CRYPTANALYTIC MACHINES IN NSA

NSA-34
30 May 1953
Wheatley, LeRoy H.

The first installment is complete on the job of writing a brief description of all analytic machinery in the Agency, whether past, present or projected. It includes 51 equipments, and later installments will add approximately 150 more machines, plus photographs of many of the equipments. To this will be added a table of contents and index by the time the project is completed. Corrections, additions and comments are invited.

May 1953

DESCRIPTION OF ANALYTIC MACHINERY

This is the first installment of a collection of machinery descriptions which will ultimately be a complete list of all cryptanalytic machines built by and for the National Security Agency or its predecessors. The purpose is to provide a brief set of introductory facts about each machine, and provide the analyst with a starting point for learning any machine.

Since these initial expositions are tentative, the reader is invited to inform Roy Wheatley, ext. 527 at AHS, of any errors or omissions noted. In limited detail, the descriptions give the name, nature, purpose, origin, function, size, speed, location, and status of all equipments whether past, present or currently projected, plus any further information considered important enough to be included.

Plans call for a complete Table of Contents, Index, and Glossary of Terms when the task is finally concluded. Logically, many minor gadgets and simple constructions are excluded for convenience and clarity, but everything considered interesting or significant is included. Their status, location and number, even their function may and do change, so the date of publications must be taken as a guide in these respects.

Numbering and naming of machines has not always been adequate, so almost every system of designation found, such as the BuShips "X and CX" list, Army's comparable "AX and AFSAF" list, local Naval "N and NC" list, etc., have been included to best insure against ambiguity.

May 1953

CRYPTANALYTIC MACHINES IN NSA

Most cryptanalysis reduces to counting, comparing, rewriting, and referring. Each of these operations by itself is simple and easily done by the proper type of machinery. When there is need to do them in combinations, or especially if a choice of methods must be made, mechanization is not so simple. For some operations the advantages of machines is evident. Some steps can be done faster, more accurately, and with better organization by machine. Theoretically with enough men and enough time anything a machine can do could be done by hand. But to do certain very routine computations, such as that done by SUPERSCRITCHER, by means of a crew of thousands of people would raise tremendous personnel problems, so that it might be impossible to actually carry this out. The old joke about solving a simple substitution by a crew of 26 factorial Chinamen is no more than a joke.

Until 1935 practically all cryptanalysis, both by the Navy and the Army, was done by hand. About that time the possibilities of accounting equipment, such as IBM (International Business Machines) and Powers, was realized and some was procured for experimental use. It was a success, and over a period of years many special techniques, unorthodox for accounting, were developed, some requiring modifications of the machines. Many special devices or gates were developed to do specialized analytic devices, the first of which was called

the GEEWHIZZER and applied to columnar transposition systems.

Vannevar Bush of Massachusetts Institute of Technology, undertook to develop a special machine for cryptanalysis. With the aid of graduate assistants this was done and the machine was shipped to the Navy in Washington in 1941. Later, two of the graduate assistants came too, John Howard and Lawrence Steinhardt. John Coombs went to the Naval Computing Machine Laboratory in Dayton to build BOMBES. The design of Bush's machine was ambitious, and provided for photoelectric comparisons of two texts for coincidence, monographic, digraphic, etc., up to nine letter repeats, for special patterns and for isomorphic repeats. In operation it proved to be slow (it printed for each comparison, no matter how uninteresting) and full of "bugs". Some of the functions were abandoned after operational and maintenance experience, such as the isomorphic repeat search. At a later time improved models were built, and still exist as the 70mm (the tape width) Comparators. They have had long and useful service.

The advent of the war in late 1941 gave great impetus to procuring mechanical aids for the cryptanalyst. The I.C. MACHINE was made to compare two texts and measure coincidences. It could compare texts up to 600 letters long at all offsets in a few seconds, and the machine was small enough to sit on a desk. In practice it did not work this way, however; the device was simple enough, but the preparation of the text onto photographic plates was not, so the machines had to be operated as a battery near the camera and dark rooms.

Another photographic device, TESSIE, was started early in 1942. It compared texts for repeats. Subsequently the Army developed a super photoelectric device, the 5202, COMPARATOR, which had much greater capacity and flexibility. These along with others formed a distinct series of photoelectric comparators, the last of which was AMBER, completed in 1947. All of these machines, except the last, contributed definitely to the prosecution of the war. In recent years photoelectric techniques have been used less than digital electronic.

The only analytic machines ever built in large quantity were the BOMBES. These were designed in 1942 with advice from the British. The Navy designed a 16-unit model of which 125 copies were made, nearly identical. To operate and maintain these around the clock took a trained crew of 800 people. The Army built a single machine called MADAME X, consisting of 144 units, which could be run as several separate machines with smaller numbers of units. It also had the advantage of trying the wheel orders in automatic succession. These BOMBES were used against the ENIGMA, the cipher machine used by the Germans for 90 per cent of their enciphering, and consequently were of the greatest importance. One estimate by the Navy was that, costing less than a cruiser, the BOMBE installation had caused the sinking of 60 German submarines. The successes against the German Army and Air were even more important.

The introduction by the Germans of new reflectors with unknown wiring led to the invention and construction of several machines,

called "SCRITCHERS", able to do the BOMBE problem without having all the enciphering elements. These machines came quite close to being digital computers and were probably the most ingenious machines built during the war. The fundamental idea of scritching is credited to the British.

After the war the comparator series continued to develop. The Navy product was GOLDBERG, which was the first machine designed to hold its data on a magnetic drum. The Army built CONNIE which used punched teletype tape. Both these comparators were influenced by the British war time machines called ROBINSON and COLOSSUS. In fact, the name GOLDBERG is an American version of ROBINSON, since the cartoonist Rube Goldberg drew weird gadgets just as Heath-Robinson did. From CONNIE was developed the more special ROBIN for making round-robins, or all comparisons. The sonic delay line machine DELLA uses a new medium, sound waves in mercury, to continue the line.

Since 1946 there have been three main lines of new developments, the exhaustive trial devices, the dictionary machines, and the cryptanalytic computers.

The exhaustive trial devices include HECATE and WARLOCK. They distinguish themselves by having very high operation rates, and by being large and working only by exhaustive trials.

The dictionary machines look up weights, meanings, etc., in a large memory. They are physically large and limited in their abilities. Their rates of operation are not so fast as HECATE, but are

high nevertheless. They started with Navy's MERCURY (a war time development, long defunct) and Army's SLIDE-RUN MACHINE, and now include DEMON I, II, and III, SKATE I and II, and SLED I and II. This last can also do such operations as dragging cribs and reading depths.

The computers were inspired by developments at Harvard and the University of Pennsylvania. They are extremely flexible, able to do almost any logical process by breaking each problem into minute steps. As a consequence of the minuteness of the steps some operations are not nearly so fast as are some more specialized devices. The machines developed at NSA are not copies of standard computers but specially designed machines with much more logical flexibility. They are ATLAS I and II, ABNER I and NOMAD.

