Please return to
William F. Friedman

Files

~~TOP SECRET~~

1st Item
Dr. 44

~~TOP SECRET~~

MACHINES IN THE SERVICE OF CRYPTANALYSIS

Presented 28 September 1954

to

Director, NSA, and his Staff

by

The Machine Division, NSA-82

~~TOP SECRET~~

Every one of us, I am sure, will agree that the greatest asset of this Agency is the skilled and experienced personnel which it proudly claims. The Machine Division is in a unique position to realize the magnitude of another great asset -- the electrical analytic machines which it operates for the Agency. By the most simple comparisons, this Agency is a giant in the use of machines. The electric power consumed by our analytic machines would supply about 1600 average homes; the 100,000 vacuum tubes which make our machines work are the rough equivalent of 5,000 TV sets; this year's budget for rental of about 320 machines from the IBM Corp will be $2 million; we will continue to receive new equipment to be owned outright by the Agency which will lift our long range expenditure for research, design and procurement of over 400 analytic machines to approximately $75 million.

These are big figures. But because of them, this Agency is equipped to do, and is doing a big job.

NSA 82, the Machine Division within Production, is proud to present the story of what these machines are and how they are used. We acknowledge that the leadership, stimulation and assistance of many organizations have made our present machine position possible. You analysts and statisticians in the operating organizations discovered and defined the needs which these machines fill. You engineers and mathematicians in Research and Development helped to design our machines and describe their use. You members of staff entities have assisted in the procurement of these expensive tools, and the manpower, the electric power, and the air conditioning required to keep them in operation.

This morning we are going to talk about the machines we have and some of the uses we make of them. Our mission is to support the analytic effort of this Agency. In order to explain how we do this we will occasionally have to trespass into the territory of cryptanalysis. The details and ramifications of our machines and the jobs we do are numerous and complex. Therefore I shall oversimplify, and I ask the indulgence of those of you whose intimate knowledge of detail is far greater than will be revealed here.

I will present facts about the speeds of machines, and will compare them to the speed of hand processes. I admit that I will not tell the whole story, for behind the performance of any machine there are numbers of people whose work is essential, but does not appear in a description of the functions of the machine. There are over 150 engineers and technicians who keep the equipment in running order, and seek to improve it by modifications.

There are 200 card and tape punchers who prepare your data to be fed into machines. Without these vital functions your jobs would not get started, and the machines would not run. The contribution of these silent partners is more obscure than that of the operators who actually run the machines, and of the methods people and programmers who in effect tell the machines how to do your jobs. Altogether, I am speaking of a division of 800 people. engaged in putting some mighty exacting jobs on some quite complex equipment.

We will first examine IBM equipment which forms the historical root of machine usage in this Agency. We will discuss in turn the classes of machines peculiar to this Agency -- the comparators, the recognition devices, and some special purpose equipments. We will examine the most modern class, the computers, and conclude with some remarks about the machines of the future.

Very few of us know as a matter of personal experience that in 1932 the Navy Security Group began using standard IBM accounting machines. Two years later the Army obtained similar machines to assist in the arduous task of preparing code books.

The use of machines toward communications intelligence goals quickly became the major emphasis. Here also a great gain was realized since copying and sorting the raw material of cryptograms was just as onerous a duty in 1934 as in 1954, and the people who had to do it were mighty few in number. The COM INT use of standard IBM by both organizations grew from 8 machines in 1934 to over 750 in WW II. At the close of the war the number of IBM units dropped to about its present level of 314, which is probably the strength at which this equipment will continue. When we notice that the speed of machines has increased since wartime days, and that great improvements have been made in the usefulness of some of them, we may not be as curtailed as the figures would indicate. This 20 year long use of IBM in such quantities is a high tribute to the usefulness and versatility of this equipment. The decodes, the organized data, the tools which help analysts with their problems flow out each day in a ribbon of paper which -- if you can bear the comparison -- would reach from Arlington Hall Station along Arlington Boulevard to Memorial Bridge.

The factors which explain and guarantee the continued use of this equipment are its reliability, its availability, and the versatility of a system whose functions are the simple ones:

to record information
to hold it
to sort and rearrange it
to combine it
to summarize it
and to list it in usable form.

And while doing all this a respectable saving of labor over hand methods is achieved.

As an example of one kind of application of standard IBM, let us consider the problem of encoded messages. Many nations rely upon code books to protect their communications. Such systems are as insecure as any substitution system provided there is enough traffic available to an organization which has the skill and the will to read them. NSA has read hundreds of codes. Standard IBM has been the machine tool most used in the job. The contribution of IBM is in accumulating, arranging and summarizing the information about all the code groups which have occurred, and presenting it in usable form. The disciplined imagination of code breakers does the rest as they examine the frequently repeated groups and the patterns which they make, and arrive at the meaning of each group in the code book. The eventual product, through many successive additions to the material for study, is a daily decode, which also may be made by IBM, and which requires only translation to make it an intelligence product.

Unfortunately the cryptographers of many nations are aware that their codes can be compromised thru volume use, and some have taken steps to prevent it. Since the repetition of code groups and phrases is the thing that lets us into a code, all they need to do is suppress those repetitions. One way in which this is done is by applying to each message a key, which is simply a strip of numbers to be combined with the stream of code groups. The code group for PERIOD which might appear 3 times in a message and thus give itself away will now appear as 3 different cipher groups because 3 different key groups fell above it as the message was enciphered.

If a fresh stream of key is used for each message, and if the key has no discernable characteristics, we would never get a look at the code itself, and would never read the system. Very often, however, only a limited amount of key is supplied, and it gets used over and over again, by design or by accident. The messages enciphered by the same key are said to be "in depth". If we can line the messages up properly with respect to the key used to encipher them, we may be able to remove the key and read the messages. Repetitions in the cipher text suggest the way in which the messages should be lined up. Although we do not yet know the key used above each column of cipher groups, we do know that it was the same key, and we will later discuss methods by which the key may be recovered.

At this point I'd like to consider the earlier problem -- how did we get the messages lined up properly in the first place? There are many methods; some involve analytic machines, some do not. When the easier hand or machine methods have failed either to find depth or to establish the unfortunate fact that it is not present, there is usually only one technique feasible. That is to use the machines called comparators. They attack the problem of depth finding by comparing every pair of messages at every possible alignment and counting the coincidences between them. For alignments which have a high level of coincidence of cipher groups or individual characters there is a possibility of depth. For alignments which have a low level of coincidence there is little likelihood of depth. An easy case to consider is that of two messages enciphered by a long strip of alphabetic key. When the messages are lined up in correct relation to each other, the number of coincidences should be as in plain text, about 7%. When they are incorrectly aligned the coincidence should fall to 4%.

By hand, the process would be managed as follows:

1. Write each message out on a long strip of paper.
2. Place the head of the second message under the tail of the first message and count how many letters of one are over identical letters of the other.
3. Slide the second to the left one letter, and repeat the counting operation.
4. Repeat the sliding and the counting operation until the tail of the second message slides off the head of the first message.
5. Examine the record of counts for those which appear significant.

