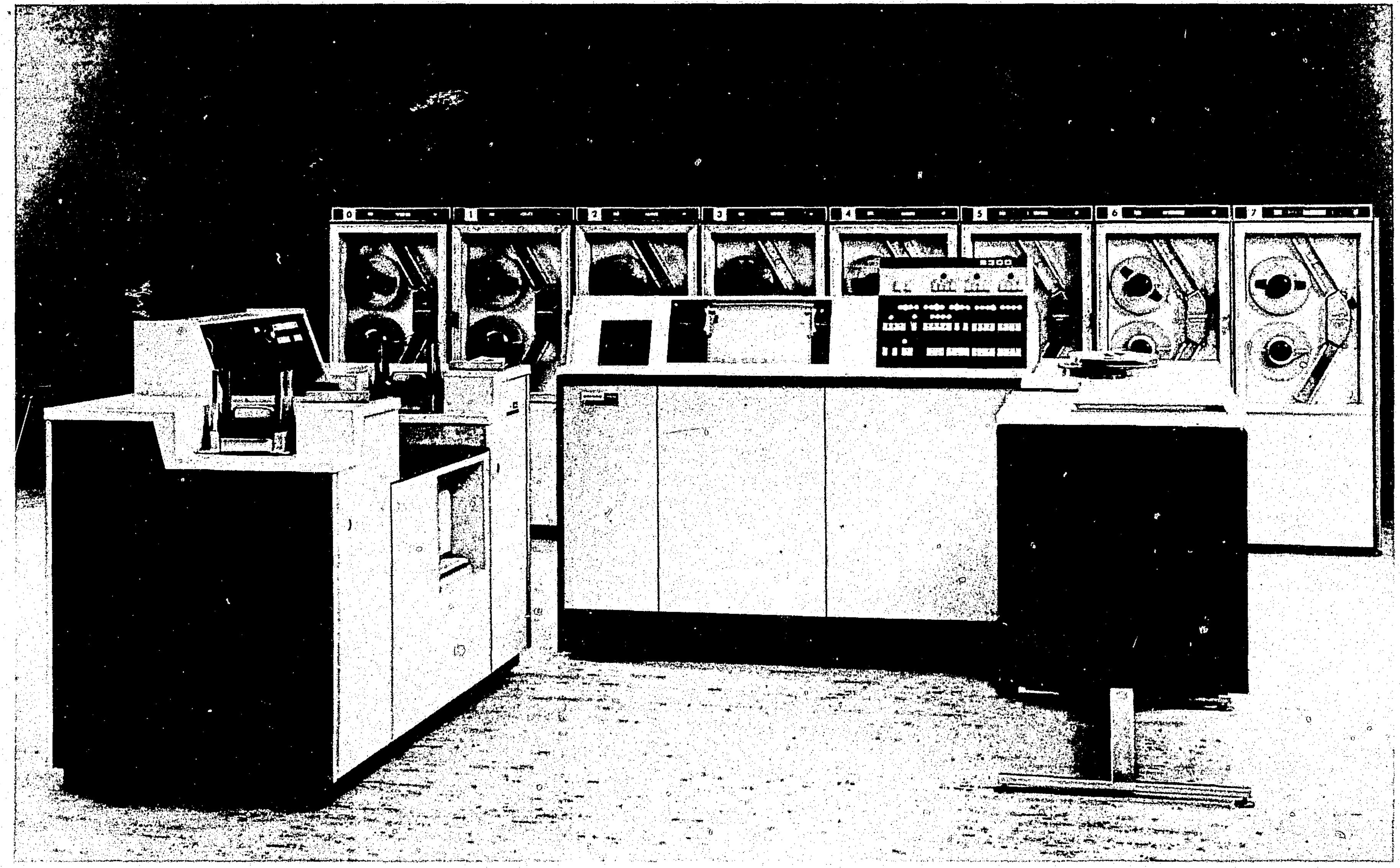
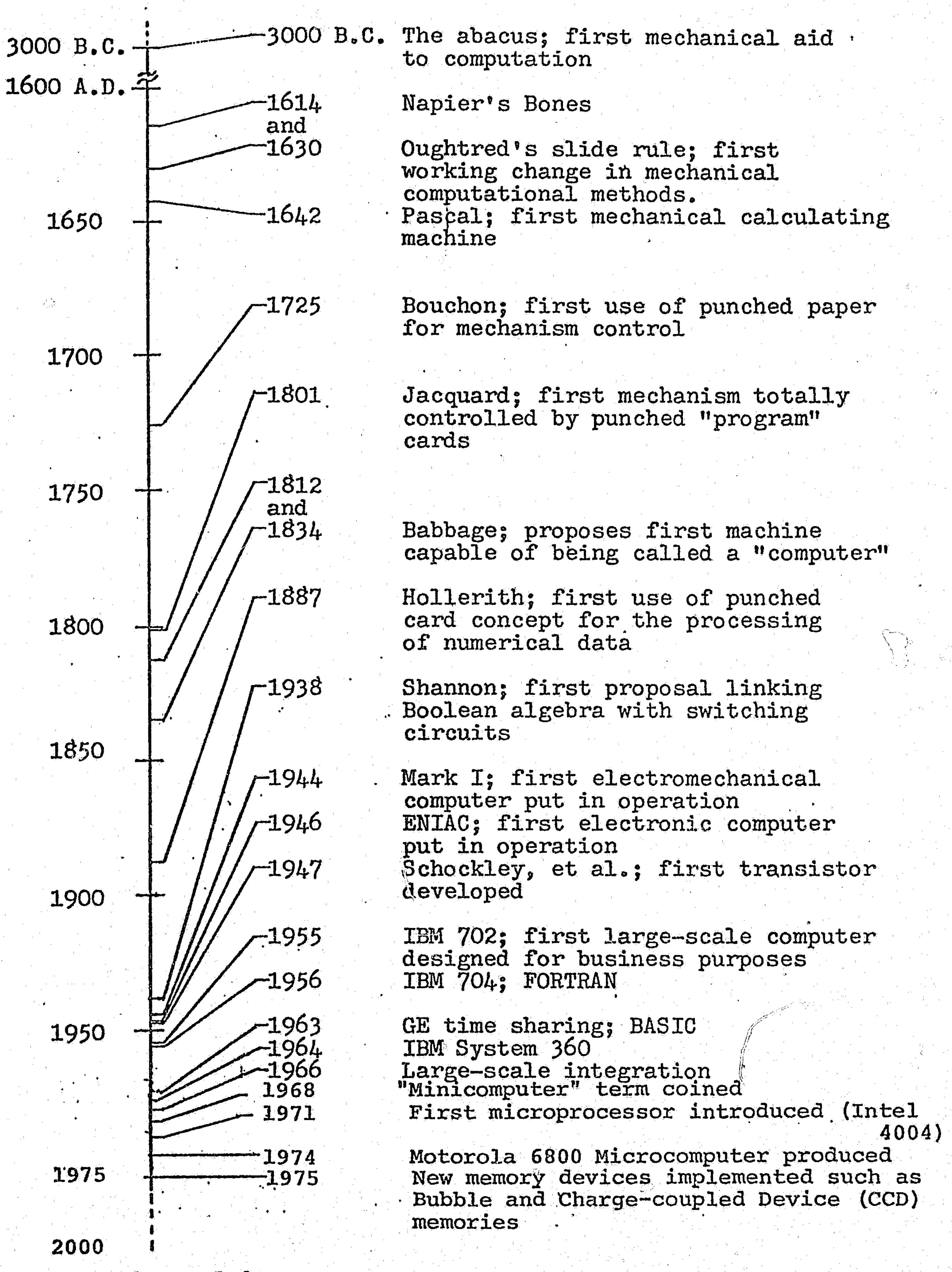


Figure 5.5. Modern electronic data processing system.

## The Nature and Structure of Typical Computers

The modern computer falls into one of two rather broad categories, digital and analog. The digital computer uses and furnishes data that is in discrete units--a sum of money, solutions to an algebraic equation, statistics based on sales data or educational processes, etc. On the other hand, the analog computer deals primarily with changing physical phenomena--rotation of a shaft, variation in gas pressure during a manufacturing process, shifting gravitational forces, movement of a gyrocompass as a missile traverses its trajectory, etc. Whereas the digital computer acts upon numbers and other such actual data, the analog computer acts upon data gained from a model or "analog" of the real occurrence. This model usually takes the form of a varying voltage whose variations are symbolic of physical changes actually occurring elsewhere.

There have been significant developments in both types, but the most publicized advances are those dealing with digital computers. It should be noted, however, that the technological feats associated with the Apollo missions and other space projects have been made possible by computers utilizing both vast digital procedures and "real-time" analog analyses ("real-time" operation refers to the processing of data rapidly enough to allow the results to affect the device or condition producing the data).



3000 B.C. The abacus; first mechanical aid to computation

1614 and 1630 Napier's Bones
Oughtred's slide rule; first working change in mechanical computational methods.

1642 Pascal; first mechanical calculating machine

1725 Bouchon; first use of punched paper for mechanism control

1801 Jacquard; first mechanism totally controlled by punched "program" cards

1812 and 1834 Babbage; proposes first machine capable of being called a "computer"

1887 Hollerith; first use of punched card concept for the processing of numerical data

1938 Shannon; first proposal linking Boolean algebra with switching circuits

1944 Mark I; first electromechanical computer put in operation

1946 ENIAC; first electronic computer put in operation

1947 Schockley, et al.; first transistor developed

1955 IBM 702; first large-scale computer designed for business purposes

1956 IBM 704; FORTRAN

1963 GE time sharing; BASIC

1964 IBM System 360

1966 Large-scale integration

1968 "Minicomputer" term coined

1971 First microprocessor introduced (Intel 4004)

1974 Motorola 6800 Microcomputer produced

1975 New memory devices implemented such as Bubble and Charge-coupled Device (CCD) memories

Figure 5.6. A Schematic Representation of Some Important Events

All computers have certain basic structural features in common; it is the varied approaches to each component which serve to make competition keen and productive. Figure 5.7. illustrates the five major components of a computer: the input medium, the storage unit or memory, the arithmetic unit, the output medium, and the control unit.

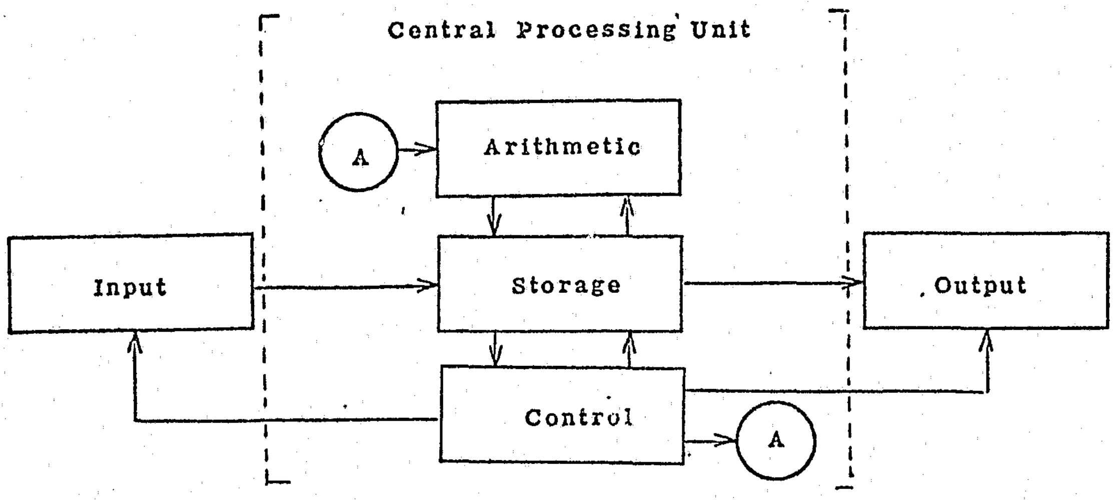


Figure 5.7. Schematic Chart of Computer Functions

## Input Medium

It is through the input medium that the program, or sequence of operations, is entered into the computer, along with the data which the program is to manipulate. The input for a particular unit may take any one of a variety of forms; in fact, the adaptability of the input device to the needs at hand often determines the effectiveness of the computation.

Certain forms of input are quite common for digital computers; one is the card reader, which senses holes punched

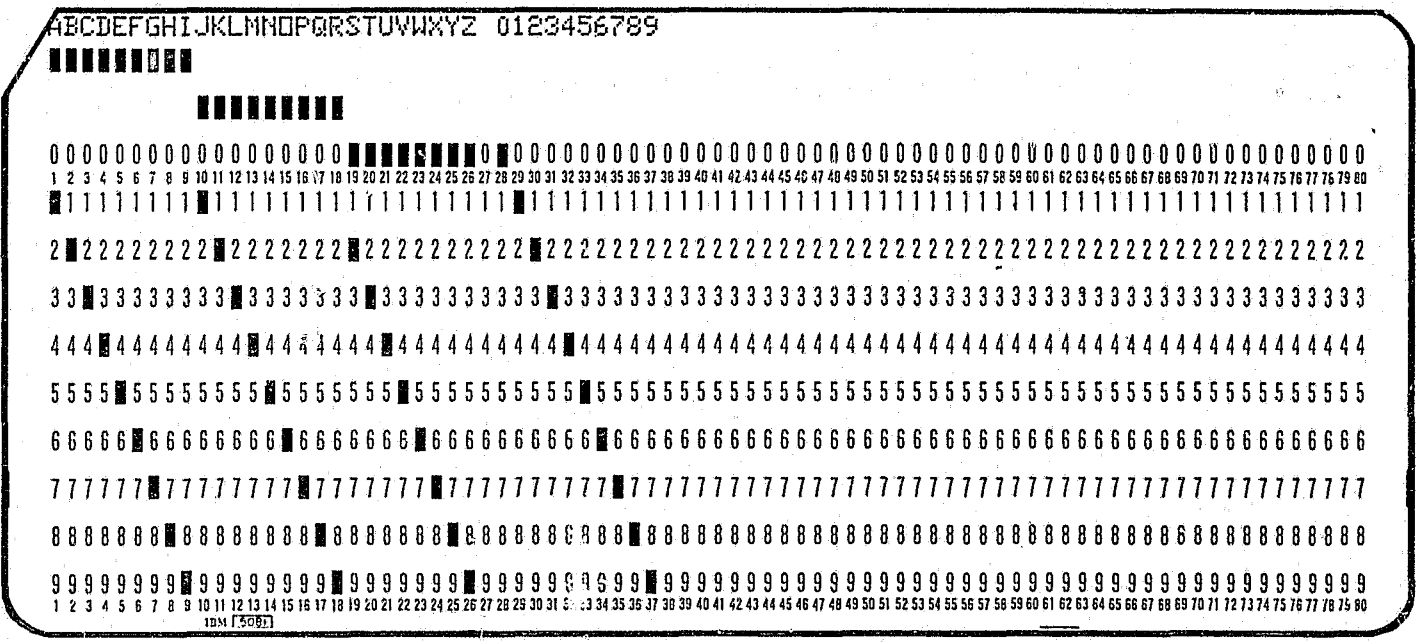


Figure 5.8. Data representation on punched card.

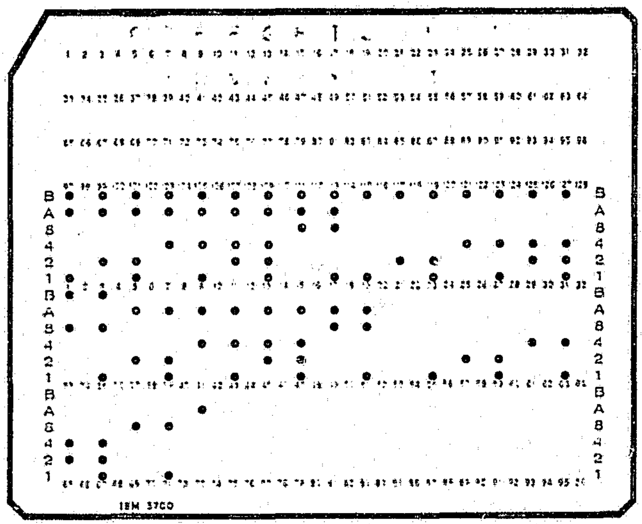


Figure 5.9 A 96-column punched card.

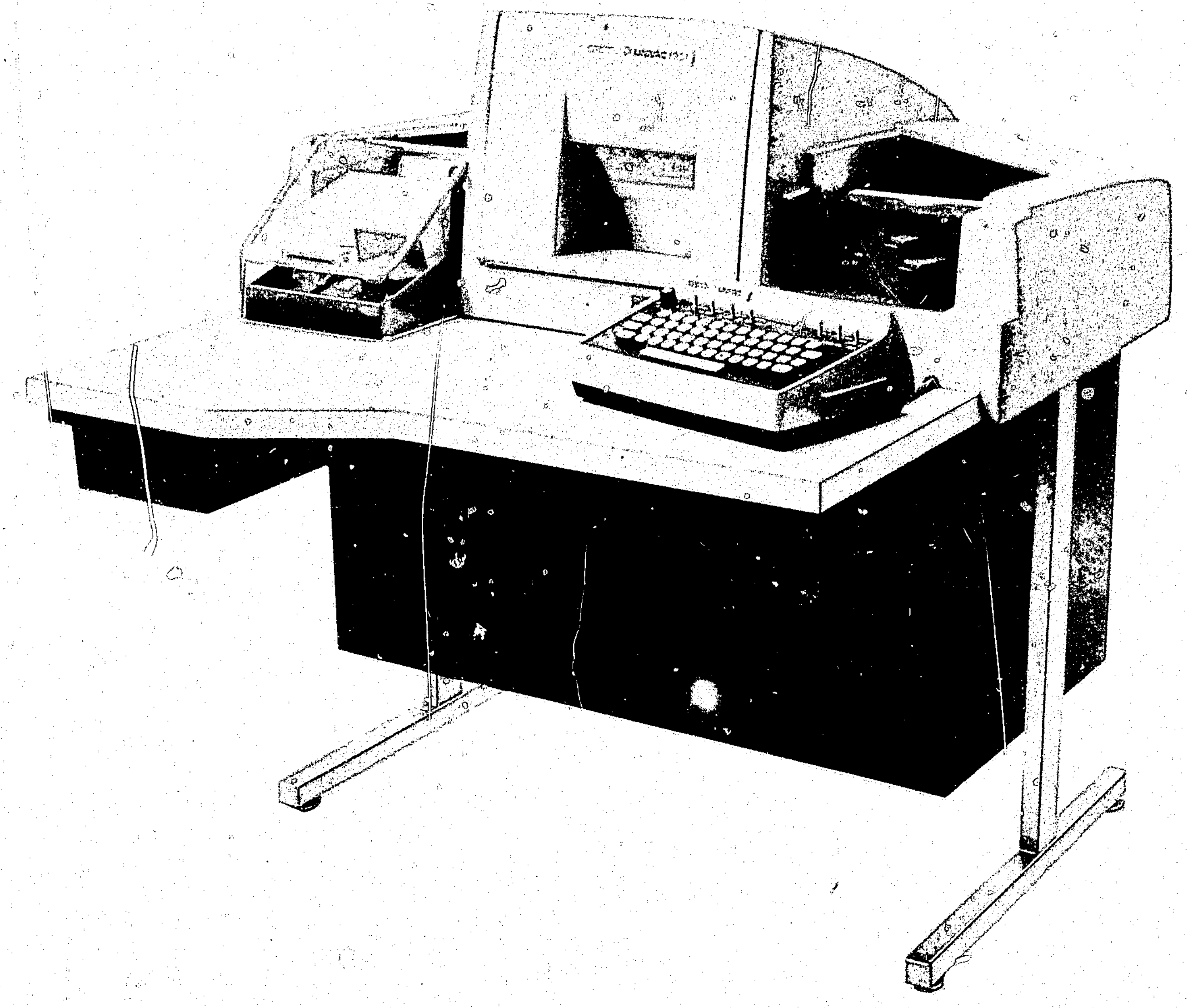


Figure 5.10. Two different keypunch for punching cards.

Fibure 5.11. Keyboard for card keypunch.

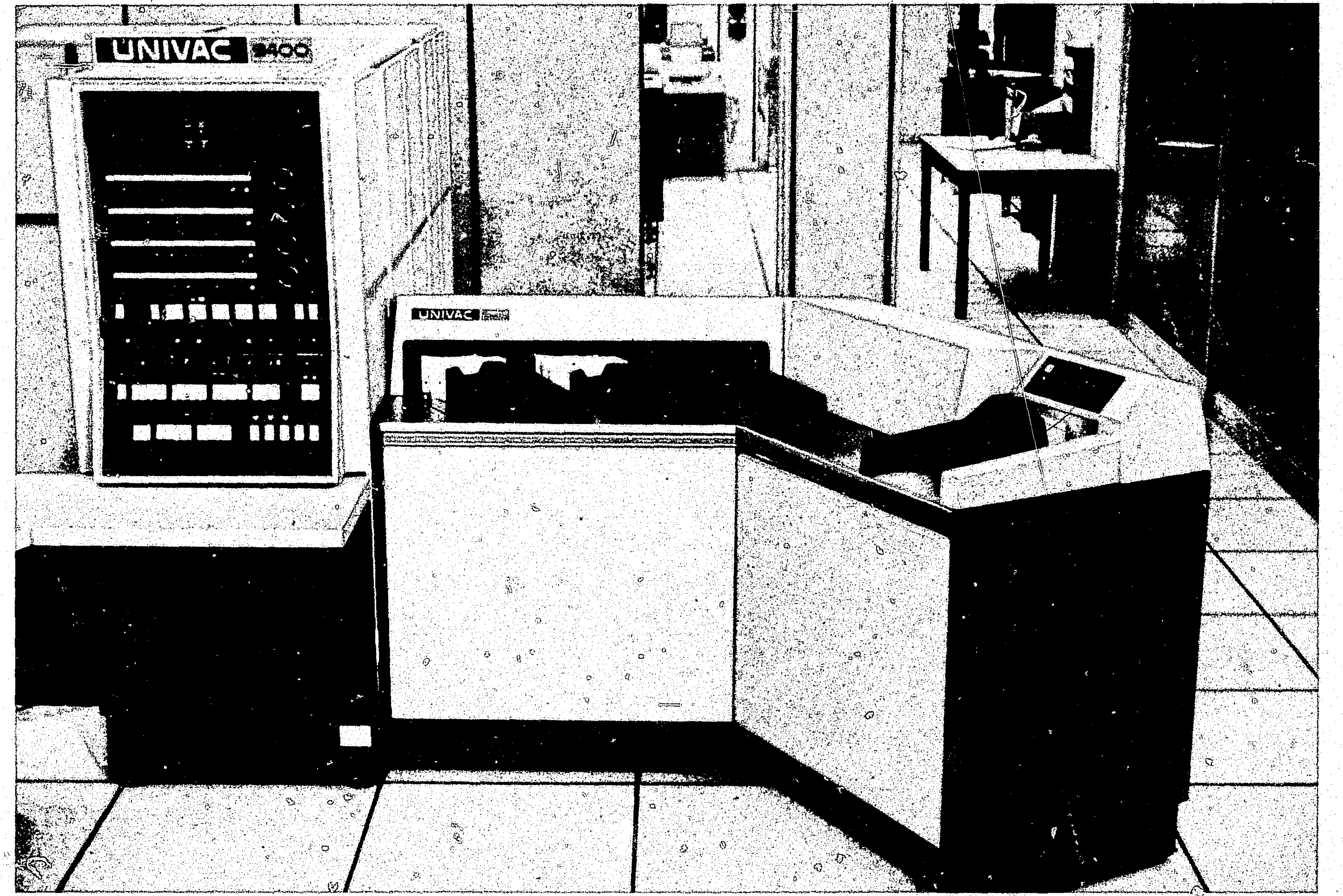


Figure 5.12. Computer card reader.

in cards or marks placed upon cards. The cards contain data or program instructions in a form easily handled both by operator and machine. The machine can read the cards rapidly (from fifty to over 1000 cards per minute), and the operator can re-order the cards, quickly replace an incorrect card with a correct one, or add or delete groups of cards with very little effort. The cards are read either electromechanically (using fine wires making electrical contact through the punched holes) or photoelectrically (either using lights coupled with light-sensitive devices, shining through the punched holes, or using such light sensitive devices to sense a reflective area on the card, placed by pencil to indicate a bit of data).

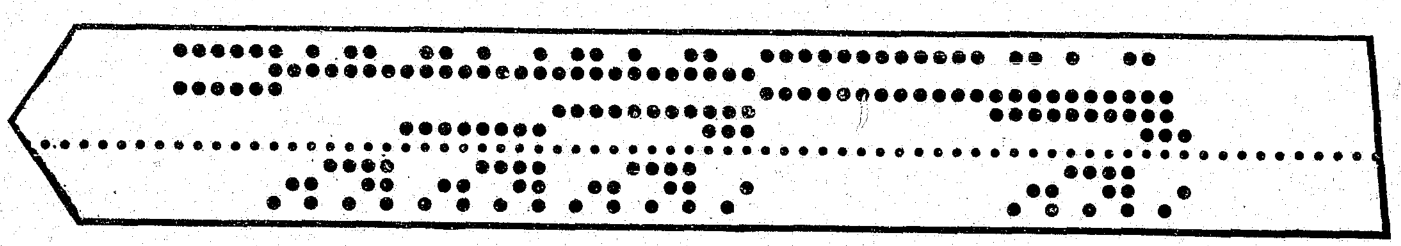
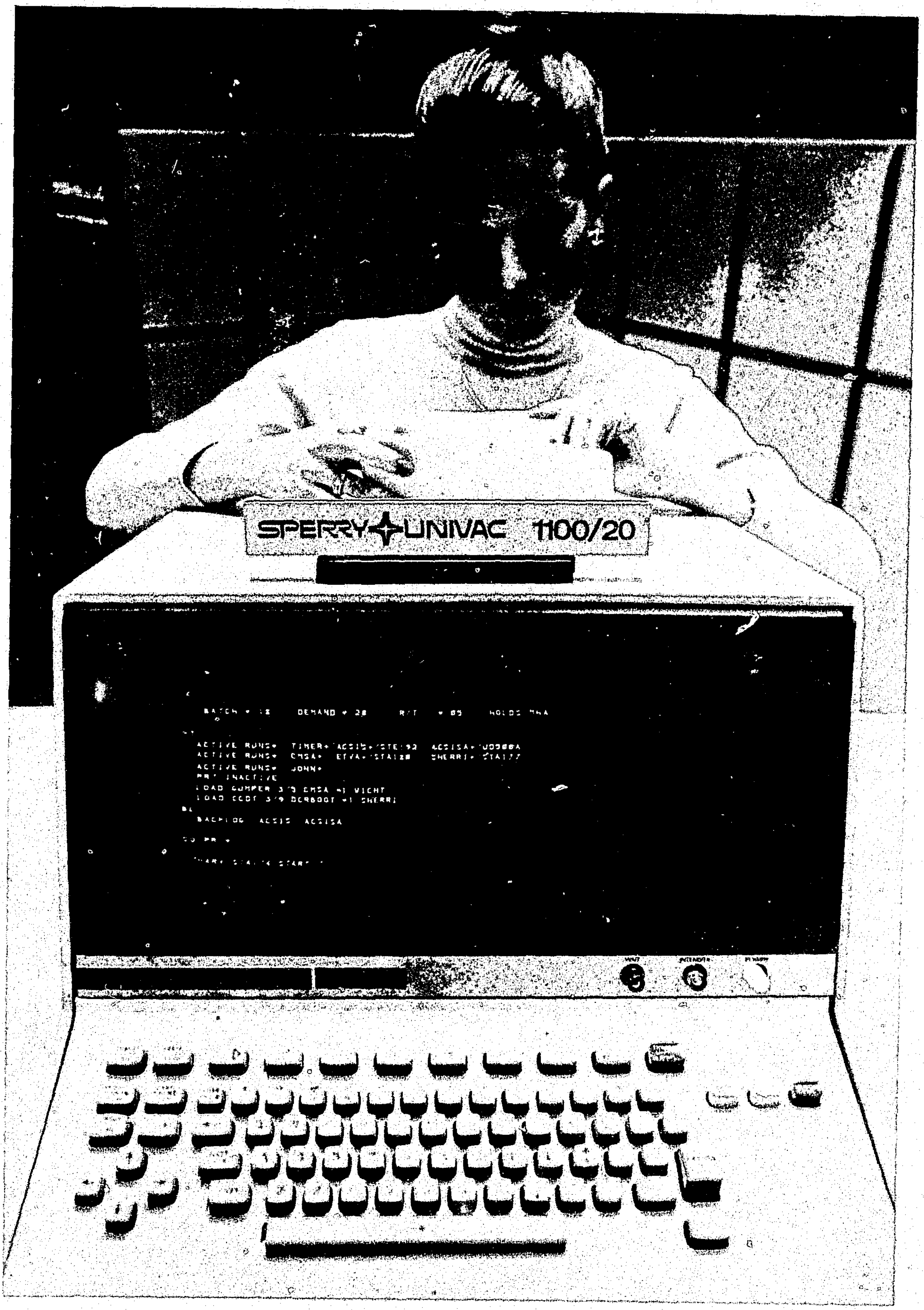


Figure 5.13. Punched paper tape.

A similar unit is the punched tape reader. A long strip of paper, rolled for convenience, is perforated so as to contain certain information, such as data or program steps; this perforated tape is then passed through either a mechanical reader or a photoelectric reader. The photoelectric reader is very similar to the card reader. The mechanical tape reader is more complex: the tape is moved so that the next set of holes is directly over a set of small pins; after the tape comes to rest, the pins are pressed by springs against the paper. Where there are holes, the pins pass through them, allowing an electrical switch to close; where there are no holes, the pins are prevented from passing through and from allowing the switch to close. The pins are then retracted to their initial positions, and the tape is moved to the next position.

Another input medium common to digital computers is the keyboard. Available from various manufacturers in many styles and with many diverse features, the keyboard is a most useful input device; it provides a printed copy of information being presented to the computer in a form meaningful to the operator. On time-sharing systems--systems which allow several users to process programs apparently simultaneously--the keyboard is the principal means of input, as well as output. On batch-load systems--systems which usually use cards or tape as input and process only one program at a time---the keyboard and its printer provide a monitor for computer function and usage. It provides notices to the operator of malfunctions or conditions that are out of the ordinary; it also provides a convenient means for diagnosing a malfunction, for cards and tapes are not so readily used as are ordinary English or FORTRAN or other statements typed with the keyboard.



```
BATCH = 12    DEMAND = 28    R/T   = 05    HOLDS NNA

ACTIVE RUNS=  TIMER+ ACSIS+/STE192  ACSISA+ UD000A
ACTIVE RUNS=  CMSA+  EIVA+/STA128   SHERRI+ STA177
ACTIVE RUNS=  JOHN+
PR? INACTIVE
LOAD GUMPER 3/9 CMSA +1 VICHT
LOAD CCDT 3/9 DERBOOT +1 SHERRI

BACKLOG  ACSIS  ACSISA

[illegible] PR [illegible]

[illegible] START [illegible]
```

Figure 5.14. Computer keyboard.

Frequently, input takes the form of magnetic tape; if a program or set of data has been developed elsewhere, perhaps on another computer, then a convenient method of transferring such information is by way of one or more reels of magnetic tape. The reader is a sophisticated version of the ordinary reel-to-reel recorder available for home or broadcast use; it is specially built to allow the tape to pass the reading heads at speeds in excess of 150 inches per second (this compares with home recorder tape speeds of seven and one-half to fifteen inches per second). Such speeds allow transfer of data at rates exceeding 6 megabits per second, at density rates of more than 7500 bits per linear inch. Proposed equipment will be able to handle data up to 15,000 bits per linear inch, an increased track density to 300 tracks per inch and increased accuracy allowing less redundancy of recording. One device uses a 12-inch wide tape, providing data transfer up to 38 megabits per second, higher than most computer channels will accommodate.

Optical character readers are also being used for direct input. Characters printed in a special typeface can be read directly by photoelectric means, allowing the input to be usable as information both by the operator and the machine. Strides have

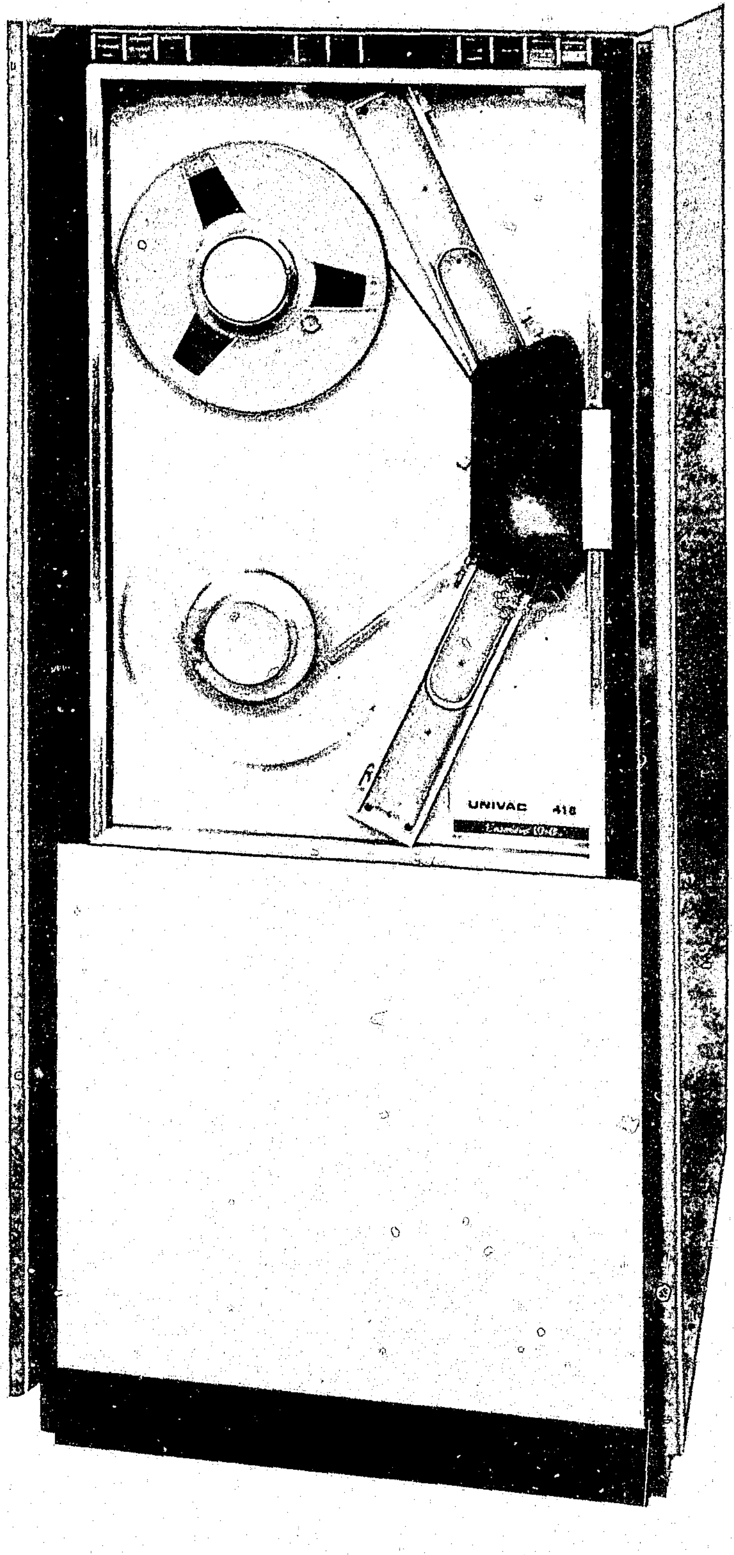


Figure 5.15. Magnetic tape unit.

been made toward recognition circuits capable of reading hand-written symbols. Carefully controlled character shapes are usable, but the general, randomly-shaped human handwriting is not yet within the reading capability of the ordinary character reader.

Storage Devices.

Once the desired program and data are inside the computer, they are stored temporarily in one of a variety of memory devices, to be recalled later as the program is executed. The same memory devices serve in other ways during the computing process.

One of the principal types of memory is the magnetic core memory. Small toroids or "doughnuts" of magnetic material called "cores" are woven, almost exclusively by hand, into a network of fine wires. The electronic circuits which control access to the memory are called "drivers"; by choosing the proper pair of wires that intersect paths at a particular toroid or core, enough electrical current can be passed through the center of the core to change its magnetic state and thus to store or "write" one bit of information. Grouping these cores into large patterns allows many computer words, each with thirty-two bits, for example, to be stored at one time; one core is used for each one of the bits of information in each computer word. It should be noted that different computers use different lengths of words; the numbers vary from eight to as many as sixty bits per word; each word is simply a grouping of bits of information usable by the computer.

Reading information stored in a core memory is very similar to storing it; a current is passed through certain wires, and if the particular core was magnetized in the right way, the current causes the magnetic state to change back to its original state. This causes a current to flow in a third wire if a "1" was stored (no current for an "0"); this third wire is called a "sense" wire, and carries the information to the driver circuits for transfer back to the computer. Since this destroys the information stored in the core, the drivers must then re-write all the bits that were read back into the core memory. Such a memory has what is called a "destructive read-out", since reading information out of it destroys the information. The core memory is a versatile and reliable memory device, and access to stored information is very rapid. It is chiefly used for storing numbers being operated upon, for storing programs, or for use as an "electronic scratch-pad" during operation.

Continued strides are being made in core technology; smaller, more reliable core elements are being produced at a lower price. Core density in 1970 was only 1678 cores per square inch, costing in a bare stack configuration (minimal circuitry) about 0.5 cents per bit. By 1973 density had improved to about 6500 cores per square inch, and costs are currently less than 0.25 cents per bit.

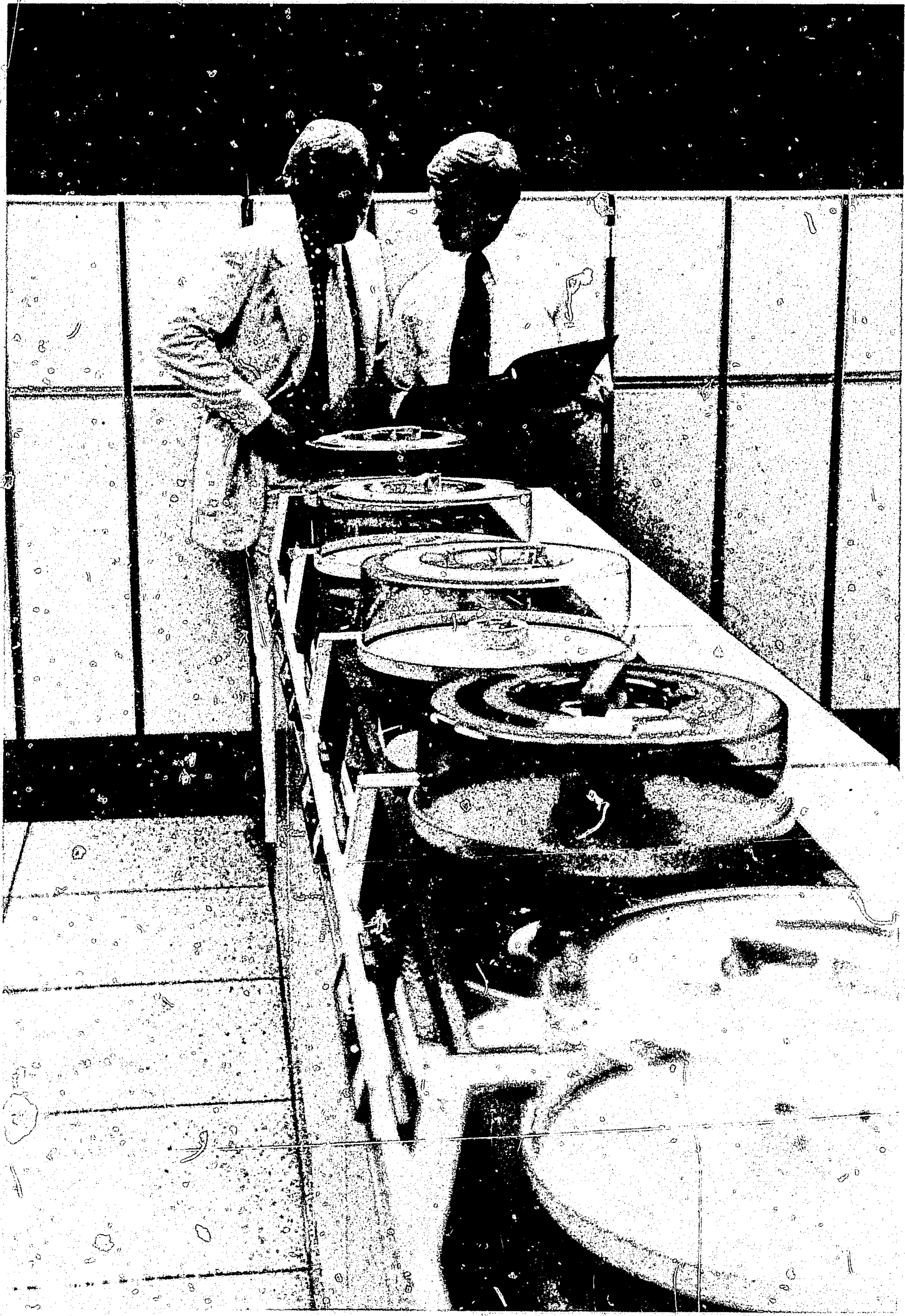


Figure 5.16. Direct access storage facility.