In retrospect these machines have seemed to create more work than they accomplish. In the original planning it was expected that the burden of hand work would be lightened and the need for personnel decreased. Although many things formerly impossible are now done, 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 best use of the machines. The reason for this can be seen by an example. A certain process called a "pass" is needed to solve a cryptanalytic problem, BOOTSTRAPS. To do this by hand takes several hundred man hours, valued at nearly $1,000. This is exorbitant, so BOOTSTRAPS was deferred in favor of more feasible jobs.

Then a method of doing a pass was devised on card equipment. By this means the cost was approximately $32.50, and several hundred passes were made. The result of a sequence of passes is the material from which cryptanalysts can proceed to a solution. The new method led therefore to more work for cryptanalysts. Each solution opened new jobs to do as well.

Then a program for making a pass on ATLAS became operational and the cost of a pass became $1.25. This is such a bargain that all available data was run through the process, making a tremendous job for cryptanalysts (and plain text). This is the way analytic machinery makes more work for the analyst rather than less.

Dr. H. Campaigne.

May 1953

AMBER (AFSAFD100, CXMP) is a photoelectric comparator, similar to HYPO, using four photoelectric cells to scan two superimposed 70mm films, apply weights and count coincidences. Two equipments, serial 1 and 2, were built by Eastman Kodak Company for Navy for depth search in JN-37, a Japanese weather system, but arrived too late in 1945 for that purpose. The contract also produced two cameras, 5'H x 11'L x 5'D (tapered) and two card readers 5'H x 9'L x 3'D . A 7'H x 8'L x 2'D unit supplies identification data to the camera. A DENSITOMETER was developed by Eastman Kodak to check AMBER film.

The gate is 160 characters deep by 320 columns wide, permitting comparison of a large block of data at one time. The scanning area of the film may be treated as two zones, such as plus and minus. Characters are read from cards and photographed as spots of light, each with a one to ten density range (0 to 100 per cent transmission factor in steps of ten) providing a system of nineteen weights. The machine can be set to find the single best point of coincidence, or all points above a pre-set threshold.

It measures 6'H x 4'L x 4'D and is now at Naval Security Station, one in Room 20109 and the other in Room 20210, doing general comparison, weighting, coincidence counting and message setting against key. The comparison rate is 800 characters per second.

Ref: NSA-181 Library
Mr. G. Kier
Mr. S. Snyder
Mr. F. Spurberg

May 1953

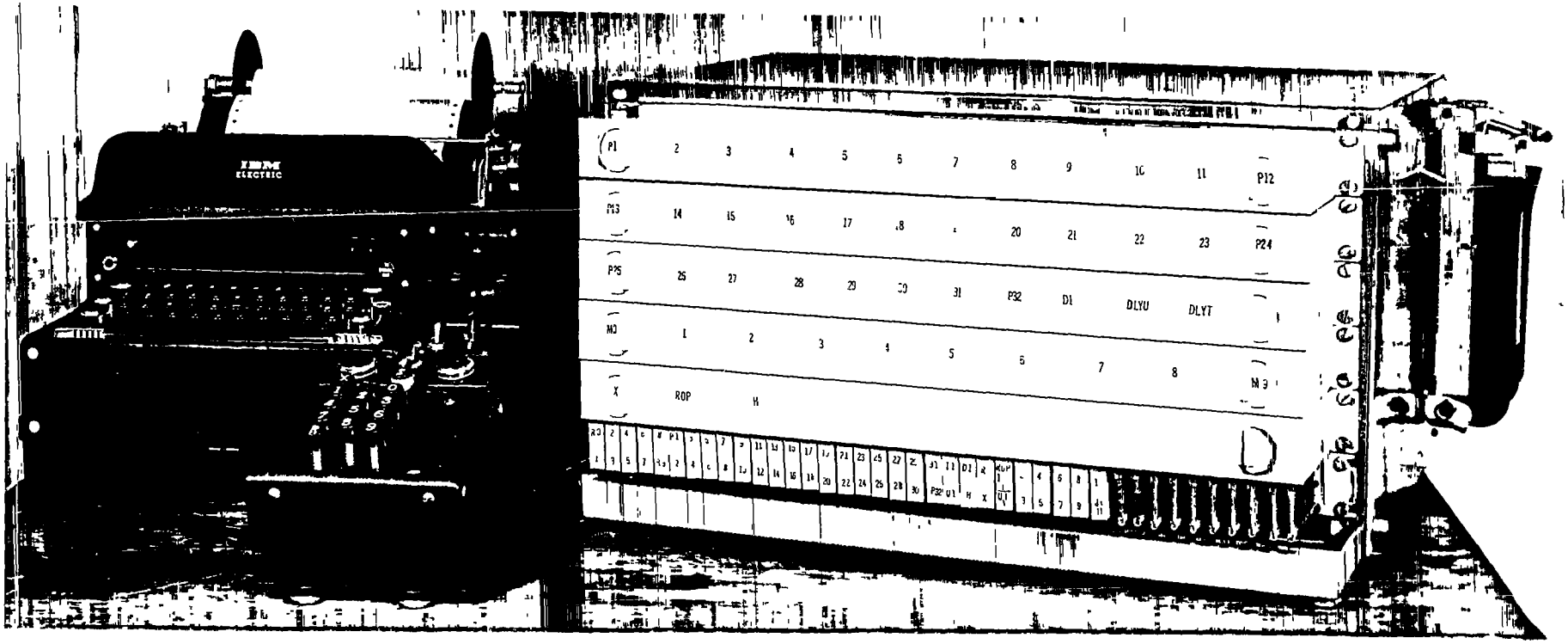
ARABIC DECIPHERING DEVICE

The ARABIC DECIPHERING DEVICE (AFSAF 45) is a relay-operated substitution device for decrypting messages in an Arabic digraphic substitution system complex by converting two digits to one Arabic letter. The one model was built by NSA-352 in 1949.

It consists of a standard digital keyboard for input, a junction box to take an 8 x 20 plugboard for substitution, and an electromatic typewriter equipped with Arabic key-slugs for output. Two digits of cipher are typed on the keyboard, combined into one impulse in the plugboard, which is wired according to a particular substitution key-list and which operates a corresponding type bar on the typewriter.

The device proved satisfactory in use, but the feature of requiring a plugboard wiring for each of a tremendous number of key-lists used in the complex of substitution systems slowed operation drastically. It is stored currently at AHS in Room 2021-A. Operation is at typing speed, up to 8 characters per second. Size is best expressed by listing the components: an IBM keyboard, an 8 x 20 junction box and an electromatic typewriter.