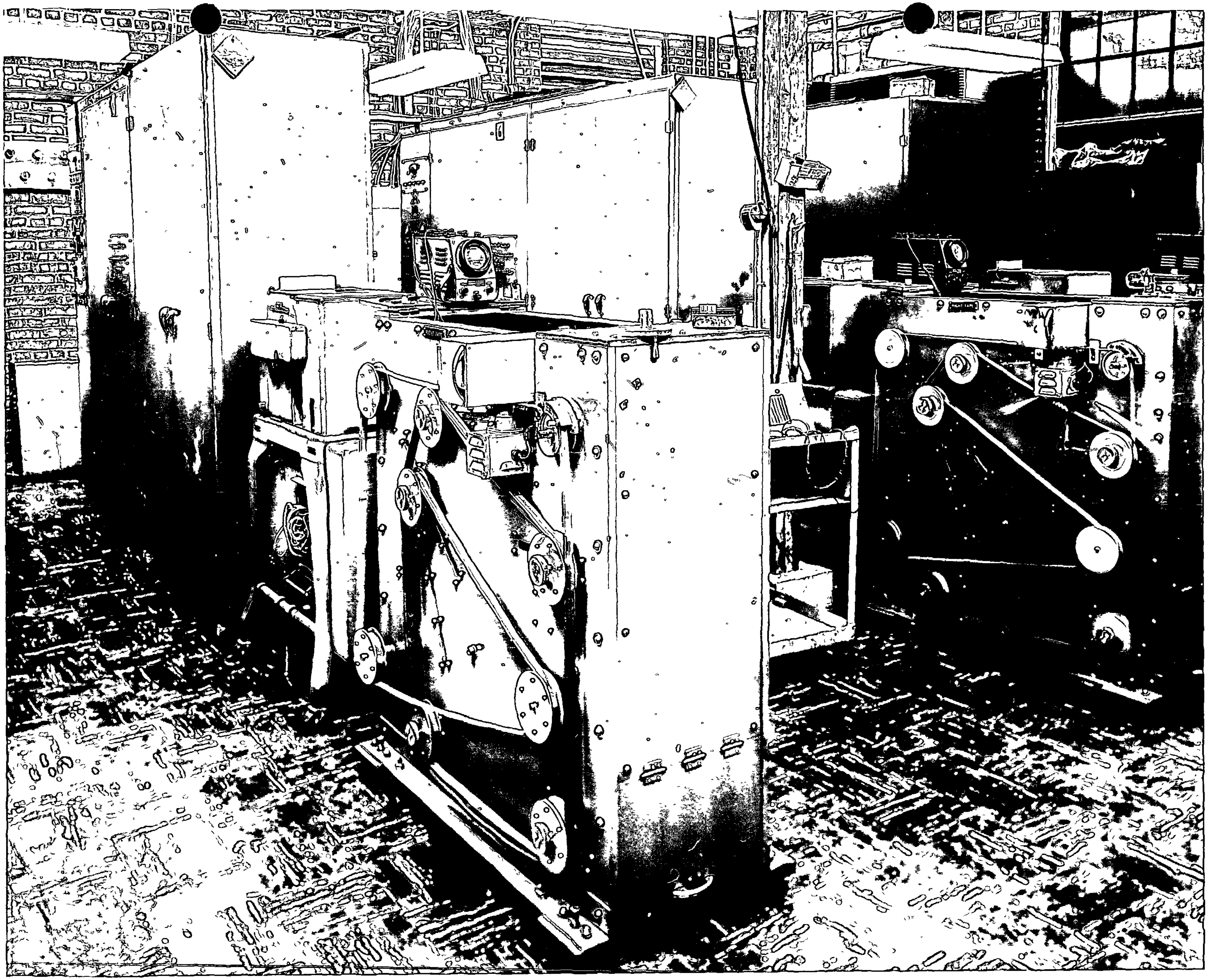
Now, how much work is involved in comparing two 200 letter messages? It is surprising to find that there will be almost 40,000 letter pair comparisons made. How long will this take? Well, if a person took one second to make each letter pair comparison, this would take him about 10 hours.

Now, what happens if a 3rd, a 4th and so on message belongs to the set and must likewise be compared each with every other? A three message set requires 3 comparisons, or 30 hours. A 4th message requires 6 comparisons, or 60 hours. Roughly, the time goes up almost as fast as the square of the number of messages. Unfortunately this is the real condition in cryptanalysis -- the number of messages to be examined is large, and the prospects of immediate success are slim. Still, the job has to be done.

Many years of designing, building and using machines of the comparator type led to a present comparator called the ROBIN, whose function is exactly that of the above problem -- to compare 2 streams of characters and count the coincidences between them. ROBIN handles its messages on punched paper tape, it looks at the characters with photoelectric cells instead of eyes, it performs its counting in electronic counters instead of by tallying. But the important thing is that it does all this at the rate of 50,000 comparisons per second. Thus if we compare one ROBIN machine with people, we would seem justified in saying that it is the equivalent of the work of 50,000 cipher clerks armed with nothing more formidable than strips of paper and a pencil. The ratio is so astoundingly in favor of the machine, 50,000 to 1, that we have entered upon a new and revolutionary era. Such machines do not save labor, they create it. Let me illustrate: Eleven ROBIN machines were used 16 hours a day for a period of 10 months on just one problem. To do the job in the same length of time by hand would have required something like 1 million people. It is not likely that we would have employed so many people for one phase of one problem. We simply would not have done it, and might have gone for years in ignorance of whether or not the phenomenon we searched for occurred in the particular traffic.

ROBIN is but one in a family of comparators. Other members of the family have contributed much to its development and each has been peculiarly useful in its own way.

The 70 MM comparator was the first tape comparator. It was designed and built during the late 30's by Dr. Vannevar Bush of MIT, and put into service in 1942. It could compare about 85 characters per second.



ROBIN

Taken by Ebaugh, NSA-81, on 8 Sept 1954.
Negatives are in NSA-8201(T).

The COPPERHEAD comparator was designed to search for two group hits in the cipher of enciphered code systems. Put into use in 1944, it became obsolete when its functions were taken over by the 701 computer.

The GOLDBERG comparator was a general purpose comparator of rather large scale. It was one of the first Agency machines to use a magnetic drum to store and handle data internally.

The above 3 machines are obsolete.

CONNIE I is a comparator which has been extremely useful in examination of teletype scrambler systems. The scanning speed of CONNIE I is 5,000 characters per second. CONNIE I was put into use in 1949. A new device on CONNIE I was the high speed printer developed for this Agency, capable of printing 7 lines per second. It had to be this fast because sometimes answers come that fast.

CONNIE II is a newer version of high speed comparator which will have greater flexibility than CONNIE I. It is now being installed in B building, and will replace CONNIE I.

A comparator known as VIVIAN is used exclusively for analysis of machine cipher. It is different from other comparators in that its comparison takes place in what is called a mercury delay line. This is a cylinder about the size of a large drinking glass filled with mercury. Information is stored in the mercury in the form of sound waves traveling through the cylinder at the rate of a million pulses per second. The first model of the machine was built in 1951.

The use of the ROBIN machine dates from 1950.