Several other types of memory devices use magnetic characteristics in their structure; instead of a core of material they make use of a thin film of material placed on some non-magnetic base. The three most common such devices are the magnetic drum, the magnetic disc, and the magnetic tape. The drum is rarely seen now in new computers, for the difficult manufacturing processes make it quite expensive. The drum consists of a cylinder coated with a thin film of magnetic material. Mounted around the periphery of the drum are numerous reading and writing devices called "heads"; the writing head causes a small magnetic field to pass through the drum's film and change the magnetic state of that particular spot. By placing enough of these heads along the drum, many circumferential tracks of spots can be used simultaneously.

As the drum revolves at a high rate of speed, the driver circuits keep track of the current location of each spot on the drum, and can call for the right information as it passes under the read head. The magnetic field in the film causes a small current to flow in the read head, and this is returned to the driver circuit to be used by the computer. The read and write heads must be mounted so close to the drum that any irregularities in the drum, in the film, or in the head alignment can cause the head to strike the drum and ruin it; it is this threat which demands such close and expensive manufacturing tolerances.

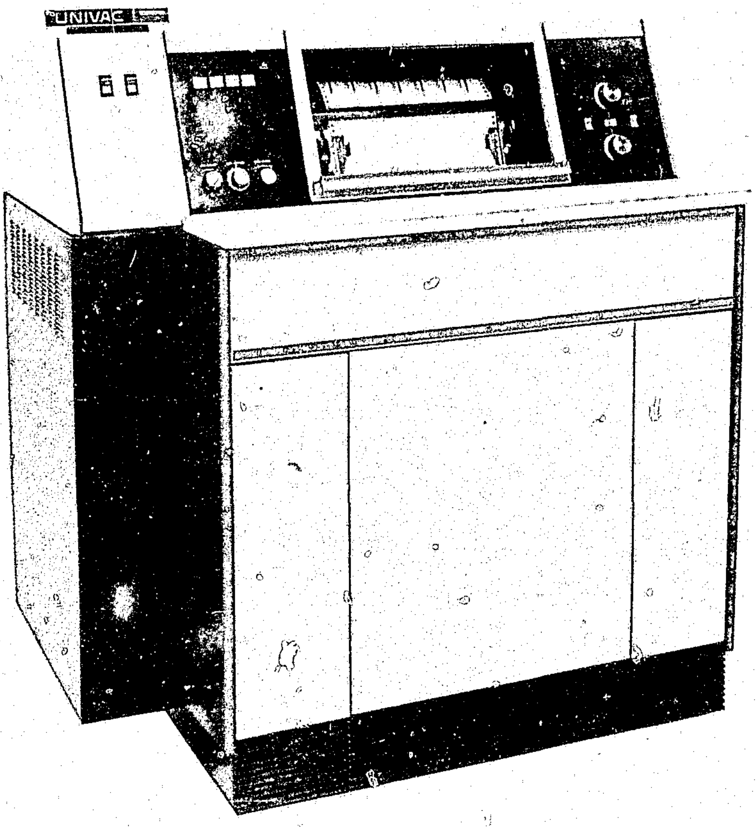


Figure 5.17. Magnetic disc.

A more recent application of thin magnetic film is the magnetic disc. Shaped like a large, thick phonograph record, the disc rotates between read/write heads at high speeds. The same read/write process is used as was used on the drum. Even though the basic idea of a rapidly moving magnetic surface is used, the disc is more efficient and more economical, because less physical space is required, less stringent manufacturing processes are involved, and less expensive materials can be used for the disc itself. In addition, several discs can be mounted in a stack, with heads mounted between them, to provide an even more compact arrangement. An additional feature is an interchangeable disc pack, allowing almost unlimited storage capacity. This allows programs using a particular language to be stored together or allows an expanded data or program library. Some smaller computer installations use an interchangeable single disc with the same results in versatility.

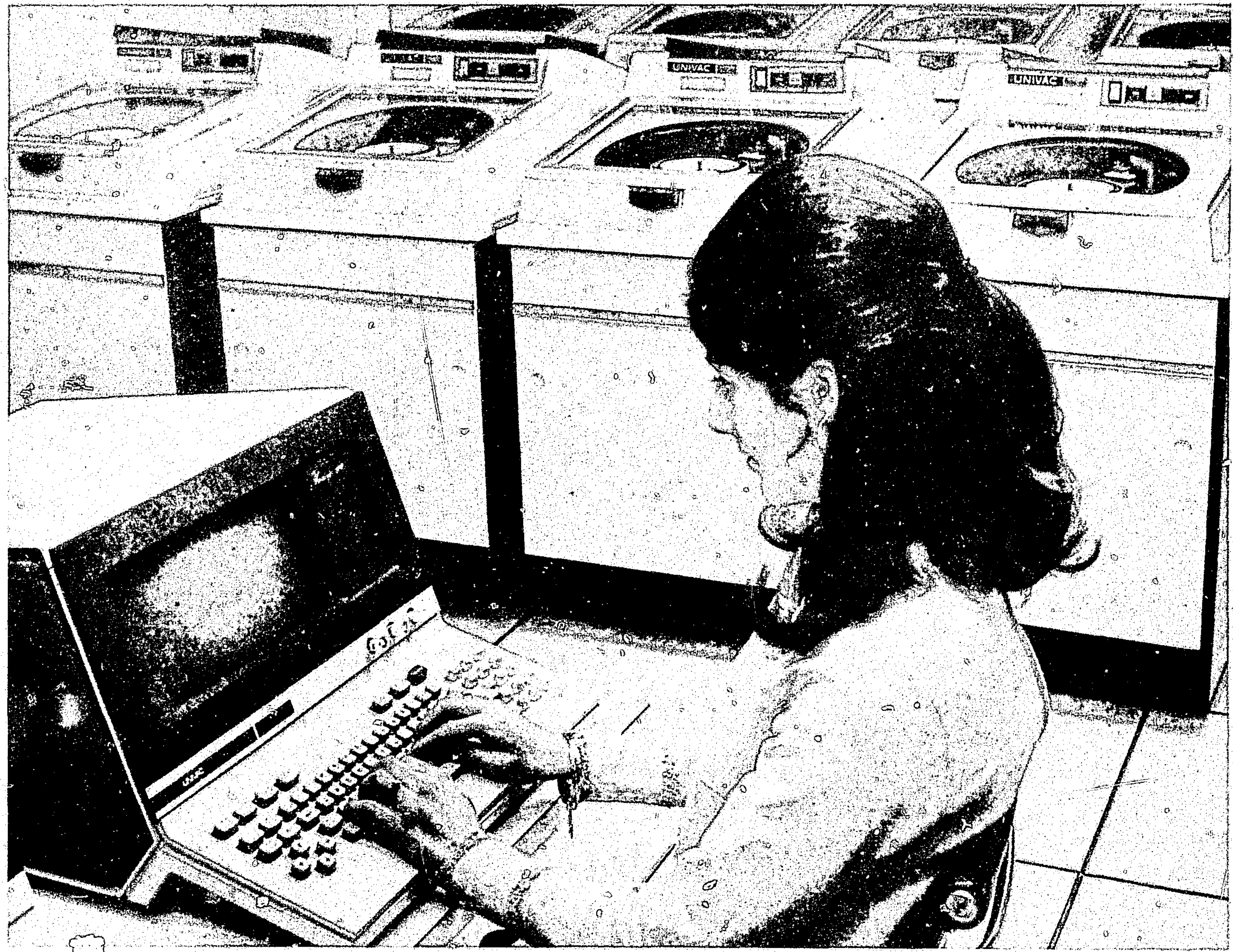


Figure 5.18. Computer console and disc

Disc memories are subject to some of the same problems as drums, but have very strong advantages. The read/write heads must fly at approximately 25 microinches from the surface, leaving little room for imperfections. Improvements in manufacturing techniques in both the disc itself and in the mechanism controlling the read/write heads are allowing great advances in bit density and track density provisions. Bit density has been improved from about 2200 bits per inch to more than 6000 bits per inch, with track densities approaching 400 tracks per radial inch. These improvements allow package storage capacities of 40, 80, and even 200 megabytes of data storage, from such manufacturers as Ampex and IBM. Projected maximum packaging density is in the neighborhood of 350 megabytes per unit.

The magnetic tape already mentioned as an input medium is also widely used a supplemental or "auxiliary" storage. Several characteristics especially qualify tape for this usage. A typical reel of tape contains some 2,400 feet of tape and can store as much information as 400,000 punched cards. Such reels are usually ten and one-half inches in diameter with large hubs. These reels of tape are primarily used for large amounts of data which need to be preserved, but which will probably be used in roughly the same sequence as it appears on the tape. The physical situation of a long piece of tape with information placed along its entire length requires that a definite, and sometimes long, time must elapse between the time that information is requested and the time

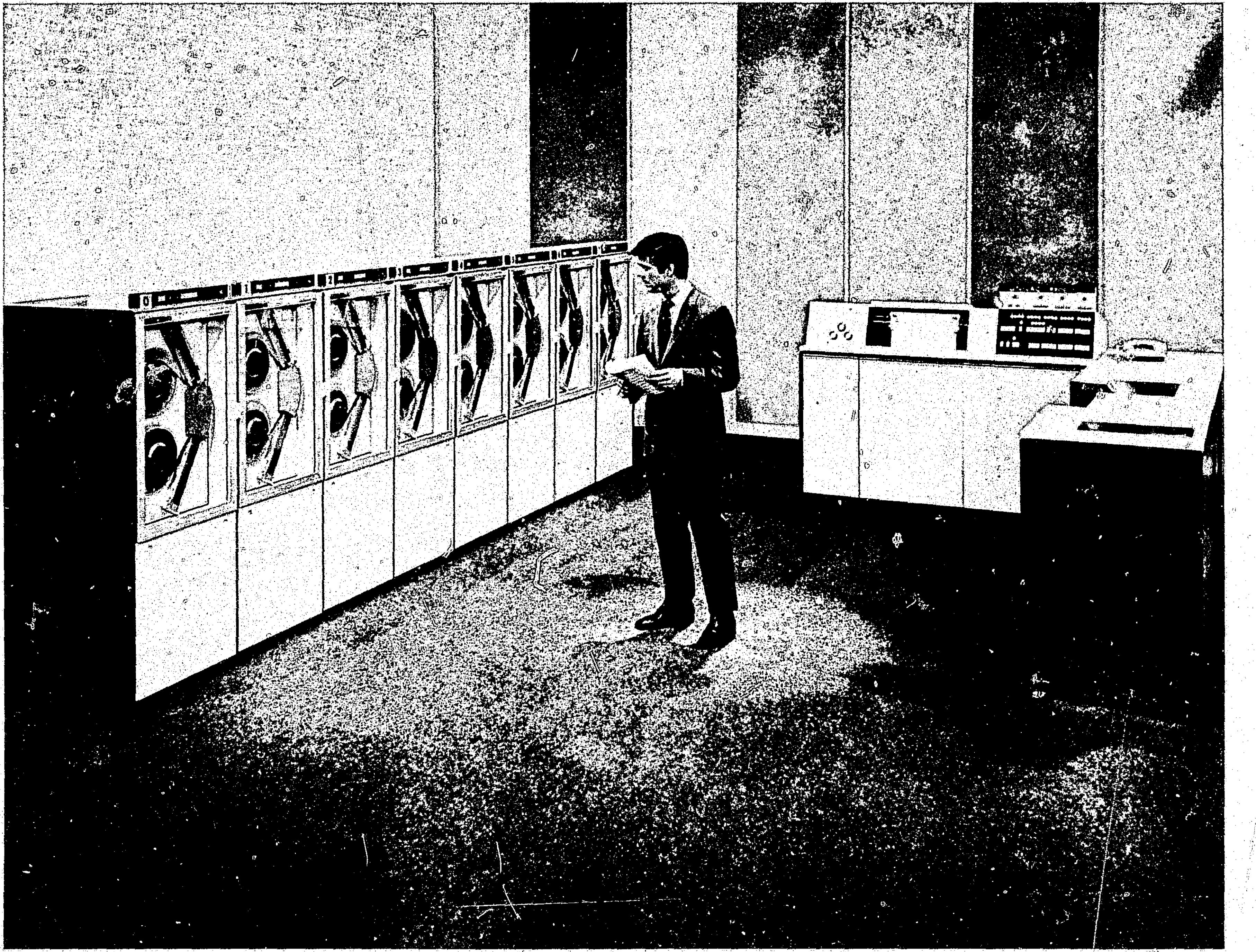


Figure 5.19. Magnetic tape units.

that its location is found on the tape. Tape is thus referred to as a "sequential" or "serial" access medium, contrasted with a "random" access medium, such as the magnetic core memory.

Similar usage is made of the Phillips design of tape cassette, especially in small computers or minicomputers, and in programmable calculators. The convenience of size and interchangeability makes the cassette a most attractive storage medium.

Research has produced several promising techniques which may someday replace or successfully compete with disc and semiconductor memories. The magnetic bubble device is one such item; the technology is a complex mixture of thin magnetic film and semiconductor theory, capable of storing some 2.5 million bits per square inch (in chips with about 16,000 bits each). Data transfer rate is above 100,000 bits per second, and access time is about 2.7 milliseconds, comparable to rotating discs.

Another advance in memory technology is the charge-coupled-device (CCD); this technique uses a capacitor-like arrangement on a simiconductor chip, and by placing a capacitative charge at selected places, data can be stored in bit form. Bit density is about 16,000 bits per chip, with latency (access time, roughly) of 128 microseconds per chip, some two orders of magnitude better than a disc. A typical CCD unit, composed of chips roughly equivalent in storage to a drum, occupies about 1/10 the volume of the drum; it weighs almost 10 times less (at 15 lb.); it consumes about 5 watts, compared with 300 watts for the drum; its access time averages 2 milliseconds, some five times faster than the drum. CCD units are volatile, that is, they lose their retention with no power; this situation is easily dealt with by providing simple power back-up in the form of several dry cells.

## Computer Control and Arithmetic Units

After the data and program directions have been entered and properly stored, the computer must begin to process the data and perform specified operations on it. The unit which oversees the entire process from input through storage and operations to output is the computer control unit. This unit interprets the program commands and determines the sequence to be followed as data is processed from input to an appropriate output. Since the control unit cannot make rational choices, all possible conditions to be encountered must be planned for. The unit can then call on its limited, but adequate vocabulary to interpret commands, and if an unfamiliar command appears, it halts program execution.

One remarkable characteristic of control units is the capacity put there by the designer to keep accurate tally of all operations performed, to keep accurate accounts of the locations of all stored information, and in the case of a time-sharing system, to keep track of which user is being served and of where his data and programs are located. The actual mechanics of performing the tasks may be straightforward, but the speed of operation is phenomenal.

Under the direction of the control unit, data is moved from input or memory to the arithmetic unit where all of the actual operations are performed. The repertoire of operations is relatively limited, including only the four arithmetic operations, numerical comparisons, and certain other algebraic functions. In most computers, the trigonometric functions are performed with series arithmetic or other software procedures; the great speed with which this is accomplished keeps the extended process from significantly slowing the program execution.

Output Devices

The results of the program's manipulation of the data must ultimately be put into some form accessible to the operator, or perhaps to some other device or computer. The medium used is known as an output. For operator usage, a printed output is commonplace.

Several categories of printers are currently in use. The keyboard, already mentioned in connection with the input function, also serves well for limited use with many systems, but especially with time-sharing systems, where it is customary. The keyboard in its various forms is relatively slow in comparison with computional speeds.

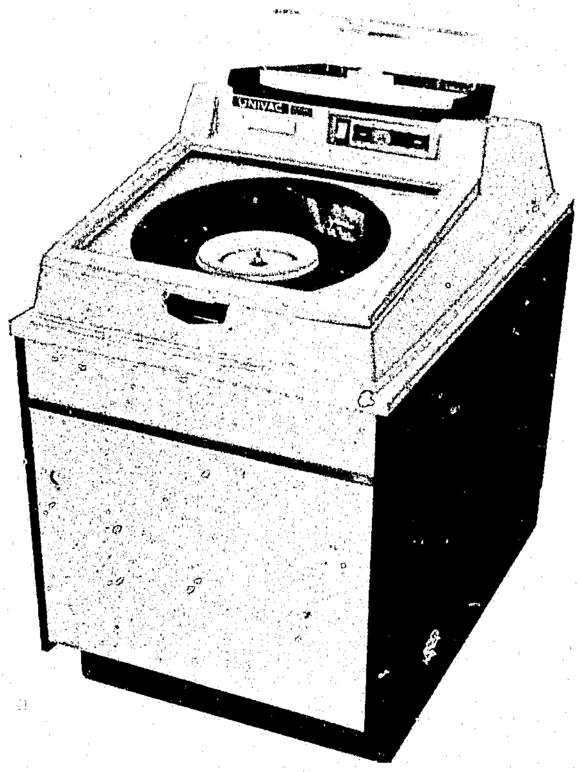


Figure 5.20. Line printer.

A different concept in printers is the "daisy wheel" printer, which uses a device very similar to the letter wheel in a label maker. The type is affixed to the end of a flexible spoke, and as the wheel is rotated rapidly, the wheel is struck at an appropriate time (determined by the circuitry) to drive the desired character against the inked ribbon and then against the paper. Typical speeds are about 30 characters per second, with greater speeds possible under carefully controlled manufacturing processes.

A printer combining some characteristics of the daisy wheel and some of the full cylinder line printer (above) is the quasi-lineserial printer utilizing a character chain or belt, with a full bank of hammers. Speeds have been attained in excess of 400 characters per second.

Faster speeds are possible with the line printer, which uses various means to print several characters in one concerted effort One of the most effective means used to accomplish this feat uses a metal cylinder engraved or molded so as to have all the alphabetic, numeric and special characters in every available printing column, placed in an order around the cylinder. As the cylinder revolves, a hammer placed in each printing column strikes the paper and ribbon against the proper character, whose position is sensed by the printing driver circuitry. Such a printer may be capable of printing more than 1000 lines per minute, each with up to 136 characters. Even at these speeds, however, the printer may not produce output as fast as the computer provides the information.

The dot-matrix mechanism is widely used in both small (20 or so columns) and large (full 132 columns) applications. The mechanism prints the characters as a combination of 35 matrix elements, arranged in five columns of seven rows each. Two major variations are common: one prints an entire character, all 35 (or fewer) elements at once; the other prints one column at a time, with the buffer circuitry keeping track of which elements of which columns are currently needed. Several copies can be made at once, and legibility is very good. Speeds up to 30 characters per second are easily obtained.

CONTINUED

1 OF 3

A device utilizing the dot-matrix approach, but without the noise of the impact solenoids, is the thermal printer, which forms characters on heat-sensitive paper. Where silence is needed and multiple copies are not, the thermal approach is most adequate.

A non-impact system in limited use utilizes electrostatic control of a charged stream of ink particles, actually painting the characters in good form. Again, multiple copies are not possible, but all such devices have trade-offs in speed, output form, and noise level.

Other output devices are specially tailored for specific requirements, such as the graphic plotter which can produce line drawings, lettering, and plots of algebraic or other functions. Cathode-ray tube displays are frequently used for output (and occasionally for input) for timesharing systems; these can provide graphic or other data quickly, and results of alterations in programming can be seen rapidly. Occasionally, output is required in the form of paper tape or punched cards, and appropriate equipment is available to accomplish this. Other equipment designed to fill a particular need is used as the situation demands.

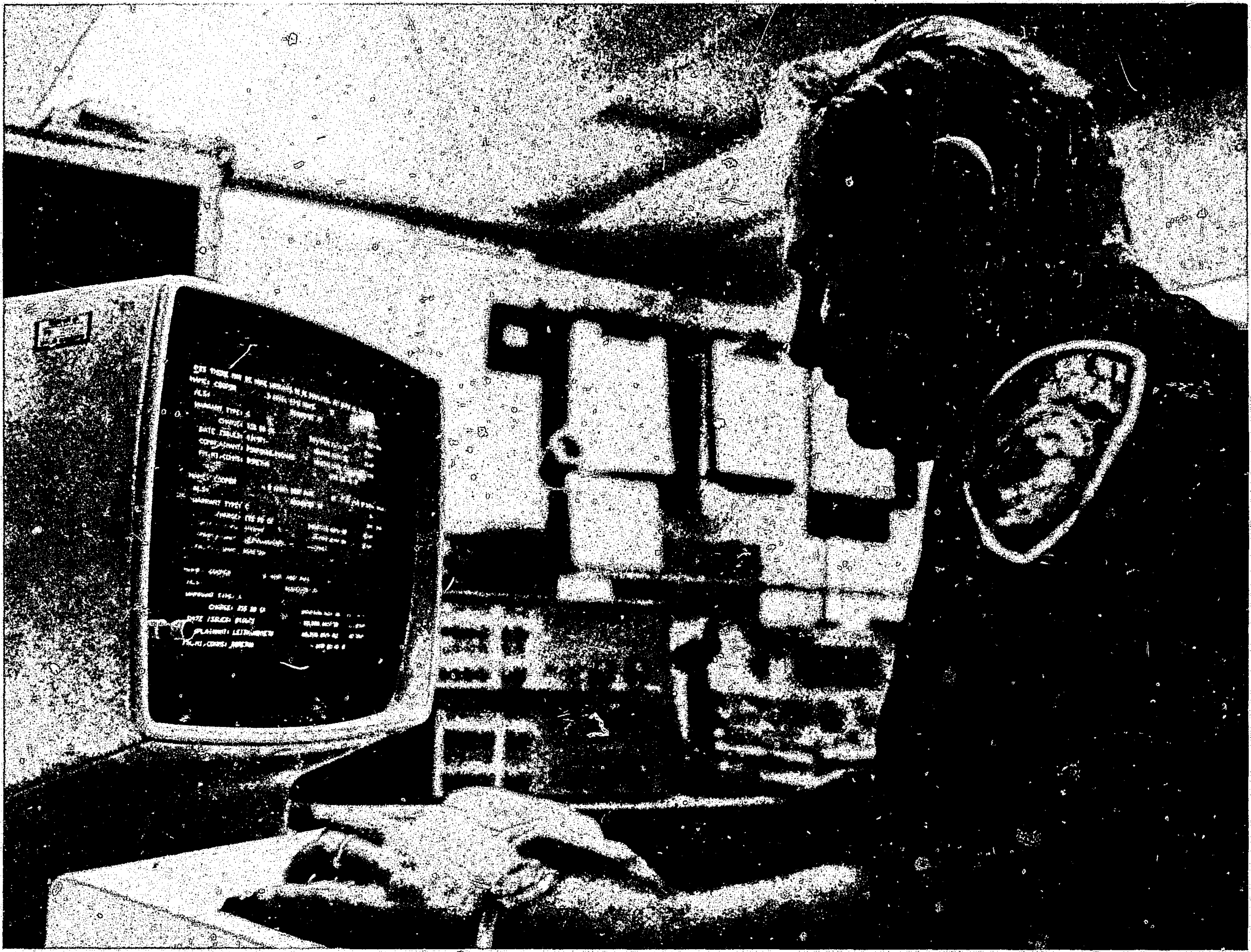


Figure 5.21. Display terminals.

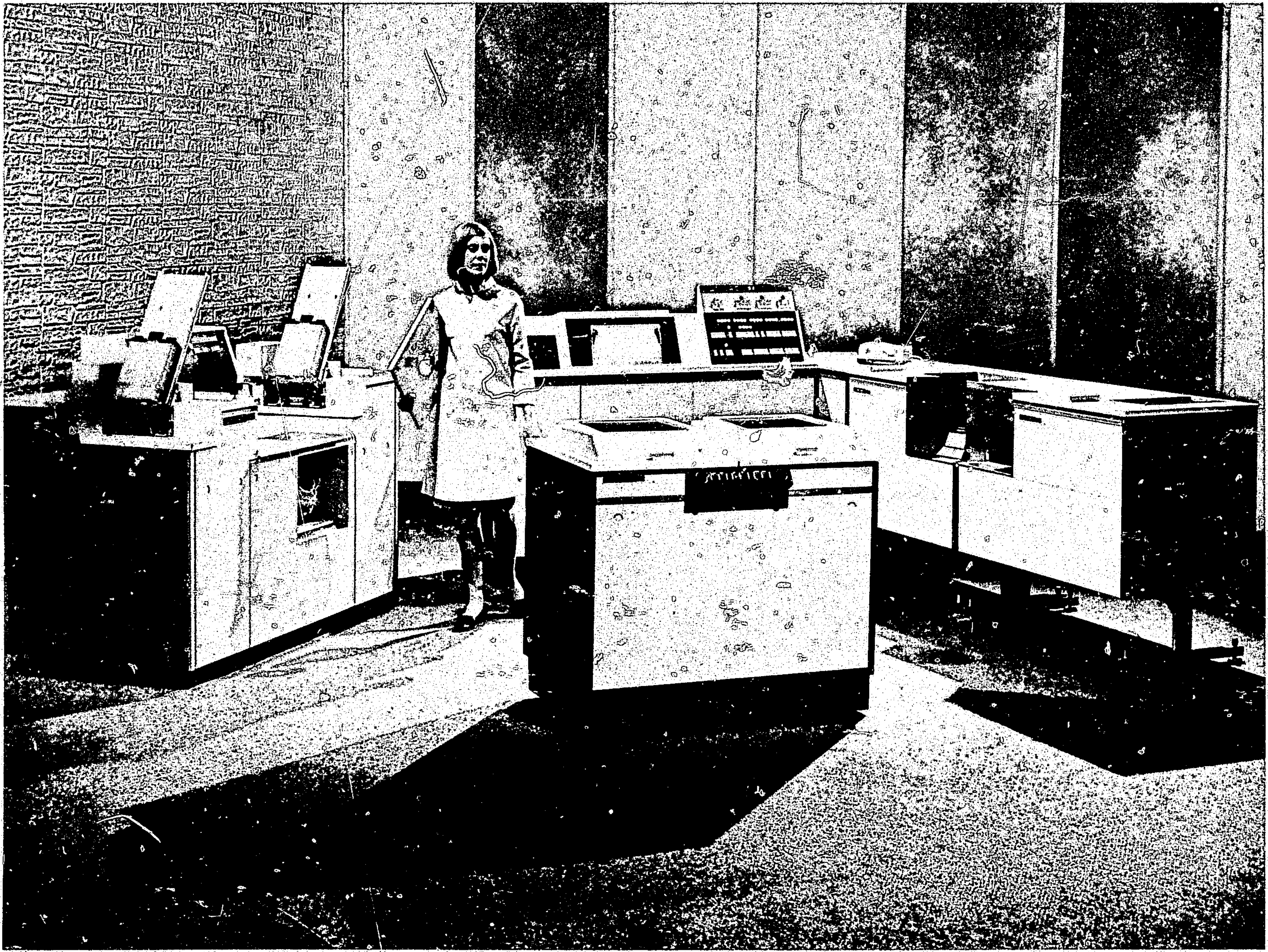


Figure 5.22. Complete computer system showing CPU, card reader/punch, disc units, magnetic tape units and line printer.

# CHAPTER VI

# COMPUTERS IN LAW ENFORCEMENT

## Why Use Computers in Law Enforcement?

The use of computers by law enforcement agencies and criminal justice departments is a relatively new innovation. More and more law enforcement agencies are turning to computers for help in solving the many and varied problems facing these agencies.

The process of gathering, interpreting, and disseminating information is an important and time consuming operation of law enforcement agencies. Computers and computer systems have shown their effectiveness in carrying out these processes in other areas, and the systems that are now operating to assist the law enforcement community are showing that the performance capabilities of computer systems can greatly enhance this community's efforts. Increasing the efficiency of processing emergency calls, more efficient utilization of man power, improved accuracy in reporting, greater return on the investment of tax dollars, more meaningful reports for management, and the delivery of timely and more complete information to dispatchers and field personnel are some examples, and arguments for implementing computer systems to augment law enforcement efforts.

From utilizing the data processing capability of a computer, to developing its telecommunication and programming capability, law enforcement agencies are tapping every advantage a computer system can offer. In doing so, these agencies are able to serve the public in a manner that was previously impossible.

## Dallas County Judicial Information System[1]

A good example of a coordinated computer system used in law enforcement is the IBM System/370 system installed for usage in Dallas County. In 1971, Dallas county began development of the criminal justice information system, designed to satisfy the law enforcement information needs of all county agencies and in addition to satisfy the requirements of the judiciary system. The civil court and the criminal justice information systems have been brought together to form the Dallas County Judicial Information System.

The success of the overall system has been the county's ability to add new reporting requirements imposed by state law and to handle the growth in quantity of data at minimum increase in cost. The system has made information available on a much wider basis than before, by use of the online video and typewriter-like terminals.

Following are some of the advantages to be derived from a judicial information system similar to the one serving Dallas County:

> Video terminals, with television-like screens, display requested information instantaneously, and other terminals provide printed copy. The result is swift access to information in formats to serve many different purposes.

[1] Information and figures courtesy of IBM.

Online jail book-in generates a centralized, alphabetically indexed data base using unique number identifiers that can be used by all authorized agencies, thereby eliminating duplication of effort and providing complete information on each defendant.

The system is linked to a state data base in Austin, the Texas state capitol, which contains information from other jurisdictions. Austin also provides a link to the National Crime Information Center (NCIC) in Washington, D.C.

Computer-assisted indexing allows case histories to be maintained and accessed by many references. The time-consuming search for an individual's case or docket number is eliminated.

The data base created through case indexing is easily expanded with additional information. Each time a transaction occurs within the judicial process, it is entered directly to the individual's file by number, providing a complete history of each case for immediate reference.

Daily, information is fed into the computer and coordinated with other data concerning the status of current cases, thus assisting the judicial administrator in setting his calendar.

The probation department uses information on file to provide a complete monetary accounting system online. The court and the probation officer have up-to-the-minute information on the probationer, including the status of his probation fee and restitution accounts.

Once pertinent information is entered into the computer files, the system can monitor all proceedings through the final disposition of the case.

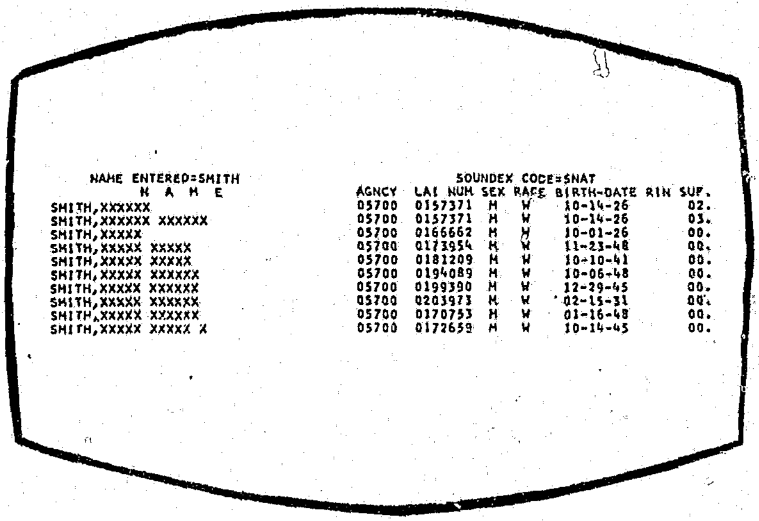
Information can be retrieved and displayed on terminals near the trial judge's quarters. The same terminal can be used to update the defendant's file.

Primary users of the system include the sheriff's office, criminal court judges, district court clerks, district attorneys, probation officers, district and county clerks and the county auditors. Services provided include (a) maintenance of files accessible online (b) generation of detailed listings throughout all phases of judicial administration and (c) extraction of administrative and statistical information. The system can be divided into two parts: criminal and civil. Our primary concern is with the information available on criminal justice. This criminal information available through the system may be classified as follows.

Criminal Identification:

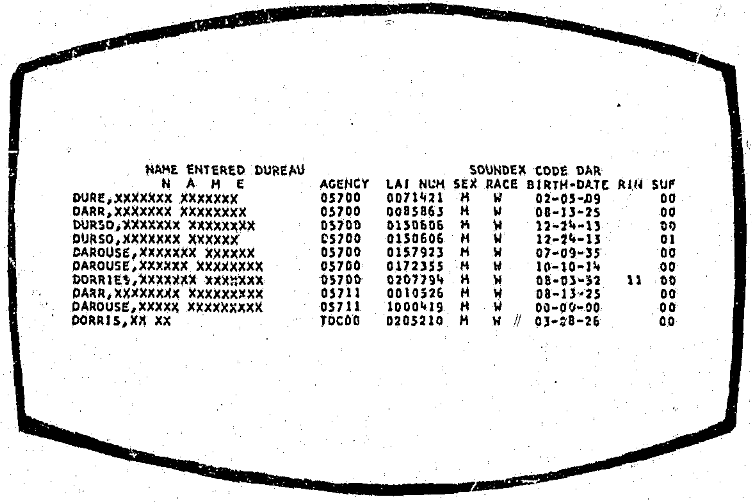
An alphabetic criminal name index is now used by the Dallas County sheriff and several agencies in north central Texas, providing online maintenance and inquiry into computer files containing about 600,000 names with personal identifiers and pointers to corresponding record jackets maintained in hard-copy files of participating law enforcement agencies.

Any of the 16 counties in the North Central Texas Region can enter data into the system. The index provides the user with information to help in the identification of suspects and renders quick access to criminal case history files.



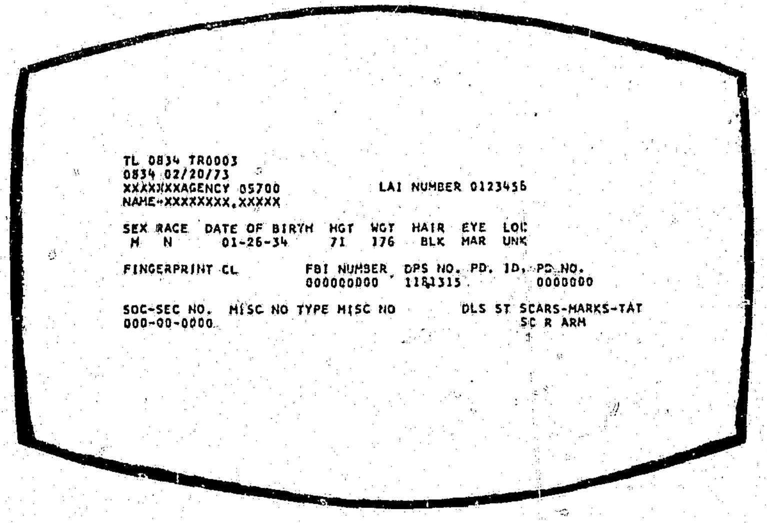
```
    NAME ENTERED=SMITH                                SOUNDEX CODE=SNAT
          N  A  M  E                 AGNCY  LAI NUM SEX RACE BIRTH-DATE RIN SUF.
SHITH,XXXXXX                         05700  0157371  M   W    10-14-26       02.
SMITH,XXXXXX XXXXXX                  05700  0157371  M   W    10-14-26       03.
SMITH,XXXXX                          05700  0166662  M   W    10-01-26       00.
SMITH,XXXXX XXXXX                    05700  0173954  M   W    11-23-48       00.
SMITH,XXXXX XXXXX                    05700  0181209  M   W    10-10-41       00.
SHITH,XXXXX XXXXXX                   05700  0194089  M   W    10-06-48       00.
SMITH,XXXXX XXXXXX                   05700  0199390  M   W    12-29-45       00.
SMITH,XXXXX XXXXXX                   05700  0203973  M   W    02-15-31       00.
SMITH,XXXXX XXXXXX                   05700  0170753  M   W    01-16-48       00.
SMITH,XXXXX XXXXX X                  05700  0172659  M   W    10-14-45       00.
```

Response to last-name inquiry for criminal identification



```
        NAME ENTERED DUREAU                         SOUNDEX CODE DAR
           N  A  M  E              AGENCY  LAI NUM SEX RACE BIRTH-DATE RIN SUF
DURE,XXXXXXX XXXXXXX               05700   0071421  M   W    02-05-09       00
DARR,XXXXXXX XXXXXXXX              05700   0085863  M   W    08-13-25       00
DURSO,XXXXXXX XXXXXXXX             05700   0150606  M   W    12-24-13       00
DURSO,XXXXXXX XXXXXX               05700   0150606  M   W    12-24-13       01
DAROUSE,XXXXXXX XXXXXX             05700   0157923  M   W    07-09-35       00
DAROUSE,XXXXXX XXXXXXXX            05700   0172355  M   W    10-10-14       00
DORRIES,XXXXXXX XXXXXXX            05700   0207794  M   W    08-03-32   11  00
DARR,XXXXXXXX XXXXXXXXX            05711   0010526  M   W    08-13-25       00
DAROUSE,XXXXX XXXXXXXXX            05711   1000419  M   W    00-00-00       00
DORRIS,XX XX                       TOC00   0205210  M   W // 03-28-26       00
```

Response to name inquiry, including sound-alike names



```
TL 0834 TR0003
0834 02/20/73
XXXXXXXAGENCY 05700                LAI NUMBER 0123456
NAME-XXXXXXXX,XXXXX

SEX RACE  DATE OF BIRYH  HGT  WGT  HAIR  EYE  LOC
 M   N      01-26-34     71   176   BLK  MAR  UNK

FINGERPRINT CL          FBI NUMBER  DPS NO. PD. ID. PD.NO.
                        000000000   1181315          0000000

SOC-SEC NO.  MISC NO TYPE MISC NO          DLS ST SCARS-MARKS-TAT
000-00-0000                                       SC R ARM
```

Identifying data display

Inquiry via video display terminals is made into the files, which contain identifying numbers; personal descriptors, including sex, race, and date of birth; and file flags for aliases and for past criminal records. The information can be updated either by data entries through the video terminals or by card input.

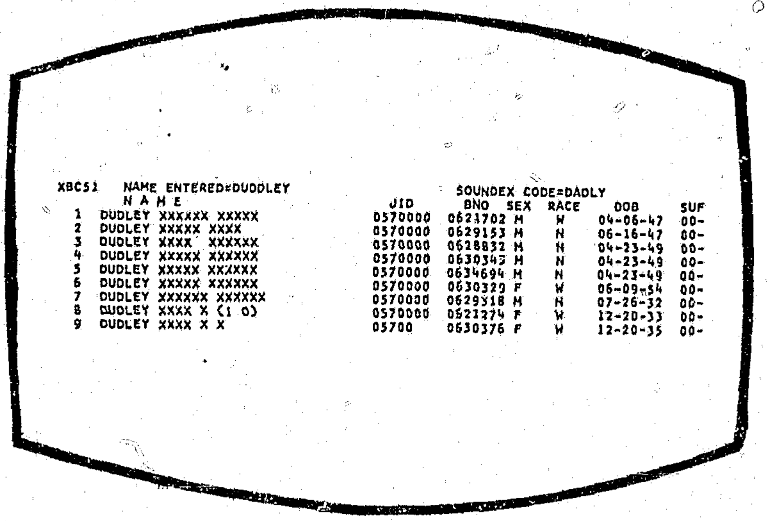
Two inquiries are possible. One, which brings up ten displays of ten names each, provides basic identification information. Such data is retrieved by using a subject's last name. (On the basis of the first inquiry, which also produces a display of sound-alike names, one or more names may be selected as warranting further investigation.

The other inquiry will produce a display of identifying numbers and physical characteristics, which are retrieved using the agency identification and the local agency identifier.