Ref: Mr. E. Azar
Mr. N. Christopher
Mr. H. Herczog
Mr. M. Pattie



ARABIC DECIPHERING DEVICE
AFSAF 45

May 1953

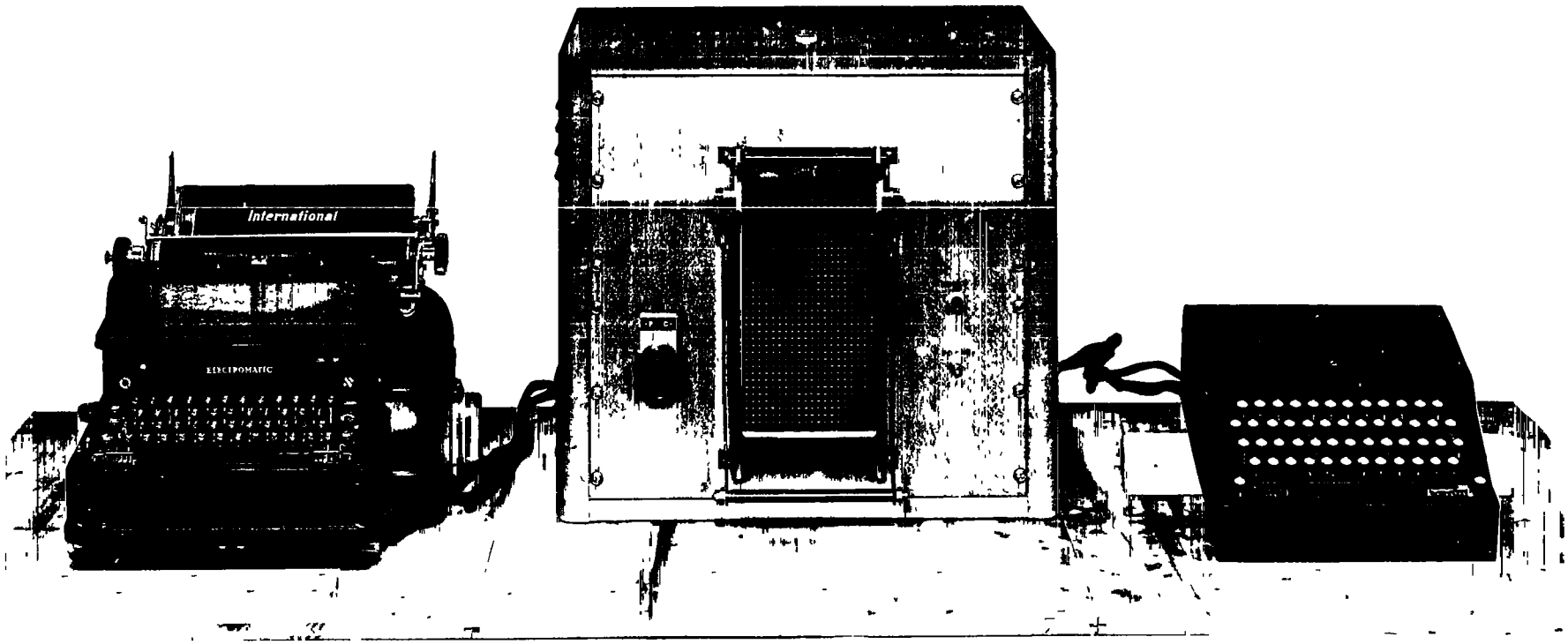
ASP

The ASP was an electromechanical device for the decryption of call signs in certain Japanese systems. One unit was completed by USNCAL in April 1944; construction of a second model was discontinued because of system change.

There were three units to the device: a kana keyboard for input, three separate plugboards (two for 48 kana and one for 10 digits) to accomplish simple substitutions by plugging, and a regeneration typewriter for output of decipherment. The machine automatically stepped to the next stecker after a decipherment.

It operated for only two or three months before the systems changed, and was an improvement over hand methods for handling a large traffic volume. Size was 2'H x 4'L x 1'D plus keyboard and regen typewriter. It has been dismantled.

Ref: CIT-21
NSA-18 files



May 1953

AUTOSCRITCHER

The AUTOSCRITCHER, or (GRAPEVINE) was a relay operated crib-tester used to solve German ENIGMA traffic through exhaustive trials. Requiring a crib of about 200-letters and known rotor wiring, it exhaustively assumed steckers (end-plate pluggings) until the correct reflector plugging and stecker were found. It was built by Army in 1944 and operated until July 1945, when the German problem ended. It was replaced by the electronic SUPERSCRITCHER, for which it served as a test model.

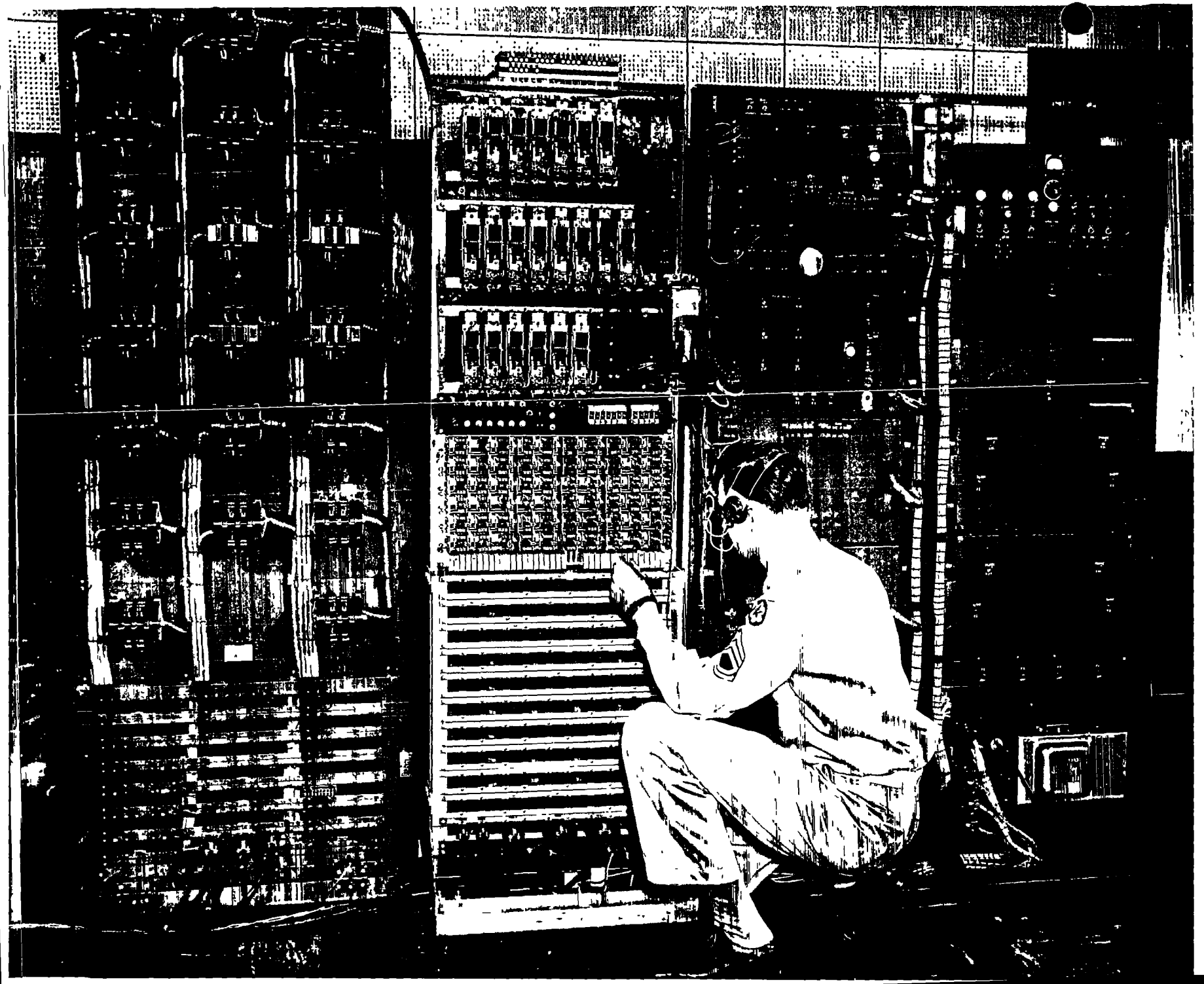
The menu (pairings of crib and cipher letters) was set up on a plugboard and an arbitrary stecker was assumed so as to satisfy the first pair of letters. Further assumptions included wheel order and no SWTO (slow wheel turn over; i.e., only fast and medium wheels involved in the movement). Each plugging assumption was automatically tested through successive pairings until eliminated, the machine sending impulses through the rotor wirings, sensing contradictions, non-contradictions and confirmations of exit points. When all letters in the menu produced no contradictions the machine stopped, allowing hand record of data for further testing. Probability of solution was about 70 per cent.