DELLA, a comparator of new type, is now being assembled at NSS. It will perform comparing operations similar to those of ROBIN but at a rate of 5 million comparisons per second instead of a mere 50,000. Such high speeds are possible because the paper tape has been replaced by magnetic tape, and because of other circuit improvements. Such high speeds are necessary because a growing backlog of work exists which can be done only by DELLA. The work on hand at present can keep DELLA occupied for more than 6 months.

Do our pet names for these machines worry you? They are very convenient to us as short identifications of a specific machine. Here's an idea of how they come about. Once upon a time a rather large cryptanalytic effort was named the PRINCESS project. A machine to perform a major part of it was christened DUCHESS. But since DUCHESS would take at least 3 years to build, a machine called COUNTESS was conceived to do part of the job. More than a year would be required to build COUNTESS, but some machine division engineers got an idea they could build an attachment to a printer in 5 weeks to do a small part of the job. Since this machine was so easy to make, it was called MISTRESS.

I have mentioned two machine components which may be unfamiliar to you. I will refer to them again, and you will doubtless hear of them in years to come, so a brief explanation may be desirable. First, magnetic tape. The magnetic tape used on our machines is very much like that used on standard voice recorders. The recordings we make are not of voice signals, but are numbers and letters. They are represented on the tape by spots of magnetization and spots of no magnetization, in much the same fashion that dots and dashes of Morse code represent characters. The chief advantages of magnetic tape are that it can be read or written upon quickly and that it is a compact and reusable storage medium. Some tape systems can record 100 characters per inch, which is a greater condensation than even printed matter. This reel, which contains 1200 feet of tape, could hold almost 1½ million characters, or the contents of a 700 page novel.

The second machine component is the magnetic drum. This is a cylinder, and comes in sizes ranging from as small as your fist to as large as its prototype, the big bass drum. The cylindrical surface is capable of being magnetized locally in tiny spots, very similar to what happens on magnetic tape. Both writing upon the drum and reading from it must be done while the drum is in motion, rotating at high speed on its axis. The reading and writing are done by what are called heads, poised just above the surface of the drum. Each head watches a particular track on the drum, and the electrical circuits external to the drum take care of switching from one track to another.

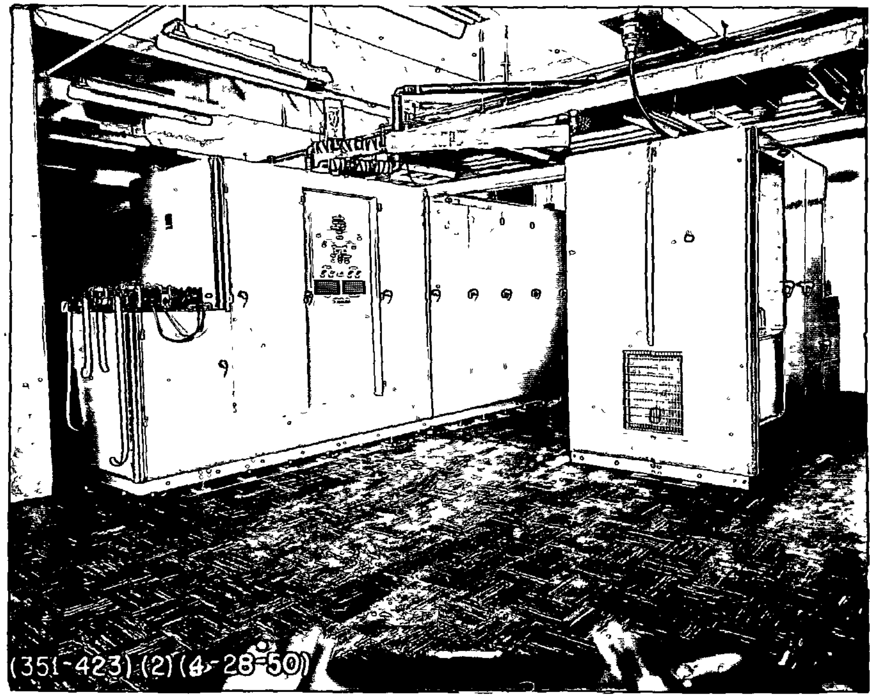
So much for the hardware; let's return to the problems which machines solve. We have seen that comparators give aid of the general nature of finding messages which have been enciphered by the same key. A natural question is "what is done to read these messages in depth"?

[redacted]

be done. How many groups must be tried? How many answers can one keep track of? How many hopeful solutions divert a person from a systematic trial of all the possibilities?

Machines cannot match people in getting ideas about what group to try, and in carrying on the sense of the text from one group to the next. But they can make a large number of tests, they are dependably accurate and thorough, they operate at high speed, and they don't get tired or discouraged. Machine aid may not be necessary, but the fact is that it is used up to the limit of our present equipment strength.

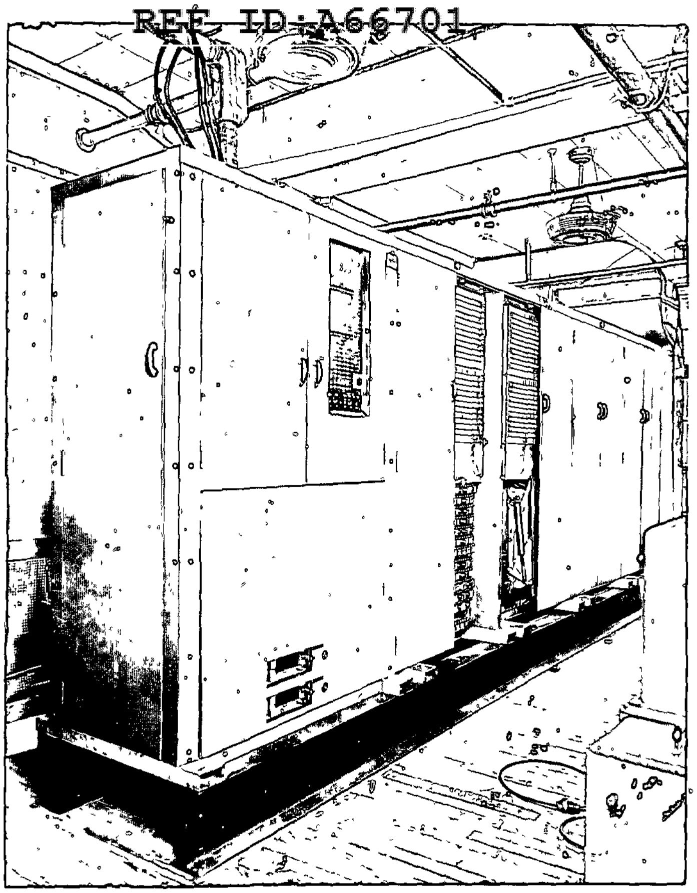
[redacted]