Book-in and Custody:

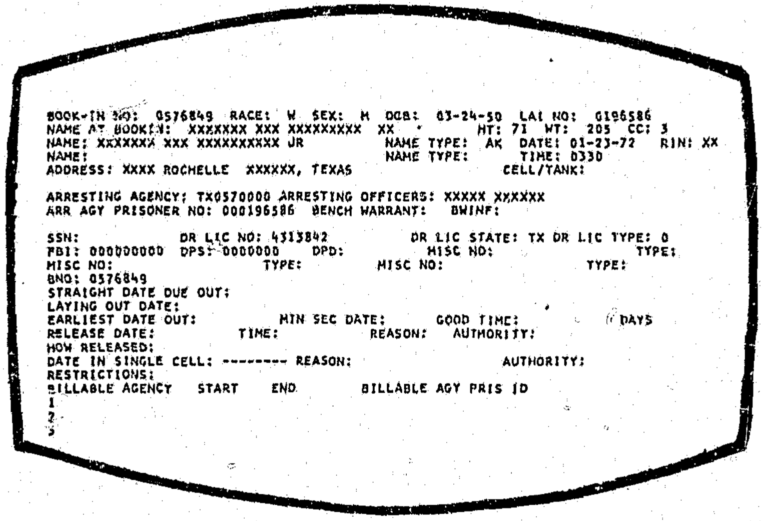
The book-in and custody subsystem provides information and services relating to the incarceration of prisoners. The computer first comes into play when a defendant is brought to the county jail and information is entered via video terminal keyboards concerning the reason he (or she) has been brought to jail, the time, where he was brought from, and in what part of the jail he will be held.

After the initial steps are completed and the defendant is in custody, the computer records all the steps involved in court



```
XBC51   NAME ENTERED=DUDDLEY                          SOUNDEX CODE=DADLY
          N A M E                            JID       BNO    SEX  RACE    DOB     SUF
   1  DUDLEY XXXXXX XXXXX                 0570000  0623702 M    W     04-06-47  00-
   2  DUDLEY XXXXX XXXX                   0570000  0629153 M    N     06-16-47  00-
   3  DUDLEY XXXX  XXXXXX                 0570000  0628832 M    N     04-23-49  00-
   4  DUDLEY XXXXX XXXXXX                 0570000  0630343 M    N     04-23-49  00-
   5  DUDLEY XXXXX XXXXXX                 0570000  0634694 M    N     04-23-49  00-
   6  DUDLEY XXXXX XXXXXX                 0570000  0630329 F    W     06-09-54  00-
   7  DUDLEY XXXXXX XXXXXX                0570000  0629318 M    N     07-26-32  00-
   8  DUDLEY XXXX X (1 0)                 0570000  0621274 F    W     12-20-33  00-
   9  DUDLEY XXXX X X                     05700    0630376 F    W     12-20-35  00-
```

Individual's complete record



```
BOOK-IN NO:  0576849  RACE:  W  SEX:  M  DOB:  03-24-50  LAI NO:  G196586
NAME AT BOOKIN:  XXXXXXX XXX XXXXXXXXX  XX  .      HT: 71  WT:  205  CC: 3
NAME: XXXXXXX XXX XXXXXXXXXX JR          NAME TYPE:  AK  DATE: 01-23-72   RIN: XX
NAME:                                    NAME TYPE:      TIME: 0330
ADDRESS: XXXX ROCHELLE  XXXXXX, TEXAS                   CELL/TANK:

ARRESTING AGENCY: TX0570000 ARRESTING OFFICERS: XXXXX XXXXXX
ARR AGY PRISONER NO: 000196586  BENCH WARRANT:   BWINF:

SSN:               DR LIC NO: 4313842          DR LIC STATE: TX DR LIC TYPE: 0
FBI: 000000000  DPS: 0000000    DPD:             MISC NO:               TYPE:
MISC NO:                  TYPE:          MISC NO:                   TYPE:
BNO: 0576849
STRAIGHT DATE DUE OUT:
LAYING OUT DATE:
EARLIEST DATE OUT:           MIN SEC DATE:       GOOD TIME:            DAYS
RELEASE DATE:          TIME:              REASON:   AUTHORITY:
HOW RELEASED:
DATE IN SINGLE CELL: -------- REASON:                          AUTHORITY:
RESTRICTIONS:
BILLABLE AGENCY   START    END         BILLABLE AGY PRIS ID
1
2
3
```

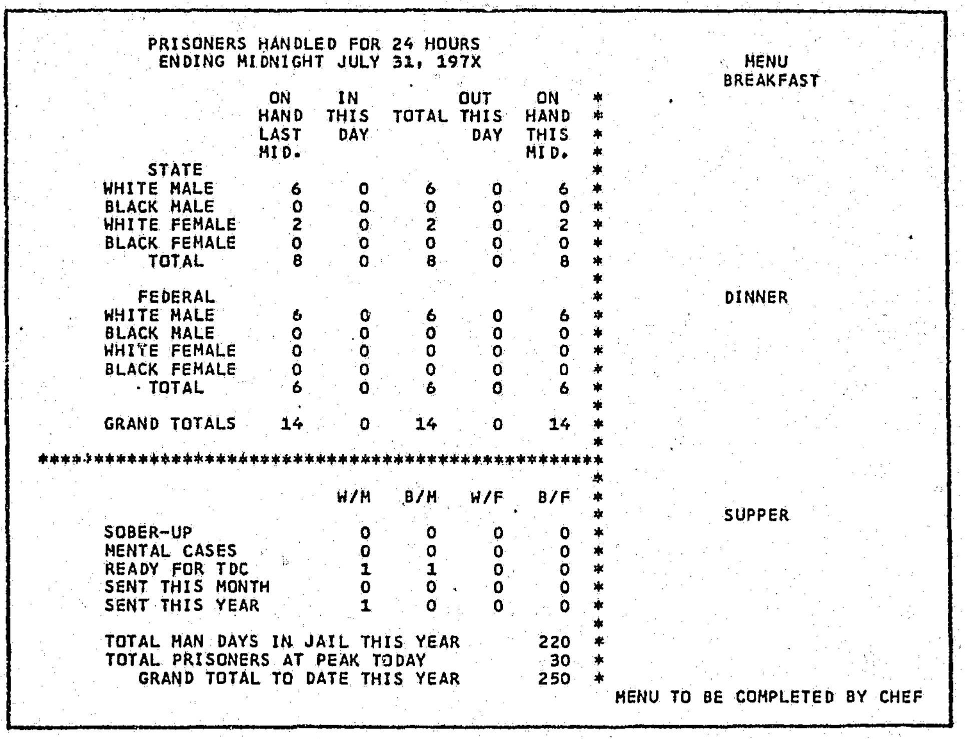
Display in response to last-name inquiry at book-in action while he is being held. When the defendant leaves custody, information is entered into the file to show his destination and other data concerning his release.

The subsystem is based on four files. The first is a hard-copy file containing data legally required to show justification for holding the prisoner and references to the location of documents that contain the signatures of the arresting and receiving officers and the right index fingerprint of the prisoner.

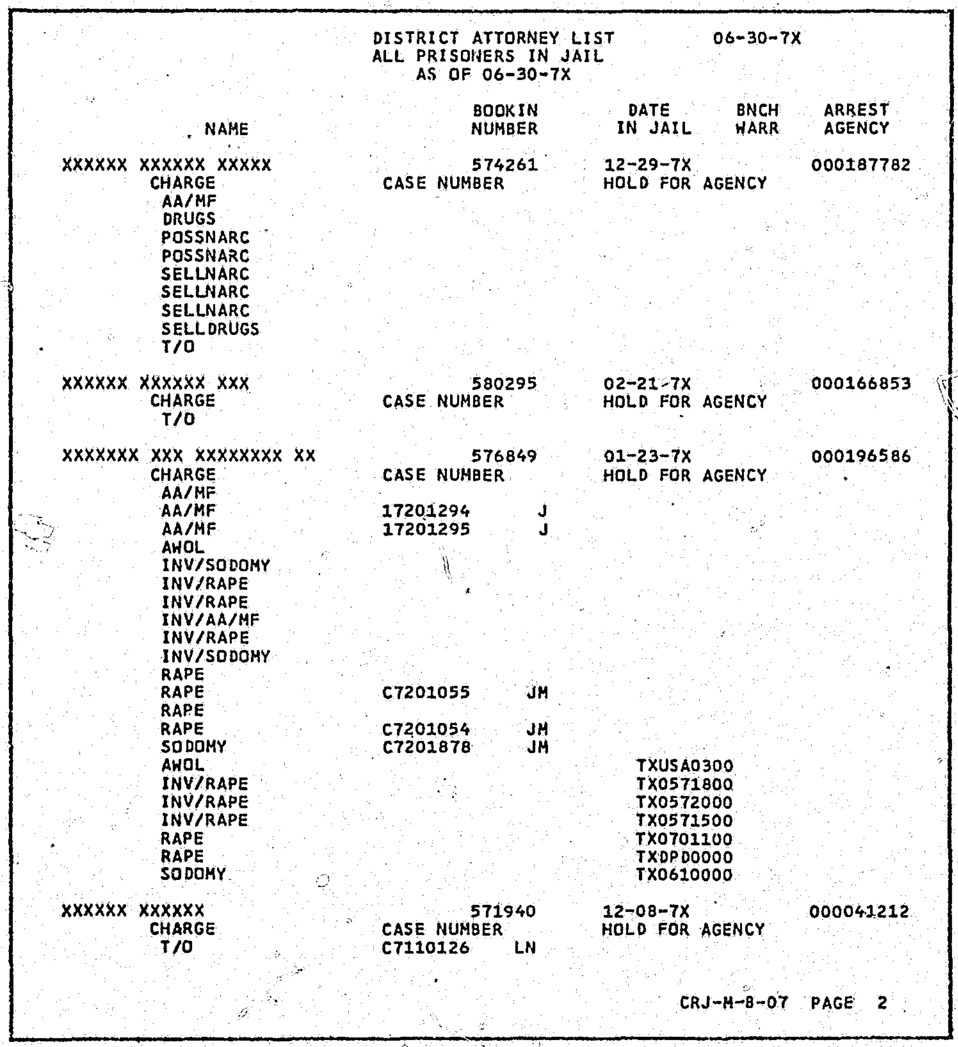
The three remaining files are maintained online by the computer. The fundamental file is organized by book-in number (assigned by the computer at the time of book-in). For each prisoner in jail during the current month, the file contains information including:

> Data legally required to hold and identify the prisoner (name, sex, race, date of birth, identifying numbers, right index fingerprint class).
>
> Data required for custodial purposes (location, behavioral or health problems, next scheduled court appearance).
>
> Data that, either as a legal requirement or as a voluntary service, may be made available to other agencies, such as the district attorney's office, to assist them in the performance of their duties.

The second file is a cross-reference file similar to that described in the section covering criminal identification, and the third contains a record of holding tanks and cells, together with



```
        PRISONERS HANDLED FOR 24 HOURS
         ENDING MIDNIGHT JULY 31, 197X                               MENU
                                                                   BREAKFAST
                     ON     IN          OUT    ON    *
                    HAND   THIS  TOTAL  THIS  HAND   *
                    LAST   DAY          DAY   THIS   *
                    MID.                      MID.   *
        STATE                                        *
    WHITE MALE        6      0     6      0     6    *
    BLACK MALE        0      0     0      0     0    *
    WHITE FEMALE      2      0     2      0     2    *
    BLACK FEMALE      0      0     0      0     0    *
        TOTAL         8      0     8      0     8    *
                                                     *
       FEDERAL                                       *             DINNER
    WHITE MALE        6      0     6      0     6    *
    BLACK MALE        0      0     0      0     0    *
    WHITE FEMALE      0      0     0      0     0    *
    BLACK FEMALE      0      0     0      0     0    *
        TOTAL         6      0     6      0     6    *
                                                     *
    GRAND TOTALS     14      0    14      0    14    *
                                                     *
*****************************************************
                                                     *
                           W/M   B/M   W/F   B/F     *
                                                     *             SUPPER
    SOBER-UP                0     0     0     0      *
    MENTAL CASES            0     0     0     0      *
    READY FOR TDC           1     1     0     0      *
    SENT THIS MONTH         0     0     0     0      *
    SENT THIS YEAR          1     0     0     0      *
                                                     *
    TOTAL MAN DAYS IN JAIL THIS YEAR          220    *
    TOTAL PRISONERS AT PEAK TODAY              30    *
       GRAND TOTAL TO DATE THIS YEAR          250    *
                                                       MENU TO BE COMPLETED BY CHEF
```



```
                              DISTRICT ATTORNEY LIST         06-30-7X
                              ALL PRISONERS IN JAIL
                                 AS OF 06-30-7X

                                          BOOKIN        DATE    BNCH    ARREST
           NAME                           NUMBER      IN JAIL   WARR    AGENCY

XXXXXX XXXXXX XXXXX                       574261      12-29-7X          000187782
        CHARGE                      CASE NUMBER       HOLD FOR AGENCY
         AA/MF
         DRUGS
         POSSNARC
         POSSNARC
         SELLNARC
         SELLNARC
         SELLNARC
         SELLDRUGS
         T/O

XXXXXX XXXXXX XXX                         580295      02-21-7X          000166853
        CHARGE                      CASE NUMBER       HOLD FOR AGENCY
         T/O

XXXXXXX XXX XXXXXXXX XX                   576849      01-23-7X          000196586
        CHARGE                      CASE NUMBER       HOLD FOR AGENCY
         AA/MF
         AA/MF                      17201294      J
         AA/MF                      17201295      J
         AWOL
         INV/SODOMY
         INV/RAPE
         INV/RAPE
         INV/AA/MF
         INV/RAPE
         INV/SODOMY
         RAPE
         RAPE                       C7201055     JM
         RAPE
         RAPE                       C7201054     JM
         SODOMY                     C7201878     JM
         AWOL                                            TXUSA0300
         INV/RAPE                                        TX0571800
         INV/RAPE                                        TX0572000
         INV/RAPE                                        TX0571500
         RAPE                                            TX0701100
         RAPE                                            TXDPD0000
         SODOMY                                          TX0610000

XXXXXX XXXXXX                             571940      12-08-7X          000041212
        CHARGE                      CASE NUMBER       HOLD FOR AGENCY
         T/O                        C7110126     LN

                                                         CRJ-M-8-07   PAGE  2
```

the names of prisoners being held in them. Inquiry capability into the latter file provides a quick search to assist in determining the best available locations for new prisoners.

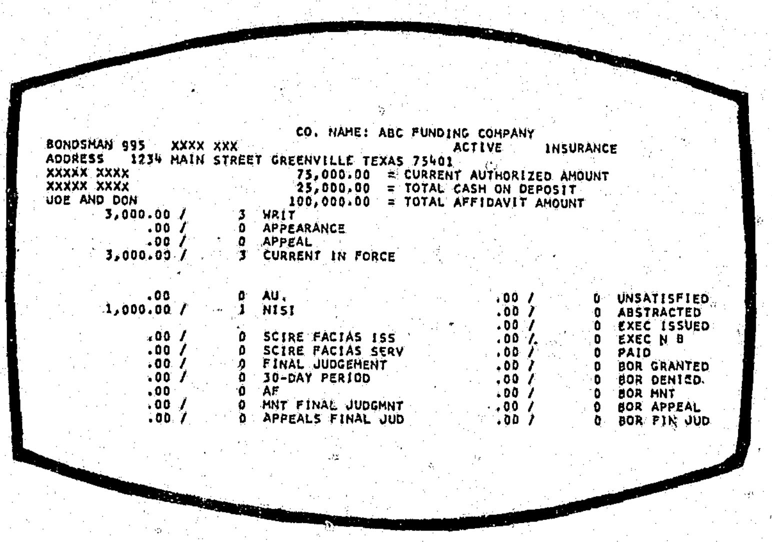
Information available through the system is updated and retrieved via video and hard-copy terminals in the book-in office, identification office, bond desk, radio room, sheriff's office, each criminal district court, district court office, and bond forfeiture office.

Bonds and Bondsmen:

The bonds and bondsmen subsystem deals with appearance, appeal, and writ bonds and their effect on each bondsman's eligibility to issue future bonds. To this end, each bond is filed in a distinct area of the cases-in-progress file, while a separate file of bondsmen is also maintained.

Appearance bonds guarantee a person's presence for a court procedure, appeal bonds enable a person to remain out of jail while a case is being appealed, and a writ bond (such as habeas corpus) guarantees that a person will be at a certain place at a certain time.

The main function of the subsystem is to keep a record of the amount of bond for each individual and a total of all bonds put up by individual bondsmen. If the sheriff, for example, wants to know how much a particular bondsman has written, he can



```
                           CO. NAME: ABC FUNDING COMPANY
BONDSMAN 995   XXXX XXX                             ACTIVE     INSURANCE
ADDRESS   1234 MAIN STREET GREENVILLE TEXAS 75401
XXXXX XXXX                 75,000.00  = CURRENT AUTHORIZED AMOUNT
XXXXX XXXX                 25,000.00  = TOTAL CASH ON DEPOSIT
UOE AND DON               100,000.00  = TOTAL AFFIDAVIT AMOUNT
     3,000.00 /     3  WRIT
          .00 /     0  APPEARANCE
          .00 /     0  APPEAL
     3,000.00 /     3  CURRENT IN FORCE

          .00       0  AU.                        .00 /     0  UNSATISFIED
     1,000.00 /     1  NISI                       .00 /     0  ABSTRACTED
                                                  .00 /     0  EXEC ISSUED
          .00 /     0  SCIRE FACIAS ISS           .00 /     0  EXEC N B
          .00 /     0  SCIRE FACIAS SERV          .00 /     0  PAID
          .00 /     0  FINAL JUDGEMENT            .00 /     0  BOR GRANTED
          .00 /     0  30-DAY PERIOD              .00 /     0  BOR DENIED
          .00       0  AF                         .00 /     0  BOR MNT
          .00 /     0  MNT FINAL JUDGMNT          .00 /     0  BOR APPEAL
          .00 /     0  APPEALS FINAL JUD          .00 /     0  BOR FIN JUD
```

Bondsman eligibility listing

search the computer files to determine if the bondsman has gone over the limit of the total amount he is eligible to write.

The subsystem also follows through on the many administrative steps involved in cases of bond forfeiture, and the sheriff can determine, via a video terminal, how many bonds a particular defendant has forfeited, thus determining whether or not a cosigner should be obtained.

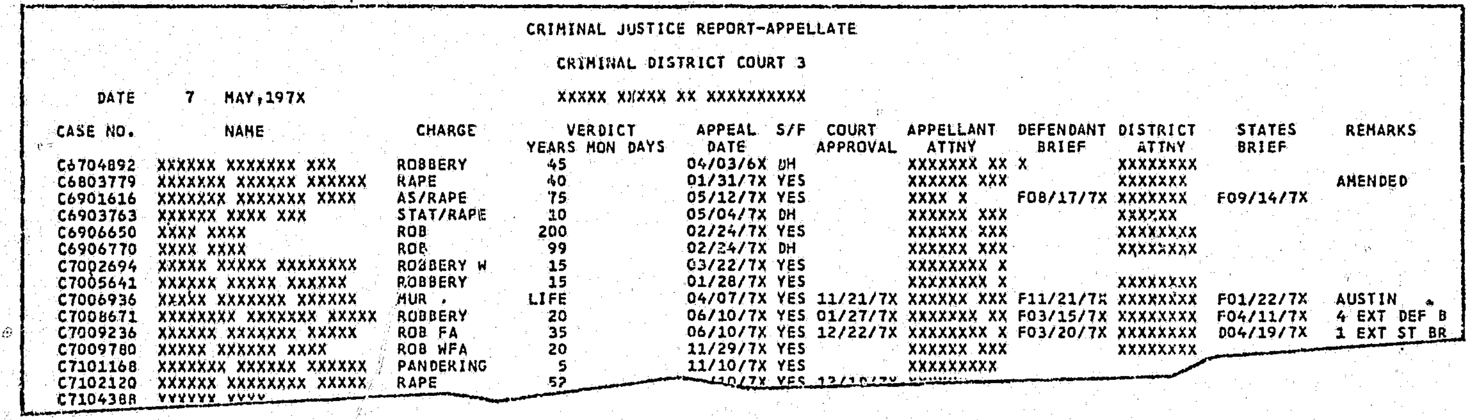
As all bond records are filed with case records, cross references are provided. Data on bonds is also provided in various printed reports.

To update bond records, appropriate postings to the bondsman files are made to show the dollar amounts of bonds attributed to each bondsman. Also maintained is a record of "pseudo-bondsmen" showing persons putting up bond who are not regular bondsmen.

Information in the files is instantly available at any time of the day, any day of the week, through inquiry via a video terminal in the bond section of the sheriff's office.

## Criminal Cases in Progress:

The Judicial Information System provides the district criminal courts, the district attorney, and district court clerks with a number of services based on past histories of cases filed within the district courts and events scheduled for the future. Case-related data is entered and maintained online, and such data



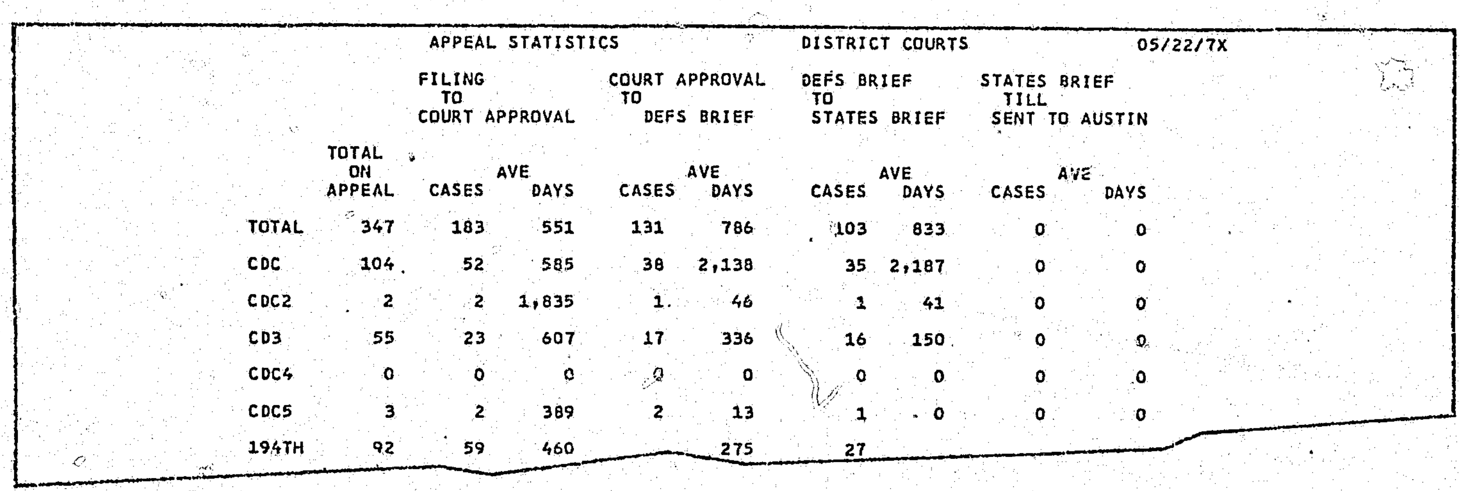
CRIMINAL JUSTICE REPORT-APPELLATE

CRIMINAL DISTRICT COURT 3

DATE 7 MAY,197X

XXXXX XXXXX XX XXXXXXXXXX

| CASE NO. | NAME | CHARGE | VERDICT<br>YEARS MON DAYS | APPEAL<br>DATE | S/F | COURT<br>APPROVAL | APPELLANT<br>ATTNY | DEFENDANT<br>BRIEF | DISTRICT<br>ATTNY | STATES<br>BRIEF | REMARKS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| C6704892 | XXXXXX XXXXXXX XXX | ROBBERY | 45 | 04/03/6X | DH | | XXXXXXX XX | X | XXXXXXXX | | |
| C6803779 | XXXXXXX XXXXXX XXXXXX | RAPE | 40 | 01/31/7X | YES | | XXXXXX XXX | | XXXXXXX | | AMENDED |
| C6901616 | XXXXXXX XXXXXXX XXXX | AS/RAPE | 75 | 05/12/7X | YES | | XXXX X | F08/17/7X | XXXXXXX | F09/14/7X | |
| C6903763 | XXXXXX XXXX XXX | STAT/RAPE | 10 | 05/04/7X | DH | | XXXXXX XXX | | XXXXXX | | |
| C6906650 | XXXX XXXX | ROB | 200 | 02/24/7X | YES | | XXXXXX XXX | | XXXXXXXX | | |
| C6906770 | XXXX XXXX | ROB | 99 | 02/24/7X | DH | | XXXXXX XXX | | XXXXXXXX | | |
| C7002694 | XXXXX XXXXX XXXXXXXX | ROBBERY W | 15 | 03/22/7X | YES | | XXXXXXXX X | | | | |
| C7005641 | XXXXXX XXXXX XXXXXX | ROBBERY | 15 | 01/28/7X | YES | | XXXXXXXX X | | XXXXXXXX | | |
| C7006936 | XXXXX XXXXXXX XXXXXX | MUR . | LIFE | 04/07/7X | YES | 11/21/7X | XXXXXX XXX | F11/21/7X | XXXXXXXX | F01/22/7X | AUSTIN |
| C7008671 | XXXXXXXX XXXXXXX XXXXX | ROBBERY | 20 | 06/10/7X | YES | 01/27/7X | XXXXXXX XX | F03/15/7X | XXXXXXXX | F04/11/7X | 4 EXT DEF B |
| C7009236 | XXXXXX XXXXXXX XXXXX | ROB FA | 35 | 06/10/7X | YES | 12/22/7X | XXXXXXXX X | F03/20/7X | XXXXXXXX | D04/19/7X | 1 EXT ST BR |
| C7009780 | XXXXX XXXXXX XXXX | ROB WFA | 20 | 11/29/7X | YES | | XXXXXX XXX | | XXXXXXXX | | |
| C7101168 | XXXXXXX XXXXXX XXXXXX | PANDERING | 5 | 11/10/7X | YES | | XXXXXXXXX | | | | |
| C7102120 | XXXXXX XXXXXXXX XXXXX | RAPE | 52 | /10/7X | YES | 12/10/7X | | | | | |
| C7104388 | XXXXXX XXXX | | | | | | | | | | |



APPEAL STATISTICS DISTRICT COURTS 05/22/7X

| | TOTAL<br>ON<br>APPEAL | FILING<br>TO<br>COURT APPROVAL<br>CASES | <br><br><br>AVE<br>DAYS | COURT APPROVAL<br>TO<br>DEFS BRIEF<br>CASES | <br><br><br>AVE<br>DAYS | DEFS BRIEF<br>TO<br>STATES BRIEF<br>CASES | <br><br><br>AVE<br>DAYS | STATES BRIEF<br>TILL<br>SENT TO AUSTIN<br>CASES | <br><br><br>AVE<br>DAYS |
|---|---|---|---|---|---|---|---|---|---|
| TOTAL | 347 | 183 | 551 | 131 | 786 | 103 | 833 | 0 | 0 |
| CDC | 104 | 52 | 585 | 38 | 2,138 | 35 | 2,187 | 0 | 0 |
| CDC2 | 2 | 2 | 1,835 | 1 | 46 | 1 | 41 | 0 | 0 |
| CD3 | 55 | 23 | 607 | 17 | 336 | 16 | 150 | 0 | 0 |
| CDC4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| CDC5 | 3 | 2 | 389 | 2 | 13 | 1 | 0 | 0 | 0 |
| 194TH | 92 | 59 | 460 | | 275 | 27 | | | |

is accessible via online terminals from the time of entry until one month after conclusion of the court term during which disposition of the case occurred.

When a person is indicted, he is issued a criminal case number, which is entered into the computer file. This represents the beginning of the computer's role in this subsystem.

After indictment, a master record showing name, book-in number, birth date, race, sex, and a sheriff's identification number is placed on file. A charge record is also entered. When a trial date is set, that information is entered, and after trial, disposition of the case, including sentence, time, and sentencing judge, are recorded. (If the person involved is placed on probation, data concerning that step, including charges, fine, and court costs, is entered).

When a case is appealed, the dates of appeal and the dates on which briefs were filed are entered into the computer files via the terminal keyboard. A disposition code is entered to indicate the outcome of the appeal--confirmation, reversal, dismissal, or a change of judgment.

If an appeal is granted, a motion may be made for a new trial, and the information, including the reason for doing so, is placed in the file. The process is repeated when a new trial is granted.

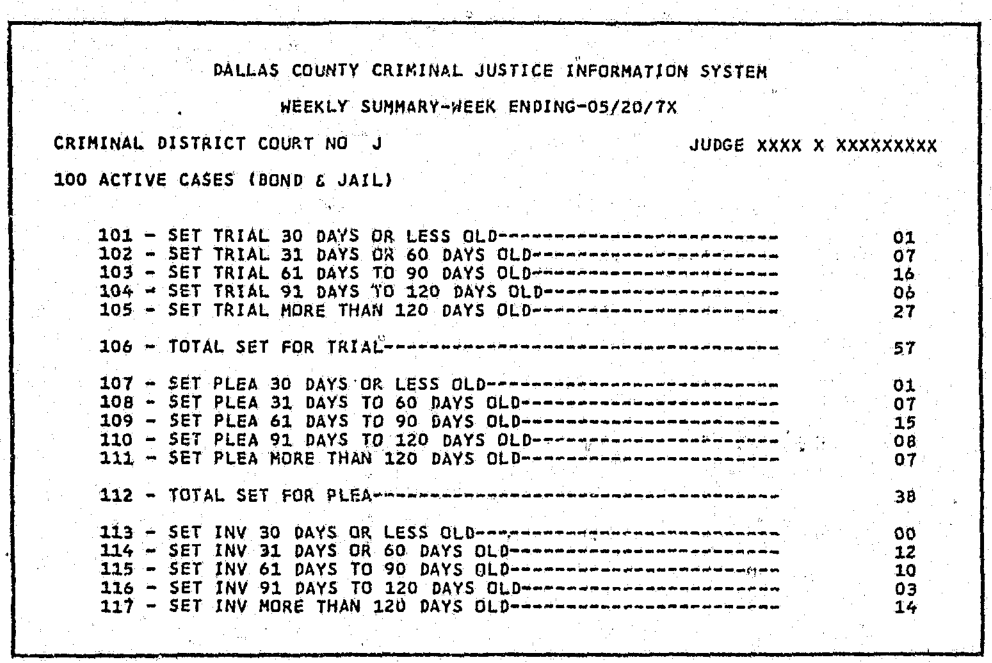
Daily and weekly summary reports are prepared for each court showing counts of cases, motions, writs, monies, etc. Status records entered into the computer file are also available by means of online inquiry through the terminals.

The case history file is fully cross-indexed by defendant name, location, descriptors, prosecutors and defense attorneys, bail bondsmen, status, and related cases. Index files are updated daily.

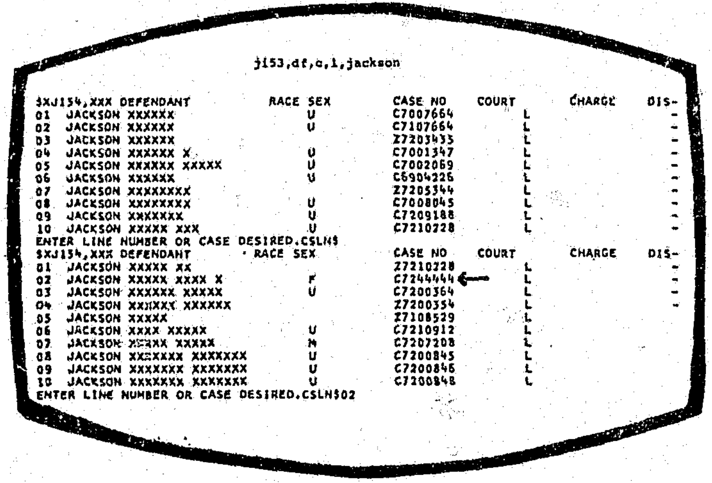
Because of the amount and complexity of data on file, several methods of inquiry have been provided so that court clerks, judges, and prosecutors may retrieve information in the manner most useful to them.

Monthly, term, and annual clerical reports are prepared for the courts, the district attorney, and the district clerks. Other reports include statistical analyses by type of offense and analyses of prosecutor performance for use by the district attorney, and court assignment and disposition lists for the district and county clerk.

A typical report, one of great value to a district judge using the system, shows all cases within his jurisdiction which are being appealed. The report provides the judge with a complete picture of each case, including date of appeal and related information.

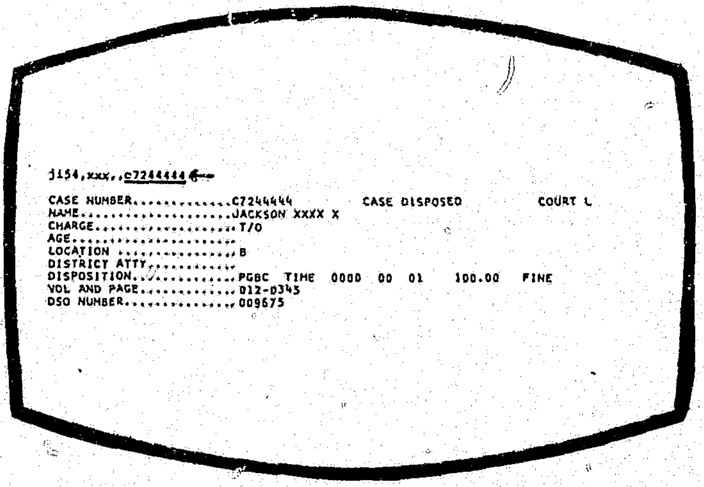


```
              DALLAS COUNTY CRIMINAL JUSTICE INFORMATION SYSTEM

                     WEEKLY SUMMARY-WEEK ENDING-05/20/7X

CRIMINAL DISTRICT COURT NO  J                       JUDGE XXXX X XXXXXXXXX

100 ACTIVE CASES (BOND & JAIL)

    101 - SET TRIAL 30 DAYS OR LESS OLD-----------------------          01
    102 - SET TRIAL 31 DAYS OR 60 DAYS OLD--------------------          07
    103 - SET TRIAL 61 DAYS TO 90 DAYS OLD--------------------          16
    104 - SET TRIAL 91 DAYS TO 120 DAYS OLD-------------------          06
    105 - SET TRIAL MORE THAN 120 DAYS OLD--------------------          27

    106 - TOTAL SET FOR TRIAL---------------------------------          57

    107 - SET PLEA 30 DAYS OR LESS OLD------------------------          01
    108 - SET PLEA 31 DAYS TO 60 DAYS OLD---------------------          07
    109 - SET PLEA 61 DAYS TO 90 DAYS OLD---------------------          15
    110 - SET PLEA 91 DAYS TO 120 DAYS OLD--------------------          08
    111 - SET PLEA MORE THAN 120 DAYS OLD---------------------          07

    112 - TOTAL SET FOR PLEA----------------------------------          38

    113 - SET INV 30 DAYS OR LESS OLD-------------------------          00
    114 - SET INV 31 DAYS OR 60 DAYS OLD----------------------          12
    115 - SET INV 61 DAYS TO 90 DAYS OLD----------------------          10
    116 - SET INV 91 DAYS TO 120 DAYS OLD---------------------          03
    117 - SET INV MORE THAN 120 DAYS OLD----------------------          14
```



```
                     j153,df,c,l,jackson

$XJ154,XXX DEFENDANT          RACE SEX      CASE NO   COURT      CHARGE   DIS-
01   JACKSON XXXXXX                 U       C7007664     L                 -
02   JACKSON XXXXXX                 U       C7107664     L                 -
03   JACKSON XXXXXX                         Z7203435     L                 -
04   JACKSON XXXXXX X               U       C7001347     L                 -
05   JACKSON XXXXXX XXXXX           U       C7002069     L                 -
06   JACKSON XXXXXX                 U       C6904226     L                 -
07   JACKSON XXXXXXXX                       Z7205344     L                 -
08   JACKSON XXXXXXXX               U       C7008045     L                 -
09   JACKSON XXXXXXX                U       C7209188     L                 -
10   JACKSON XXXXX XXX              U       C7210228     L                 -
ENTER LINE NUMBER OR CASE DESIRED.CSLN$
$XJ154,XXX DEFENDANT        · RACE SEX      CASE NO   COURT      CHARGE   DIS-
01   JACKSON XXXXX XX                       Z7210228     L                 -
02   JACKSON XXXXX XXXX X           F       C7244444 ←   L                 -
03   JACKSON XXXXXX XXXXX           U       C7200364     L                 -
04   JACKSON XXXXXX XXXXXX                  Z7200354     L                 -
05   JACKSON XXXXX                          Z7108529     L
06   JACKSON XXXX XXXXX             U       C7210912     L
07   JACKSON XXXXX XXXXX            M       C7207208     L
08   JACKSON XXXXXXX XXXXXXX        U       C7200845     L
09   JACKSON XXXXXXX XXXXXXX        U       C7200846     L
10   JACKSON XXXXXXX XXXXXXX        U       C7200848     L
ENTER LINE NUMBER OR CASE DESIRED.CSLN$02
```

Response to last-name inquiry



```
j154,xxx,,c7244444 ←

CASE NUMBER..............C7244444          CASE DISPOSED           COURT L
NAME.....................JACKSON XXXX X
CHARGE...................T/O
AGE......................
LOCATION ................B
DISTRICT ATTY............
DISPOSITION..............PGBC  TIME  0000  00  01    100.00   FINE
VOL AND PAGE.............012-0345
DSO NUMBER...............009675
```

Response to case-number inquirv

A statistical report is also illustrated. It shows appeal information relating to cases within district court jurisdiction, and it is used by the district attorney's office to determine average times involved to see cases through the various stages of appeal.

Adult Probation:

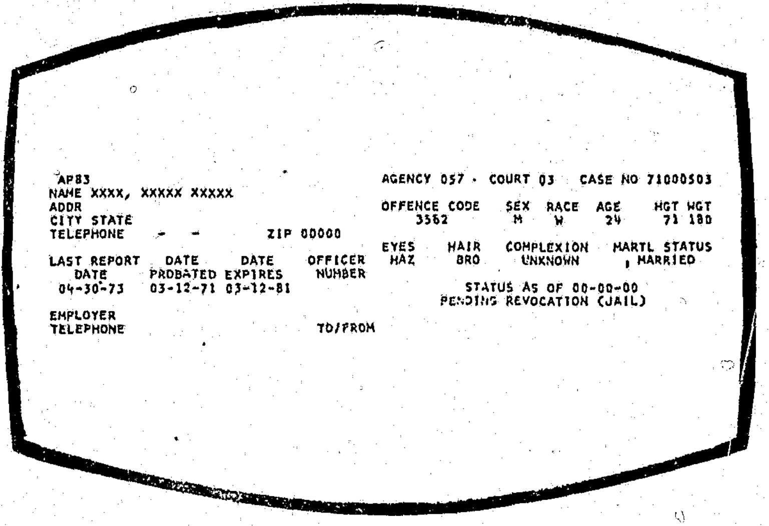
The adult probation subsystem performs two main functions: to provide information of use to the probation officer and the court and to provide accounting information regarding probation fees and restitution accounts.

Files used in this subsystem include personal information, the offense, the time when probation starts and ends, employment data (including salary, employer, and employment address), and the probation charge (usually $10 a month, but a judge may establish another amount).

Eleven terminals located in district court offices, in the probation office, and at cashier stations provide online information in several formats.

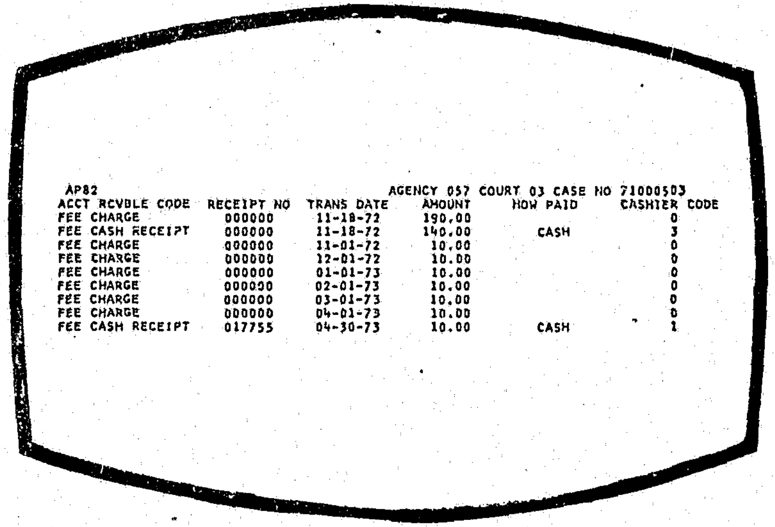
Three of the available video displays, achieved by entering the probation number as an inquiry on the terminal, are illustrated here.

The first shows a profile of the probationer, the second shows his payments and charges (delinquency will be indicated in such a display), and the third provides his account balance.