The machine measured 8'H x 10'L x 3'D . Average set-up time was 30 minutes, but running time was as much as ten to fourteen days, three shifts a day. Speed was 25 tests per second. Being slow,

AUTOSCRITCHER (Cont'd.)

rather inflexible and inconvenient for testing and maintenance, it was dismantled.

Ref: M.A.C. Outline #20
Mr. R. Bowman
Mr. R. Moulton
Mr. J. Raisch



AUTOSCRITCHER
(GRAPEVINE)

~~TOP SECRET~~

~~FROTH~~

~~TOP SECRET CANOE~~

May 1953

B-211 STECKER FINDER

The B-211 STECKER FINDER was a special purpose generator designed by ASA for use in conjunction with the condenser-type FREAK (refer to M.A.C. Outline #11) in statistical solution of the stecker of one coordinate of the [redacted] B-211 matrix. It was built by ASA in 1947.

The machine had two sets of 25 relays, [redacted] FREAK made a statistical tally of the coordinates resulting from combination of generated key and fractionated tape. A record of results (in tape and print) permitted the operator to select favorable cases.

Not much use was made of this generator, due to failure of FREAK. Rate of speed was about 17 minutes per message. It was considerably smaller than a typewriter, and is now dismantled.

Ref: M.A.C. Outline #57
Mr. M. Collins
Mr. R. Gordon
Mr. J. Russell

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

May 1953

CAMEL

The name CAMEL is a phonetic rendering of CML, the abbreviation for CHARACTERISTIC MESSAGE LOCATOR, which was a 6-unit relay gate designed to operate with a 405 TABULATOR in locating CI (Cryptographic Instruction) messages. These messages contained a conversion square to be used in certain Jap Army systems. It was built by Army's F Branch for B Branch, delivered in February 1945 and is now dismantled.

The device was designed to make use of the fact that the Japanese frequently sent a conversion square for a particular period as a message. A line of 10 digits, 0 to 9 in some one of its 10! (= 3,628,800) permutations, was represented as ten four-digit groups. The machine deciphered a message using the current square and matched resulting plain groups ten at a time against these ten known groups. In the right set of messages ten such sequences of the ten groups would be found. A print of all the plain text was made and an indication was given of every hit.

Average rate was one card every 15 seconds plus print time. It measured 7'H x 4'L x 2'D .

Ref: NSA-354B files
Mr. S. Kullback
Mr. F. Mayol
Mr. J. Raisch

~~TOP SECRET CANOE~~

May 1953

CHINESE TYPEWRITER

The CHINESE TYPEWRITER (IDEOGRAPHIC TYPEWRITER, CARD-OPERATED CHARACTER TYPEWRITER) draws stylized characters with no curved lines and no shading on eight levels or more using a special set of type slugs. It was built by International Business Machines Corp., in 1946 using the duplicating portion of an 053 CARD-OPERATED TYPEWRITER and a plugboard.

A file of cards has been developed for all code groups in the system and their equivalent Chinese character, listing the consecutive typewriter functions and key strokes required to "draw" the character. This is accomplished by graphing each character, then reducing the elements in each graph square to the closest related stroke. An IBM card is prepared in special coding for each character and its cipher text code group, averaging 20-25 strokes, and some totaling 55 or 60. A deck of these is read by the machine through a plugboard to the 053 duplicating unit. Using all the typewriter functions and a special set of 42 key slugs, the typewriter draws the stylized characters required by the deck. One type slug face (supplied by International Business Machine Corp.) is a Roman alphabet on lower case and the straight strokes for forming the Chinese characters on upper case.

It measures 3'H x 5'L x 2'D and operates automatically at a rate of 10 strokes per second. It is still available for use at Arlington Hall Station in Room 1605-A.

Ref: Machine Branch Annual Report, 1946
Lt. T. Myers
Mr. J. Powers

May 1953

CONNIE I and II

CONNIE, (AFSAF-1, AFSAF-D/1A) is a general purpose teletype-tape comparator, used for polygraphic coincidence counting, of up to pentagraph size. Model I was experimental, completed by Army in October 1949, just after the merger. A contract for an expanded equipment, model II, (AFSAF-1-1, now AFSAF-D/1A, sometimes called the new or expanded CONNIE), was let to National Union Radio Corporation with an expected delivery date of August 1953. IDA, (AFSAF-1-X, or AFSAF-D/52), is a modification of CONNIE and is described under that title.