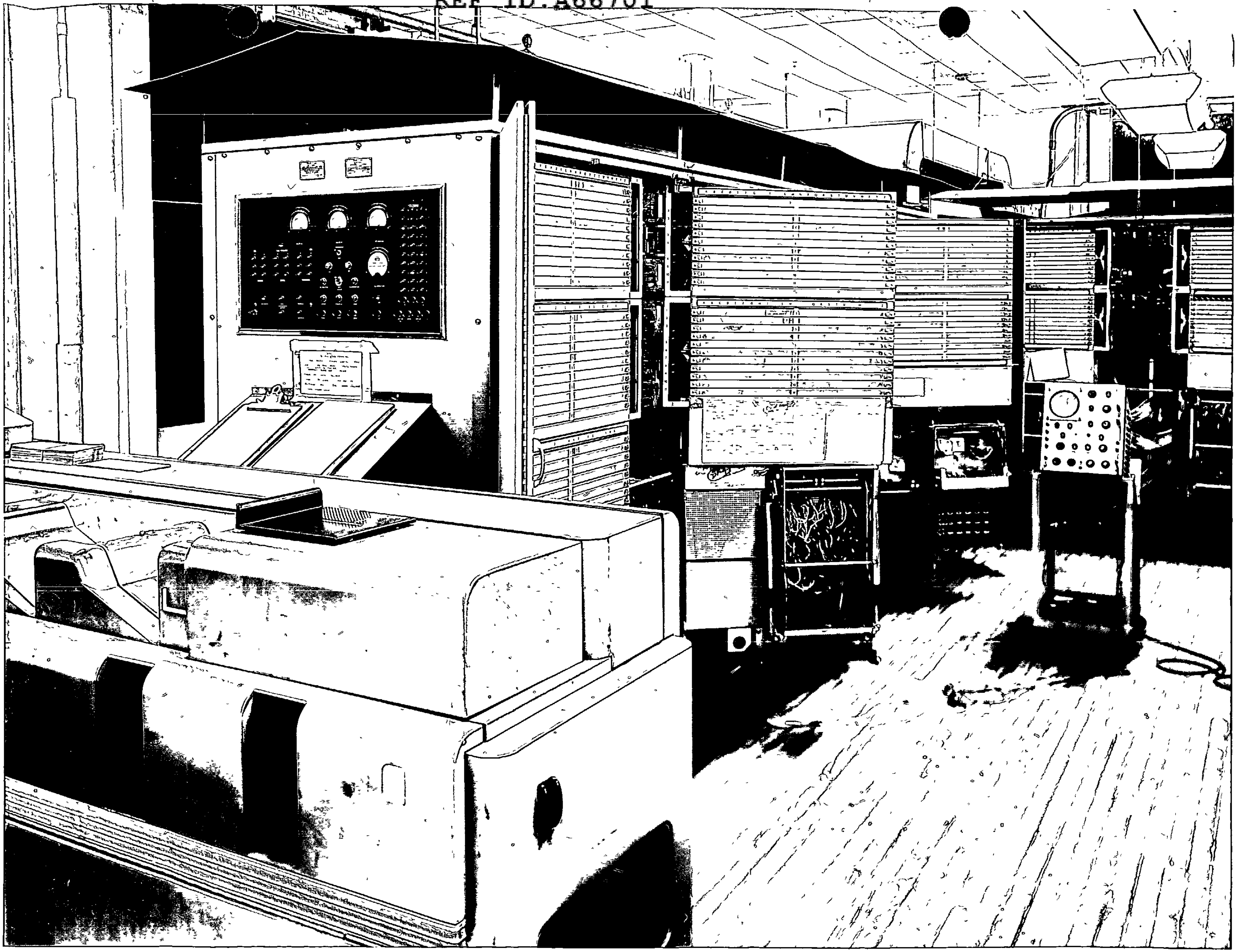
(351-423) (2) (4-28-50)

351-423) (1) (4-28-50)

DEMON II
AFSAF 77
CXNS
serial 2



SKATE II



Sled

Taken by Mr. Ebaugh, NSA-81, on 8 Sept 1954.
Negatives are in NSA-8201(T).

SLED I

EO 3.3(h)(2)
PL 86-36/50 USC 3605

I do not wish to give the impression that the output of the machine is a completely deciphered message. At one point there may be a gap because the vocabulary of the machine was too limited; at another a multitude of answers which we hope contains the correct one. The selection of final answers and the completion of the message are tasks which properly a person should do. We hope, however, that his energies have been saved for this final process by letting the machine do the dirty work of trying countless possibilities.

Occasionally our analysts have good reason to suspect that key used on other messages and recovered by various devious means has been used again. If we could only try all that key on messages as they come in, some of them would read. This is a very sound proposition -- the way to read a message is to read it. There is a [redacted]

DEMON and SKATE could be called single or multi-purpose machines. SLED advances into a new dimension, that of a general analytic machine. SLED has had many applications in which it is more than a recognizing machine. There are two things which allow this, first, the fact that internal components can be joined together in a large variety of ways so that SLED becomes a different machine for each problem. Second, several methods of scoring results are available. Examples of problems for which the machines was not designed, but to which it has made significant contribution are those concerned with wired rotor encipherment.

We have been tälking of examples of limited specialization. A comparator is applicable only where comparing and counting will reveal something of significance about a set of messages. Although we might do comparing using other machines, a well-designed comparator can beat all types of machines at its job. A recognition device is pointed in another direction -- at combining material in many ways, and selecting those combinations which are declared to be meaningful. Even as we build machines for special purposes, however, we try to make them more useful by being more flexible in the problems they can handle. But occasionally the volume or complexity of a given type of job is so great that equipment may be justified for just one purpose. We will sacrifice generality for specialization and flexibility for speed.

MAISIE is an example of a machine which was designed for just one purpose -- to decode messages. You understand that there is no magic in this -- the machine only supplies the meanings of code groups which we already know. We are seeking to save the valuable time of linguists so that it will not be spent in fumbling with a bulky code book. Over the years this process has been performed on standard IBM equipment. The IBM process requires 9 distinct machine operations to produce a set of decoded messages. After key punching the original message, we number the several cards and remove the heading cards which separate one message from the next. We have to make one card for each code group. The code groups must be sorted in numerical order; a master deck of cards containing code group and meaning has to be merged into the single code cards from the messages; the meanings have to be gang punched from the master cards into the message cards. The cards must be rearranged into their original message order, and then we are ready for the listing of the decoded message. If a machine could be devised which would eliminate these many cards we would have a better process. The saving on card costs would be trivial, but the saving of labor and machine costs, and of elapsed time would be significant.

These ideas led to our present decoding machine called MAISIE. Technological progress produced the magnetic drum which is MAISIE's equivalent of the code book. On the surface of the drum it is possible to store the 10,000 groups of a particular code and their meanings. MAISIE takes in the original key punched cards and looks up each group on the drum. If the meaning of the group exists on the drum, MAISIE sends it to the printer to be listed. MAISIE works fast enough to keep up with the maximum speed of the printer -- that is, it can look up 150 groups each minute. While MAISIE is fast in its final phases, and has succeeded in simplifying the operation of decoding from 9 operations to only 3, the keypunching must still be done, and takes as long as it ever did, so the total job of machine decoding using MAISIE is only about twice as fast as IBM decoding.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

We wish we had had MAISIE during the Korean war. We made thousands of decodes by IBM, and they were of great assistance to analysts working on that area. Even a mere doubling of the speed of production would have been a blessing to them.