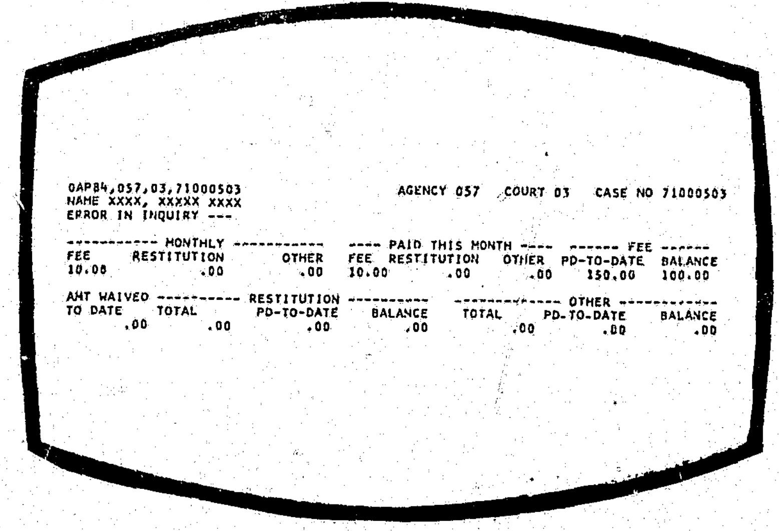
```
 AP83                                             AGENCY 057 . COURT 03   CASE NO 71000503
NAME XXXX, XXXXX XXXXX
ADDR                                              OFFENCE CODE   SEX  RACE  AGE    HGT WGT
CITY STATE                                            3562        M    W    24      71 180
TELEPHONE    -   -          ZIP 00000
                                                  EYES    HAIR   COMPLEXION   MARTL STATUS
LAST REPORT   DATE      DATE     OFFICER          HAZ     BRO     UNKNOWN     , MARRIED
   DATE     PROBATED EXPIRES     NUMBER
 04-30-73   03-12-71 03-12-81                              STATUS AS OF 00-00-00
                                                       PENDING REVOCATION (JAIL)
EMPLOYER
TELEPHONE                             TO/FROM
```

Probationer profile



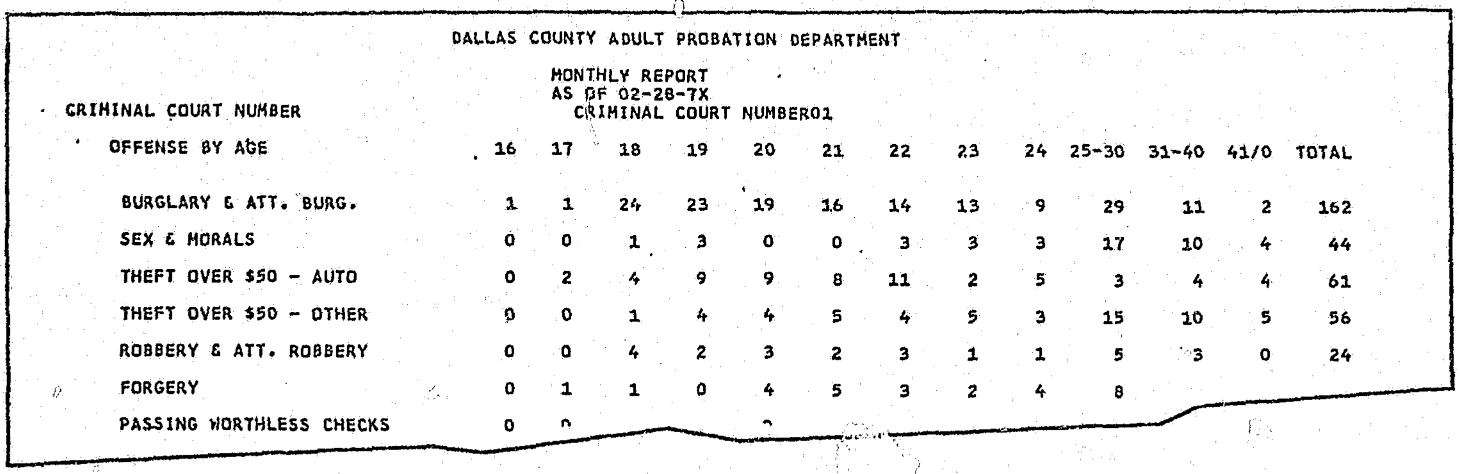
```
 AP82                                          AGENCY 057 COURT 03 CASE NO 71000503
ACCT RCVBLE CODE  RECEIPT NO  TRANS DATE    AMOUNT      HOW PAID      CASHIER CODE
FEE CHARGE          000000     11-18-72     190.00                           0
FEE CASH RECEIPT    000000     11-18-72     140.00        CASH               3
FEE CHARGE          000000     11-01-72      10.00                           0
FEE CHARGE          000000     12-01-72      10.00                           0
FEE CHARGE          000000     01-01-73      10.00                           0
FEE CHARGE          000000     02-01-73      10.00                           0
FEE CHARGE          000000     03-01-73      10.00                           0
FEE CHARGE          000000     04-01-73      10.00                           0
FEE CASH RECEIPT    017755     04-30-73      10.00        CASH               1
```

Probationer payments and charges

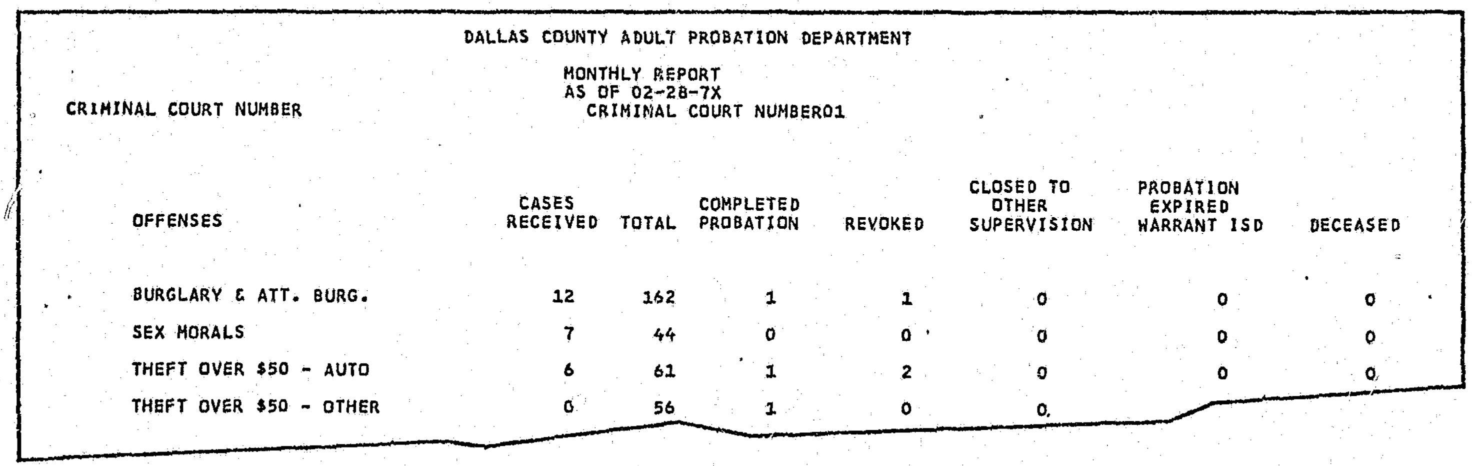


```
0AP84,057,03,71000503                            AGENCY 057   COURT 03   CASE NO 71000503
NAME XXXX, XXXXX XXXX
ERROR IN INQUIRY ---

----------- MONTHLY -----------   ---- PAID THIS MONTH ----  ------ FEE ------
FEE      RESTITUTION         OTHER   FEE  RESTITUTION   OTHER  PD-TO-DATE  BALANCE
10.00             .00          .00   10.00         .00     .00     150.00   100.00

AMT WAIVED ---------- RESTITUTION ----------    -------------- OTHER ------------
TO DATE      TOTAL      PD-TO-DATE     BALANCE     TOTAL    PD-TO-DATE      BALANCE
      .00         .00         .00         .00         .00         .00          .00
```

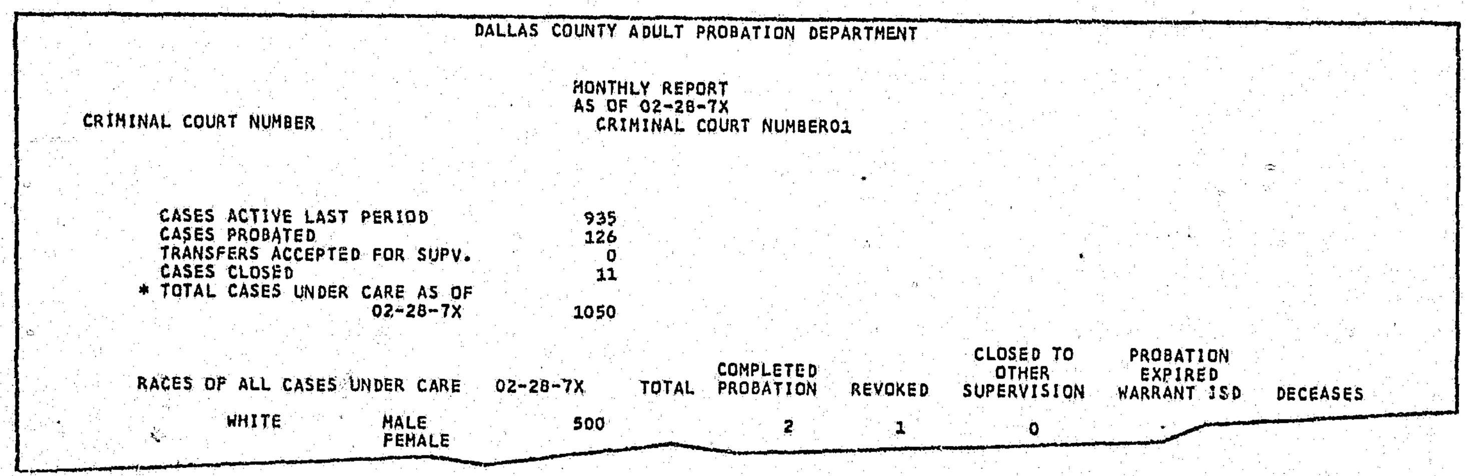
Probationer account balance



```
                              DALLAS COUNTY ADULT PROBATION DEPARTMENT

                                         MONTHLY REPORT
                                         AS OF 02-28-7X
   CRIMINAL COURT NUMBER                   CRIMINAL COURT NUMBER01

      OFFENSE BY AGE                 16   17   18   19   20   21   22   23   24  25-30  31-40  41/0  TOTAL

       BURGLARY & ATT. BURG.          1    1   24   23   19   16   14   13    9    29     11     2    162
       SEX & MORALS                   0    0    1    3    0    0    3    3    3    17     10     4     44
       THEFT OVER $50 - AUTO          0    2    4    9    9    8   11    2    5     3      4     4     61
       THEFT OVER $50 - OTHER         0    0    1    4    4    5    4    5    3    15     10     5     56
       ROBBERY & ATT. ROBBERY         0    0    4    2    3    2    3    1    1     5      3     0     24
       FORGERY                        0    1    1    0    4    5    3    2    4     8
       PASSING WORTHLESS CHECKS       0
```



```
                              DALLAS COUNTY ADULT PROBATION DEPARTMENT

                                         MONTHLY REPORT
                                         AS OF 02-28-7X
  CRIMINAL COURT NUMBER                    CRIMINAL COURT NUMBER01


                                                                       CLOSED TO     PROBATION
                                      CASES            COMPLETED                OTHER         EXPIRED
      OFFENSES                      RECEIVED   TOTAL   PROBATION    REVOKED    SUPERVISION   WARRANT ISD    DECEASED

      BURGLARY & ATT. BURG.            12       162        1           1           0             0             0
      SEX MORALS                        7        44        0           0           0             0             0
      THEFT OVER $50 - AUTO             6        61        1           2           0             0             0
      THEFT OVER $50 - OTHER            0        56        1           0           0
```



```
                              DALLAS COUNTY ADULT PROBATION DEPARTMENT

                                         MONTHLY REPORT
                                         AS OF 02-28-7X
   CRIMINAL COURT NUMBER                   CRIMINAL COURT NUMBER01


        CASES ACTIVE LAST PERIOD             935
        CASES PROBATED                       126
        TRANSFERS ACCEPTED FOR SUPV.           0
        CASES CLOSED                          11
      * TOTAL CASES UNDER CARE AS OF
                         02-28-7X           1050

                                                                       CLOSED TO     PROBATION
                                                       COMPLETED                OTHER         EXPIRED
     RACES OF ALL CASES UNDER CARE   02-28-7X   TOTAL   PROBATION    REVOKED    SUPERVISION   WARRANT ISD    DECEASES
           WHITE            MALE        500                  2           1           0
                            FEMALE
```

## An Example of Information Processing, Storage, and Dissemination

The National Criminal Justice Reference Service, offers a wide range of information services to the nation's law enforcement and criminal justice community. This service provides information on research literature significant to criminal justice, distributes publications, answers inquiries, makes referrals, sends out listings of documents and announcements, and has established a clearing house for information on the energy crisis as it affects the criminal justice system.

The basic information source is a computerized data base of almost 10,000 documents. Material in the data base includes bibliographic information, descriptive abstracts, and is indexed according to established criminal justice terminology. Hard copies of all items in the data base are maintained for reference purposes, and many are available for distribution.

Having begun operations in 1972, nearly 19,000 registered users now avail themselves of this service. Any individual or agency involved, or interested in law enforcement may become a registered user by filling out an interest profile. A comprehensive list on over seventy-five subjects, ranging from alcoholism to rehabilitation is available for determining an interest profile.

This system began international operations in 1973. As the first such Federal system in the field, the National Criminal

Justice Reference Service stands as an example for topic information storage. Without this system large amounts of data would exist in numerous locations, and be obscure to the most diligent researcher.

## Existing Systems and Their Operations

A) Huntington Beach, California's "Command and Control" system, developed by Motorola, was the first computer-aided system in the nation. The nerve center of the system is the computer and CRT Video Display Terminals. The individual officers in the field are equipped with the Motorola MODAT mobile digital communications system, linked to his Motorola MICOR mobile two-way radio or the HT-220 HANDIE-TALKIE two-way portable radio. The Motorola teleprinter furnishes the patrol units with a permanent and instant hard copy of all communications. The Motorola Insta-Call communications recorder provides for immediate rechecking of any complainant's call if there is any doubt as to its content. Located in the police department's communication center is a Microfiche display screen which is capable of calling up more than 75,000 different map negatives. The total system is geared to city-wide usage through Digital 11/15 computers, and master reports are furnished through a Burroughs' computer.

When a complaint is called in, the computerized Command and Control System allows the complaint officer to receive the call, which is simultaneously registered on his and the dispatcher's CRT Video Display Terminals. The display itself includes the time and date (registered automatically), and the complaint officer adds the complainant's name, address of the incident, and nature of the incident. The dispatcher is also equipped with another CRT unit which presents him with the status of every police officer in the field. This status information includes - available, en route, at the scene, on investigation, or at station, and is controlled by the mobile units.

When the dispatcher makes his determination on assignment, he activates the system both verbally and electronically. As he is telling the field officer of the assignment, he activates the mobile teleprinter, which provides a foolproof backup. This hard copy of all communications both reduces time in copying assignments and errors or repeating of messages.

Silent burglar alarms are directly connected to the system. In the event that one is triggered, the computer automatically selects and notifies the patrol unit in that particular location that can respond the fastest. This feature eliminates the time that would be required by the complaint officer and dispatcher, allowing for faster response time in emergency situations.

The Huntington Beach system can also access the California Law Enforcement Teletype Service, and is utilized by both the Fire Department and Harbor Patrol. All agencies agree that the system is providing faster response time in emergency situations, greater accuracy of communication, superior utilization of manpower, and a much more efficient return on the investment in tax dollars.

The time element has been greatly reduced through computer usage, but another feature is the compilation of data, providing management with information for planning and better decision making. The data management system is a facet which is saving many man hours in the compilation of reports such as those which the department sends to the FBI and Uniform Crime Reports. A special 80 character line, programmed for input at the CRT's and accompanying every complaint entry, provides for coded information concerning the disposition of every case. This information is used, along with the original entries, to provide the department with operational management and modus operandi systems. Among the data which is compiled daily within the system for future evaluation and use are original data elements such as daily case numbers, date and time of entries, time of dispatch, time of officer reponse, arrival and clearance, time of disposition, list of officers assigned, address of incident, response district, area or police beat number, responding agency, initial classification, and priority and file retention identification.

B) The New York City Police Department's Communications Division's SPRINT, Special Police Radio Inquiry Network, is a computer assisted dispatch system geared to fast and efficient processing of public complaints. Around the clock, every day of the year, it's 62 emergency operators - including four Spanish-speaking - receive more than 19,000 requests for assistance and inquiries from the public. Part of its critical responsibility is the job of relaying an average of 1,100 reports of fire to the Fire Department, and hundreds of calls for ambulances. In 1973, Communications Division's police radio dispatchers transmitted two-and-one-half million radio runs to police officers on patrol. Transmitting via UHF and VHF radio frequencies, Communications Division (CD) messages link radio motor patrol units, detective cruisers, Emergency Service rescue squads, and aviation units. The present number of broadcasts is a reduction of 15% from pre-SPRINT days. This has been accomplished through screening, i.e. referring non-emergency calls to local precincts and non-police matters to other appropriate city, state, and federal agencies.

The system utilizes two IBM 360 computers and telecommunications hardware to keep the entire system from bogging down under the massive volume of calls for police assistance. CD is arranged into five area radio rooms corresponding to the city's boroughs. Each area has its own battery of dispatchers and emergency operators, called turret operators. Incoming calls are intercepted by an automatic call distributor (ACD). This device identifies the borough the caller is dialing from and automatically channels the call to the appropriate turret operator servicing that area. The ACD polls each operator's position until it locates one which isn't already servicing a call. During peak periods, overflow is directed to additional turret operators or to those concerned with other boroughs that are idle. Each turret operator and dispatcher has the capability of accessing adjoining zones, thereby allowing for a coordinated effort between many zones directed by a single dispatcher.

After receiving a call, the turret operator, by using a combination of coded messages and regularly spelled out words, feeds the caller's name, nature of the complaint, address and incidental details into the computer through his CRT Video Display Terminal. The total incident display presents the turret operator with all the relative information, including the turret operator's identification number, date and time the message was received, and its numerical order among all the calls received during the 24 hour period. After recording all the information the turret operator keys the SPRINT system and the computer analyzes the information, searching for errors. A report bearing a nonexistent address for example will be rejected due to the pre-programming of all valid addresses within the city.

Several means are available to the turret operator to overcome filing misinformation into the computer. First, all messages received are recorded twice. Five master tapes, 40 recording tracks on each, constantly revolve in a secured tape room within the center, auditing every conversation. A second recording device, called a message repeater, is affixed to the turret operator's desk and wired directly into his CRT. This repeater can record a full three hours of conversations, between complainants, radio dispatchers, and patrol units. This feature allows for playback of a complaint in the event that a caller floods the operator with hasty information and hangs up. This repeater obviates the need to disturb the master tape; no interruptions occur and no cumberson cross-filing system is necessary.

The SPRINT computer is also programmed to preclude human error. Built into the system are special alias, place name, and misspelling files. The former category consists of an extensive cross-reference of streets, major traffic arteries, and intersections which have more than one name or designation, or were once known by another name. The place name file lists 13 categories of places such as schools, hospitals, hotels, theaters, and parks. The misspelling file contains thousands of commonly misspelled names of streets, which means that the computer will scan this file before rejecting a location as being nonexistent.

When the computer accepts the total display information, it determines the precinct of occurrence, the appropriate patrol car to service the call, and alternate units available for response. A summary, one-line coded message is then presented on the dispatcher's display screen. Up to ten individual incidents can be viewed at one time, and during peak periods the terminal can be keyed to allow a dispatcher to view up to 99 incidents. The dispatcher assigns priorities according to the nature of the incidents, and then broadcasts them to the computer selected patrol unit. Once assigned, he keys his monitor, which brings up the more in-depth Total Incident Display. From it he can relate to the investigating officers all the details of the complaint as reported, and any additional information the computer was able to analyze pertinent to the original information. Precinct sector maps displayed on a lighted viewing screen permit dispatchers to assist field units in the investigation of complaints. Detailed on them are addresses within each precinct sector, diagrams of buildings' lines, and the location of alleyways and yards not visible to the investigating officer from the street. Once an assignment is given to a patrol unit, the computer sets a prescribed amount of time for its completion. If a disposition is not returned within the allotted time, the computer automatically generated an overdue signal, upon which the dispatcher can act.

The Central Complaint Desk Unit continually receives computer printout sheets listing, by precinct, all reported crimes transmitted by radio dispatchers. Throughout the day, each station house is required to supply the complaint desk with the precinct complaint number identifying the investigating officer's reports. That information is recorded and filed for reference. Statistical reports are generated from the various information entered into the data base, compiled on a daily basis. Some examples of reports are: Hourly job distribution list - weekly report indicating the work load performed by each precinct unit, and the average time each unit requires to service a call; Workload summary - weekly report by day and tour, listing total number of jobs occurring within a sector, the number of jobs each patrol unit processed inside/outside its sector, and also makes a comparison with the previous week's statistics; Monthly Personnel Evaluation Report - measures performance of CD workers, number of hours worked, whether as turret operator or dispatcher, their error percentage, and this report is used for training purposes.

The SPRINT system is connected to a teletype network that can access the Mayor's office, JFK and La Guardia airports, the police commissioner's office, and the Transit police. Programmed into the computer are listings of stolen vehicles, impounded vehicles, stolen merchandise, and warrants for wanted individuals. Future plans include accessing the National Crime Information Center at FBI headquarters. The second IBM 360 computer, the capacity of which is being studied and evaluated, is expected to augment SPRINT with terminals installed in each precinct station. As the system stands, it is increasing the efficiency of processing emergency calls, while decreasing police response time. It is also providing management and field personnel with invaluable information, from which more efficient allocation of police resources can be realized.

C) At the district level, Queens County, one of the five boroughs comprising New York City, is equipped with a Miraquic identification and coding system. This system was designed to decentralize certain criminal records. Based on the discovery that most criminals are recidivists, and tend to restrict their activities to a limited geographic area, this system was inaugurated in March of 1973.

Miraquic (Kodak Miracode II Queens Identification and Coding) utilizes microfilm equipment to record mug shots and arrest information, and a viewing screen system which can access the microfilm files according to a coding system. Two separate banks of records are maintained; and record being the related information concerning a criminal. One file bank contains fingerprints, the other contains photos and arrest records. The information is recorded directly on microfilm, and stored in 16mm cassettes, each of which contain 600 records. Dividing the system into two files reduces search time.

The photo area arrest record file consists of a laminated card, one side contains the prisoner's mug shot - side and front view, while the other side contains the previous arrest information reduced in size. By coding in information the bank can be searched electronically very rapidly for specific descriptions. Twenty-five different categories are used for coding, including precinct of arrest, sex, race, vehicle, organized crime, alias, M.O., build, scars, tattoos, etc. By noting one or more descriptors, a victim can be presented on the viewing screen with all known offenders possessing that or those characteristics. Before this systems inauguration, a victim would have to go to the main headquarters in Manhattan and look through volumns of mug shots, many of which were not even close to the description of the offender.

The fingerprint file contains sets of fingerprints. Each single fingerprint is assigned a three digit number based on the pattern, the count or tracing and the core. With this coding system it is possible to search the files with only one or partial print; a feature not present in previous methods.

The Miraquic system, although it does allow for random search of the respective files, is not computer controlled. Systems that utilize a computer are much more expensive, which is a problem when considering the large number of units that would be required at district levels. This system is also much more reliable, not requiring the maintenance or subject to memory loss in the event of failure.

D) The police in Oakland, California use a high-speed digitalized computer system that borrows heavily from data handling technology developed in recent years for the U.S. armed forces. Key parts of the squad cars' systems are a terminal, a keyboard the size of a portable typewriter, a radio transmitter, and an electronic city map. At police headquarters, they have a small computer, another keyboard, terminal, and a large screen map. To run a check on a license plate, a policeman needs only to key in the letters and numbers of the license plate into the keyboard which is mounted on the transmission hump before the cruiser's front seat. Each letter and numeral is converted to binary code and radioed back to headquarters. The computer passes the request to PIN, the Police Information Network, which is a computer facility serving nine counties in the San Francisco area. In from 6-60 seconds, the information is transmitted back to the video-screen in the patrolman's terminal. Information provided includes the 1974 tag number; the year, make and model of the car registered for that tag; the registered owner's name and address; any warrants outstanding against the owner; and the fact of the car's theft if it was reported stolen. If the car is from some other part of California or out-of-state, the patrolman can check the license with the FBI's NCIC by punching in other buttons on the keyboard.

E) Glendale, California has also developed a computer based management information system for its police. Its computer operates with real-time data by receiving and storing data concerning requests for assistance as an accident occurs. Its system provides route dispatching of cars through the computer. When a citizen calls for assistance, the computer gets the telephone message that is typed in by the officer taking the call, selects the car most appropriate, and transmits the dispatch message on a mobile output device.

Some police cars are equipped with an electronic map fixed to the dashboard. The patrolman simply inserts into the frame the street map of the area he is working and touches his finger to the nearest intersection. The pressure-sensitive back of the map holder determines the coordinates of the position, converts it to binary, and transmits this information back to headquarters. With this device, dispatchers can tell at a glance where the cars are, determine when a car is inappropriately out of service, and also permit tactical maneuvers with a number of cars, such as blocking of escape routes.

F) Tampa, Florida police use computer prepared exception reports to curb crime by selectively deploring its force to city areas where the incidence of crime deviates from the norm. The system works by dividing the city into a network of 200 grids. The size and shape of a grid is determined by natural boundaries, crime frequency, and population density. After analyzing various statistical inputs for robbery, burglary, and other crimes, their computer prints out a map of the city, showing the sections of the city where crime is on the rise. Monthly reports are now printed out, but weekly and daily reports are also available. These same techniques are applied to traffic safety. As a result, the city showed a 6.9% decrease in crime after using exception reports for a year, which is more than any other city its size in the nation.

G) Police in Illinois use microfilming procedures to publish its "wheel book". The wheel book consists of over five million vehicle registrations and is used for registration checks, tracing delinquent parking ticket violations, and in the driver's license administration. Before microfilming, it included 147 books and now it is a 48 ounce packet of 4 x 6 cards known as microfiche. A card is put into a TV-like viewer which is supplied by the state to 800 law enforcement agencies. Then the Computer Output Microfilming, or COM, converts the data into a readable form on microfilm. It can be connected directly to the computer for on-line operations or the magnetic tape units for later use. Paper facsimiles of any document can also be supplied in seconds. It takes less than ten seconds to search the book and new material can be added on at any time. Random searches can also be made when only the date or time of day is known relating to a particular request.

H) A police computer in Indianapolis, Indiana retrieves names from its files on a sound-alike basis when correct spellings are not known or when spelling errors are made.

## Traffic Control

Most American cities will sooner or later computerize the control of street lights. When traffic control was computerized in New York in 1969, the rush hour accident rate was halved, there was a 70% reduction in the number of stops, and there was a 35% reduction in driving time. New York's Traffic Commissioner, Theodore Karagheuzoff, says "Making more traffic move faster is not the principle object of this system. This purpose is to enable traffic to move more efficiently so that our streets can make their maximum contribution to the transportation of people and goods."

Other benefits seen from computerized traffic control include: a less expensive alternative to street widening, reduced air pollution because of more efficient operations, and a reduced accident rate because of fewer stops and less driver irritation, and a historical data base for analysis of future transportation needs, reduced operating costs for motorists, and reduced street maintenance.

In the most sophisticated systems, cars are detected either by overhead ultrasonic devices or inductive loops buried in the pavement. Ultrasonic sensors are often chosen over those buried in the streets because the streets are torn up so often. The transducer portion of the sensor beams an ultrasonic wave at the highway. The solid-state receiver, mounted in a weatherproof cabinet on a pole, develops an output signal only when the reflective time is altered by a passing car. The sensors are checked about 60 times per second. Magnetic loops are also used for the detection of traffic. Frequency shift keyed-tone terminals feed the data from the loop detectors and controllers to the computer. The data received is transmitted to a central control office over telephone lines. Pulses sent by wires to the control center are translated into traffic density, volume, and speed data. Most systems use software packages and rely on historical analysis of traffic. The computer compares the traffic pattern to a pre-stored pattern in memory to see which one it most resembles, and then selects and operates a corresponding control pattern. It overrides the last program sent by the computer. The computer provides all the system logic and timing required.

Los Angeles has a system that figures out new signal patterns as it controls traffic. While one part runs the current pattern, another part uses new data to run series of simulations until it finds a pattern that cuts the predicted "delay time" to a minimum. A signal pattern is based on three variables: "cycle time," or the interval from one green light to the next; "split," which is the ratio of green to red time; and "off-set," the interval between a green light at one intersection and a green light at the next.

Some studies suggest there are really only about twenty really different weekday traffic patterns, although IBM offers a package of 500 signal patterns. One doesn't want to work with too many patterns because a change takes from 8-15 minutes for the period of transition. New York doesn't make a change more than once an hour.

A keyboard input/output console allows the traffic engineer to take control of an individual intersection and make timing adjustments for unforeseen circumstances such as an accident, weather, or holidays. There is also a fire pre-empt button to give the right-of-way to emergency vehicles and also a remote police panel that allows the police to adjust the machine status during nonworking hours.

The system also included a secondary or fall-back operation where it reverts to local equipment in case of failure. Otherwise the system operates 24 hours a day, 7 days a week, and 75% of the time without an operator.

An electronically controlled display map provides real time data as to the state of each signal and indicates the presence or absence of traffic in various areas. There is also automatic reporting systems available that print hard copy reports indicating the status of equipment, and also includes timing, volume, and speed data.

Traffic control systems are costly. In New York, it costs about $2000 per intersection. A federal program called TOPICS, or Traffic Operations to Increase Capacity and Safety, is supported by the Highway Trust Fund. The federal government usually pays 50% for a state-approved TOPICS program. SIGOP stands for Signal Optimization Program and is a cooperative project between the Federal Highway Administration and six selected cities--Kansas City, Cincinnati, Indianapolis, Seattle, Miami, and San Antonio. The cities pick the streets to be computerized and collect data on the traffic. FHA then furnished the SIGOP tape. No funds are provided, but the only cost is staff time because no new equipment is needed.

Los Angeles also developed a computer system with sensors buried in the highways to cover 42 freeway miles. In addition to traffic guidance, it also controls on and off ramp traffic with lights, lights up electronic signs along the freeway to inform motorists of traffic problems ahead, and lights up signs telling motorists to tune in to local radio stations.

## Conclusion

Computers have shown to be an effective tool in the preparation and deliverance of meaningful management data for the leadership of law enforcement agencies at all levels. The data management systems alone may prove to be the most important breakthrough. This facet alone accounts for saving years of man hours in the preparation of reports. Statistics, that before were either nonexistent or late in compilation, are providing leaders with daily information upon which they may base their decisions.

The systems now in operation are freeing more police officers for field duty, at a more efficient level of performance. Through the computers' multiprogramming capability, more calls are being handled faster and with greater accuracy, saving valuable time. This feature places police officers at the scene of an emergency situation faster than ever before, and provides him with assistance in efficiently and effectively handling these situations.

The taping capability of computerized systems allows dispatchers to recheck information, and these tapes also are proving invaluable in the courtroom. The district attorney is able to describe events in detailed chronological order, giving precise times and locations, thanks to the programming of these computer systems.

The telecommunications capability, and real time operating of these computerized systems is another invaluable aspect. Other departments, such as fire departments, and teletype services, may be linked to the systems, allowing for superior efficiency in the handling of emergency situations. Coordinated efforts may be carried out easily and smoothly, thanks to dispatchers possessing terminals that allow for multi-call and inter-zone handling.

The efficient and effective utilization of computer systems presently in operation points the way for others to follow. The State of Texas for example, is planning a study to investigate the possibilities of computerizing some of the state's city police departments. With computer equipment becoming more economical and compact, it seems inevitable that one day the entire nation will be linked together, one system accessing another, in the fight against crime, and in the effort to better handle emergency situations.

# BIBLIOGRAPHY

1. A Command and Control System; Law & Order, Vol. 22, no. 5, May 1974.

2. A Comprehensive Reference Service Few People Know About: Law & Order, Vol. 22, no. 10, October 1974.

3. Bauer, Chief E.O., Morel, Mayor Emery B., "Turn Police Files Into Information Centers," American City, Vol. 86 (May 1971), p. 14-16.

4. "Computer Aids Police Management," American City, Vol. 87 (February 1972).

5. Computers and Professional Criminals in Great Britain; Computers and People, Vol. 23, no. 7, July 1974.

6. "Computers for Cops," Newsweek, Vol. 79 (June 5, 1971).

7. "Computerized Police Assignments," American City, Vol. 86 (March 1971).

8. Deweese, J. Taylor, "Giving the Computer a Conscience," Harper's Magazine, Vol. 247 (November 1973).

9. "Electronic Traffic Cops Take on Bigger Jobs," Business Week, No. 2184 (July 10, 1971).

10. Miraquic; Police News of New York, page 29, October 1974.

11. New York City Police Department Communication Division; NYPD Printing Section.

12. Solomon, Stephen, "Now Computers Guide You Through Traffic Snarls," Popular Science, Vol. 198 (January 1971).

13. Sprint; Police Department, City of New York, PIB 72.

14. Webb, Lee, "Computerized Police Systems in the US?," Current, Vol. 132, (March 1971).

15. Wilkins, Roger, "The Threat of Law Enforcement Technology," Current, Vol. 139 (October 1971).

# CHAPTER VII

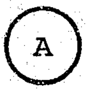
## FLOWCHARTING

The successful solution of a problem, whether manually or on an electronic computer requires completion of three main "solution" steps. First, the problem and desired results must be completely understood; next, the solution to the problem must be logically designed; finally the necessary tasks to solve the problem are undertaken. The first two steps of a solution are especially important. They may be considered independent from the third and completion may be demonstrated by a flowchart.

A flowchart is a graphical representation of the step-by-step solution of a problem and aids the problem solver by clearly defining what task should be accomplished and at what time.

Communication of ideas and techniques are aided greatly by flowcharts. This is particularly true if one is trying to explain a problem's solution to another person not familiar with terminology or procedures. For example, an analyst may have designed a solution to a particular problem and wants a computer programmer to place this solution on an electronic computer. A precisely defined flowchart demonstrating this solution is almost a necessity for the successful translation of the analyst's ideas into a computer program.

Well written flowcharts are in most cases easily understood, even by those unfamiliar with flowcharting techniques. For example, by knowing the use of the connector,

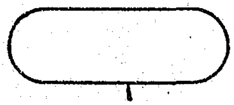


which simply connects parts of a flowchart, one can understand the solution of the problem illustrated in Figure 7.1. By learning how systematically to solve a problem on a computer, an individual might adopt this approach in everyday life.

## Flowcharting Symbols

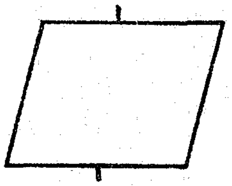
A flowchart is designed to aid someone in designing and understanding the solution of a problem. For this reason certain functions accomplished in the problem's solution are represented by characteristic flowcharting symbols. Thus, at a glance, we can determine what type of operation is to be performed, without having to actually read the instructions for the operation.

In order to immediately find the beginning and end of a flowchart the following symbol is used.



A single work such as START, BEGIN, STOP, OR END is sufficient to completely define this "terminal" operation.

The "input/output" symbol implies that information or data is to be obtained from an outside source (input) or that information is to be given to an outside source (output). With this type of input/output symbol, one should be certain that the comment inside the symbol specifies whether the operation is input or output and if appropriate, what hardware device is being used.



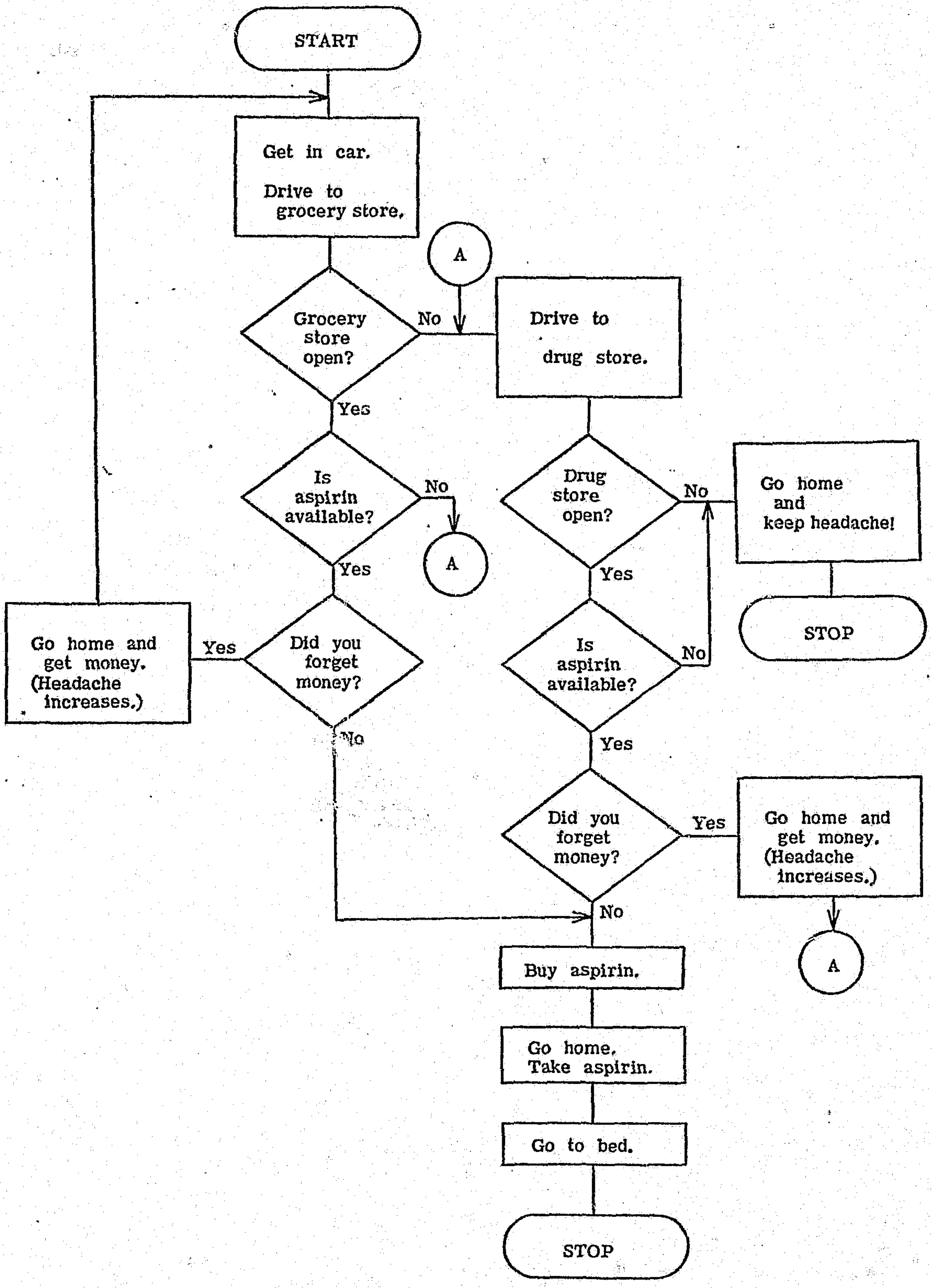
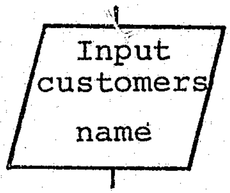
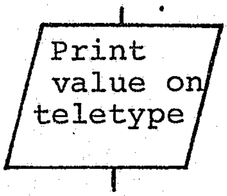


Figure 7.1 Example of Flowcharting Technique

For example we might use

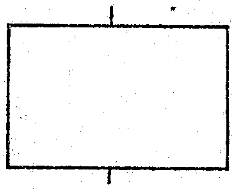


or

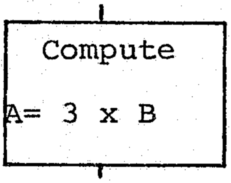


There are other specific symbols one may use for input/output depending on the input or output medium. However, the symbol above can always be used as long as adequate comments are given within the symbol.

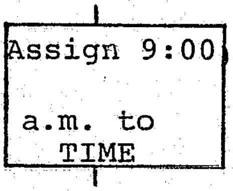
The symbol used to indicate an operation, process or definition of a variable is



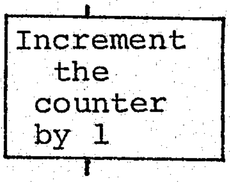
For example, we might say



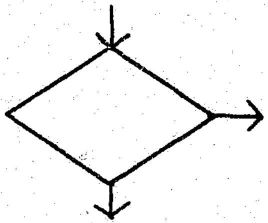
or



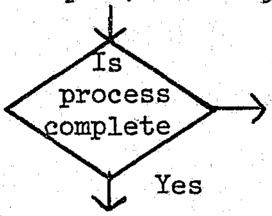
or

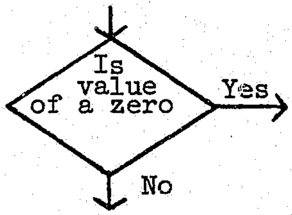


Whenever a decision is to be made in the flowchart, the following symbol is used.