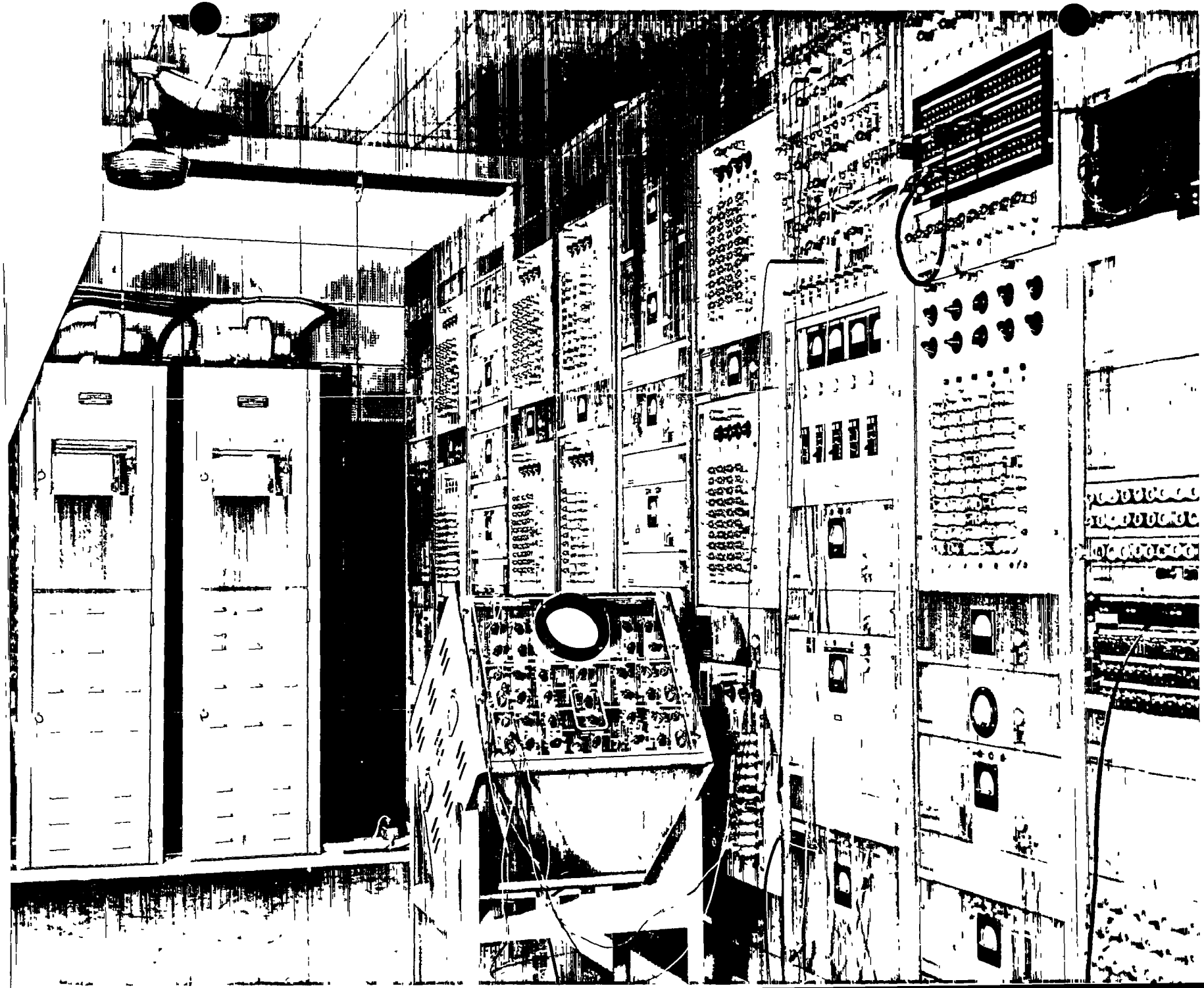
Input for both is a high-speed dual tape drive, a pair of photoelectric tape readers operating at 5000 characters per second. Output is to two AFSAF-44-1 DIGITAL RECORDERS. In the fall of 1951, four Remington Rand card readers were also provided for model I to hold one stationary card apiece and supply a crib or pattern, such as for a notched wheel, thus simulating regular wheel motion. Characters are scanned, stored electronically and treated cyclically, making successive matches against text. In general, the machine counts binary coincidences, combines these internally for character coincidence, and matches totals against a preset threshold.

CONNIE II will have several improvements: a 32 x 32 magnetic binary matrix, a criterion generator with a variable threshold print control and auxiliary storage unit. It will handle larger numbers at a much faster rate and will permit weighting and variable grouping.

CONDIE I and II (Cont'd.)

Model I measures 8'H x 33'L x 2'D plus the photoelectric reader input. It is now in use at Arlington Hall Station in Room 0413-B and has a rate of 5000 comparisons per second. Model II will also operate at Arlington Hall.

Ref: Mr. W. Cole
Mr. J. Deutsch
Mr. R. Gordon
Miss M. Hobbs
Mr. J. May
Mr. J. Powers



CONNIE I
AFSAF 1
with two AFSAF 44 WHEATON
DIGITAL RECORDERS (left) for output

~~RESTRICTED~~

May 1953

COPPERHEAD

COPPERHEAD (AFSAF-94, CXMN, CXPC) is a relay-operated photo-electric comparator for locating double group repeats at equal interval in two cipher messages by comparing the messages on 70mm tape at all juxtapositions. This is in effect a depth search. Four such were built for Navy by National Cash Register Co., the first in 1944. Also, four punches were built. Models II through V were planned but never materialized. A TAPE CHECKER (see CIT paper 22) was developed in 1944 to improve tape accuracy.

Up to 250 cipher messages are punched into a pair of opaque 70mm plastic tapes by means of a 70mm tape punch (considered a part of the machine but actually separate) at an average rate of 40 messages per hour. A whole group is punched per frame using binary code which requires five of the twenty-six tape levels for each digit. The two tapes being matched are complementary to one another, so that a hit appears as a blackout to two of the 100 photoelectric cells. A hit stops the machine for manual recording.

COPPERHEAD I is faster and scans a wider span than the BABY BRUTE FORCE DEVICE or TESSIE II (100 groups simultaneously versus IBM's 17 groups and TESSIE's 20 groups). It is currently in use at Naval Security Station in Room 4152 and measures 9'H x 6'L x 3'D, plus a small tape punch. The machine operates at 4000 frames per second.

Ref: Brief Descriptions of RAM Equipment
CIT 11, 22, 24, 41, 42, 94
M. A. C. Outline #14
Mr. J. Stapleton

~~RESTRICTED~~

~~CONFIDENTIAL~~

May 1953

COUNTESS

COUNTESS (AFSAM D/13) is to be a limited purpose group-I.C. device to do a round robin search for monographic through pentagraphic coincidences either adjacent or split up in any or all phases. The one model ordered was completed in 1952 by NSA-354. Plans for a COUNTESS II (sub-project 351-437-53) were dropped when it was found that modifications could be completed in 1953 to provide all the features desired. It is one of the PRINCESS equipments, comparing over a wider than usual span of text, $2^{10} = 1024$ characters.