As is typical of many machines, applications were found for MAISIE which go beyond her obvious capabilities. Techniques have been developed which allow her to do decipherment as well as decoding. In one particular application MAISIE does polyalphabetic decipherment of a two letter code at the rate of 50 digraphs a minute, which is ten times the IBM speed and 25 times the hand speed.

[redacted]

which govern the nature of the key it produces.

However, when two messages on the same key are not available, or will not yield enough key to work with, machine assistance is available and essential. This may range from having special counts made on standard IBM equipment on into the use of the newest class of machines, the computers. The computers can handle a statistical approach to the problem of wheel recovery. They accept messages representing about 2,000 letters of consecutive key, write the cipher out in various patterns, perform certain calculations and come up with suggested wheel patterns. They are even used to make an exhaustive check on the validity of patterns which people have developed, but which have not yet been proved to be perfect.

The second problem, that of finding what part of the long and fully known key stream was used to encipher a particular message is the one we have worked at longer using machines. You appreciate that if we know the key stream and know where in the stream the message was enciphered, all we have to do is remove the key from the cipher to get the plain text. The oldest attack on the problem is the method of cribbing. The term crib refers to a word, or a phrase which probably is contained somewhere in the plain text of the message at hand. If the probable word or phrase can be placed at the correct spot in the message, it will yield a little bit of key.

```
              AIHAMTESPR          TRNNFRT
KEY                     CBYWYEUSMZ

CIPHER        DNTPSGLSYTFZKJFNMRSGLDAVIYF

CRIB                    XCONTRIBUT

TEXT          XVOLUNTARY          IONSXTO
```

This little bit of key will be somewhere in the long stream which the machine can produce. If we can find this little bit in the long stream, the key that is adjacent to it will allow us to recover the plain text which is adjacent to the crib. Of course we may place the crib against the cipher message in the wrong place.

```
KEY           APHCLXTTSM

CIPHER        DNTPSGLSYTFZKJFNMRSGLDAVIYF

CRIB          XCONTRIBUT
```

EO 3.3(h)(2)
PL 86-36/50 USC 3605

If we do we are looking for a bit of key which should not exist in the long stream, and we will probably not find it. Or again, if our probable word fails in all positions, it probably wasn't in that message, and we'll have to try a different word. If you'll just consider hunting for a particular ten letters of key thru a stream of 101 million, when there is a possibility of their not being present, I think that you will realize why machine aid on this problem is used and appreciated.

[redacted]

~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

Since WW II we have seen the rapid growth of a new class of equipment both within the Agency and in the outside scientific and business world; these are the electronic digital computers. The versatility of these computers is well demonstrated by their variety of applications -- from prediction of presidential election results to aero-dynamics research; from supply inventory work to automatic translation; from number theory research to cryptanalysis.

NSA has currently, we believe, the largest computer installation in the world, a fact which we solicit your cooperation in keeping out

~~TOP SECRET~~

of the newspapers. The largest outside computer installation we know of has 3 computers; the National Security Agency has five, and 2 more are now being crated for delivery next month.

	INITIAL COST	WE HAVE	DATE RECEIVED
ATLAS I	$1,300,000	2	1950, 1954
ABNER	$ 600,000	1	1952
IBM-701	$ 33,000 (monthly)	1	1953
ATLAS II	$2,300,000	1	1953

You notice that these machines are expensive. Another indication of how expensive they are is the fact that private owners and government agencies who rent their computers to others charge from 50 to 300 dollars per hour of use.

The public press has already created the proper atmosphere of amazement about computers. The high speeds of computers allow them to do in hours what a clerk or a mathematician would take years to do. They are not baffled by complexity, they are capable of doing a problem two different ways to ensure accuracy, they never get tired. Our computers are like those on the outside, so there is no need to try your patience with facts to amaze. We shall spend a few minutes considering the basic structure of any computer. After that we will examine some of the general uses which are made of our computers.

Of what does a computer consist?

First there must be a means of getting information into the system; we call this input. Punched cards, punched paper tape, and hand operated pushbuttons are some of the ways of talking to the machine. Once the information is converted into the kind of electrical signals that the computer can digest it is normally stored in a portion of the machine for later reference. This part we might call its memory, or storage. It may help you to think of this as thousands of pigeonholes, each capable of receiving, holding, and giving out a number or an alphabetic quantity the size of a code group. There are many kinds of components which provide storage; as examples we might recall the magnetic drum and magnetic tapes that I memtioned earlier.

There is an upper limit to the amount of information some components can hold; for example, a magnetic drum is limited by its size. The only present medium with unlimited capacity is magnetic tape -- simply put on another reel. These storage systems have been the subject of much research, for besides quantity stored we want of them another characteristic -- the ability to get to any one of thousands of pieces of information in the shortest possible time. A curious paradox exists -- if it takes up little space, you can't get at the information quickly; if you can get at it quickly it takes a lot of room to house it. Until research provides the one right answer, we compromise. Have one storage system for quickness, another for greater volume, perhaps a third for unlimited capacity.

There is always an arithmetic unit in which addition, subtraction, multiplication and division can be performed.

The results which a computer develops or finds must be presented in normal language, so some type of output is provided. This may be a printed record, or may be a medium from which a printed record can be made -- punched cards or punched tape.

Finally we must deal with the question, how does the computer know what to do? Well, these machines are guided through what is called a program. This is a list of detailed instructions which tell the machine not only the operations to be performed, but the specific data to be used in each operation and where to put each result. The program must take care of every possible condition encountered in a sequence of operations, all checks to guarantee that the machine is not making errors, all specifications for retaining information and printing the answers. The program must even contain an instruction to stop when the desired procedure has been completed. This program which instructs the machine to perform some three dozen simple operations upon the thousands of pieces of information which it holds in its memory, is usually itself stored in this memory. This has several advantages, one of which is that once started the machine requires no further human or outside aid, but becomes quite automatic. Another is that once the program is stored in the machine it can be operated upon like any other piece of data in the memory. This allows us to write certain basic instructions which cause the computer to change many details and in effect make up its own program as it goes along. For operations which are repeated many times, this is economical, both in the time of people who could not possibly hope to write as speedily as the computer, and in the storage of the program which may be much less than if absolutely every detail were specified. This leads us to the final element of any computer, the control. This part takes care of selecting the instructions in the proper sequence, interpreting them for "what do we want to do", and "on what piece of data are we to operate". It selects the data, and sets up circuits in the machine so that the operation is executed properly. These steps take place so rapidly that they seem simultaneous to us and almost unimportant. But the control is the heart of the machine.