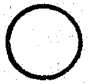


Notice that, unlike the input/output and processing symbols which have one line in and one line out, the decision symbol has two ways to exit from the symbol. This is of course necessary, since a decision is made. Since decisions will be accomplished by answering a question, the possible answers must be noted outside the symbol. For example, we might say





With the four symbols just discussed, the only remaining symbol necessary for flowcharting is the connector symbol



which has been previously introduced.

Several firms produce templates which aid rapid sketching of a flowchart. A list of symbols in Figure 7.2 provides a summary of the standard shapes and a brief description of the use of each.

For the final flowchart to be as useful as possible, it should follow certain convention, as well as use the standard symbols.

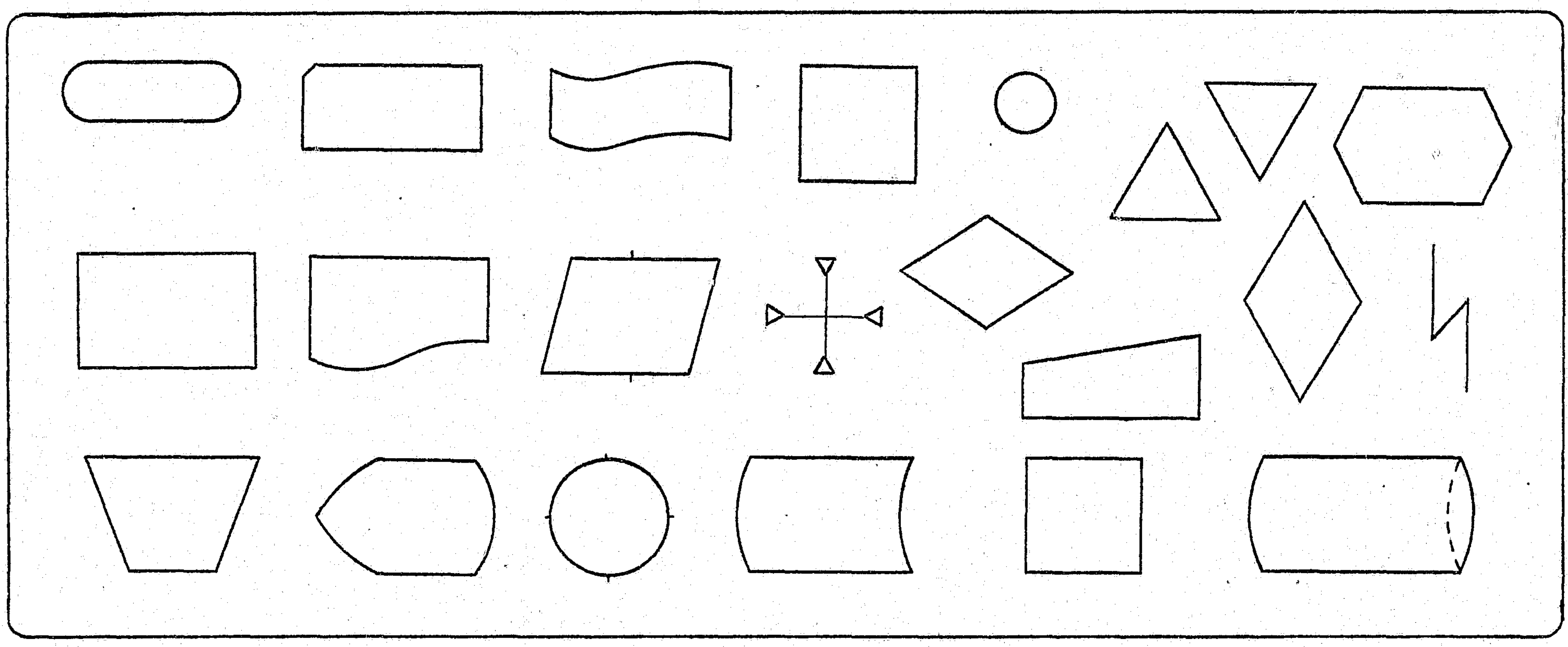
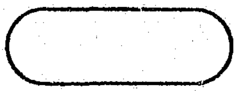
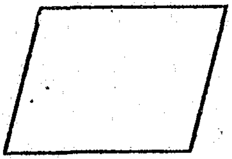


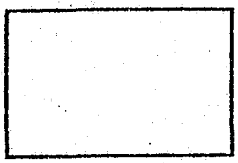
Figure 7.2. Flowcharting template and meaning of symbols.



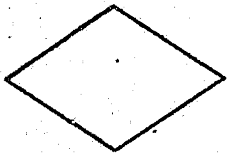
A terminal point; the first or last item in a chart or in a subroutine.



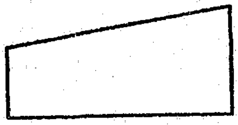
Input/output; by previously determined means, such as keyboard, tape, line printer, etc. Additional symbols are used (see below) to specify a particular medium.



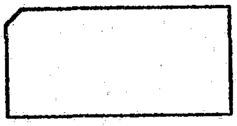
Predefined process or comment; indicates an operation or definition of variable, or a programmer's relevant comment, usually in dotted structure.



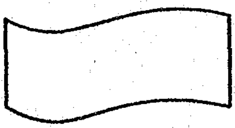
Decision; allows insertion of a decision-making apparatus, as in interval selection, counter comparison or update, loop exit, etc.



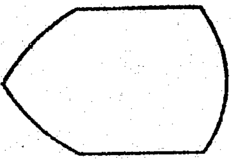
Manual input; usually by keyboard, a supplement to above "input/output."



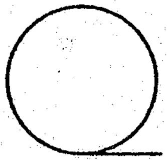
Punched card



Punched tape



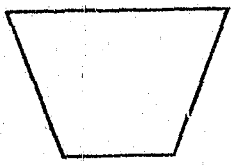
CRT display



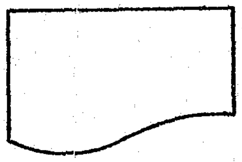
Magnetic tape

Additional symbols for specifying a particular medium of input or output.

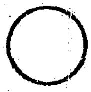
Fig. 7.2 Continued



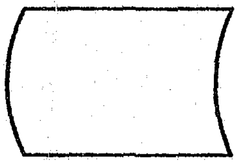
Manual operation; any operation performed externally to an existing machine set-up, done by the operator or other personnel.



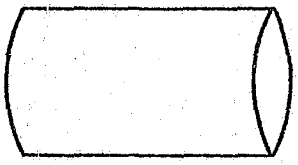
Document; sometimes used to designate a "hard-copy" output; any printed item used for input or output.



On-page connector; used to allow flow lines to continue where otherwise they would cross; must be coded, such as "A1," and should be placed so as to flow down or to the right.



On-line storage; any medium used as intermediate storage.



Magnetic disc or drum; used for a specifically assigned storage.

Fig. 7.2 Continued

Flow lines should be either down the page or to the right. Where this is not practical, use arrowheads to indicate the direction of flow or use the on-page connector. Lines of flow should not cross on the page; this is yet another instance where the on-page connector is useful.

## Flowcharting Examples

As demonstrated by the flowchart at the beginning of this chapter, problems solved using flowcharts do not have to be implemented on a computer. Most that are, however, have similar operations of data input, data processing and data output. Since most programs are written to process several sets of input data, loops are generally set up to input the next set of data if the processing is not complete. Figure 7.3 illustrates a typical flowcharting example.

Flowcharts may be written in a variety of ways, using mathematical equations, English-language descriptions or abbreviated notation, to describe the operation being performed.

### Summing

Two important techniques are quite often found in flowcharting, summing and counting. Figure 7.4 illustrates the summation process. One should keep in mind what is actually occurring when a value is added to another. The computer equivalent of

$$SUM = SUM + A$$

is the following: load the contents of the variable SUM into a register, add the contents of the variable A to that register and finally, store the register's contents into SUM (remember

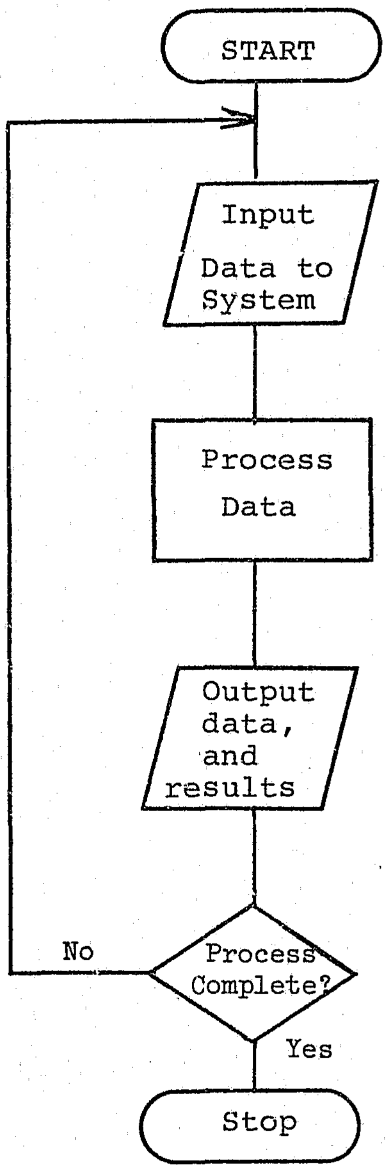


Figure 7.3. A Typical Flowchart

that each variable has a storage location in memory set aside for it). When performing a summation then, the variable containing the sum must first be initialized to zero. The addition process mathematically is then the following:

$$SUM = (\ldots((( \underbrace{(SUM + A_1)}_{\text{SUM after the first addition}} + A_2) + A_3) + A_4) + \ldots)$$

where the $A_i$ refers to the i-th value in the sum and the variable SUM on the right is initialized at zero. The notation SUM ← ( ) is sometines helpful to denote the "replacing" of the contents of a variable with the quantity on the right-hand side.

The "programming" equation

$$SUM = SUM + A$$

is certainly not a mathematical equation but refers to replacing the old contents of the variable SUM with SUM + A. One might better comprehend the operation using the equivalent notation

$$SUM \leftarrow SUM + A.$$

Counting

Figure 7.5 shows the use of a counter in a flowchart. Quite often, one needs to know how many tiems a variable has been read in or how many times a loop has been accomplished. Counting is similar to summing, in that a variable, say I, after being initialized, is incremented by a set amount, say 1. Notice that Figure 7.5 allows for the input and addition of 10 values of a variable A.

Figures 7.6 and 7.7 are two other versions of Figure 7.5, both in error. If a program were written according to Figure 7.6, the loop would be an "endless" one since each time the decision symbol is reached, I is equal to 1. Figure 7.7 would not produce

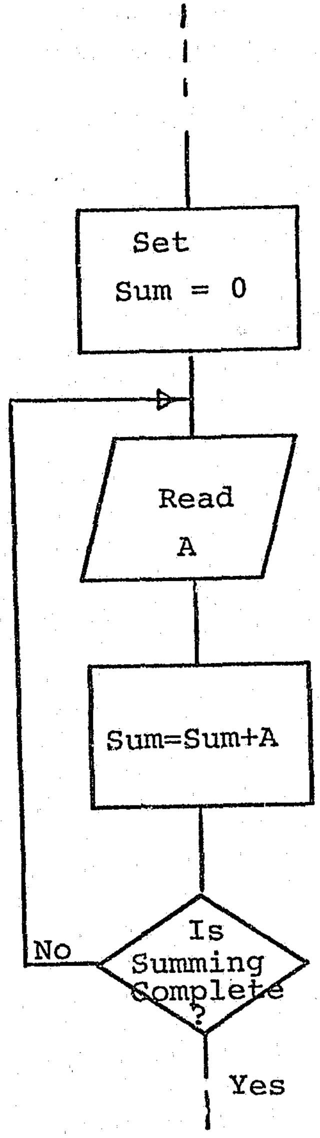


Figure 7.4. Example of Summing

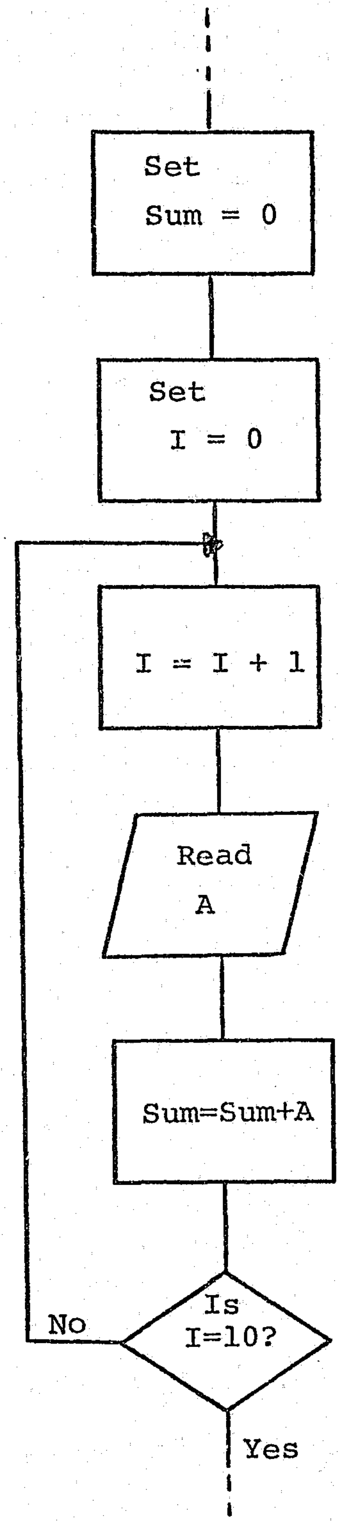


Figure 7.5. Example of Counting

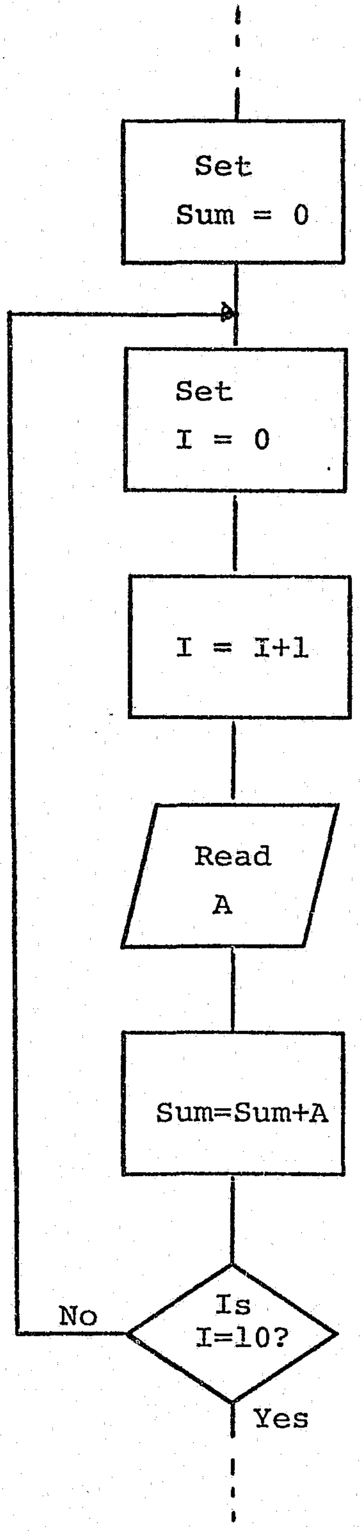


Figure 7.6. Figure 7.5 redrawn with error

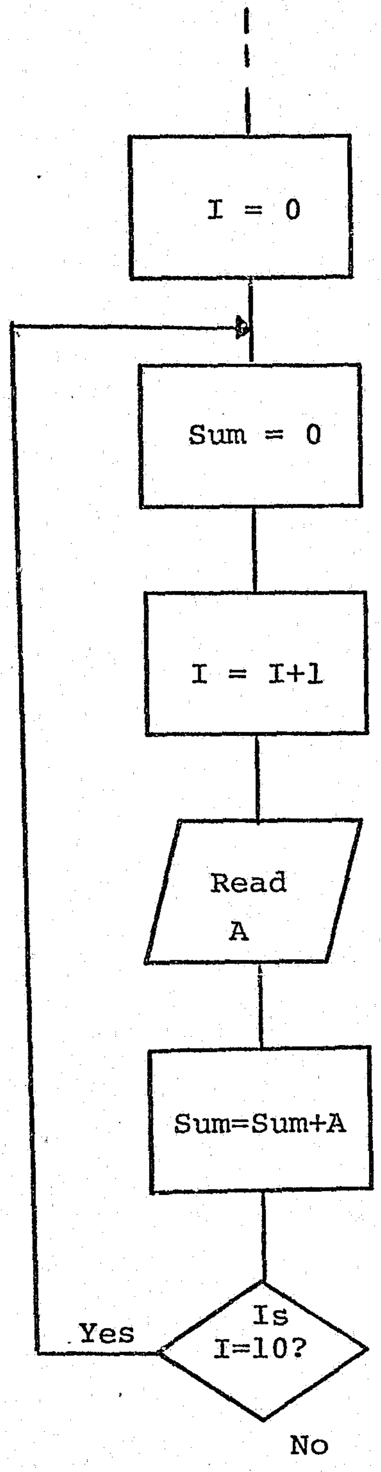
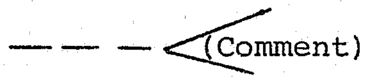


Figure 7.,7. Figure 7 :5 redrawn with error

an endless loop but would instead, give an incorrect result for the sum. Since SUM is reinitialized each time the loop is started, the value stored in SUM upon completion of the tenth pass through the loop would be the tenth value of A.

## Comments

A flowchart should be written in a fashion which makes the problem solution it represents as meaningful and easily understood as possible. Whenever a step in the flowchart requires an operation that might need explanation or when, for emphasis, an additional statement on an operation is desired, a comment may easily be supplied by use of the symbol



Figures 7.8 and 7.9 give flowcharts for the computation of the arithmetic mean of a set of 100 numbers, where Figure 7.9 has comments supplied to the flowchart shown in Figure 7.9. These figures also illustrate the three important techniques of looping, summing and counting.

## PROBLEMS

1. Prepare a flowchart which will compute and output the sum of the first ten integers.

2. Prepare a flowchart which will calculate the sales tax for an item and give its total cost (consider sales tax to be 5¢ on the dollar).

3. Write a flowchart to find how much tip would be left, given the price of the meal and assuming the tip should be 15% of the price of the meal.

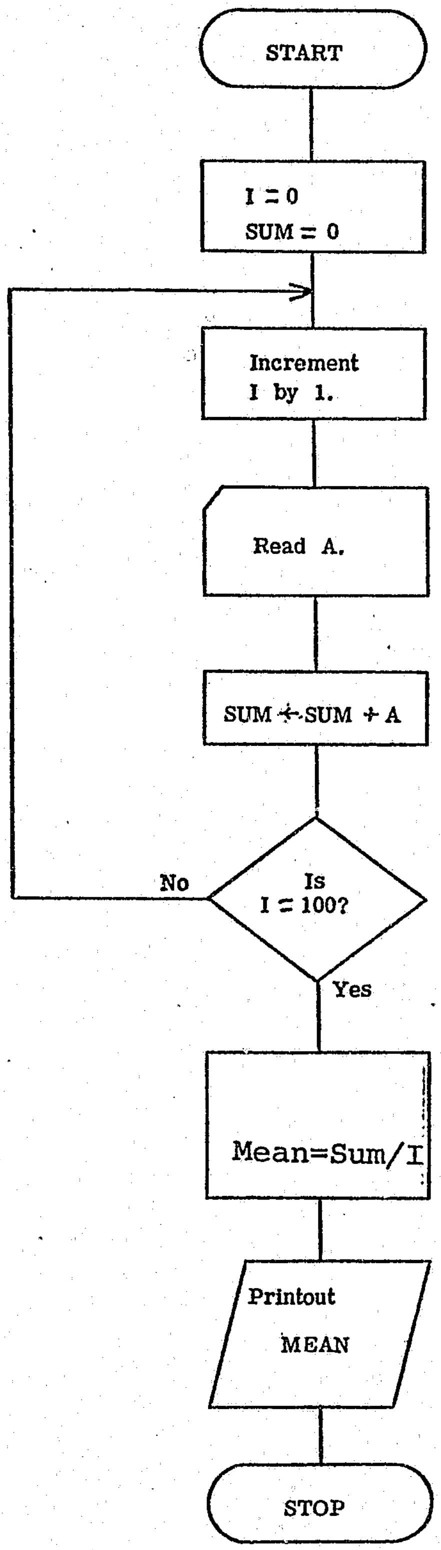
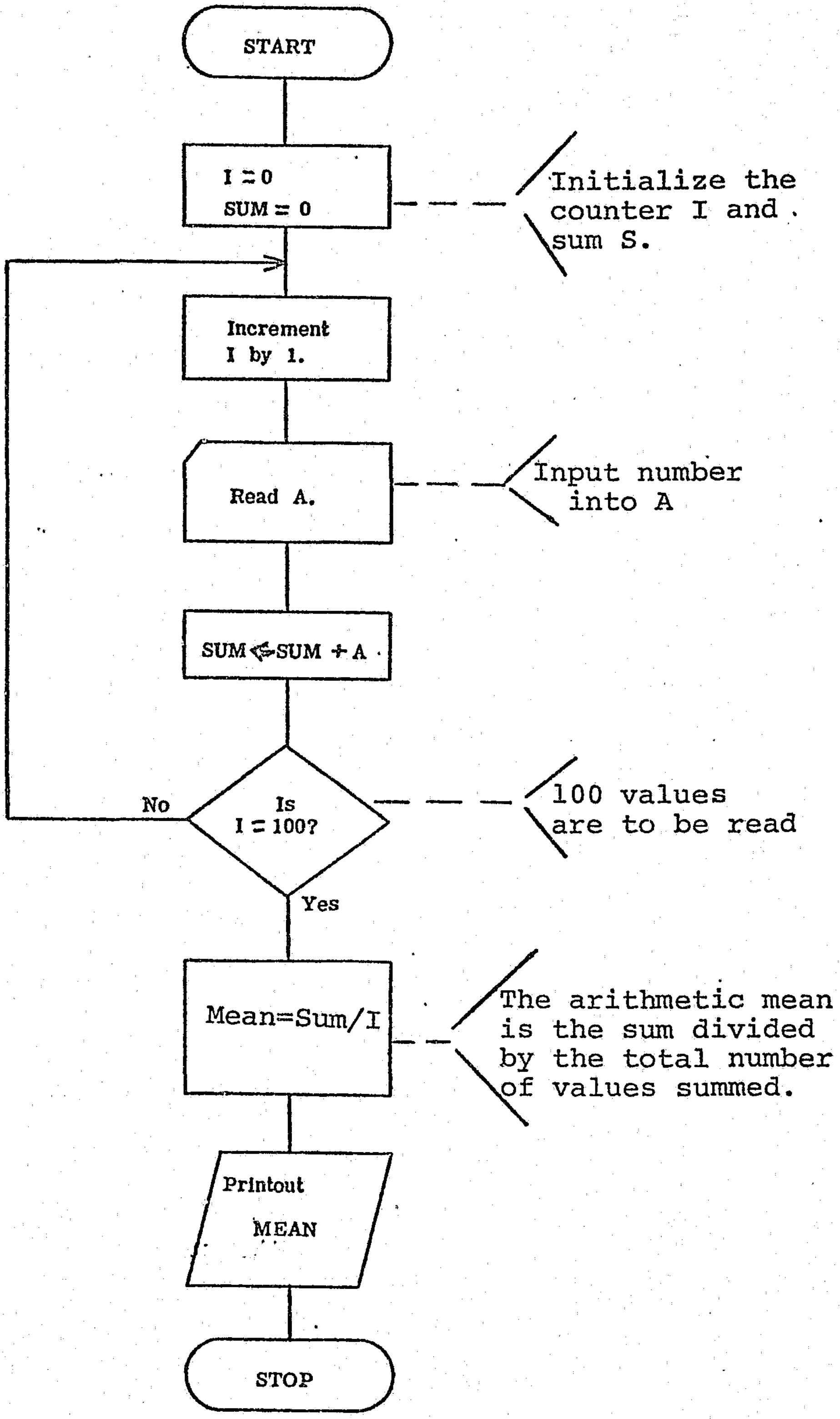


Figure 7..8 Flowchart to Find the Mean of a Set of Data



Initialize the counter I and sum S.

Input number into A

100 values are to be read

The arithmetic mean is the sum divided by the total number of values summed.

Figure 7.9 Flowchart in Figure 7.8 redrawn with comments.

4. Assume that you are analyzing data on burglaries and that data is available on file for each case as shown in Table 1. Figure 7.10 shows a flowchart of finding the total number and compiling a list of all burglaries in Sector 2 occurring between 9:00 p.m. and 11:00 p.m.

Solve problems 1-5 using flowcharts, assuming data is available as shown in Table 1.

(1) List all burglaries that occurred in the city between January 1 and February 15.

(2) List all single family burglaries from Section 4 between April 1 and April 10.

(3) Find the total number of burglaries in Section 1.

(4) Find the average number of burglaries that occurred during January in Sector 4.

(5) Find the number of multi-family burglaries in each sector for the month of February.

Table 1

| Data Available | Description |
|---|---|
| Sector | Sector of city between 1 and 8. |
| Address | Street address of burglary |
| Type of Residence | Single family or multi-family |
| Date | Day, month and year of burglary |
| Time | Hour and minute of burglary |

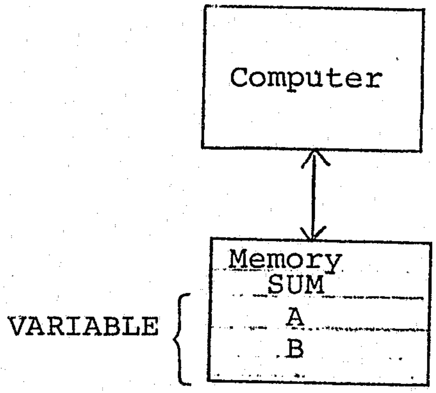
## INTERPRETING A FLOWCHART

In addition to being able to write a flowchart one should (in some job situations perhaps even more importantly) be able to understand someone else's flowchart. Flowcharts are valuable teaching aids and communication devices. Figure 7.11 is an example of a flowchart which might be used in demonstrating the necessary steps of a police officer's accident report.

Figure 7.12 is another flowcharting example. Follow the flow of the problem solution and determine the output that would be generated at the output steps.

## SUBSCRIPTS AND ORDERING

The variables such as SUM, A, etc., used in previous discussions occupy one storage position in the memory of the computer system. For example, we might envision this storage as follows:



Thus each variable is stored in one memory slot.

Many computer applications require the usage of large sets of values for a single variable. For these cases one may use subscripts on the variable, such as $A_1$, $A_2$, $A_3$. Thus rather than using A, B, C, D, E for 5 values we might use $A_1$, $A_2$, $A_3$, $A_4$ and $A_5$. (For simplicity, we will use the notation A(1) instead

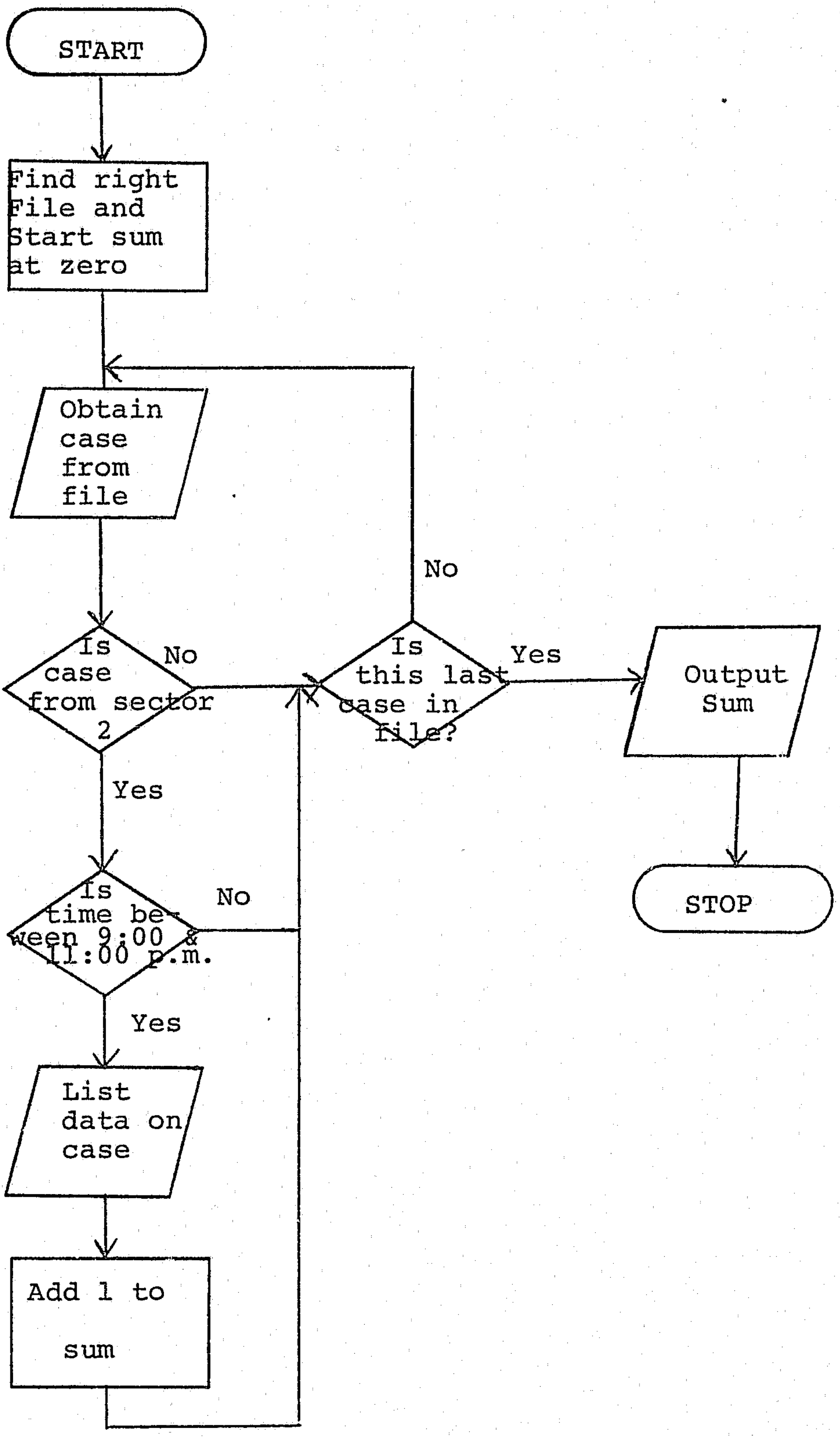


Figure 7.10 Example for problem (4).

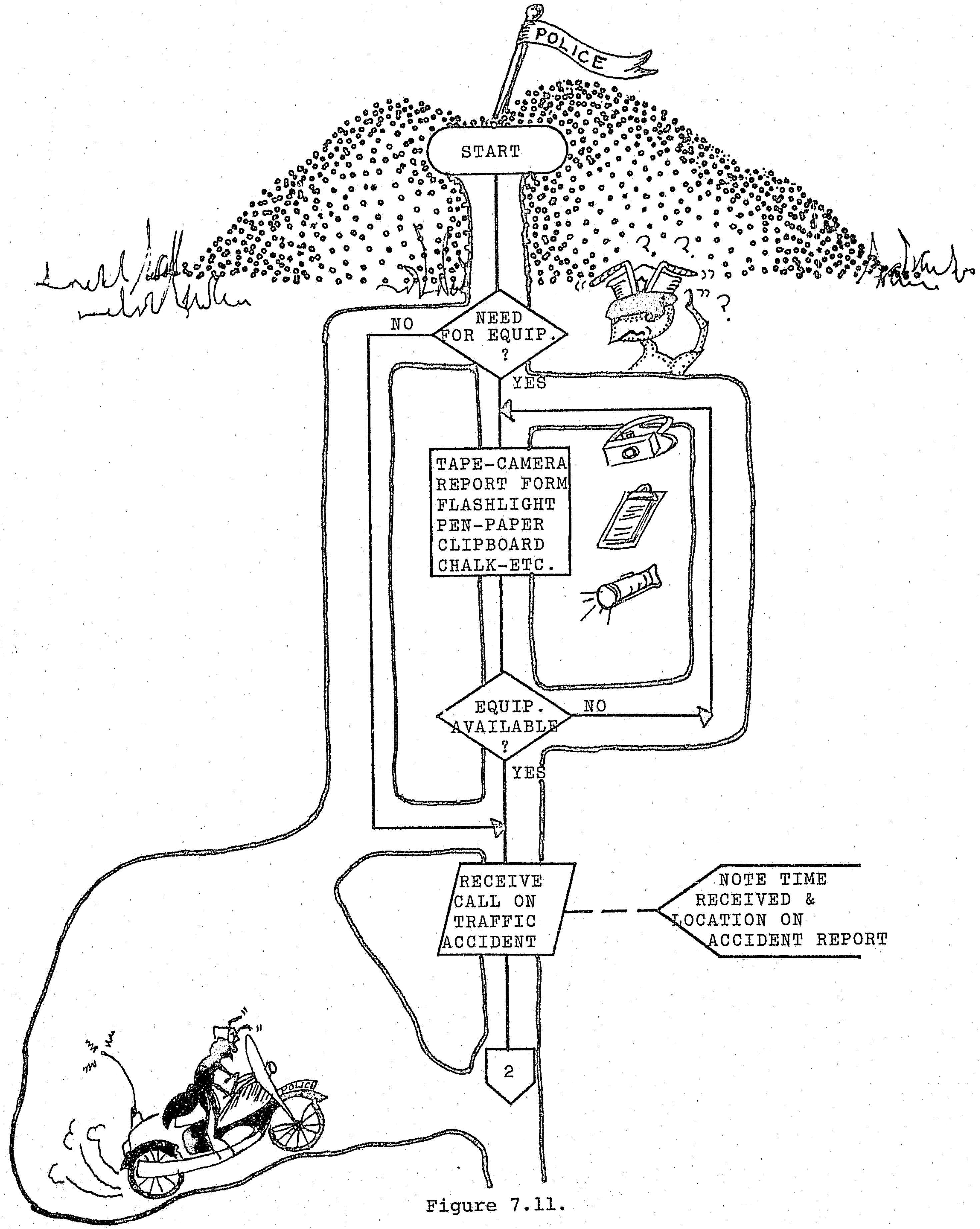
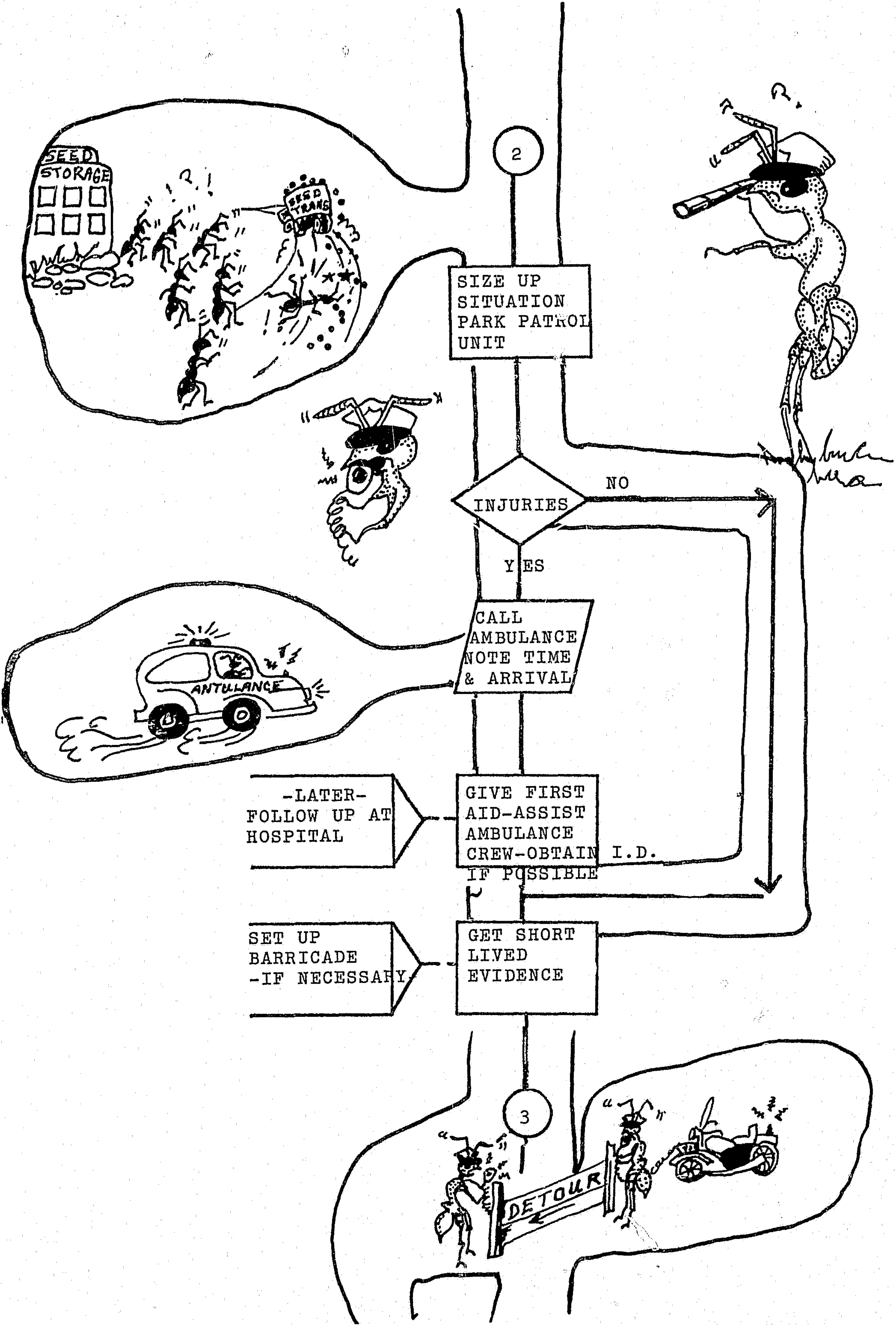
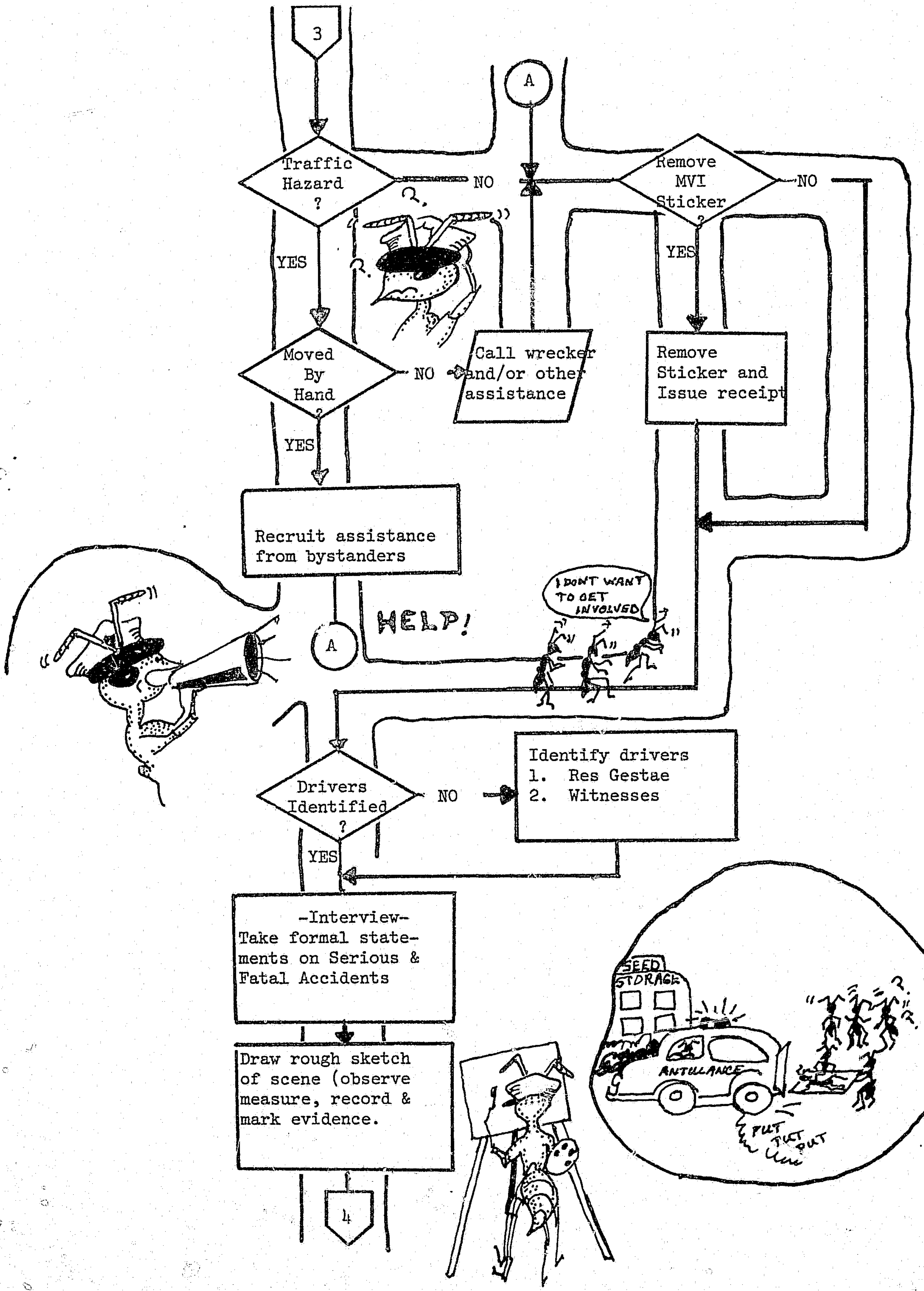
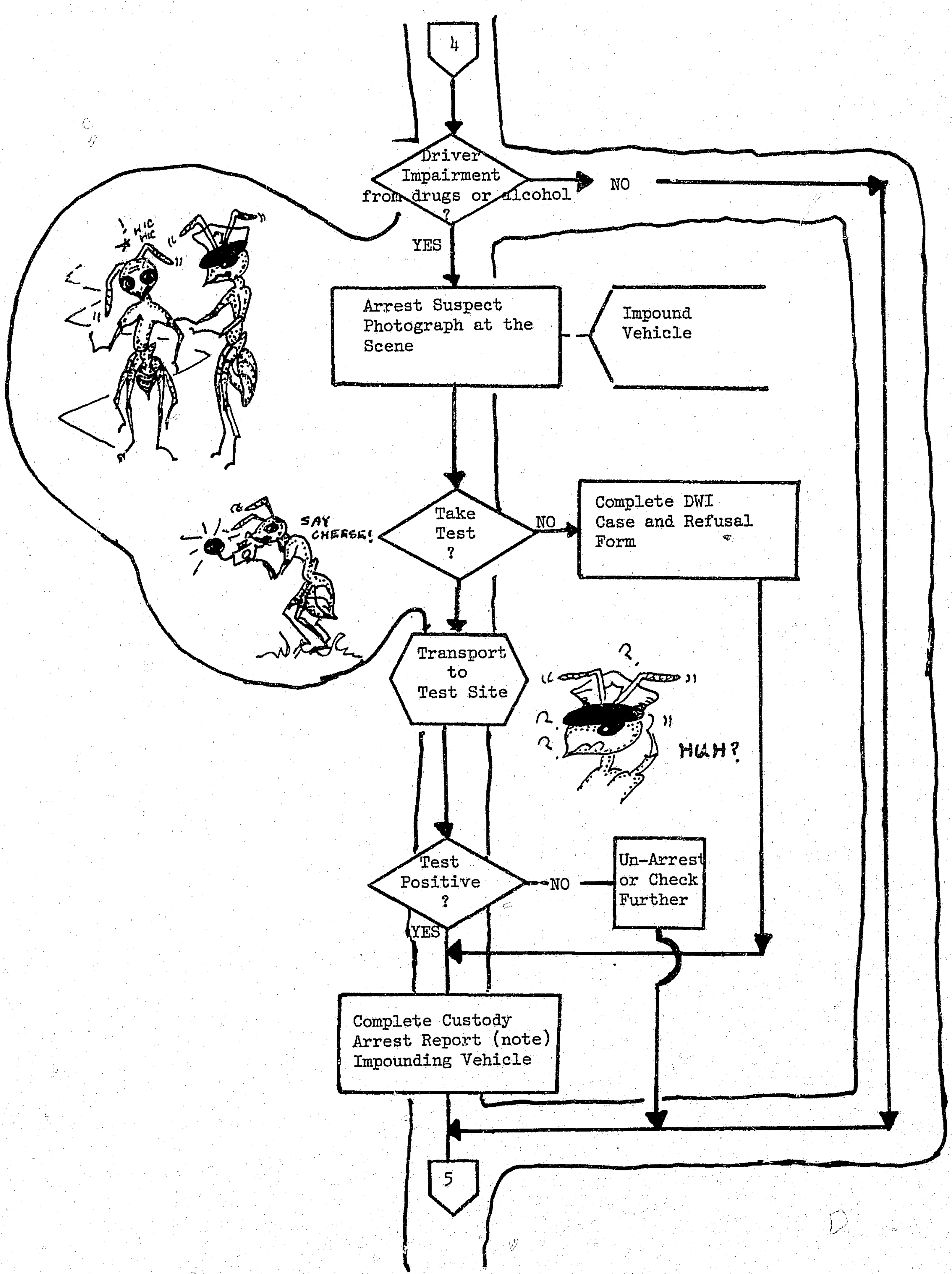
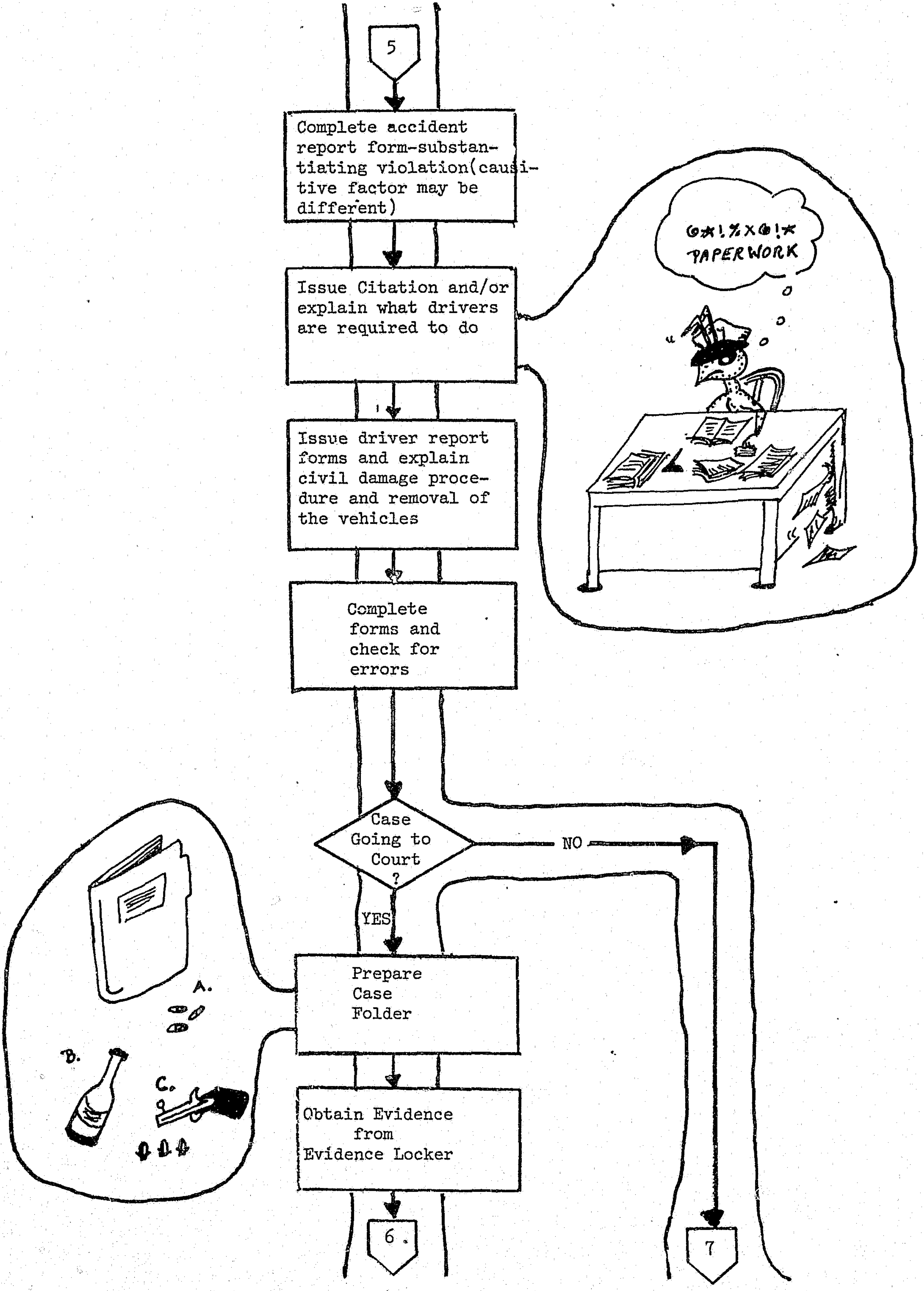