A 517 REPRODUCER PUNCH operating at 40 to 50 cards per minute, 60 characters per card or a high-speed teletype tape reader at 100 characters per second is the input. Characters are inserted successively into a 5-place A-register and also onto a magnetic drum which feeds all preceding characters to a 5-place B-register. The drum holds $2^{10} = 1024$ characters, the contents of 17 IBM cards, and at each revolution feeds all the characters it then holds through the B-register where they are compared electronically with the contents of the A-register. Through plugging, search can be made for any coincidence up to pentagraphic length in any phase. It calculates the statistic $\Delta = \sum \frac{f(f-1)}{2}$. Hits are wired to one or more of 10 decade counters which are flexibly interconnectable by plugging, each having separate presettable thresholds. When a counter threshold is exceeded, the machine stops and another 517 REPRODUCER punches as

~~CONFIDENTIAL~~

COUNTESS (Cont'd.)

many as 20 identification characters, the contents of the 10 counters and an indication of which counter caused the hit. Dits and blanks are allowed for and the drum automatically limits the length of text acceptable to 1024, causing a punch-out and starting a new cycle, whenever the capacity is exceeded. There are plans to provide means of making lengths of text as low as 100 characters cause a punch-out.

Size is: 8'H x 26'L x 2'D plus two 517 PUNCHES and a tape reader. Drum speed is 7200 revolutions per minute, resulting in up to 125,000 comparisons per second. It will operate at Arlington Hall Station.

Ref: Mr. W. Grogan
Mr. J. Hyduke
Mr. J. Powers

May 1953

DELLA 1 and 2

DELLA (AFSAF D/51-1 and -2) is an electronic round robin comparator using sonic delay lines to match data from magnetic tapes at a megacycle pulse rate. It counts character or variable group hits and lists or punches indications of all matches which exceed a predetermined value. Two equipment were ordered from Technitrol Engineering Co., of Philadelphia. The first operational model was delivered July 1952. A second is due by July 1953. In general, DELLA is designed to do a round robin comparisons of 1000 messages of various lengths up to 1000 characters each in about 17 hours of machine time.

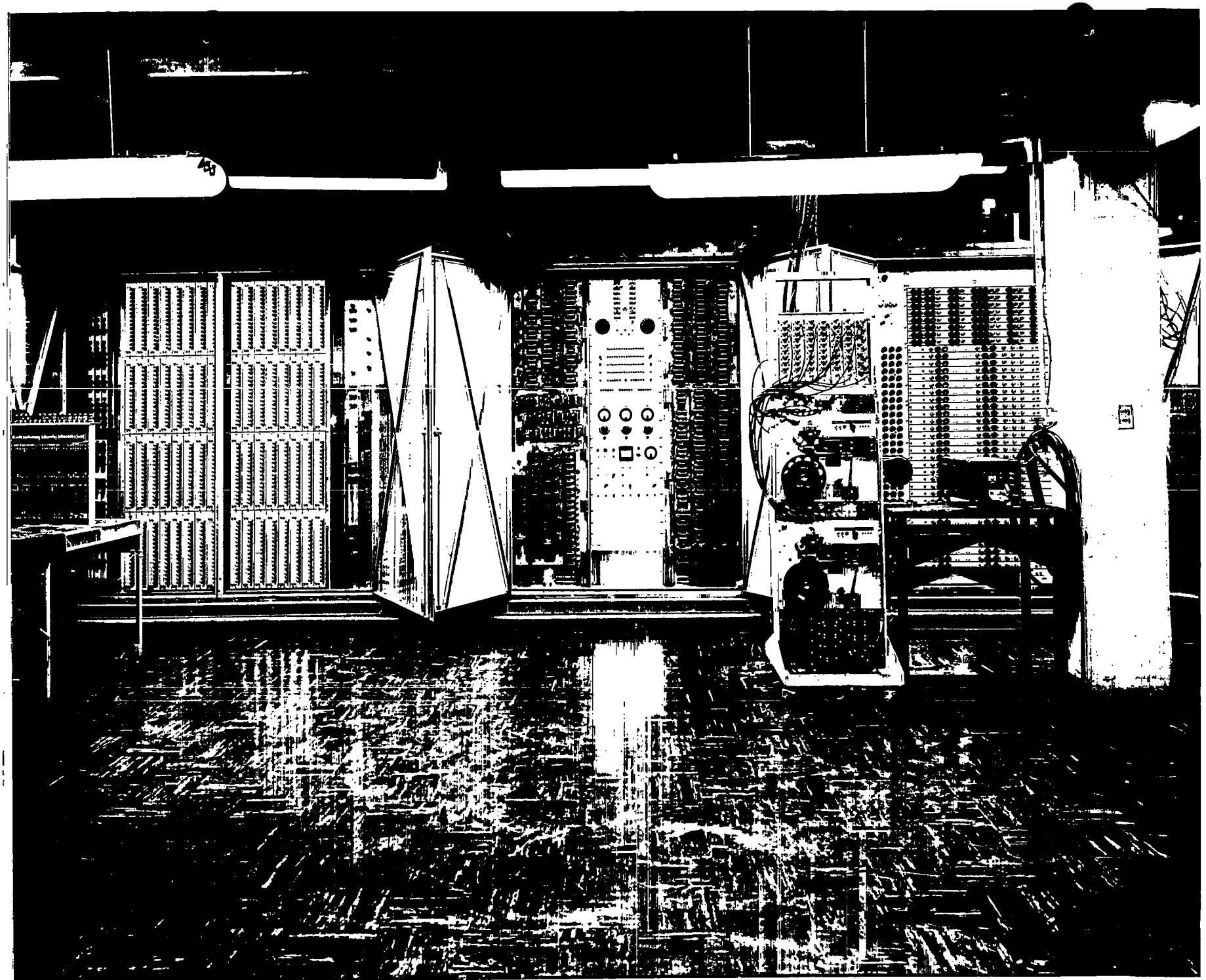
Originally designed for round robin search only, later changes have made possible isomorphic search and mixed monograph-digraph hit counts as well as matching groups between tapes (not within tapes) if so desired. Input is by two or four magnetic tapes as in ABNER. Normally, one half of the messages are put on one tape, and half on the other. Pulsing is at megacycle rate resulting in eight to ten million comparisons per second. Sixty-four mercury delay lines (half the number but identical with those in ABNER) provide the acoustic storage. Comparison circuits and counters are provided for 64 offsets simultaneously. Group length is variable and machine operation is asynchronous, controlled by signals to indicate completion of various steps, sequences, etc. Length and scoring of hits is flexible and easily controlled by switches. Output is to punched tape, and perhaps eventually to an AFSAF 44-1 Printer. Physical units include: Memory,

~~CONFIDENTIAL~~

DELLA 1 and 2 (Cont'd.)

sixty-four counters, timing, control, 4 Raytheon-type magnetic tape inputs, a tape punch output and p wer supply. Its size as 7'H x 16'L x 2'D , plus a motor and a generator unit. It has just completed its initial tests at Naval Security Station in Room 4050 using paper tapes.