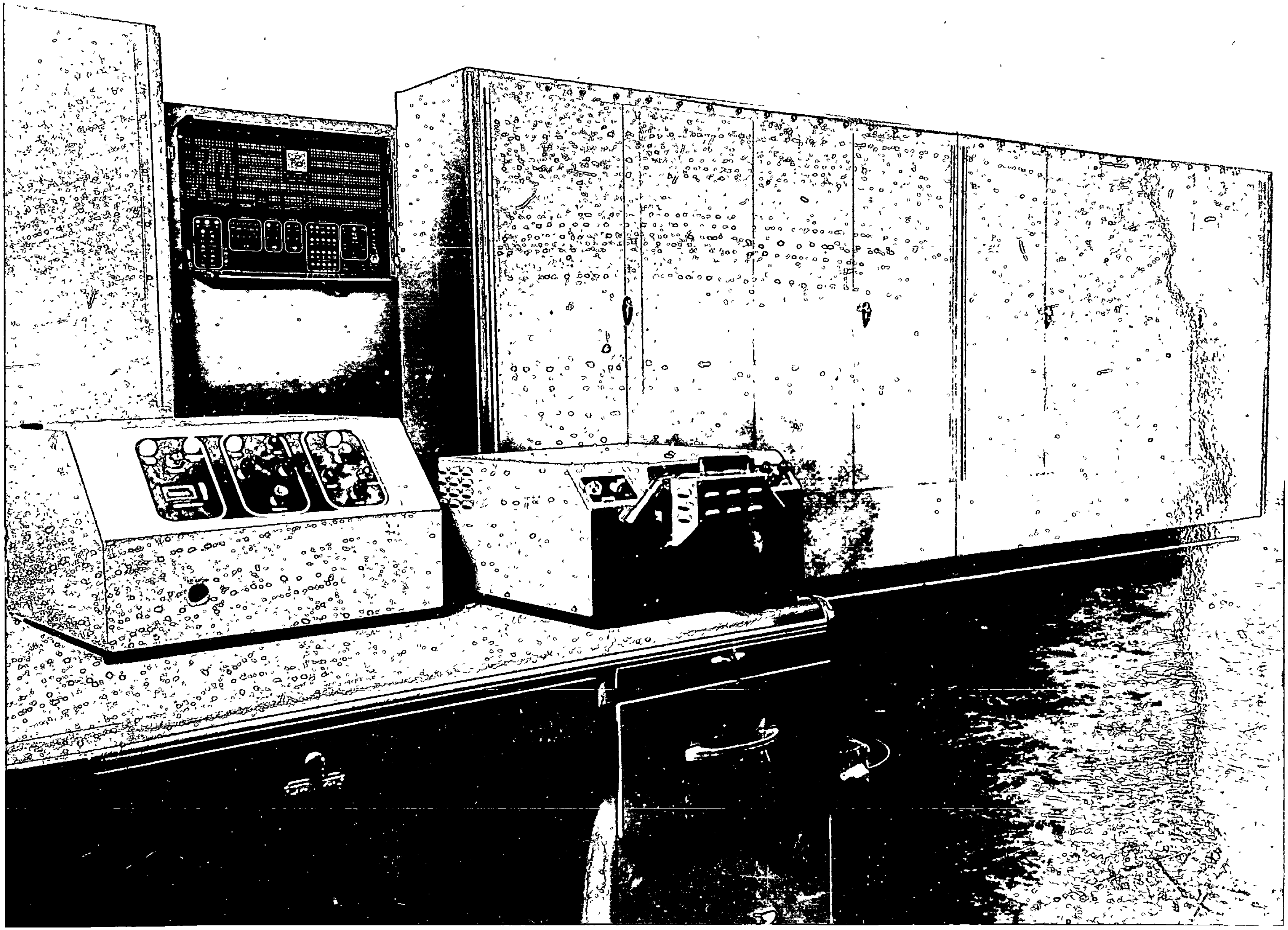
One might characterize computers as very fast, and capable of accurate memory of a rather large amount of material. One might also call them very stupid in that every step must be guided by detailed instructions. But we must give them credit for being above all, obedient. Like many people, they will swiftly and eagerly do wrong when they are wrongly instructed. In performance the machine is only as good as the people who define the problems and run the equipment. The writing of programs for the Agency has become a new profession which requires deep knowledge of the machine, excellent appreciation of cryptanalytic techniques, much logical skill, and a great deal of patience. The maintenance of such complex machines requires a Sherlock Holmes in the field of electronics, for the trouble must be located before it can be cured.

Here are the computers used by this Agency.

ATLAS I was our first high speed computer. It was built for us by Engineering Research Associates, now a part of Remington Rand. We have two of these machines. From time to time modifications are made to take advantage of technological advances; for example, high speed magnetic core storage is to be added in 1955.

ABNER is a computer of which the Agency is proud with the pride of parenthood. Almost all of the design and construction was done by Agency engineers. ABNER contains some special commands and facilities which make it somewhat more adaptable to cryptanalytic problems than computers primarily designed for mathematical computation. It is almost impossible to get a good picture of ABNER because of the limited space in which it is installed. We expect a second ABNER this fall.

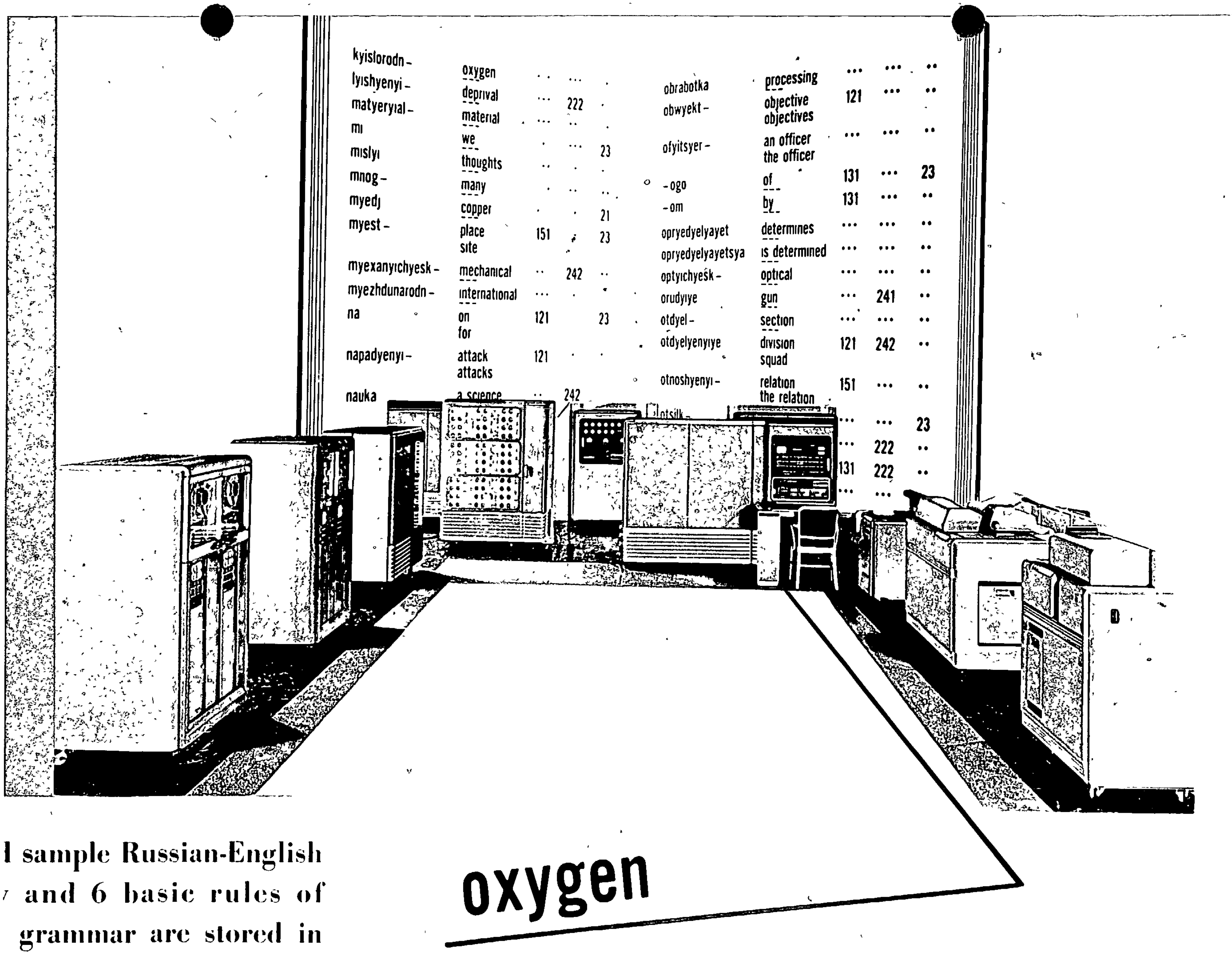
The 701 computer is an IBM product. When we rent this and other machines from IBM, we get the services of full time maintenance men;