POLICE
START
NEED FOR EQUIP. ?
NO
YES
TAPE-CAMERA
REPORT FORM
FLASHLIGHT
PEN-PAPER
CLIPBOARD
CHALK-ETC.
EQUIP. AVAILABLE ?
NO
YES
RECEIVE CALL ON TRAFFIC ACCIDENT
NOTE TIME RECEIVED & LOCATION ON ACCIDENT REPORT
2
POLICE

Figure 7.11.


2
SEED STORAGE
SEED TRANS
SIZE UP SITUATION PARK PATROL UNIT
INJURIES
NO
YES
CALL AMBULANCE NOTE TIME & ARRIVAL
ANTULANCE
-LATER- FOLLOW UP AT HOSPITAL
GIVE FIRST AID-ASSIST AMBULANCE CREW-OBTAIN I.D. IF POSSIBLE
SET UP BARRICADE -IF NECESSARY-
GET SHORT LIVED EVIDENCE
3
DETOUR


3
A
Traffic Hazard ?
NO
Remove MVI Sticker ?
NO
YES
YES
Moved By Hand ?
NO
Call wrecker and/or other assistance
Remove Sticker and Issue receipt
YES
Recruit assistance from bystanders
I DONT WANT TO GET INVOLVED
HELP!
A
Drivers Identified ?
NO
Identify drivers
1. Res Gestae
2. Witnesses
YES
-Interview-
Take formal statements on Serious & Fatal Accidents
Draw rough sketch of scene (observe measure, record & mark evidence.
SEED STORAGE
AMBULANCE
PUT PUT PUT
4


4
Driver Impairment from drugs or alcohol ?
NO
YES
HIC HIC
Arrest Suspect Photograph at the Scene
Impound Vehicle
Take Test ?
NO
SAY CHEESE!
Complete DWI Case and Refusal Form
Transport to Test Site
HUH?
Test Positive ?
NO
YES
Un-Arrest or Check Further
Complete Custody Arrest Report (note) Impounding Vehicle
5



5

Complete accident report form-substantiating violation(causi-tive factor may be different)

Issue Citation and/or explain what drivers are required to do

Issue driver report forms and explain civil damage procedure and removal of the vehicles

Complete forms and check for errors

Case Going to Court ?

NO

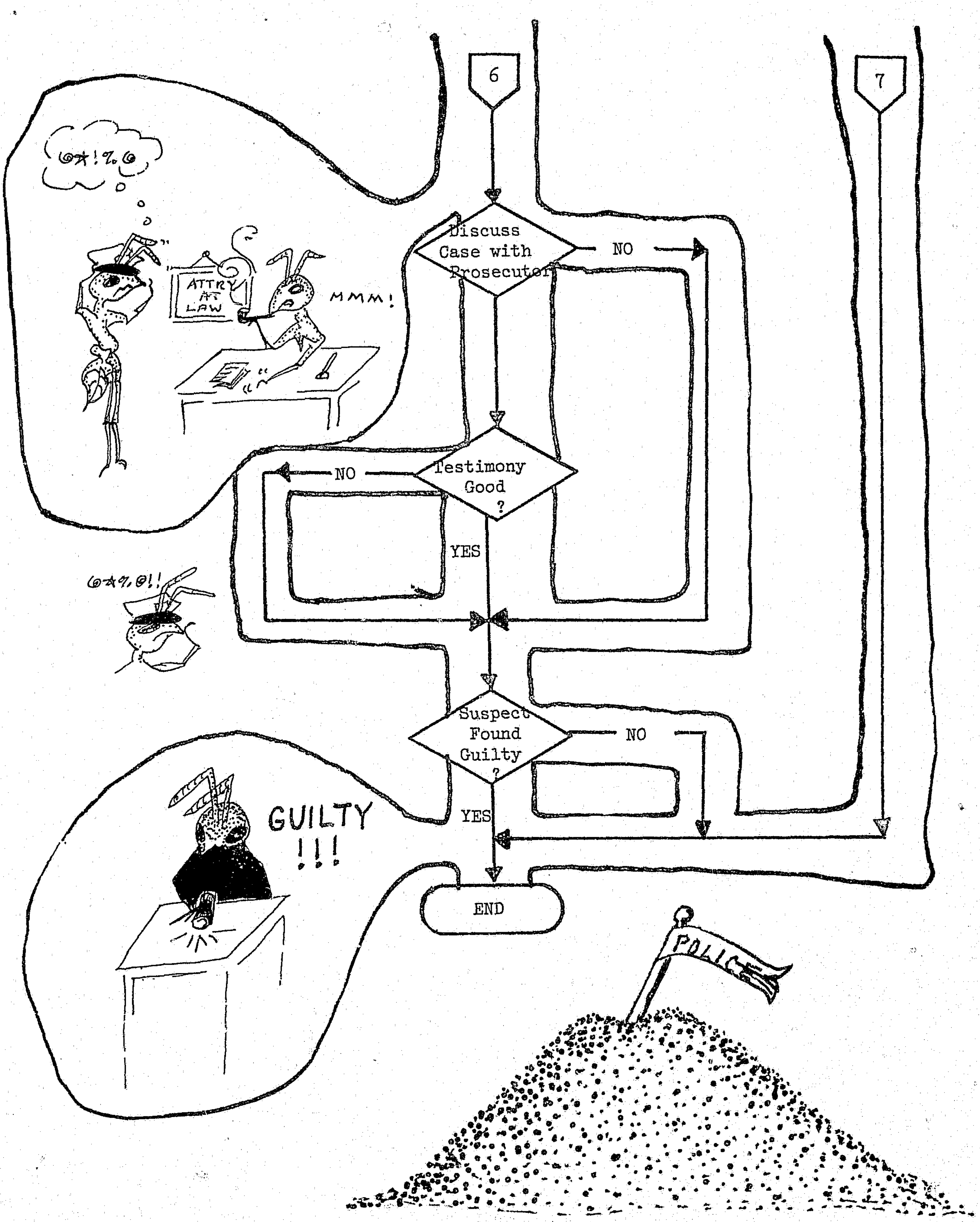
YES

Prepare Case Folder

Obtain Evidence from Evidence Locker

6.

7


6
7
Discuss Case with Prosecutor
NO
ATTRY AT LAW
MMM!
Testimony Good ?
NO
YES
Suspect Found Guilty ?
NO
YES
GUILTY !!!
END
POLICE

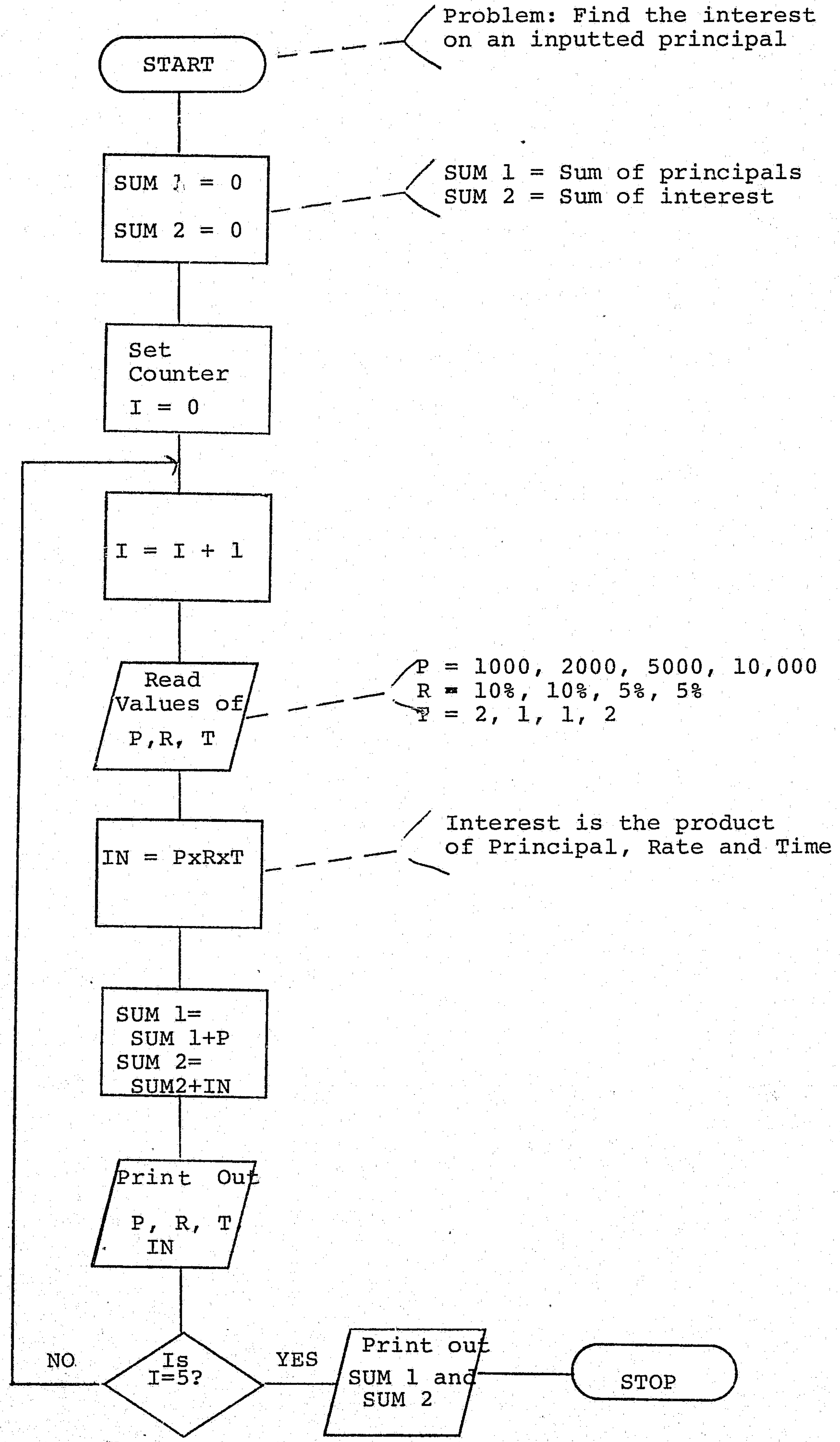
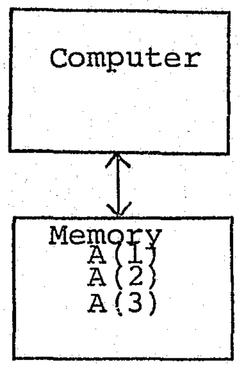
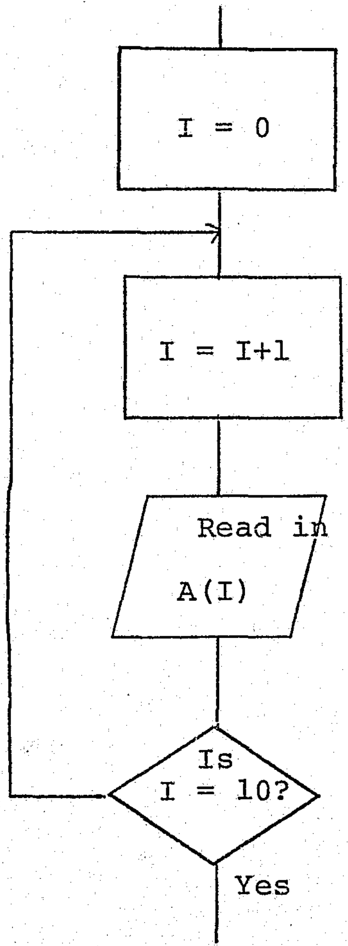


Figure 7.12. Example for interpretation.

of $A_1$.) Subscripted variables are stored in memory as follows:



The subscript ( the number inside the parenthesis) may also be a variable, so that we may refer to A(I) where I has been previously set to some value. If I is 10, then A(I) is refering to the 10th value of the subscripted variable A or A(10). Thus the following sequence would read 10 values into the subscripted variable A.



One application where subscripts usage is employed is shown in Figure 7.13. Notice that this is Figure 7.12 redrawn with an added flexibility of being able to process 10,20 or any number of input data sets of P, R and T. Also notice that when using a subscripted variable in a process, the complete expression is necessary, such as

IW = P(I) x R(I) x T(I)

Subscripted variables may be used in place of any simple variable. There are cases however, when subscripted variables are necessary for a problem's solution, i.e., simple variables are not adequate for the solution. Such a problem is that of placing numbers in ascending order or placing names in alphabetical order.

Assume we have a set of numbers (say account numbers) of size 100 which we want to place in ascending order. We must have all 100 values available to us at one time in order to be able to compare each and arrange them in proper order. Figure 7.14 shows the solution to this problem.

There are several things to note in this flowchart. First our technique is to move the largest value of the 100 numbers to the bottom, or to variable A(100). We accomplish this by first comparing A(1) to A(2). If A(1) is smaller than A(2), we leave the two numbers alone. If however A(1) is larger than A(2) we want to swap the two numbers so that A(2) will contain the larger value. We then compare A(2) to A(3) etc., continuing to swap if the first value is larger so that we finally have the largest value at the bottom or in A(100). We then want to move the next largest to A(99) so we move the "bottom" B up to 99 by setting B=B-1.

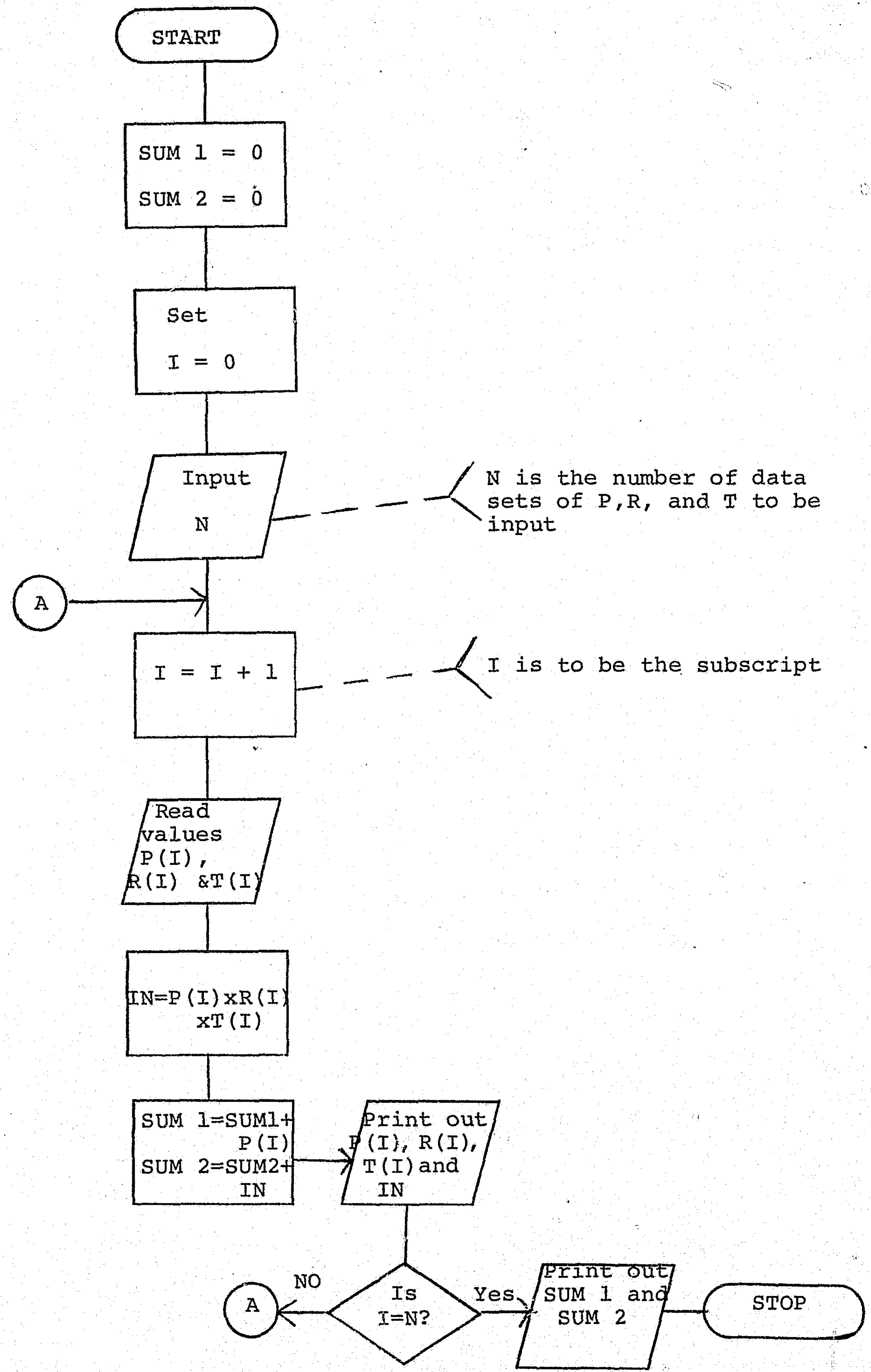

START
SUM 1 = 0
SUM 2 = 0
Set
I = 0
Input
N
N is the number of data sets of P,R, and T to be input
A
I = I + 1
I is to be the subscript
Read values P(I), R(I) &T(I)
IN=P(I)xR(I) xT(I)
SUM 1=SUM1+ P(I)
SUM 2=SUM2+ IN
Print out P(I), R(I), T(I) and IN
NO
A
Is I=N?
Yes
Print out SUM 1 and SUM 2
STOP

Figure 7.13. Figure 7.12 redrawn using subscripts.

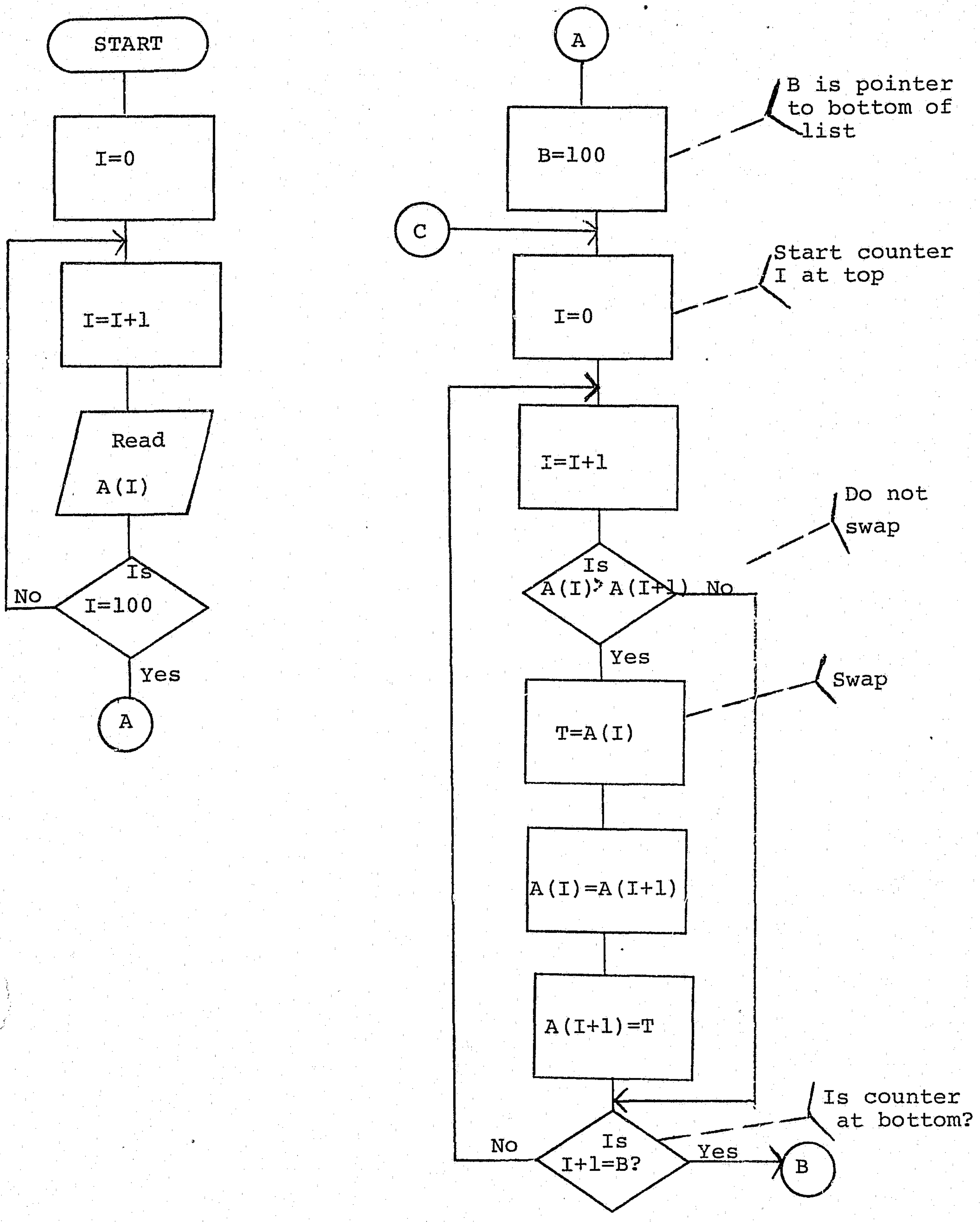


Figure 7.14. Ordering

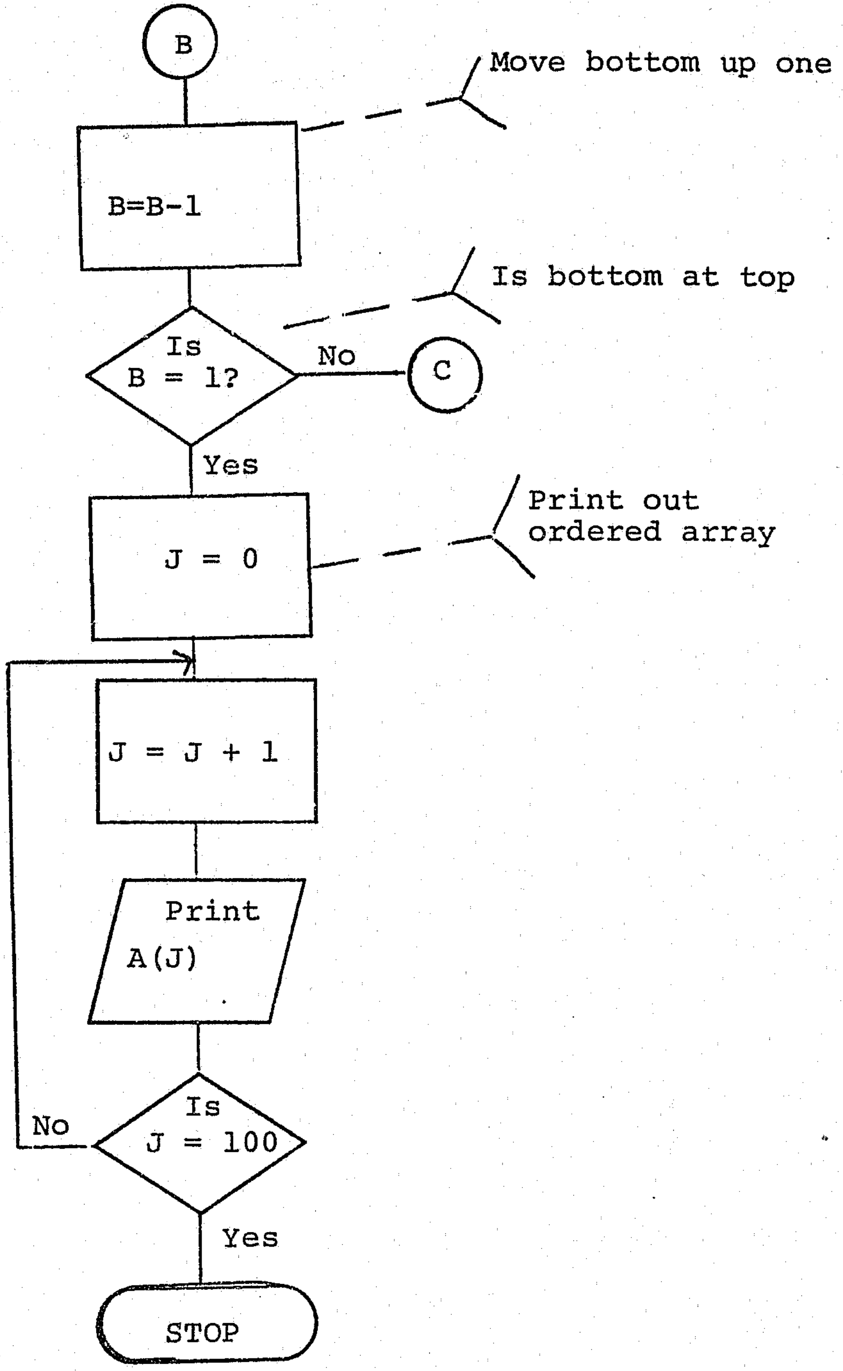
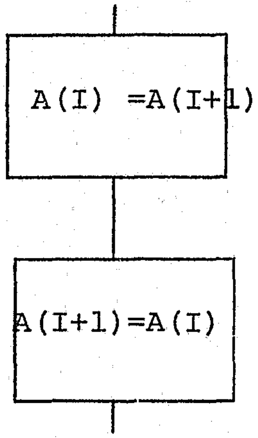
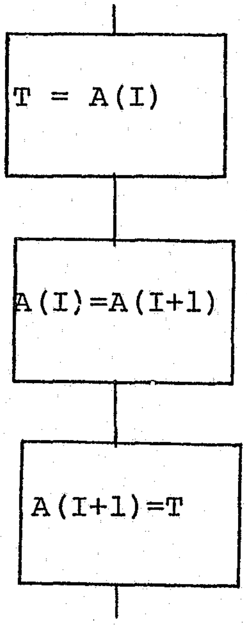


Figure 7.14 (cont.)

Now consider the process of swapping. We want A(I) set to A(I+1) and A(I+1) set to the value contained in A(I). We cannot however, accomplish this task by saying



since then both A(I) and A(I+1) would be the same value. Let A(I) = 15 and A(I+1) = 10 and go through the two processes above. We must therefore use a temporary storage slot for one of the values - we call it T in our flowchart. Take the two values 15 and 10 for A(I) and A(I+1) and go through the following:



Alphabetic variables such as names may be arranged in alphabetical order in the same fashion as in Figure 7.14 where we consider A<B<C ---< Z.

Quite often, we may have associated variables such as account numbers A(I) and balances B(I), and we may wish to arrange the sets in increasing order according to account numbers. We accomplished this feat in a similar fashion as described above, remembering to swap both A(I) with A(I+1) and B(I) with B(I+1).

The following exercises should be accomplished to gain experience in arranging quantities in order.

PROBLEMS

1. Redraw figure 7.14 so that the number of entries in the array is a variable.

2. Redraw figure 7.14 so that the numbers are in decreasing order.

3. Assume you are to input two sets of values into two arrays, say district numbers and number of burglaries in each district. Prepare a flowchart to arrange the two arrays such that the number of burglaries are in increasing order. Then write out the district number with the largest and smallest number of burglaries along with the associated number in each. Make your flowchart work for a variable number of sets of data.

4. Read in a set of values of a variable and find the largest and smallest without using subscripts.

5. Today, computer systems have been installed in a few of our supermarkets. Write a flowchart which would add a cart of groceries (remember to separate the taxable and non-taxable items) and total the bill. Also determine how many stamps that the customer receives).

| | | |
|---|---|---|
| one stamp for each penney: | 1¢ | $10.00 |
| two stamps for each penney: | $10.00 | $20.00 |
| 3 stamps for each penney: | $20.00 | $50.00 |
| and 5 stamps for each penney: | $50.00 | |

Money paid in the 5% sales tax does not go toward receiving stamps.

6. Write a flowchart to balance your check book. Take into account that you may have made a deposit after the bank cutoff date, the bank service charge, the cost of purchasing checks and the checks you have written that are outstanding and not included on your statement.

7. When goods are sold on credit, creditors usually grant discounts for early payments. Flowchart a program to compute the discount and the net amount if paid within the discount period. Read in the invoice amount and the percent of discount. List the invoice amount, the percent of discount, the amount of discount, and the net amount after taking the discount.

# CHAPTER VIII

## PROGRAMMING IN BASIC

The electronic computer is designed to accomplish one thing--to solve problems. The computer however, is not a "thinker" but a "doer", doing only what is told in the specific sequence it is told. The actual problem solution must be designed and then communicated to the computer in a language the computer system can understand. The translation of a problem solution into a computer language is referred to as programming.

There are many different computer languages (well over 300) all designed to work on a particular system and/or to accomplish specific tasks. For example, the FORTRAN language is designed for scientific applications, COBOL for business type problems, etc. The specific language we will study in detail is the BASIC computer language, designed primarily for timesharing or interactive computer systems.

We will assume that adequate time has been spent on flowcharting which aids in designing the solution of a problem, and concentrate on the necessary instructions which will translate that solution into a BASIC program.

There are two general categories of BASIC items: program commands and system commands. System commands deal with the actual implementation of a program on a computer system and vary in form from one system to the next. Program commands deal with the actual problem solution and are generally more standard than are the system commands. We will then concentrate our discussion on the program commands, for with a knowledge of these we can write our programs and then implement these programs by studying the system commands of our particular system.

## Statement Numbers and Variable Names

Every statement in a BASIC program must have a statement number such as 20 READ A . Where 20 is the statement number these numbers are important for two reasons. First, we can reference this statement at other points in our program and secondly, we may insert a new line preceding this statement by using a number of say 19. We will return to this point later so for now let us just say we will need to number all statements and that it is advisable to number them in increments of 10 such as

```
10     (Statement #1)
20     (Statement #2)
            .
            .
            .
```

Numeric variables used in a BASIC program must be named in a specific way, by use of a single letter, or a single letter followed by a single digit. Thus allowable variable names include

A, B, F, Z, A1, W5, Z1.

If a variable is to contain a character string such as a name of address, then we follow the letter or letters and number by the dollar sign $. Thus A1$ and Z$ are permissible character variable names.

Permissible values assigned to a numeric variable A would include 5, 71 or 51.6, while the variable B$ could be set to JIM, INDIANA, etc.

## Data Input

As was stated in the previous chapter on flowcharting, most problems to be solved on a computer involve the basic operations of data input, data processing and data output. In BASIC, input is accomplished by either of two commands, READ or INPUT. The READ command requires that the data be placed in a DATA statement. For example:

```
         .
         .
         .
10 DATA 15
20 READ  A
         .
         .
         .
```

would allow the value 15 to be input to the variable A. The command

```
         .
         .
         .
30 INPUT A
         .
         .
         .
```

would require that the input to A be typed in from the terminal (after the "?" is supplied by the computer).

The sequence

```
          .
          .
          .
10 DATA 'JOHN DOE', 15
20 READ N1$, A
          .
          .
          .
```

would set the character variable N1$ to be set to "JOHN DOE" while the numerical variable A is set to 15.

## Processing of Data

Processing of data is accomplished by the LET command, along with the operational symbols and functions allowed by BASIC. For example, the execution of the program segment

```
      .
      .
      .
10 DATA  15
20 READ   A
30 LET    B = A/3 + 2 * A
      .
      .
      .
```

would set B to 35.

Operations of addition, subtraction, multiplication and division are devoted by use of the following symbols

| | |
|---|---|
| + | addition |
| - | subtraction |
| * | multiplication |
| / | division |

Exponentiation (or raising to a power) is accomplished by use of either ** or ↑.

Thus

```
50 LET  F =  (10-3+1) *2 +3 ** 2
```

would set the variable F to 25.

The output of data may be accomplished by the PRINT command. For example, the execution of the following program segment would cause

```
THE VALUE OF B IS 35
```

to be printed on the terminal.

```
      .
      .
      .
10 DATA 15
20 READ  A
30 LET   B = A/3 + 2 * A
40 PRINT  "THE VALUE OF B IS", B
      .
      .
      .
```

In a PRINT statement, several variables may be printed on a single line as long as they are separated by commas. Statements inside quotation marks in a PRINT command are printed when the computer executes that particular PRINT.