Ref: Mr. R. Bowman
Mr. W. Cole
Mr. J. Powers



DELIA
AFSAF D51

~~SECRET~~

~~CONFIDENTIAL~~

May 1953

DUCHESS

DUCHESS (AFSAF-D68) will be a "group IC" device which differences two sequences of 300 characters each at flush start, testing the result for group repeats. Part of the Princess project, the set of devices designated as "high speed statistical placode diagnostic equipment", it is to be the ultimate equipment for which COUNTESS and MISTRESS and CONSORT (the group-IC attachment to SLED) are interim devices. Two models are contemplated, but no full contract has yet been let, although International Business Machine Corporation has already constructed input, output and differencer units. Delivery was planned for 1953.

Using a number of magnetic drums, DUCHESS stores 1000 sequences of 300 digits each and matches each sequence flush with another similar set of sequence strips, searching for group repeats in the result. The test used is the group IC test, $\sum \frac{f(f-1)}{2}$, and is applied to four and five-digit groups.

Outstanding feature of the machine is its huge rate of speed, - all pairings of 1000 magnetic strips, or 1 million matches in an hour. Size has not yet been determined. It will be located at AHS.

Ref: Mr. R. Bowman
Mr. J. Deutsch

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

RESTRICTED

May 1953

EXPANDED COMPARATOR

The EXPANDED COMPARATOR (AFSAF-27) was a photoelectric comparator, an enlarged version of the 70mm COMPARATOR designed to match two tapes or films in search of various coincidences. Hogan Laboratories built the one model in 1950 for Army as an experimental model to test a method of making comparisons. The electronic circuitry worked properly but some of the mechanical features were unsatisfactory.

The device recognized and counted characters or groups of pattern coincidences, using binary electronic counters and twelve pluggable recognition units. It could be plugged to indicate when a threshold had been exceeded, could do weighting, or divide the field of viewing into sub-fields for high-low comparisons. A photoelectric cell scanned each of 272 possible spots (16 levels by 17 frames in the gate at one time). Two or three films or tapes, each up to 200 frames long, were placed in the gate and the fast film was pulled by at a rate of 1000 frames per second. Output was to (1) a matrix of neon lights indicating visually which of the 272 photoelectric cells was receiving light, to (2) a built-in recording device which gave a print-out at user's option on facsimile paper, or to (3) an applique unit built to record decimally the totals in the binary electronic counters.

Never intended for operational use, it has been dismantled. There were four major units, the largest measuring 7'H x 4'L x 6'D ;

RESTRICTED

~~RESTRICTED~~

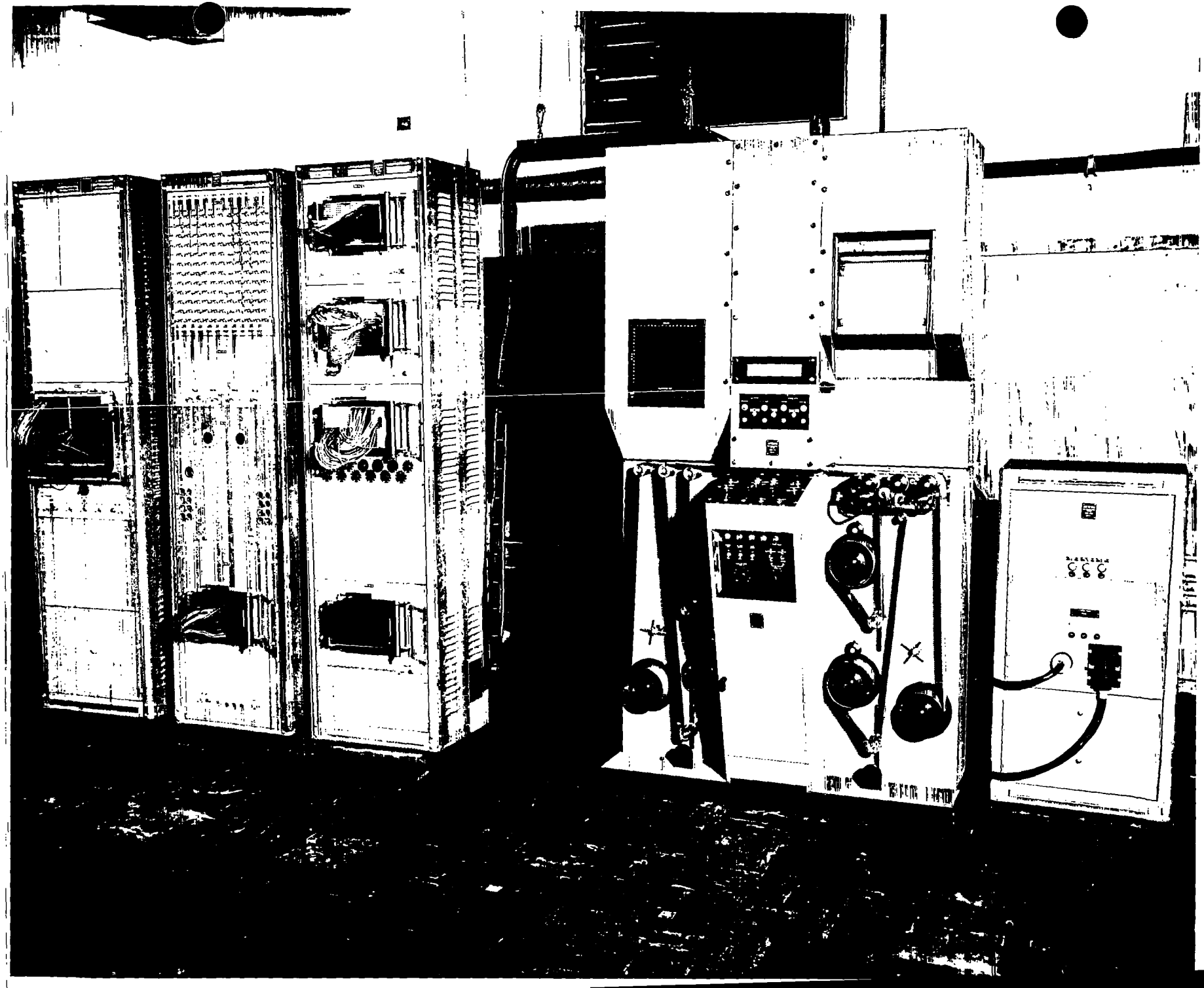
EXPANDED COMPARATOR (Cont'd.)

the other three together measuring 7'H x 6'L x 2'D , plus power supply and a small applique printer unit. Rate of comparison was effectively 272,000 individual comparisons or 1000 matrix comparicons per second.