ATLAS I
AFSAF 70, CXMX, ERA 1101

ABNER

Taken by Mr. Ebaugh, NSA-81, on 8 Sept 1954.
Negatives are in NSA-8201(T).

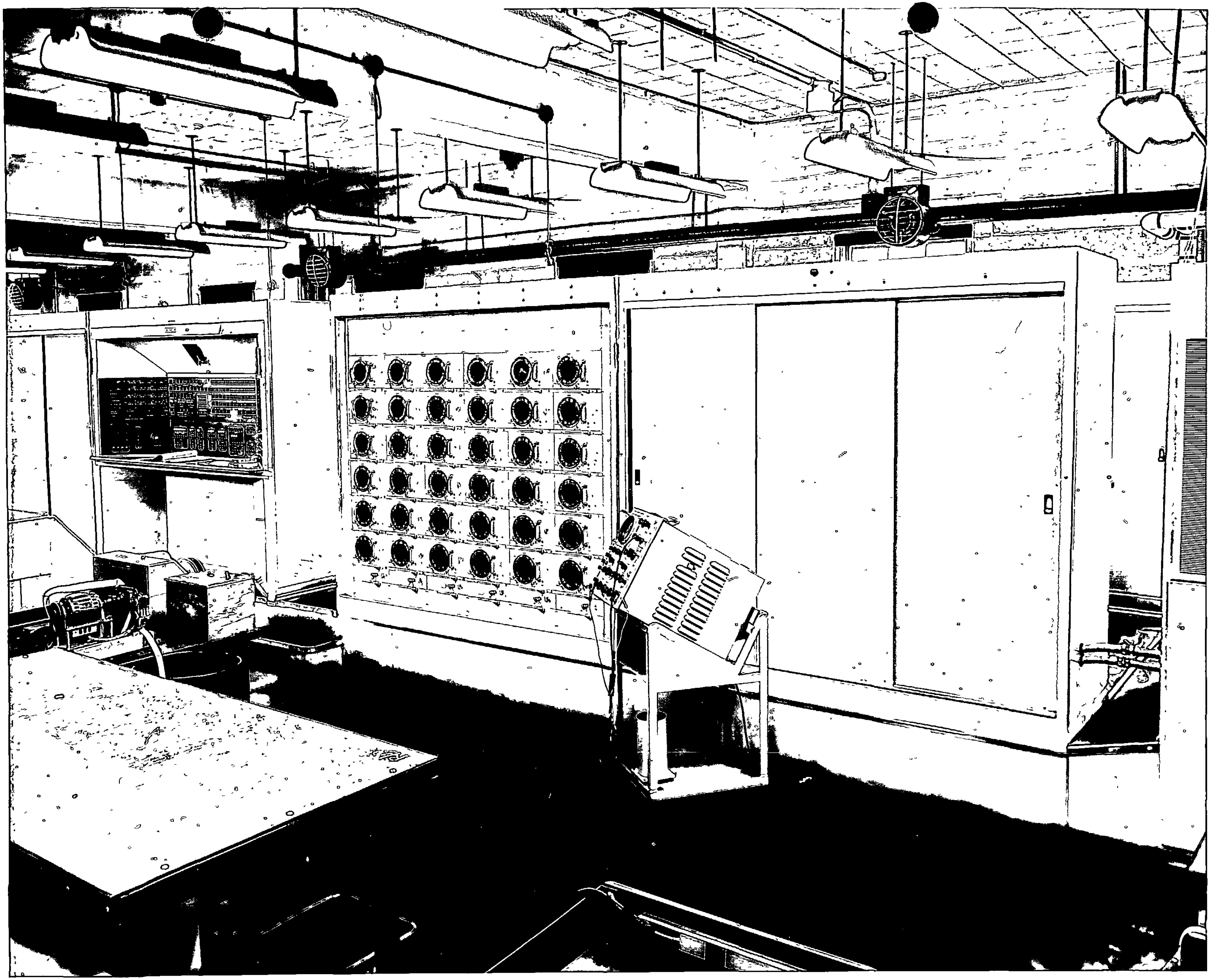


kyislorodn -	oxygen	. .	. . .	.
lyishyenyi -	deprival	. . .	222	.
matyeryial -	material	. . .	. .	.
mi	we	.	. . .	23
mislyi	thoughts	. .	.	.
mnog -	many	.	. .	. .
myedj	copper	.	.	21
myest -	place site	151	.	23
myexanyichyesk -	mechanical	. .	242	. .
myezhdunarodn -	international	. . .	.	.
na	on for	121		23
napadyenyi -	attack attacks	121	.	.
nauka	a science	. .	242	

obrabotka	processing	. . .	. . .	. .
obwyekt -	objective objectives	121	. . .	. .
ofyitsyer -	an officer the officer	. . .	. . .	. .
-ogo	of	131	. . .	23
-om	by	131	. . .	. .
opryedyelyayet	determines	. . .	. . .	. .
opryedyelyayetsya	is determined	. . .	. . .	. .
optyichyeśk -	optical	. . .	. . .	. .
orudyiye	gun	. . .	241	. .
otdyel -	section	. . .	. . .	. .
otdyelyenyiye	division squad	121	242	. .
otnoshyenyi -	relation the relation	151	. . .	. .
otsilk -		. . .	. . .	23
		. . .	222	. .
		131	222	. .
		. . .	. . .	

l sample Russian-English
, and 6 basic rules of
grammar are stored in
)l.
s in the Russian language

IBM EDPM, Type 701



Atlas II

Taken by Mr. Ebaugh, NSA-81, on 8 Sept 1954.
Negatives are in NSA-8201(T).

ATLAS II - ERA 1103

we furnish operations and programming personnel. This is not a picture of our 701 installation, which like ABNER is difficult to photograph, but we have every unit represented here.

ATLAS II is another ERA product, and will shortly be joined by a second machine. The second machine will have a magnetic core storage system, which is the newest fast, compact, and reliable method of storing information.