## Looping, Remarks and End

Looping is accomplished in BASIC by use of the logical transfer commands such as IF (expression) THEN m. For example, the following program segment allows the processing of three input data values and would result in the data output of 5, 9 and 4.

```
         .
         .
         .
10  DATA  16, 64 9
20  LET  I = 0
30  LET  I = I + 1
40  READ  A
50  LET B = SQR(A) +1
60  PRINT  B
70  IF  I # 3 THEN 30
         .
         .
         .
```

Notice that a counter I is required and must be initialized properly.

By studying all the program commands and the functional and operational symbols used in BASIC any of the flowcharts written in Chapter II may be converted to a BASIC program. The following program corresponds with the flowchart in Figure 7.8. The only commands not previously discussed are the END command which must be final command of any program and the REM statements which are simply used to insert comments in a program. REM statements are not executed and may be used to document a program.

```
 10      REM  *** A PROGRAM TO COMPUTE THE MEAN ***
 20      REM  THE DATA IS TO BE INPUT FROM TERMINAL
 30      LET  I = 0
 40      LET  S = 0
 50      LET I = I + 1
 60      INPUT  A
 70      LET  S = S + A
 80      IF  I # 100  THEN 50
 90      LET M = S/100
100      PRINT "MEAN IS", M
110      END
```

Many errors in a program, whether caused by typing or logic, are detected by the computer. Appropriate error messages are then given, allowing the programmer to correct the statements before rerunning the program. Figures 8.1-8.4 show a typical attempt at typing in the previous program, where ten values rather than 100 are to be input.

In Figure 8.1, the first error detected by the computer, is the absence of a line number for the statement

```
LET  S = 0.
```

(The "READY" is a statement by the BASIC compiler signifying that it is ready for additional commands). Note that the LIST command is used, giving the current form of the program being written. When the RUN command is given, an additional error is denoted by the compiler. In this case, the PRINT statement in line 100 is in error. The correction for this statement is shown in Figure 8.2 along with the new listing and run. Notice that the correction is obtained by simply typing in a new line 100.

```
10 REM ***A PROGRAM TO COMPUTE THE MEAN***
20 REM ***THE DATA IS TO BE INPUT FROM TERMINAL***
30 LET I=0
LET S=0

? WHAT?
READY
40 LET S=0
50 LET I=I+A
60 INPUT A
70 LET S=S+A
80 IFI<>10 THEN 50
90 LET M=S/10
100 PRINT MEAN IS",M
110 END


LIST


10 REM ***A PROGRAM TO COMPUTE THE MEAN***
20 REM ***THE DATA IS TO BE INPUT FROM TERMINAL***
30 LET I=0
40 LET S=0
50 LET I=I+A
60 INPUT A
70 LET S=S+A
80 IFI<>10 THEN 50
90 LET M=S/10
100 PRINT MEAN IS",M
110 END

READY


RUN



? ILLEGAL VARIABLE IN LINE 100


TIME: 0.15 SECS.

READY
```

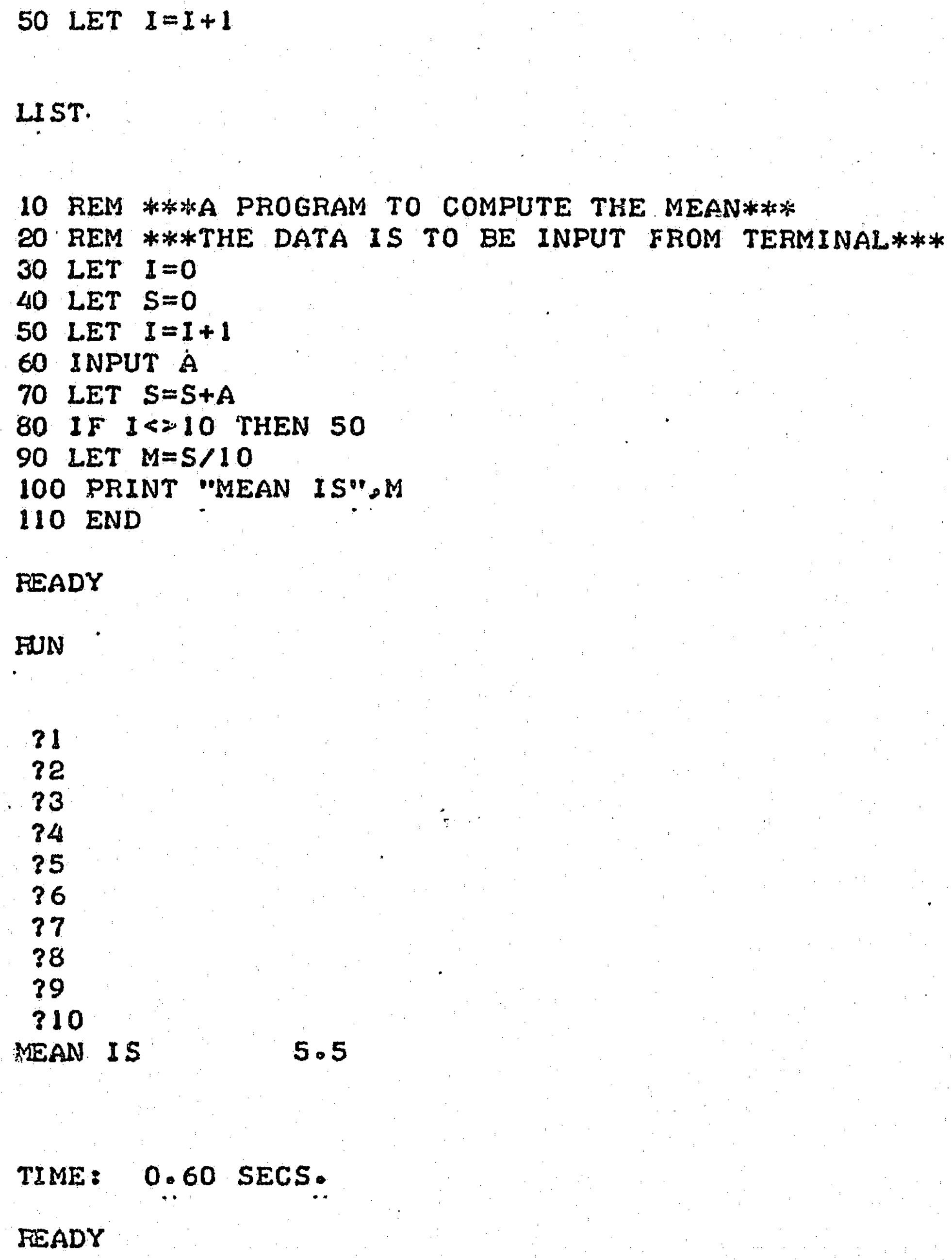
Figure 8.1. Run 1 for example.

A different type of error and one which is not "caught" by the compiler is evident in Figure 8.2. Data input is accomplished but for only 5 values of A rather than the 10 desired. This logic error must be found by the programmer without diagnostic messages from the computer. Upon examination, one sees that statement 50 is in error.

Figure 8.3 shows the correct version of the program, along with a sample run. Figure 8.4 shows the insertion of a new line in the program which better documents data input. Notice once again, the ease of adding lines of code by simply using the appropriate line numbers.

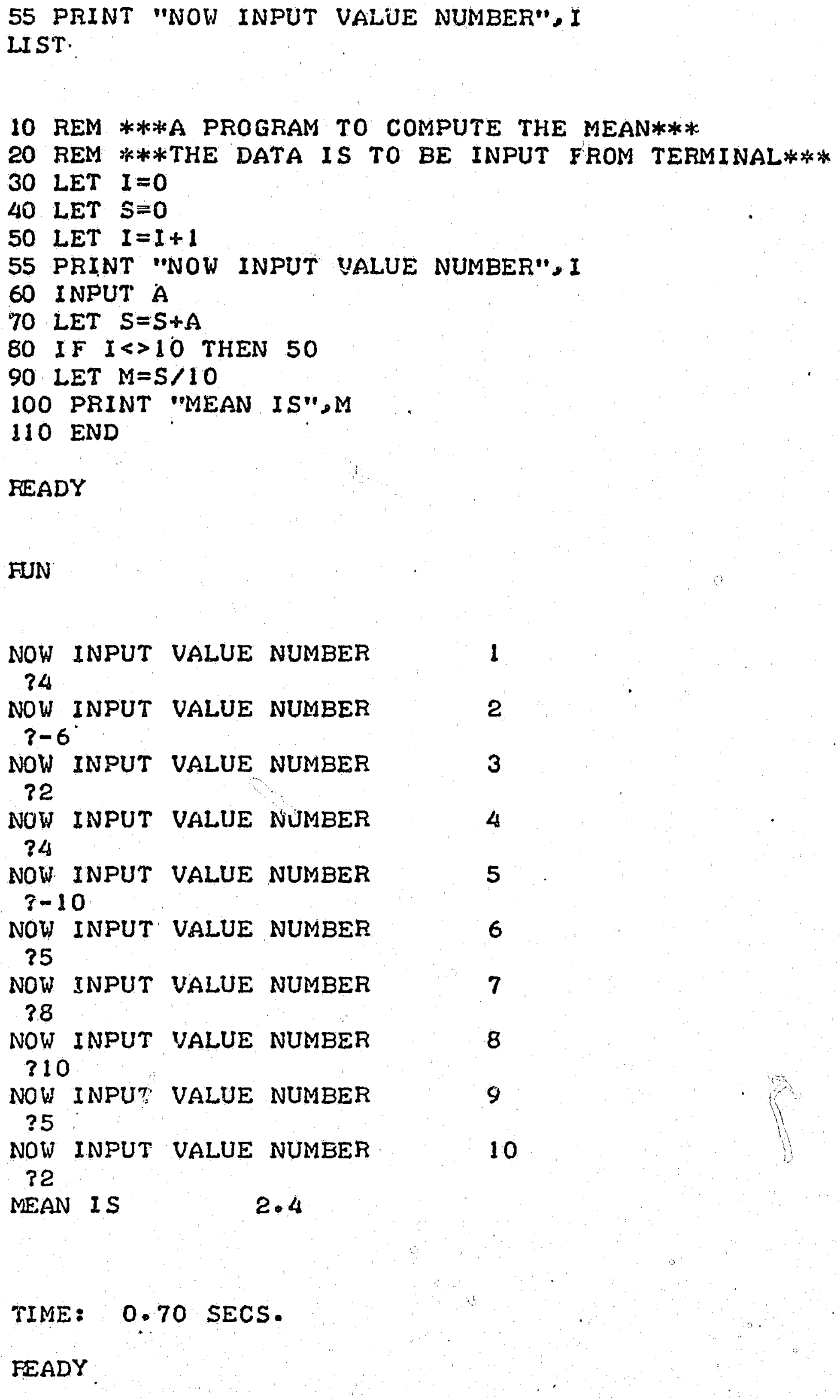
```
100 PRINT "MEAN IS",M


LIST


10 REM ***A PROGRAM TO COMPUTE THE MEAN***
20 REM ***THE DATA IS TO BE INPUT FROM TERMINAL***
30 LET I=0
40 LET S=0
50 LET I=I+A
60 INPUT A
70 LET S=S+A
80 IF I<>10 THEN 50
90 LET M=S/10
100 PRINT "MEAN IS",M
110 END

READY

RUN




 ?1
 ?2
 ?3
 ?4
 ?5
MEAN IS         1.5


TIME:  0.30 SECS.

READY
```

Figure 8.2. Run 2 for example.



```
50 LET I=I+1


LIST


10 REM ***A PROGRAM TO COMPUTE THE MEAN***
20 REM ***THE DATA IS TO BE INPUT FROM TERMINAL***
30 LET I=0
40 LET S=0
50 LET I=I+1
60 INPUT A
70 LET S=S+A
80 IF I<>10 THEN 50
90 LET M=S/10
100 PRINT "MEAN IS",M
110 END

READY

RUN


 ?1
 ?2
 ?3
 ?4
 ?5
 ?6
 ?7
 ?8
 ?9
 ?10
MEAN IS         5.5


TIME:  0.60 SECS.

READY
```

Figure 8.3.  Run 3 for example.



```
55 PRINT "NOW INPUT VALUE NUMBER",I
LIST


10 REM ***A PROGRAM TO COMPUTE THE MEAN***
20 REM ***THE DATA IS TO BE INPUT FROM TERMINAL***
30 LET I=0
40 LET S=0
50 LET I=I+1
55 PRINT "NOW INPUT VALUE NUMBER",I
60 INPUT A
70 LET S=S+A
80 IF I<>10 THEN 50
90 LET M=S/10
100 PRINT "MEAN IS",M
110 END

READY


RUN


NOW INPUT VALUE NUMBER        1
 ?4
NOW INPUT VALUE NUMBER        2
 ?-6
NOW INPUT VALUE NUMBER        3
 ?2
NOW INPUT VALUE NUMBER        4
 ?4
NOW INPUT VALUE NUMBER        5
 ?-10
NOW INPUT VALUE NUMBER        6
 ?5
NOW INPUT VALUE NUMBER        7
 ?8
NOW INPUT VALUE NUMBER        8
 ?10
NOW INPUT VALUE NUMBER        9
 ?5
NOW INPUT VALUE NUMBER        10
 ?2
MEAN IS        2.4


TIME:  0.70 SECS.

READY
```

Figure 8.4. Run 4 for example.

As is the case for flowcharting, programming is a "learn by doing" subject. Initial programs should be simple and easily understood, with more complex problems coming after the student is familiar with terminal usage and system commands. Several examples follow, demonstrating various programming techniques.

```
LIST


10 REM
20 REM PROGRAM FOR ADDING PAIRS OF NUMBERS
40 S=0
50 READ A,B
60 IF A=0 THEN 100
70 S=A+B
80 PRINT A,B,S
90 GO TO 40
100 PRINT "END OF LIST."
110 DATA 1,9,75,144.3,3,99,0,0
120 END

READY

RUN


1          9           10
75         144.3       219.3
3          99          102
END OF LIST.


TIME:   0.13 SECS.

READY
```

Figure 8.5. Example program which reads in pairs of numbers and computes the sum of these numbers.

CONTINUED

2 OF 3

```
LIST


10 REM
20 REM PROGRAM FOR SUMMING 12 VALUES READ IN
30 REM
40 N=12
50 S=0
60 READ I
70 S=S+I
80 N=N-1
90 IF N<= 0 THEN 110
100 GO TO 60
110 PRINT "SUM =";S
120 DATA 2,4,6,8,10,12,14,16,18,20,22,24
130 END

READY


RUN


SUM = 156


TIME:   0.05 SECS.

READY
```

Figure 8.6. Example showing the addition of 12 input values.

```
LIST


30 REM
40 REM THE PROGRAM WILL GENERATE THE
50 REM FIRST TEN INTERGERS AND COMPUTE
60 REM THEIR CUBES (POSITIVE INTEGERS).
70 REM
80 I=10
90 PRINT "INTEGER","CUBE"
100 J=0
110 J=J+1
120 K=J**3
130 PRINT J,K
140 IF J>=I THEN 160
150 GO TO 110
160 END


READY


RUN


INTEGER       CUBE
 1             1
 2             8
 3             27
 4             64
 5             125
 6             216
 7             343
 8             512
 9             729
 10            1000

TIME:  0.23 SECS.

READY
```

Figure 8.7. Example problem for computing cubes of integers.

```
LIST


30 REM
40 REM THE PROGRAM WILL GENERATE THE
50 REM FIRST TEN INTEGERS, CALCULATE THEIR
60 REM SQUARES, AND PRINT THE RESULTS.
70 REM
80 S=0
90 I=10
100 PRINT "NUMBER","SQUARE","SUM OF SQUARES"
110 J=0
120 J=J+1
130 K=J**2
140 S=S+K
150 PRINT J,K,S
160 IF J> =I THEN 180
170 GO TO 120
180 END

READY


RUN

NUMBER         SQUARE           SUM OF SQUARES
 1              1                1
 2              4                5
 3              9                14
 4              16               30
 5              25               55
 6              36               91
 7              49               140
 8              64               204
 9              81               285
 10             100              385

TIME:  0.35 SECS.

READY
```

Figure 8.8. Example showing computation of squares and summing.

## BASIC System Commands

[Used outside a program, not as part of a program statement] These system commands are always dependent on the particular system being used, with the command names usually differing. However, the command functions listed here are common to most systems.

SCRATCH
SCR

Clears the user's working area of all programs, information, instructions, enabling a clear beginning for writing a program.

GET-

Calls a program from a particular library, places it in the user's working space, ready for running, listing (unless protected), modifying, etc.

Example:

| | |
|---|---|
| GET-$START | calls program from system library |
| GET-*TEST1 | calls program from group library |
| GET-GLIST | calls program from user's own library |

NAME-
NAM-

Gives the program in user's working space a particular name (one to six characters, the first of which must not be $ or *); must be done before program can be saved.

Example:

NAM-GMATH

SAVE
SAV

Places program in user's working area into user's library, if properly named.

RUN

Causes program previously written into or otherwise placed into the user's working space to be executed.

RUN-n

Causes execution to begin at statement n.

Example:

RUN-1000

LIST
LIS

Causes the listing, in order of statement numbers, the program currently in user's working area.

LIS-*n*

Causes listing to begin at statement *n*.

Example:

```
LIS-250
```

LIS-*n*,*m*

Causes listing to begin at statement *n*, and cease at statement *m*.

Example:

```
LIS-250, 1000
```

LIS-P<br>
LIS-*n*,*m*,P

As above, but with the listing spaced at the appropriate places to allow cutting the list into 8½" x 11" pages.

OPEN-(name),*r*<br>
OPE-(name),*r*

Opens a file with the specified name, with *r* records of 256 words length each.

Example:

```
OPE-STU1, 60
```

RENUMBER<br>
REN

Causes the program statements to be renumbered. Unless otherwise indicated, the first statement becomes 10, and succeeding statements are numbered in increments of 10.

REN-*n* — Causes the first statement to be numbered *n*.

REN-*n*,*i* — Causes the first statement to be numbered *n*, with increment of i.

REN-*n*,*i*,*p* — As above, with *p* the first statement to be renumbered.

REN-*n*,*i*,*p*,*q* — As above, with the renumbering continuing through statement *q*.

Example:

```
REN-300
REN-400, 15
REN-1000, 5, 200, 400
```

(It should be noted here that all references in such statements as GØTØ n, IF...THEN n, GØSUB *n*, etc. are also properly renumbered.)

KILL-<br>
KIL-

Deletes an entire program (that named after the hyphen) from the user's own library. Also used to delete a file.

Example:

```
KIL-GMATR
```

TIME
TIM

Returns the current amount of console time, and the cumulative time used on the particular access level.

DELETE-n
DEL-n

Deletes statements in the current program beginning at statement n and continuing to the END statement.

DEL-n,m

Deletes all statements beginning at statement n and continuing through statement m.

Example:

```
DEL-8000
DEL-100, 200
DEL-1  (equivalent to SCR)
```

PUNCH
PUN

Causes the current program to be both listed and punched onto paper tape, if the tape punch is turned on.

PUN-n
PUN-n,m
PUN-P
PUN-n,m,P

Causes listing and tape punching as above, with parameters functioning as with LIST.

Example:

```
PUN-100, 500, P
```

XPUNCH
XPUN
XPUN-n
XPUN-n,m
XPUN-P
XPUN-n,m,P

Produces a listing and tape punching as above, but with a special punch at the end of each line which allows the tape to be used for the reading of data into a program.

## BASIC Program Commands

[Used only in a numbered program statement]

n REM

A comment statement, not executed by the computer; used for reminders, comments, identification of sections, instructions to the user. Any combination of keyboard characters may be used after REM.

Example:

```
10 REM *** A SAMPLE PROGRAM ***
```

n DATA

A list of items to be used by the program during a READ statement. May be numerical or alphanumerical, as required by the program.

Example:

```
        20  DATA 2, 5, 9, 14, 20, 27, "ABC"
```

n READ

Causes the data in a DATA statement to be read into the program, and stored under the specified name. DATA statements are used sequentially as they are placed in the program; there is no restriction on the actual placements of the DATA statements.

Example:

```
        30  READ A, B
```

This would, using 20 DATA above, first assign 2 to A, 5 to B; if the same READ statement were repeated with a different statement number, then 9 would be assigned to A, 14 to B.

n PRINT var.
n PRINT "@#"

n PRINT

Causes the value of the variable, or the characters between the quotation marks, to be printed out on the terminal. With no variable or character, causes a carriage return and a single linefeed.

Example:

```
        40  PRINT A, B
        45  PRINT "PLEASE INPUT THE VALUE
                  OF C"
```

If the variables or characters strings are separated by commas,

```
        40  PRINT A, B
        41  PRINT A, F$, B
```

then the items are separated into columns whose first elements are at twelve-space increments. If, however, the items are separated by semi-colons, the printing is contiguous, that is, not separated at all.

```
        42  PRINT A; B
        43  PRINT A; F$; B;
        44  PRINT "END"
```

In line 42, the value for B would be printed immediately after the value for A. In line 43, similar printing would occur; the semi-colon at the end, however, makes the next printing (from line 44) occur immediately after the value for B.

n INPUT var.

Requests information from the operator or program user. Generates a "?" and pauses for input; assigns the value input to the specified variable name.

Example:

```
50  INPUT C
```

n D =...
n LET D =...

Assigns the value of the formula, expression, or constant on the right to the variable named on the left. All variables or function arguments used on the right must have been previously given a value.

Example:

```
60  D = 3*A + 2*B + C
60  LET D = 3*A + 2*B + C
```

This would multiply 3 times the value of A, 2 times the value of B, and add these two products to the value of C; this resulting value would then be assigned to D.

n GØTØ m

Causes a direct, unconditional jump or branch to statement number m.

Example:

```
80  GØTØ 800
```

n GØTØ A OF $s_1$, $s_2$, $s_3$, . . . ; $s_r$

Takes the integral value of A (if not an integer) and goes to that numbered item in the series $s_1$, $s_2$, $s_3$, . . . , $s_r$.

Example:

```
800  GØTØ A OF 230, 740, 420, 630
```

If A has the value of 3, then the program goes directly to 420. For A = 0 or A > 4, the command would be ignored.

n GØSUB m

Unconditional jump to a subroutine of any length. Upon arrival at the RETURN statement in the subroutine, the program returns to the statement following the GØSUB statement.

Example:

```
420   GØSUB 600
```

n RETURN

Terminates the subroutine, and returns the program to the statement following the GØSUB statement. Must be the last executable statement in a subroutine.

Example:

```
610   RETURN
```

n IF (expression) THEN m

Examines the variables and their relationship in the expression. If the condition is true or is non-zero, then the program branches to statement number m. If the condition is not true or is zero, then the command is ignored.

Example:

```
600   IF A  = 1 THEN 30
601   IF A THEN 50
```

n FØR A = m TØ p
n FØR A = m TØ p STEP r
q NEXT A

A looping command, performing the statements between the FØR ... and NEXT ... statements the indicated number of repetitions. The step size is optional, 1 unless otherwise given. Loops may be nested, but not overlapped. After the last iteration, the program moves to the statement following the NEXT ... statement.

Example:

```
230  FØR I = 1 TØ 10
231  PRINT "X"
232  NEXT I
233  FØR I = 1 TØ 5
234  FØR J = 1 TØ 3
235  PRINT "Y"
236  NEXT J
237  NEXT I
```

n DIM A[20,20], F$[72]

Specifies the maximum working size of a matrix variable (such as 20 rows and 20 columns for matrix variable A) or for a string variable (such as 72 characters for string variable F$). Every matrix or string variable must be dimensioned before it is used in a program.

## BASIC Functional or Operational Symbols

X,Y,A1, etc.

Variables; may be used for integral or real values; any single letter or single letter followed by a single-digit number may be used.

A,B[3,2], etc.

Matrix variables; used to designate entire arrays, or to designate a single element of an array, as B[3,2], the element in the third row and second column of the array named B. It should be noted that considerable sophistication in programming is necessary before work with arrays should be attempted.

A$,F$, etc.

String variables; used to designate a particular group of alphabetic, numerical, or special characters. Each system contains its own syntax for working with strings, and these rules must be followed exactly.

=

A dual function symbol. Used as an ordinary algebraic equality symbol, when it appears in an IF ... THEN statement.

```
250  IF A = 200 THEN 610
```

Also used as an assignment operator; the single variable on the left is assigned the value possessed by the variable or numerical expression on the right.

```
     260  A = 2*X + 3
     270  LET B = A
     280  A = A + 2
```

It should be noted that every variable appearing on the right in an assignment statement must have been given some numerical value previously. A frequent procedure to take care of this involves giving all variables a value of 1 or 0 early in the program. Any subsequent assignment will take precedence.

```
     17  A = B = 0
     17  LET A = B = 0
```

In example line 280 above, the same variable is used on both left and right sides. In such a case A will now have the value of 2 more than its previous value (which is now destroyed).

<
<
<=
>=

Symbols with usual algebraic meaning. Occur normally only in IF . . . THEN statements.

```
     190  IF A<= B THEN 9999
     191  IF C > A THEN 401
```

#
<>
><

Not equal. Usually found only in comparison in IF . . . THEN statements.

```
     192  IF B # 3 THEN 9999
     193  IF C + 2<> A - 5 THEN 293
```

*

Multiplication operator

```
     101  A = 2*B*C
```

+

Addition operator

```
     102  D = A + B + 11
```

-

Subtraction operator

```
     103  B = D - A - 3
```

/

Division operator

```
     104  C = B/D
```

As in all uses of real number arithmetic, the value of the denominator must never be zero. In some systems, the maximum size of number representation places a practical minimum size limitation on the denominator; that is, the system may interpret a very small number as it would zero for these purposes.

↑
**

The exponentiation operator. The base may be an integral or real number, but the exponent must be a one- or two-digit integer.

```
     105  B = C↑3 + D↑A
```

This is allowed if A is an integral value at the time of execution.

( )
[ ]

Grouping symbols. These are used as in ordinary algebraic usage, and should be used liberally to ensure both the operator's and the machine's ability to properly interpret a statement. Most compilers treat both shapes of symbols interchangeably.

```
     106  C = (B - C)/A
```

is not the same as

```
     107  C = B - C/A
```

↑
* or /
+ or -

The order of operations is given from first (at the top) to last (at the bottom) unless grouping symbols change the priorities. The operators * and / are taken in order from left to right, as are + and -.

```
     108  A = B + C/D↑3
```

would be evaluated as if it had been written

```
     108  A = B + [C/(D↑3)]
```

SIN(X)
CØS(X)
TAN(X)

Computes the usual trigonometric functional values of the argument, such as X, which is in radians.

```
     111  A = SIN(3)
     112  B = CØS(A) + 3
     113  C = [TAN (A)]↑2
```

ATN(X)

Computes the inverse tangent function in radians of the argument, such as X.

```
     114  D = ATN(C)
```

SQR(X)

Computes the square root of the argument, if the argument is non-negative.

```
     115  E = SQR(D + 2)
```

ABS(X)

Computes the absolute value of the argument.

```
    116  B = ABS(B + C)
```

INT(X)

Computes the greatest integer less than or equal to the argument.

```
    117  F = INT[SQR(B)]
```

LØG(X)

Computes the logarithm to the base e of the non-negative argument.

```
    118  G = LØG(B + E)
```

EXP(X)

Computes the value of e raised to the Xth power.

```
    119  C = EXP(D)
```

System limitations vary, but the EXP argument may usually be nonintegral.

ØR

Logical operator used in comparisons. Uses usual Boolean logic approach: if either comparison is valid, then the transfer is made.

```
    121  IF [(A = C) ØR (A = B + 3)] THEN 180
    122  IF [(D < 5) ØR (D > 20)] THEN 401
```

AND

Logical operator used in comparison. Uses usual Boolean logic approach: only if both comparisons are valid will the transfer be made.

```
    123  IF [(A = D) AND (B > 3)] THEN 298
    124  IF [(D >=5) AND (D<= 20)] THEN 321
```

Other logical comparisons are possible. If a given variable or expression is non-zero, then its "truth value" is assumed to be 1, and Boolean comparison is based on that value. If a variable or expression is zero, then its "truth value" is also zero.

```
    125  IF A THEN 501
```

This would transfer control only if A had a non-zero value.

```
    126  IF A AND B THEN 521
```

This would transfer control only if both A and B had non-zero values.

NØT

Causes the opposite truth value to be assigned.

```
    127  IF (NØT A) THEN 643
```

This would transfer control only if A has a zero value, giving NØT A a non-zero value.

## Suggested Sources for Supplementary Material

Coan, J. S. Basic BASIC: An Introduction to Computer Programming in BASIC Language. Rochelle Park, N.J.: Hayden, 1970.

Estes James W., and Estes, B. Robert. Elements of Computer Science. San Francisco: Canfield Press, 1973. Especially note chap. 8, "Programming Languages."

Farina, Mario V. Elementary BASIC with Applications. Englewood Cliffs, N.J.: Prentice-Hall, 1970.

________. FORTRAN IV Self-taught. Englewood Cliffs, N.J.: Prentice-Hall, 1966.

Gately, W. U., and Bitter, G. G. BASIC for Beginners. New York: McGraw-Hill, 1970.

Hare, V. C. BASIC Programming. New York: Harcourt, Brace & World, 1970.

Kemeny, J. G., and Kurtz, T. E. BASIC Programming. New York: Wiley, 1970.

McCracken, Daniel D. A Guide to FORTRAN IV Programming. New York: Wiley, 1972. Especially note pp. 47-48, "A Checklist for Program Checkout."

Nolan, Richard L. Introduction to Computing through the BASIC Language. New York: Holt, Rindhart and Winston, 1969. Especially note chaps. 2-6, and appendix A, "Time-sharing BASIC and Batch-mode BASIC."

Pavlovich, J. P., and Tahan, T. E. Computer Programming in BASIC. San Francisco: Holden-Day, 1971.

Smith, R. E. Discovering BASIC: A Problem Solving Approach. Rochelle Park, N.J.: Hayden, 1970.

Spencer, Donald D. A Guide to BASIC Programming: A Time-Language. Reading, Mass.: Addison-Wesley, 1970.

________. Computers in Action: How Computers Work. Rochelle Park, N.J.: Hayden, 1974. Especially note chap. 7, "The Language of the Computer," and chap. 8, "Introduction to Computer Programming."

________. Computers in Society: The Wheres, Whys, and Hows of Computer Usage. Rochelle Park, N.J.: Hayden, 1974.

Weiss, Eric A., ed. Computer Usage: Fundamentals. New York: McGraw-Hill, 1969.
Especially note chap. 12, "FORTRAN, COBOL, and other Programming Languages," chap. 15, "Techniques for Computing Scientific Problems," and chap. 19, "Specifying and Documenting Computer Programs."

# CHAPTER IX

# PRIVACY ACT

In 1974, the Federal government passed the "Privacy Act of 1974" to restrict the dissemination of criminal record information.

In the past, police agencies could make criminal record information available to anyone asking for it. These agencies could also refuse this information to almost anyone. What occurred was that private individuals could obtain criminal history checks on certain persons if they were in "good" with the police. The Federal government realized that this dissemination was discriminative in nature and that controls were needed to protect the privacy of individuals included in the records.

The Privacy Act seeks to protect the privacy of these individuals included in the records of the Federal Bureau of Investigation, criminal justice agencies receiving funds directly or indirectly from the Law Enforcement Assistance Administration, and interstate, state, or local criminal justice agencies exchanging records with the FBI, or these federally funded systems. At the same time, these regulations preserve legitimate law enforcement need for access to such records.

In order to interpret this Act and to establish guidelines for all responsible agencies to follow, the Department of Justice released information concerning this Act on May 20, 1975. The guidelines, "Criminal Justice Information Systems", were submitted by Attorney General Edward H. Levi to the federal register for documentation and have become the basis guidelines for state and local government.

The remaining portion of this chapter contains these guidelines. The Texas Crime Prevention Institute believes that this material will be useful to you in your work within the criminal justice system.

# CRIMINAL JUSTICE INFORMATION SYSTEMS

## Subpart A - General Provisions

## Subpart B - State and Local Criminal History Record Information Systems

## Subpart C - Federal System and Interstate Exchange of Criminal History Record Information

Authority: Pub. L. 93-83, 87 Stat. 197, (42 U.S.C. 3701, et seq; 28 U.S.C. 534), Pub L. 92-544, 86 Stat. 1115.

SUBPART A - GENERAL PROVISIONS

Section 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the completeness; integrity, accuracy, and security of such information and to protect individual privacy.

Section 20.2 Authority.

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93-83, 87 Stat. 197, 42 U.S.C. 3701, et seq. (Act), 28 U.S.C. 534, and Pub. L. 92-544, 86 Stat. 1115.

Section 20.3 Definitions.

As used in these regulations:

(a) "Criminal history record information system" means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation or dissemination of criminal history record information.

(b) "Criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

(c) "Criminal justice agency" means: (1) courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(d) The "administration of criminal justice" means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(e) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed - civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial - defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(f) "Statute" means an Act of Congress or State legislature of a provision of the Constitution of the United States or of a State.

(g) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(h) An "executive order" means an order of the President of the United States or the Chief Executive of a State which has the force of law and which is published in a manner permitting regular public access thereto.

(i) "Act" means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701 et seq. as amended.

(j) "Department of Justice criminal history record information system" means the Identification Division and the Computerized Criminal History File systems operated by the Federal Bureau of Investigation.

## SUBPART B - STATE AND LOCAL CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

### Section 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of the Act.

(b) The regulations in this subpart shall not apply to criminal history record information contained in: (1) posters, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) court records of public judicial proceedings compiled chronologically; (4) published court opinions or public judicial proceedings; (5) records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses; (6) announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonable contemporaneous with the event to which the information relates. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section.

Section 20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to LEAA by each State within 180 days of the promulgation of these regulations. The plan shall set forth operational procedures to -

(a) Completeness and accuracy. Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central

State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information to assure that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period. (2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) Limitations on dissemination. Insure that dissemination of criminal history record information has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Such other individuals and agencies which require criminal history record information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure

the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section 524(a), and provide sanctions for the violation thereof;

(5) Agencies of State or federal government which are authorized by statute or executive order to conduct investigations determining employment suitability or eligibility for security clearances allowing access to classified information;

(6) Individuals and agencies where authorized by court order or court rule.

(c) General policies on use and dissemination. Insure adherence to the following restrictions:

(1) Criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual (except under Section 20.21(b) (3), (4), (5), (6)), if an interval of one year has elapsed from the date of the arrest and no disposition of the charge has been recorded and no active prosecution of the charge is pending;

(2) Use of criminal history record information disseminated to non-criminal justice agencies under these regulations shall be limited to the purposes for which it was given and may not be disseminated further.

(3) No agency or individual shall confirm the existence or non-existence of criminal history record information for employment or licensing checks except as provided in paragraphs (b)(1), (b)(2), and (b)(5) of this section.

(4) This paragraph sets outer limits of dissemination. It does not, however, mandate dissemination of criminal history record information to any agency or individual.

(d) Juvenile records. Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need of supervision (or the equivalent) to non-criminal justice agencies is prohibited, unless a statute or Federal executive order specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in Section 20.21 (b) (3), (4), and (6).

(e) Audit. Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated.

(f) Security. Insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated, a criminal justice agency shall -

(1) Institute where computerized data processing is employed effective and technologically advanced software and hardward designs to prevent unauthorized access to such information;

(2) Assure that where computerized data processing is employed, the hardware, including processor, communications control, and storage device, to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice;

(3) Have authority to set and enforce policy concerning computer operations;

(4) Have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area where such information is stored, collected, or disseminated;

(5) Select and supervise all personnel authorized to have direct access to such information;

(6) Assure that an individual or agency authorized direct access is administratively held responsible for (i) the physical security of criminal history record information under its control or in its custody and (ii) the protection of such information from unauthorized accesses, disclosures, or dissemination;

(7) Institute procedures to reasonably protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters;

(8) Provide that each employee working with or having access to criminal history record information should be made familiar with the substance and intent of these regulations; and

(9) Provide that direct access to criminal history records information shall be available only to authorized officers or employees of a criminal justice agency.

(g) Access and review. Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that -

(1) Any individual shall, upon satisfactory verification of his identity be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by Section 20.3 (b).

Section 20.22 Certification of Compliance.

(a) Each State to which these regulations are applicable shall with the submission of each plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include -

(1) An outline of the action which has been instituted, At a minimum, the requirements of access and review under 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth all non-criminal justice dissemination authorized by legislation existing as of the date of the certification showing the specific categories of non-criminal justice individuals or agencies, the specific purposes or uses for which information may be disseminated, and the statutory or executive order citations.

Section 20.23 Documentation: Approval by LEAA.

Within 90 days of the receipt of the plan, LEAA shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by LEAA will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certication(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by December 31, 1977, except that a State, upon written application and good cause, may be allowed an additional period of time to implement Section 20.21(f)(2). Certification shall be submitted in December of each year to LEAA until such complete compliance. The yearly certification shall update the information provided under Section 20.21.

Section 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

Section 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a fine not to exceed $10,000. In addition, LEAA may initiate fund cut-off procedures against recipients of LEAA assistance.

SUBPART C - FEDERAL SYSTEM AND INTERSTATE EXCHANGE OF CRIMINAL HISTORY RECORD INFORMATION

Section 20.30 Applicability.

The provisions of this subpart of the regulations apply to any Department of Justice criminal history record information system that serves criminal justice agencies in two or more states and to Federal, state, and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems. These regulations are applicable to both manual and automated systems.

Section 20.31 Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall operate the National Crime Information Center (NCIC), the computerized information system which includes telecommunications lines and any message switching facilities which are authorized by law or regulation to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information. Such information includes information in the Computerized Criminal History (CCH) File, a cooperative Federal-State program for the interstate exchange of criminal history record information. CCH shall provide a central repository and index of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies.

(b) The FBI shall operate the Identification Division to perform identification and criminal history record information functions for Federal, state, and local criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by Federal statute, state statute pursuant to Public Law 92-544 (86 Stat. 1115), Presidential executive order, or regulation of the Attorney General of the United States.

(c) The FBI Identification Division shall maintain the master fingerprint files on all offenders included in the NCIC/CCH File for the purposes of determining first offender status and to identify those offenders who are unknown in states where they become criminally active but known in other states through prior criminal history records.

Section 20.32 Includable offenses.

(a) Criminal history record information maintained in any Department of Justice criminal history record information system shall include serious and/or significant offenses.

(b) Excluded from such a system are arrests and court actions limited only to nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders shall also be excluded unless a juvenile offender is tried in court as an adult.

(c) The exclusions enumerated above shall not apply to Federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of these Regulations.

Section 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in any Department of Justice criminal history record information system will be made available:

(1) To criminal justice agencies for criminal justice purposes; and

(2) To Federal agencies authorized to receive it pursuant to Federal statute or Executive order.

(3) Pursuant to Public Law 92-544 (86 Stat. 115) for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by Federal or state statutes and approved by the Attorney General of the United States. When no active prosecution of the charge is known to be pending arrest data more than one year old will not be disseminated pursuant to this subsection unless accompanied by information relating to the disposition of that arrest.

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses.

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonable contemporaneous with the event to which the information relates.

Section 20.34 Individual's right to access criminal history record information.

(a) Any individual, upon request, upon satisfactory verification of his identity by fingerprint comparison and upon payment of any required processing fee, may review criminal history record information maintained about him in a Department of Justice criminal history record information system.

(b) If, after reviewing his identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he must make application directly to the contributor of the questioned information. If the contributor corrects the record, it shall promptly notify the FBI and, upon receipt of such a notificaiton, the FBI will make any changes necessary in accordance with the correction supplied by the contributor of the original information.

Section 20.35 National Crime Information Center Advisory Policy Board.

There is established an NCIC Advisory Policy Board whose purpose is to recommend to the Director, FBI, general policies with respect to the philosophy, concept and operational principles of NCIC, particularly its relationships with local and state systems relating to the collection, processing, storage, dissemination and use of criminal history record information contained in the CCH File.

(a) The Board shall be composed of twenty-six members, twenty of whom are elected by the NCIC users from across the entire United States and six who are appointed by the Director of the FBI. The six appointed members, two each from the judicial, the corrections, and the prosecutive sectors of the criminal justice community, shall serve for an indeterminate period of time. The twenty elected members shall serve for a term of two years commencing on January 5th of each odd numbered year.

(2) The Board shall be representative of the entire criminal justice community at the state and local levels and shall include representation from law enforcement, the courts, and corrections segments of this community.

(b) The Board shall review and consider rules, regulations, and procedures for the operation of the NCIC.

(c) The Board shall consider operational needs of criminal justice agencies in light of public policies, and local, state and Federal statutes and these Regulations.