I agree with you that dollars, massive equipment, components and amazing speeds are still no indication of why this agency has computers. The real question is, what have they done for us, what can they do? Theoretically they can do anything, since they present us the opportunity to layout the simple operations in any combination that we wish to achieve our purpose. Practically, there are limitations of capacities and time. An impressive total of 350 programs has been written, each designed to fill some need of the Agency. We think enough of the usefulness and the economics of our computers that as soon as they can be staffed they are in operation 24 hours a day and there is still more demand for their use than we can fill.

Among the simpler types of jobs have been programs to perform routine decryption of messages, to make and score frequency distributions, and to perform calculations associated with direction finding, the multiplication of matrices, and various other mathematical jobs. Here, the computers allow us to complete relatively simple tasks in a fraction of the time previously required. A simple example of this kind of use of a computer is found in a diagnostic program on ABNER. For many years it has been the dream of cryptanalytic people to have counts of many varieties made on messages before an examination of them was undertaken. Even with our many other machines, we could not find the time to do this. This ABNER program provides a large number of related yet varied tallies on a message. It has recently had wide use on small and hitherto unworked systems. Just about every count and scoring a cryptanalyst will want for initial examination is made in about 20 minutes per message, about the time he would use in making a simple tally of letter frequencies.

The single greatest stream of endeavor for computers has been attack upon problems whose intricacy and size never permitted machine treatment before. The mathematicians of Research and Development [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

other, and provided one can assume or develop some facts about the nature of the different keys which were used to encipher them. The processes are highly sophisticated, and only machines like computers can carry out the manifold computations in a reasonable amount of

[redacted]

There are large jobs, to be done only once, which have been approachable in the past only by building a piece of machinery to do each one. Since the computers can be directed to do almost any problem, we can sometimes let the computer be the special machine, as directed by its program. Investigations of this kind generally arise out of a desire to have some thousands of letters of key generated by a newly posed rule, so that our security organization can pass judgement upon the practical results of the use of the new key generation technique. Computers can serve as a stop-gap until special machines can be built. The Machine Division a year ago had a request for a desk side device to perform simple decipherment. A month was required to build the device. But in 10 days a computer program was in operation to do the decipherment and was used until the special device was available.

As an investigative tool, the computers allow us to examine the virtue of analytic approaches. Several programs on 701 and ABNER

[redacted]

deals with the possibility of machines and processes. Is it possible for a machine to accept incoming teletype tape and produce a message which is cleared of all nonessentials, which is in a standard format, ready for hand work or for machine work? As a by-product of the processing can we produce cards to be used for other machine work without the intervention of keypunching, which always will be a slow process when done by hand. Such researches into the field of automatic editing are under way. They may point to better computer techniques, they may reveal how a special machine could be built to do the job better than the present combination of machine and hand methods.

Finally, we would all be disappointed if the coming of new machines did not relieve us of some of the older machines and techniques. Certain special-process machines were embarrassing us by the space they took up and the excessive amount of fixing they required. As soon as the computers could demonstrate their equivalence or excellence in this field, out went COPPERHEAD, the multiple group repeat device; out went O'MALLEY, a special machine used to perform crossproduct multiplication and summation. The computers now handle their functions.

In summary, our uses of computers are:

1. Time-saving
2. Intricate cryptanalytic attacks
3. Special one-time jobs
4. Investigative tools
5. Replacement of other machines and techniques

A few years from now a more systematic story can be told of how computers help this Agency. The immediately possible has been done; investigations which will produce long range results have been started; the computers are getting into hitherto unapproachable fields of machine processing; they are replacing other machines. As they find their own limitations they will help to describe the machines of the future.

Now, what about the machines of the future:

Even today plans are under consideration which include in our future equipment the latest technological advances and permit new applications of machines to our problems. During the next few years you may expect to see experiments and actual performance in some of the following fields:

1. Data handling - IBM 702, 703
2. Plotting of D/F and radar location
3. Automatic scanning
4. Automatic editing and card punching
5. Central computation under decentralized control
6. Special functions using generalized components
7. Automatic reading

Next Spring a whole new vista in data handling will open when we receive the IBM 702 Tape Processing Machine and the 703~~File Maintenance~~ Machine and ancillary equipment. While this equipment can compute, it

~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

is different from a computer. The rest of our computers work most efficiently on problems which allow small input, large processing, and small output of answers. The 702 complex will work well on problems with large input, large processing and large output. This should make it possible for us to give problems such as traffic analysis the high speed high volume processing which they have never had.

[redacted]

At present 35 clerks scan the automatically recorded intercept of plain text to sift from it items of intelligence value. Their guide is their human intelligence and the ability to remember certain key words they have been told to watch for. The very existence of recognition devices which can recognize such uniform data as code groups is a challenge to us to build machines which scan faster than people. The machines will be capable of making a message print at the same time, at line printer speed rather than in a separate operation at typewriter speed.

I have already mentioned automatic editing experiments on the computers. We will someday see machines which will perform this function probably at greater speeds than computers. Savings of 60 to 1 over hand methods are anticipated.

Industrial applications have demonstrated that a central computer can serve the needs of decentralized users. The users will teletype their problem into the central machine, and in minutes they will receive an answer based on all the data available at the central machine. The users could be two floors above, or they could be across an ocean.

Generalized components will be built which can be attached in many different ways to make machines for special purposes. The time involved in building special purpose machines may be reduced from 2 or more years to 2 or more months. Incidentally, we have done this thru the years as over 75 attachments were built to be used with IBM for special functions. What is envisioned here are devices of far greater complexity and speed which will deal primarily with machine cipher problems.

~~TOP SECRET~~

Ambitious strides are being made in the field of automatic reading. Machines will scan hard copy and translate the letters on it into paper tapes, IBM cards or such other media as will serve further machine processes. Our keypunchers are not at all dismayed by this development for they know that no machine will successfully decipher the handwriting of a left handed Lower Slobbovian as it looks on the fourth carbon. Keypunchers still have a future.

Speaking of futures, does it seem that if you're not in the machine division, you haven't one? Far from it. Machines are directed by the ideas and the efforts of people. The results they find are examined and used by people. Often the more machine help available, the more work done. Dr. Campaigne, in describing the impact of machines on handwork states "... there are in fact more hand jobs than before. These require more analytic ability and bring more pressure on the people in order to make the best use of the machines."

The panorama of our analytic machines which you have just seen includes something of the past, the present, and the future. The Machine Division shares the hope of our Agency that we will be of aid in keeping our country out of war. But if we got into a war, what could we do?

If the past war is any indication, communications intelligence would be of inestimable value, and analytic machines would provide more of it. Unfortunate disclosures have made public knowledge of this country's success against enemy communications in the last war. Fortunately this public knowledge does not indicate that 750 IBM machines and some 200 other analytic machines were in part responsible for the success and the volume of the success. Even today we are under orders to guard these past successes as securely as our present ones. Yet there is every reason to expect that since those infant agencies succeeded so splendidly in the days when they were learning how to use machines to perform cryptanalysis, this present organization could do an even better job today should the emergency be upon us. It may be upon us today. We are ready for it.