(d) The Board shall review and consider security and privacy aspects of the NCIC system and shall have a standing Security and Confidentiality Committee to provide input and recommendations to the Board concerning security and privacy of the NCIC system on a continuing basis.

(e) The Board shall recommend standards for participation by criminal justice agencies in the NCIC system.

(f) The Board shall report directly to the Director of the FBI or his designated appointee.

(g) The Board shall operate within the purview of the Federal Advisory Committee Act, Public Law 92-463, 86 Stat. 770.

(h) The Director, FBI, shall not adopt recommendations of the Board which would be in violation of these Regulations.

Section 20.36 Participation in the Computerized Criminal History Program.

(a) For the purpose of acquiring and retaining direct access to CCH File each criminal justice agency shall execute a signed agreement with the Director, FBI, to abide by all present rules, policies and procedures of the NCIC, as well as any rules, policies, and procedures hereinafter approved by the NCIC Advisory Policy Board and adopted by the NCIC.

(b) Entry of criminal history record information into the CCH File will be accepted only from an authorized state or Federal criminal justice control terminal. Terminal devices in other authorized criminal justice agencies will be limited to inquiries.

Section 20.37 Responsibility for accuracy, completeness, currency.

It shall be the responsibility of each criminal justice agency contributing data to any Department of Justice criminal history record information system to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

Section 20.38 Sanction for noncompliance.

The services of Department of Justice criminal history record information systems are subject to cancellation in regard to any agency or entity which fails to comply with the provisions of Subpart C.

Edward H. Levi,
Attorney General.

Richard W. Velde,
Administrator, Law Enforcement
Assistance Administration

Dated May 15, 1975

# CHAPTER X

## THE NEED FOR COMPUTER SECURITY

As the manipulation of data has been relegated to machine control more and more, there has been an increasing number of incidents involving the misuse of stored information. The most notorious of these incidents has been that of Equity Funding, in which dummy records were created and stored on a computer system to pump up the "net" worth of the company.

This event, however, was but one of the occurrences. For the period between 1964 and 1972, the Stanford Research Institute has noted a total of 76 separate cases of sabotage, theft, copying data, tampering, masquerading, and fraudulent activities. Of these, 61% were cases of theft and tampering with data alone.

As an indication of the already expanded use of data banks and other information storage and retrieval systems, one has only to look around him. Figure 10.1 gives an idea of the vastness of this use for only a few selected agencies.

As files such as these are expanded and new ones created, the necessary considerations for keeping the data as well as the system that manages it secure must be incorporated in any EDP system.

| FILE MAINTENANCE AGENCY | NO. OF FILE SUBJECTS |
|---|---|
| Defense Department files | |
| Names of persons exposed to radiation | 150,000 |
| Family housing information system | 465,000 |
| Civilian personnel data bank | 55,000 |
| Defense industrial security programs | 1,600,000 |
| Navy manpower and personnel management information system | 1,400,000 |
| Justice Department files | |
| Civil disturbance file | 13,000 |
| Organized crime intelligence unit | 200,000 |
| FBI's National Crime Information Center | 95,000 |
| Other Government Agencies files | |
| National Driver Registration Service | 2,600,000 |
| Passport applicants of law enforcement interest | 240,000 |
| Banking Industry | |
| Bank of America individual accounts | 14,000,000 |
| Bank of America personnel files | 41,000 |
| Commercial Report Agencies | |
| TRW Credit Data | 30,000,000 |
| Insurance Companies | |
| Mutual of Omaha - applicant health recordc | 8,500,000 |
| Mutual of Omaha - benefit history files | 5,000,000 |
| Mailing List Companies | |
| R. L. Polk & Company names and addresses on file | 200,000,000 |
| College and Universities | |
| University of Maryland Personal & demographic records | 158,000 |
| Admission records | 131,000 |
| Accounts receivable from students | 60,000 |

FIGURE 10.1

## Provisions for Security

Basically, system security is the protection against the accidental or intentional destruction, disclosure or modification by a person who is unauthorized to do so.

Providing for this security can be thought of as a threefold project. First, proper management of the computer facilities is a must. A part of the reason the Equity Funding scandal succeeded is that there was no overseer of the company's programmers. Several programmers were given the initial assignment at Equity of generating model policies for the company. This included creating fictitious records as a part of the models. These modelled records were then sent to other programmers who were unaware that they were mere models, and the records were processed as though they were actual data. In a properly managed plant this could not have been possible.

In addition to the appropriate controls on the workers, care must be taken in deciding who is authorized to access a computer system, including its data storage. This encompasses the installation and maintenance of physical provisions for securing a computer system, which is the second of the three measures.

Some measures for material security include barriers preventing entrance to the actual computer area. Locks, gates, and alarms are already in use, particularly in applications where safety and security were a major concern even BEFORE the installation of EDP systems. Nowadays, restricting entry to a system involves not only such measures, but it incorporates the employment of guard personnel to check ID badges and oversee the use of the system to prevent any misuse.

Devices that were originally designed to prevent accidental data destruction now play at least a minor role in security. Magnetic tape, for example, utilizes a write-lock ring to prevent writing when the ring is removed. Similarly, most Disk Operating Systems, as well as those using other system resident devices, have WRITE LOCK or WRITE ENABLE switches that control the function permitted on that peripheral device.

The final category of safeguarding a system is through the application of software to monitor access to the system. Such software can, of course, be totally hardware independent, or it can function with peripherals designed expressly as protection devices.

Peripherals of this sort are primarily devoted to uniquely identifying a user in order to permit or deny access to the system.

Systems already in use check punched or magnetic characters on a special card, such as those employed in the on-line operations just implemented for Master-Charge. In addition, there has been early research in detecting patterns in signatures, voiceprints and fingerprints. Measuring the length of a person's fingers, supposedly as identifiable as fingerprints, has drawn some interest.

Naturally, the control of similar devices could be granted to system software of the right variety. At present such programs already hold a protection function. In telecommunications environments, some Input/Output Control Systems are responsible for encrypting data prior to transmission. For the most part, this encoding is done by adding/subtracting a random key number to the data at the transmission point. Upon reception, the same key number is subtracted/added to yield the original data. While such a key number algorithm can theoretically be broken, it provides a degree of protection in that only sender and receiver really know the key. To prevent accidential disclosure, the machine itself can be programmed to perform the encryption.

Monitors in timesharing systems further serve in identifying users and in recording the essentials of a users account (time used, cost and the like). When a user attempts to log onto a system, the supervisor usually calls a routine that checks a master file for the identifier, or user number. If it is a valid number, the user's account is checked to see if his password is valid and his account is not overdrawn. If these checks are all right, the user is permitted to continue. Where certain devices require serial processing and are protected by the use of passwords, a similar search routine is called so the monitor can deny or permit access.

A splendid example of such file protection exists by considering the use of protect (or access) codes. The PDP 11/20, manufactured by Digital Equipment Corporation, utilizes the protect codes as outlined in Figure 10.2 and demonstrated in 10.3. The directory shown in 10.1. shows the files, their lengths, creation dates (in this case, the dates are default dates for the system), and the access codes for the disk area with a user identification code of (20,20). The protect code for the PDP is a three digit octal number in which the 6th and 7th bits indicate functions permitted the owner, and the bits 0-5 denote functions allowed other users using (20,20). The chart in Figure 10.2. explains the details of choosing a code to be assigned a file.

| 7th BIT | 6th BIT | 5th BIT | 4th BIT | 3rd BIT | 2nd BIT | 1st BIT | 0 |
|---|---|---|---|---|---|---|---|

OWNER USER GROUP OTHERS

| OCTAL NUMBER | FUNCTIØNS PERMITTER USER<br>DELETE | <br>WRITE | <br>READ | <br>RUN |
|---|---|---|---|---|
| 0 | YES | YES | YES | YES |
| 1 | NO | YES | YES | YES |
| 2/3 | NO | NO | YES | YES |
| 4/5 | NO | NO | NO | YES |
| 6/7 | NO | NO | NO | NO |

FIGURE 10.2

```
DISK  (20,20)

DIRECTORY DKØ:  (2Ø,2Ø)

Ø1-Apr-74                                      CREATION DATE

RRFLIB.OBJ      26     16-JAN-7Ø    <233>
MEBLIB.OBJ      24     17-JAN-7Ø    <233>
BAJØ7 .OBJ      33     16-JAN-7Ø    <233>
GLORIA.OBJ       8     17-JAN-7Ø    <233>
KSR   .OBJ       1     17-JAN-7Ø    <233>
GLORII.OBJ       8     19-JAN-7Ø    <233>

TOTL  BLKS:    1ØØ
TOTL  FILES:     6
                                               PRØTECT CØDE

FILE NAME
```

FIGURE 10.3

## Security Check Lists

Securing a computer system is one of the main concerns for management. A number of precautions to increase safety of organizations that rely heavily on computers are often overlooked. A system can never be 100% secure but certain precautions may be listed that should be examined to determine the security of a computer system. The following checklists were completed by DCF Systems Ltd., 74 Victoria St., Toronto, Canada, and have appeared in various issues of COMPUTER WORLD magazine.

### I. ACCESS CONTROL

1. Have a single entrance to the operations area monitored by the receptionist or keep it locked.

2. Install a key lock, a cipher lock or a badge-operated lock on the door to the operations area.

3. Issue badges with new encoding and change locks periodically.

4. Identify all keys to the operations area with a registration number, logged in a control book when issued, and marked with the words "Do Not Duplicate."

5. Instruct the operations staff to memorize lock combinations rather than write them on paper to avoid compromising the security measures.

6. Establish a procedure to protect the integrity of the security system if an employee loses a badge or key.

7. Keep all service entrances to the computer center locked after normal working hours, attach entrances to an audible alarm which sounds if any door is opened and inspect all entrances to make sure they are secure.

8. Use sensors to detect magnets and to prevent them from being brought into the computer center.

9. Locate the operations control area just outside the computer room but adjacent to it.

10. Protect the computer input and output areas with a glass partition, a teller's cage or passthrough window.

11. Maintain a log of all deliveries to and pickups from the computer center, showing the date and time, description of the materials and employee authorization.

## II. INPUT AND OUTPUT CONTROL PROCEDURE

1. Establish a procedure for submitting jobs to the computer room, such as having users fill out a job request card containing their name and department, the account number to which the job will be charged, a time estimate of the job, and operator instructions.

2. Delegate to an I/O control clerk responsibility for:

   a. Recording receipt of input data, as well as input control totals, in a control log.

   b. Insuring that corrections are marked off in a log when they are re-entered into the system.

   c. Insuring that rejections from the processing cycle are entered in an error log.

   d. Expediting important jobs.

   e. Assuring an effective and efficient work flow into and out of the computer room.

   f. Reconciling output control totals to input totals.

   g. Checking the quality of output reports.

   h. Distributing reports to authorized recipients.

3. Retain original input documents in some form to serve as backup or as proof in the case of fraud, and store them in a secure location.

4. Store blank forms in a secure location before they are used, and establish procedures to control their usage and to record destroyed copies of sensitive forms such as checks.

5. Maintain additional supplies of forms used in critical jobs, so that operations will not be delayed after a disaster while waiting for a new supply.

6. Distribute output reports quickly after completion, and store them in a secure location until they can be distributed.

7. Periodically review and update lists of authorized recipients of output reports.

8. Establish stringent controls on the method of distributing sensitive reports to other geographical locations.

9. Retain copies of key output reports as backup either in their original form or on microfilm.

## III. LIBRARY PROCEDURES:

1. Limit access to the library by keeping the door locked at all times or by assigning a full-time librarian, or an operator after normal working hours, to monitor access.

2. Prohibit programmer access to production tapes on disks or documentation without written authorization.

3. Maintain a log of programs and data files in the library.

4. When not in use, store all programs and data files in a locked safe or cabinet whose locks or combinations are changed periodically.

5. Instruct the librarian to release programs and files only when computer runs are authorized and scheduled.

6. Have the librarian record the return of programs and files after computer runs, thereby providing a record of their usage and a cross-reference between tapes or disks and computer runs.

7. Establish special stringent procedures for obtaining sensitive files from the library.

8. Use tape reels and disk packs which have special labels which can be detected by a sensor in order to prevent theft.

## IV. COMPUTER ROOM OPERATING PROCEDURES

1. Consider using special printers or output terminals to handle the printing of sensitive data, such as salary data or market forecasts, and consider having a representative of the user department and the computer room shift supervisor present.

2. Supervise computer operations at all times to insure that no operator can use your computer equipment and time to run jobs for outsiders without your knowledge.

3. Establish procedures for preauthorization of all overtime use of the computer equipment, programs, tapes and disks.

4. Insure there are operating instructions for every job in the computer center, that they are properly updated when changes are made, and that they are frequently reviewed by the shift supervisor to insure that standards are being maintained.

5. Clearly document rerun procedures for each system to reduce the possibility of operator error.

6. Schedule all computer processing for operational systems to reduce peak workloads and thereby reduce the risk of operator error.

7. Delegate to a production scheduler or controller the responsibility for dispatching jobs to the computer room, recording which equipment is used, what time the job is submitted and what time it is completed, and for following up data not yet received when a job is scheduled.

8. Record the progress of jobs through the computer room on a run control log showing estimated versus actual times, reruns, errors, restarts and interruptions.

9. Insure that all systems provide a set of standard messages and instructions to the operator under various conditions, thereby reducing the requirement for the operator to make decisions.

10. Establish procedures to protect the computer during off-shift hours, such as: locking computer room doors, having security guards check all cabinets and doors to make sure they are locked, giving guards a list of authorized off-shift personnel, keeping a log of off-shift computer users, recording meter readings before and after off-shift hours.

## V. DATA SECURITY

1. Screen requests for new applications to determine their legitimacy, and to determine if continual use of the system by a given user yields more information than he is entitled to have.

2. Use techniques such as verifying key input fields, balancing input fields to predetermined totals, using computer-generated input, and writing edit routines to check the accuracy and completeness of data.

3. Design system with adequate internal program controls to insure the accuracy of data and the correctness of computations.

4. Maintain counts of the records on file before and after processing, and reconcile file control totals for individual computer runs with transaction and input control totals.

5. Compare output control totals with predetermined totals to insure that no records were lost during processing.

6. Design systems with exception reports of transactions rejected by the system.

7. Design systems with helpful console error messages.

8. Insure that programmed controls are not being overridden, by performing periodic audit tests of the system.

9. Provide the internal audit group with a copy of all operational program documentation for computer systems and notice of all system changes.

10. Maintain an inventory of all tapes, disk files, programs and supporting documentation; update it regularly as system changes are made; and audit the inventory periodically.

11. Keep periodic tests of production programs, program dumps or traces and transaction journals to provide an audit trail of computer systems.

## VI. VITAL RECORDS PROGRAM

1. Have the internal audit department determine the specific importance and sensitivity of all records.

2. Assign responsibilities to assure that information which is necessary to reconstruct the vital records of the organization is always up-to-date and readily available.

3. Have the internal audit department designate the files to be considered vital to the organization and, therefore, to be protected by:

> On-site protection, such as three-generation backup for magnetic tapes, vaults or special filing cabinets.
>
> Duplication of records onto media such as paper, magnetic tape or microfilm.

4. Maintain an inventory of vital information needed to recreate data and operate a backup facility (for example, vital applications, equipment configuration, engineering change levels, operating system and version, program library, data files, programs and program documentation, operating documentation, supplies and other materials required for immediate recovery processing).

5. As new systems are created and existing systems altered, create new back-up for these programs and the associated documentation promptly, and store it at the backup location.

## VII. PROGRAMMING CONTROLS

1. Supervise your systems and programming personnel in the careful design, testing and maintenance of programs.

2. Establish standards for designing, programming, testing, documenting and operating systems and periodically review programs and documentation to ensure that standards are being met.

3. Establish a procedure for authorizing all program changes and formally approving the changes before they become operational.

4. Keep a record of all changes to programs, the reasons for the changes, dates of the changes, the authorization, their effects on the program and cross-reference to other programs that might be affected; notify users of the changes; and have management review this change record periodically.

5. Establish controls to ensure that the review and approval procedures are not being bypassed, for example:

   a. Control final program assemblies so that only the approved program is installed.

   b. Periodically compare disk programs to control copies on another medium.

   c. Include with output a listing of the job control language to ensure that an unauthorized program has not been executed.

   d. Keep a tight control over the access to, and use of, programs and files by systems analysts and programmers.

   e. Review the software library periodically to ensure that a complete set operating documentation exists for all applications.

## VIII EQUIPMENT REPAIR

1. Review statistical records of equipment utilization, job accounting and on-line activity, such as input and output volumes, processing and turnaround times, in order to anticipate overloading and to ensure acceptable operating performance.

2. Consider monitoring computer usage by separate console in a secure area.

3. Run periodic tests on equipment to spot malfunctions; for example, before critical jobs are run.

4. Follow the manufacturer's recommended environmental specifications and schedule of preventive maintenance for the equipment.

5. Clean or change air conditioning filters periodically as specified by the manufacturer. Use Underwriter Laboratories Class 1 filters.

6. Clean magnetic tapes and drives periodically as specified by the manufacturer. Use a nonflammable solvent.

7. Note defective areas on tapes and disks encountered during computer operations; keep a log of such defects and use a tape tester periodically to identify defects on tape.

8. Record each end-of-job on the console log along with the operator's comments as to successful completion or any unusual event which occurred.

9. Record all hardware and software "crashes", stating the reason, the time, the remedial action, whether a core dump was taken and who made the entry.

10. Retain the console log sheets for at least one year.

11. Instruct the senior shift supervisor to review the console log sheets daily to detect improper operating procedures, suspicious reruns or unauthorized runs.

## Data Securing Engineering

As the utilization of automated data systems increases, there will be an increasing concern for "intruder interactions" and the engineering and programming capacity to deal with it. (5) To stave future episodes of Equity Funding, auditing and control programs are being developed. Cullinane Corporation has already marketed an EDP Auditor and a Culprit package that uses a series of monitor programs to control access to their systems.

To prevent physical tampering, basic designs have been altered in a few cases. The Basic Computing Arts, Inc. of Palo Alto, California, markets a system comprised of a minicomputer and a larger host computer (an IBM 360 or 370). This Data Sentinel has the minicomputer sealed in a "tamper-proof" case and tapped with alarms and a single relay to the host. In this case, the minicomputer peforms the guardian functions of user identification and checking the legitimacy of all software. One of the singular applications of this system, installed at the Crocker National Bank in San Francisco, authenticates software by a check sum algorithm and comparing this sum to a stored total input when the software is first implemented. If the two sums check, the program is permitted to be executed by the host computer.

One of the systems now lauded as extremely secure did not even begin as a security concern. Honeywell's MULTICS system, developed in conjunction with MIT and the Bell Labs and now available on the Honeywell 6184, has a file structure that provides the added security now hailed. In this system files are divided into segments and arranged hierarchically in concentric circles. The innermost rings, containing the monitor and vital system software, is accessible only by the MULTICS system itself. Outer rings are available for users. By selecting the appropriate access code (and thereby the segment) a user determines the degree of file protection desired.

Advancements such as these will no doubt continue; however, careful analysis of a systems needs is necessary since costs increase as security measures are implemented. For example, the MULTICS system, including CPU and a number of peripherals, can cost upwards of $1.5 million. Furthermore, as checks of users to determine accessibility increase, the efficiency of a system is decreased due to the time necessary for table and file searches. In addition, with the implementation of federal laws governing data protection, file sizes will no doubt increase, thus requiring more storage devices. Soon, files on persons (data banks, credit bureaus, etc.) will be forced to contain source listing, creation dates, list of those eligible to access that file, and other related information. It has been estimated that, considering such required information and a probable growth in numbers of files of 10%, the files on people in existence would double in size in only seven years.

Considering the present clamor over protecting data systems, it is hardly necessary to expound on its importance. Effective data security engineering is and will be of great concern to all who use EDP systems.

# BIBLIOGRAPHY

1. Computer Abstracts, London, Technical Information Company, 1973, Volume 17, No. 10.

2. Davis, Ruth M., "Privacy and Security in Data Systems," Computers and People, Volume 23,3, March 1974, pp. 25-27.

3. Digital Equipment Corporation, DOS/BATCH File Utility Package (PIP) Programmers Handbook, Monitors Version V09, August 1973, pp. 3-12.

4. Feistel, H., "Cryptography and Computer Privacy: protecting personal data banks," Scientific American, 228, May 23, 1973, pp. 15-23.

5. "Outwitting the Computer Swindler," Computer Decisions, Volume 5, No. 9, September 1973, pp. 12-16.

# CHAPTER XI

## COMPUTER CRIMES

Cropping up with disturbing frequency is a new brand of criminal specializing in theft by computer. The computer, in the hands of skilled operators bent on theft, fraud or sabotage has become a major crime problem for business and government. In fact, experts believe that illegal use of computers is the fastest growing type of white-collar crime. Computer-related crime is difficult to detect. It is more profitable, less dangerous, and easier to commit than many other kinds of criminal activity.

The range of crimes made possible by computers runs from simple embezzlement to destruction of official information stored on data banks. Computer criminals have stolen trade secrets, valuable equipment and millions of dollars from banks, private companies and government agencies. Also, computers make excellent partners in crime because they do exactly what they are told and can be programmed to cover their tracks completely. Types of fraud most easily accomplished with a computer include disbursement, inventory and payroll fraud.

### Disbursement Fraud

Disbursement Fraud has accounted for more embezzlement losses than all others. This scheme is quite simple, "your company is fooled into paying for goods and services that it did not receive or did not receive in full measure."

A perfect example of this scheme is the Equity Funding Scandal where over a million dollars was embezzled. This was the biggest insurance swindle and one of the biggest swindles of any in history. In one of its subsidiaries, 58% of the 97,000 policies listed on the books were nonexistent. Also, on Wall Street, Equity Funding's more than 7,000 stockholders were in danger of losing at least $114 million; based on the deflated price of their stock. The greatest fact of this incident is that neither standard auditing practices nor Wall Street analysis was sophisticated enough to detect it. Equity Funding's fraud went to the extent of programming fake death certificates into the computer, to cover the fraud trail further. Investigators found an office with 10 employees whose job was to simply forge documents.

The common characteristics in most disbursement frauds is that the embezzler has to have inside help, someone who has access to the accounting files and is able to manipulate them. In other words one must be a responsible and trusted employee to make this scheme work.

## Inventory Fraud

Inventory Fraud is generally easier than disbursement fraud since it is easier to convert goods to cash than it is to cash fraudulent checks. Computerized inventory systems lend themselves to penetration for two basic reasons: they account for a large amount of materials, and the controls on access systems are normally lax.

To demonstrate that size is of no factor, consider a recent Boxcar theft as an example. Employees of Pen Central Railroad allegedly manipulated the inventory files to shuttle out 217 boxcars. The employees altered the inventory files to reflect that the cars were either scrapped or wrecked when they were actually shipped to another company's yard and repainted.

Sales Manipulation

Sales manipulation is the manipulation of shipments, sales, and billing procedures. The embezzler confuses his company into:

shipping a product to a customer without sending the bill,

shipping one thing and billing the customer for something else,

billing a shipment at the wrong price,

granting improper credits or adjustments on returned or damaged products,

manipulating the sales commission allowances, and discounts on merchandise shipped.

An example of this type of inventory fraud is the Pacific Telephone Company rip-off. Twenty-one year old Jerry Neal Schneider broke the security code of Pacific Telephone and was able by Touch-Tone telephone to place large orders of equipment. Investigators found $100,000 in stolen equipment and said that Schneider was involved in the thefts for 5 years. Schneider served forty days in jail, and is now into the business of advising clients on how to prevent computer thefts.

The common characteristic of most inventory frauds is that almost every embezzler sets up his own legitimate company to sell the merchandise.

A suggestion for preventing inventory fraud is to have a complete personnel department check of employees and to juggle responsibilities between employees. A complete security check on the ethics and responsibilities of the employees should be conducted. This is costly but not as costly as illegal entry into your system.

Payroll Fraud

Payroll fraud is the act of padding the payroll with nonexistent employees and/or leaving former employees on the payroll after termination.

An example of this occurred when an employee at the welfare department entered fraudulent data into the payroll system and stole $2.75 million. He entered a fictitious work force identified by fake social security numbers. The fake employees were processed and each paid. The conspirators were uncovered by accident when police discovered a batch of over a hundred fraudulent checks in a car. The companies had ~~to be~~ infiltrated from within. Trusted employees were the embezzlers and had access to manipulate the files.

For a larger company it is hard to keep track of all of the part time employees that they hire. A responsible personnel department would be greatly needed in this case. The department must keep thorough files on all employees and if extra help is hired they must be thoroughly recorded into the system. The delivery of the checks to the employees should be orderly and security should be tight. When picking up checks, employees should be required to identify themselves and sign for their checks. All checks should be accounted for when they are processed and delivered to the correct person. As further examples of computer crime, consider the following:

A chief teller at a branch of the Union Dime Savings Bank in New York was charged with embezzling 1.5 million dollars from the bank's deposits. He was caught when a bookie was raided and it was found that the teller had been gambling up to $30,000 a day. He was making $11,000 a year at the bank.

An insurance company employee heard that he was going to be laid off, and programmed the computer to automatically erase the payroll tape when his employee identification number was dropped, resulting in a huge expense for the company.

In another case, in Salinas, California, an accountant embezzled $1,000,880 from his company by recording higher payments for raw materials in the company computer than the company actually paid. He arranged for the computer to place the excess cash in his own dummy companies, and then programmed it to advise him how much money he could withdraw from those companies without raising suspicion. He was caught six years later when greed drove him to start making withdrawals of $250,000 a year.

A Washington, D.C., man takes the prize for elegant and successful simplicity. He pocketed all the deposit slips at the writing desks of the Riggs National Bank and replaced them with his own electronically coded forms. For three days, every customer who came in without a personal slip and used one of the "blank" forms was actually depositing money into the thief's account.

## Computer Criminals

Now let's take a look at what sort of people are involved in computer crimes. Donn B. Parker of Stanford Research Institute says that they are young and intelligent, usually between 18 and 30 years of age. They usually are not professional criminals. They are outwardly loyal and trustworthy and have never been in trouble with the law. They were in trusted positions before they committed their crime and are highly motivated and seem to be challenged by the prospect of beating a complex system and overcoming protective devices, as much as by any monetary reward. Many computer criminals strongly believe that any information found unprotected in a computer is in the public domain and can be utilized by anyone who discovers it. Others rationalize that stealing from large corporations is not really a crime. Knowing what the criminals are like has not solved the problem. Mr. Parker says that spotting the crook before he commits a crime is next to impossible.

For computer experts, this is the most disturbing aspect of the computer crime wave, that most of the culprits have been caught by accident. What makes these criminals so hard to catch is the extraordinary complexity of the computer programs themselves. The only sure way of detecting manipulations of such programs would be to devise another computer program capable of auditing the machines' internal operations. Unfortunately, no one in computer research today knows how to write such a program. Mr. Parker guesses that the ratio of undiscovered to discovered crimes may be on the order of a hundred to one.

For the time being, computer companies are restricted to improving the security systems inside their computers. Honeywell has devised a scheme called MULTICS, that restricts the total amount of information available to any individual user of a computer system. In 1972, IBM began a $40 million, five-year program to improve its data-security systems. The National Security Agency and the Advanced Research Projects Agency of the Department of Defense are conducting independent research on protecting military and classified data stored on federal computers. Moreover, the problem has given rise to a peripheral data-security industry made up of over 20 private companies. Computer manufacturers are trying to develop systems that will be more resistant to manipulation. The consensus of the experts seems to be that it is possible to design penetration-proof operating systems, but that they are not likely to be commercially available in large systems in less than four years, at the earliest. Then they will have the problem of deciding what to do with the existing systems. Some advocate the use of separate minicomputers and software as gatekeepers, to handle the chores of user identification and access control. The main purpose is to remove these sensitive functions from the intricate maze of a main operating system. A number of companies are working on devices that will recognize personal insignia such as the shape of a hand or the unique motions an individual makes as he signs his name. While some companies are showing more and more interest in these new developments, other manufacturers contend that it's pointless to bring out systems capable of resisting sophisticated attack unless their customers adopt better physical security measures in their own installations, as well as better screening of computer employees. We approach the problem of computer security in more detail in the next chapter. However, a brief list of computer crime prevention tips are to:

> Limit the number of employees who have access to the data stored in the computer.
>
> Switch computer users frequently to different machines and programs.
>
> Separate computerized check-writing operations from the departments that authorize checks.
>
> Use secret passwords to gain access to different computer programs and change the passwords often.
>
> Be sure the computer is programmed to sound an alert automatically when repeated attempts are made by computer users to enter incorrect passwords.
>
> Adopt procedures whereby those using the system have to enter their names or initials each time they have access to the system.
>
> Random monitoring of computer transactions.
>
> Provide detailed accounting of computer-usage time. If a job begins to take twice as long, analysis may indicate it is because the program has been modified to tamper with data files.

A last approach for controlling computers crime is for companies to report the crimes and for the law to administer harsh punishment. Some banks and companies admit that when an incident is discovered, the corporate victims try to avoid the embarrassment and loss of confidence that publicity might bring.

About 85% of detected frauds are never brought to the attention of law-enforcement people. What often happens is that the offender, once detected, is required to make restitution and then leave - sometimes even getting severance pay and letters of reference to speed him away.

Without adequate punishment the computer criminals will never be stopped. The electronics expert in Los Angeles, having served 40 days for his thefts from Pacific Telephone and Telegraph, is now back in business, advising clients on how to secure their computers against illegal entry.

# BIBLIOGRAPHY

(1) Alexander, Tom, "Waiting for the Great Computer Ripoff", Fortune, July 1974, pp. 143-150.

(2) "Conning by Computer," Newsweek, April 23, 1973, pp. 90-91.

(3) "Key-Punch Crooks," Time, December 25, 1972, p. 98.

(4) "On the Coast-to-Caost·Trail of Equity Funding," Business Week, April 21, 1973, pp. 68-72.

(5) "Spotting the Computer Crook", Science Digest, October 1973, p. 39.

(6) "The Computer Thieves," Newsweek, June 18, 1973, pp. 109-112.

(7) "Using Computers to Steal - Latest Twist in Crime," News and World Report, June 18, 1973, pp. 39-42.

# COMPUTER DATA STORAGE

(An Example)

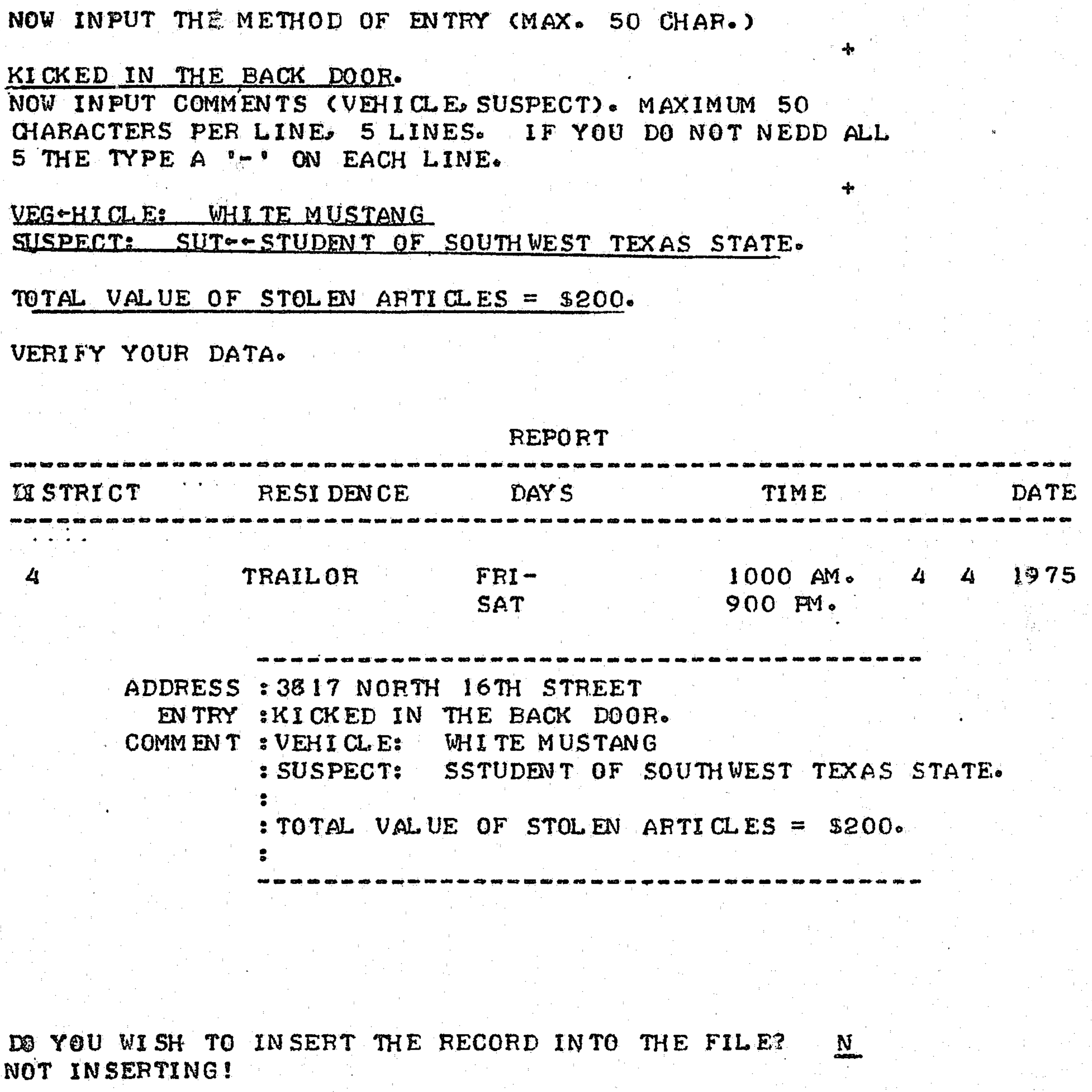
One of the crime analyst's biggest jobs is the organization of data for analysis. The electronic computer may be of most use to the analyst as a data storage and retrieval system. By use of the speed at which data can be recovered from the storage devices and by using the programming languages of the computer to sort information prior to print out, the analyst can save many hours of "clerical" work and concentrate on analysis and interpretation.

Figure 1 is an example of how a computer can "converse" for input of data on a burglary. The information typed by the person entering data is underlined. Keep in mind that a computer programmer is responsible for the conversation. We do not want to give the impression that the computer is really "talking". Notice how easy it is to enter a report to the computer's file. In practice, a simplified code similar to those previously discussed, would most probably be used in order to speed up the data entry.

Figure 2 shows how a computer can sort information out of a file, based upon input from the analyst. Again the entry is conversational and easily understood.

```
BASIC
GO:
OLD OR NEW FILE:     POL←←←OLD
FILE NAME: POLICE
FILE IDENTIFIER OR "RESTART": 7928
 COPIED FILE   POLICE
READY
READPF 4016 POLFILE
 COPIED FILE   POLFILE
READY
RUN
POLICE RECORDS:  VERSION 041775
PLEASE ENTER THE CODE TO ACCESS THIS PROGRAM.      114
DO YOU WISH TO ADD A RECORD? Y
POLICE RECORDS:  INSERTING!
INTO WHICH DISTRICT DO YOU WISH TO INSERT THE RECORD (1-8)? 4
INSERTING INTO DISTRICT  4 .
PLEASE ENTER THE TYPE OF RESIDENCE AS FOLLOWS:
               1.  APARTMENT
               2.  SINGLE FAMILY HOUSE
               3.  MULTI-FAMILY HOUSE
               4.  TRAILOR
4
ENTER THE LOCATION (MAX. 1 LINE).
3817 NORTH 16TH STREET
ENTER THE DAYS OF THE WEEK WHEN THE CRIME TOOK PLACE,
USING THE FOLLOWING CODE:

1.  SUNDAY      2.  MONDAY      3.  TUESDAY     4.  WEDNESDAY
5.  THURSDAY    6.  FRIDAY      7.  SATURDAY

ENTER A TWO DIGIT NUMBER WITH THE FIRST DIGIT BEING WHEN
THE CRIME MAY HAVE STARTED, AND THE SECOND WHEN IT IS
BELIEVED TO HAVE STOPPED.  FOR EXAMPLE,  IF THE CRIME MAY
HAVE OCCURED ANYTIME BETWEEN MONDAY AND FRIDAY, THEN THE
CODE WOULD BE AS FOLLOWS:      26
67
ENTER THE TIME WHEN THE CRIME MAY HAVE BEGUN AND THE TIME
WHEN IT STOPPED (MILITARY TIME). EX: 1700, 1900
1000, 2100
ENTER THE DATE WHEN THE CRIME BEGAN IN THE FOLLOWING FORM:
               EXAMPLE:  DD,MM,YYYY
                    14,9,1954 WOULD BE SEPT. 14,1954.      4,4,1975
```

Figure 1



```
NOW INPUT THE METHOD OF ENTRY (MAX. 50 CHAR.)
                                                    +
KICKED IN THE BACK DOOR.
NOW INPUT COMMENTS (VEHICLE, SUSPECT). MAXIMUM 50
CHARACTERS PER LINE, 5 LINES.  IF YOU DO NOT NEDD ALL
5 THE TYPE A '-' ON EACH LINE.
                                                    +
VEG←HICLE:  WHITE MUSTANG
SUSPECT:  SUT←←STUDENT OF SOUTHWEST TEXAS STATE.

TOTAL VALUE OF STOLEN ARTICLES = $200.

VERIFY YOUR DATA.


                                  REPORT
----------------------------------------------------------------
DISTRICT       RESIDENCE      DAYS          TIME               DATE
----------------------------------------------------------------

 4             TRAILOR       FRI-          1000 AM.    4   4   1975
                             SAT           900 PM.

               ----------------------------------------
      ADDRESS :3817 NORTH 16TH STREET
        ENTRY :KICKED IN THE BACK DOOR.
      COMMENT :VEHICLE:  WHITE MUSTANG
              :SUSPECT:  SSTUDENT OF SOUTHWEST TEXAS STATE.
              :
              :TOTAL VALUE OF STOLEN ARTICLES = $200.
              :
               ----------------------------------------



DO YOU WISH TO INSERT THE RECORD INTO THE FILE?   N
NOT INSERTING!
```

Figure 1 (Continued)

```
DO YOU WISH TO ADD A RECORD? N
DO YOU WISH TO WITHDRAW INFORMATION?   Y
WE ARE CURRENTLY ABLE TO SORT RECORDS ON 7 ITEMS.
YOU MAY SORT ON JUST 1 OR YOU MAY SORT ON ALL 7 OR
YOU MAY SORT ON ANY NUMBER IN BETWEEN.
WHEN I ASK IF YOU WISH TO SORT ON A CERTAIN ITEM PLEASE
RESPOND WITH YES OR NO.
DISTRICTS?N
RESIDENCE?N
DAYS OF THE WEEK?   Y
ENTER THE CODE AS FOLLOWS:
1. SUNDAY       2. MONDAY       3. TUESDAY      4. WEDNESDAY
5. THURSDAY     6. FRIDAY       7. SATURDAY
INPUT A TWO DIGIT NUMBER.  EX. 26 = MON-FRI        34
TIME?    N
DAY OF THE DATE?    N
MONTH OF THE DATE? N
YEAR OF THE DATE?   N
INPUT OF INFORMATION COMPLETE!


                              REPORT
------------------------------------------------------------
DISTRICT      RESIDENCE      DAYS          TIME          DATE
------------------------------------------------------------

 1           APART.         SUN-          1 AM.      1  1  1975
                            SAT           1200 PM.

                   ---------------------------------------
      ADDRESS :516 BROADWAY, CORPUS CHRISTI TX. 78415
        ENTRY :BROKEN LOCK ON THE SIDE DOOR.
      COMMENT :VEHICLE:  1968 FORD CONVERTABLE
              :SUSPECT:  2 WHITE MALES.
              :THE PEOPLE WERE ON VACATION.  THEIR NEIGHBORS
              :SAW TWO MEN LOOKING AROUND THE YARD ABOUT
              :NOON THE DAY BEFORE.
                   ---------------------------------------

 2           S HOUSE        MON-          1200 AM.   2  2  1975
                            FRI           1200 PM.

                   ---------------------------------------
      ADDRESS :5209 LAMP POST LANE SAN MARCOS.
        ENTRY :BROKEN WINDOW
      COMMENT :VEHICLE-  UNKNOWN
              :SUSPECT-  UNKNOWN
              :
              :-
              :REFER TO REPORT 24464 FOR DETAIL INFORMATION.
                   ---------------------------------------
THAT IS ALL THE RECORDS!
END -- POLICE RECORDS
DO YOU WISH TO ADD A RECORD? N
DO YOU WISH TO WITHDRAW INFORMATION?    N
READY
```

Figure 2

END