Ref: Mr. E. Fleming
Miss M. Hobbs
Mr. J. Raisch
Mr. S. Snyder

~~RESTRICTED~~

~~RESTRICTED~~



~~RESTRICTED~~
SECRET

~~RESTRICTED~~

May 1953

FREAK I

The FREAK (AFSAF-24, MULTIPLE FREQUENCY COUNTER, later called FREAK I, RELAY FREAK or CONDENSER FREAK to distinguish it from the ELECTRONIC FREAK which superceded it) was a relay operated frequency counter. It used condensers for storage of totals, to make monographic and digraphic counts of digital or literal text, handling up to 32 character alphabets. One model was built by Army in late 1943. It proved to be unreliable and was dismantled. The B-211 STECKER FINDER was designed to operate in conjunction with FREAK but saw little usage due to the counters erratic performance.

It consisted of two tape readers, a bank of relays, 32 x 32 or 1024 sets of seven condensers each, a scanning circuit, and an electromatic typewriter. The machine distributed successive digraphs read from two tapes to the proper set of condensers. A ring circuit automatically distributed text for a monographic distribution. The device also evaluated $\sum \frac{N(N-1)}{2}$, for each distribution.

It consisted of five relay racks and measured 9'H x 8'L x 2'D plus two tape readers for input and a regeneration typewriter for output. Rate of operation was 6 characters per second and final recording took 14 minutes for a full width of 32. Its major use was on HAGELIN problems and for cyclic distribution.

Ref: M.A.C. Outline #11
Mr. J. Russell

~~RESTRICTED~~

~~SECRET~~
~~RESTRICTED~~

May 1953

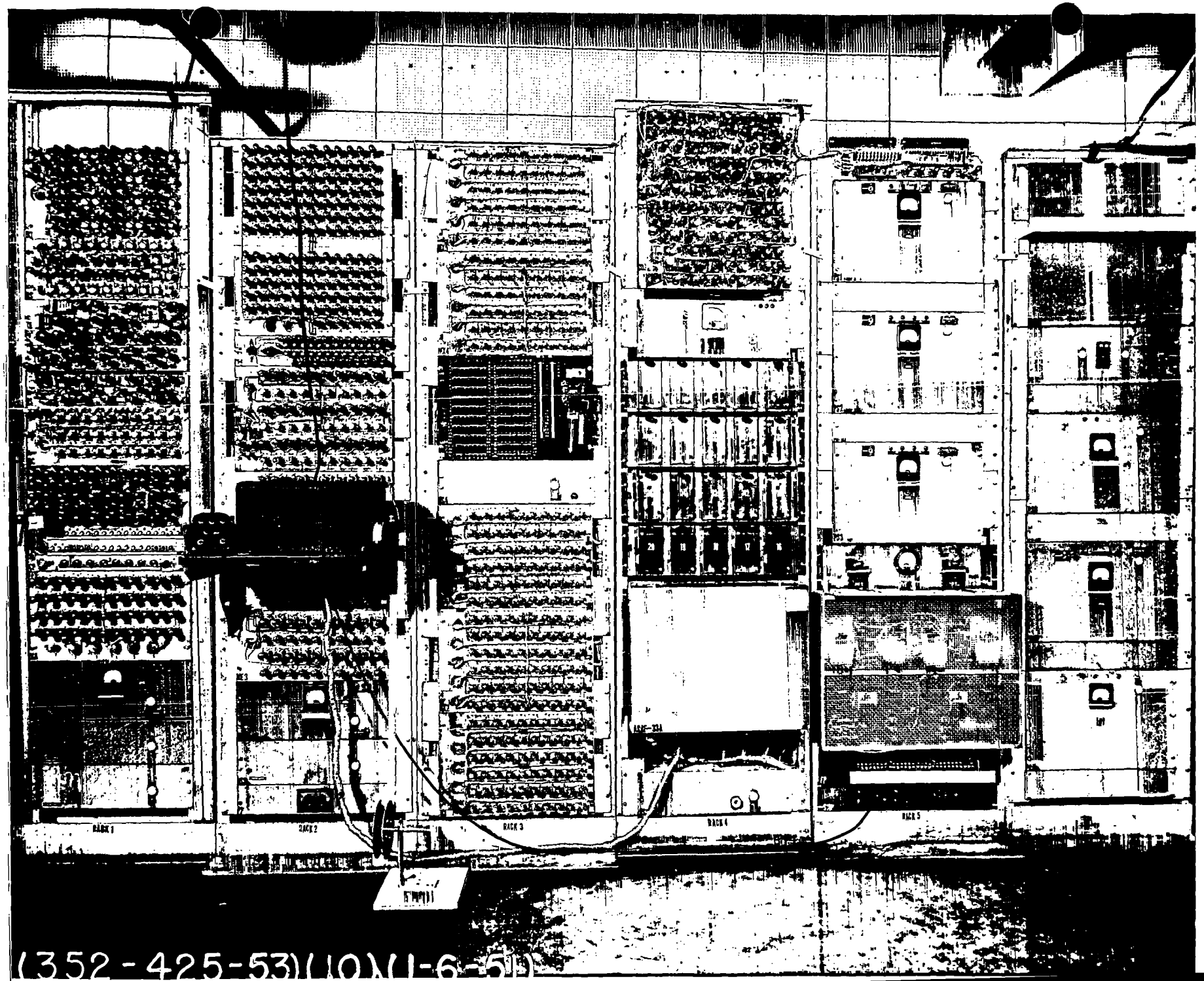
FROG

FROG (AFSAF-33, B-211 CRIBDRAGGER, [redacted]) is an electronic message setter for solving traffic from a straight-plugged (at the top) B-211 cipher machine. It was designed and completed by NSA-352 on 1 July 1950. Original plans called for one engineering model and one operational model. Serial 1, a bread-board model, proved quite efficient and is still in use. Serial 2 is under study by NSA-35B. There are plans to contract soon for its construction, with delivery expected in September 1953. The name, FROG was only recently applied to the machine when plans for Serial 2 were initiated and has since been applied to both.

A maximum crib of 20 letters is represented as a 20-card deck, usually by drawing one pre-punched 3 x 5 card per fractionated letter of crib. Each card contains coded punches in a 30 x 5 matrix. The 30 levels provide for the combined minimum cycle of a 15 and 10 wheel. The five positions in the vertical dimension provide for the five columns of the internal B-211 fractionating square. This plain text deck and a cipher text tape are fed into the machine which goes through the full cycle, testing all motions and turnover possibilities, at the same time checking for bottom stecker at every setting.

A crib can be tested in all positions of a 500 letter message in about 6 or 7 hours. The machine measures 6'H x 12'L x 1'D (6 frames, incorporating a ring of 30 thyratron tubes). Serial 1 is located at AHS in Room 0414-B.

Ref: Mr. J. Cochran
Mr. M. Collins
Mr. R. Moulton
T/SA 11
T/CA 12



(352-425-53)(10)(1-6-61)

FROG I
AFSAF 33, B-211 CRIBDRAGGER,
B-211 SOLUTION DEVICE

~~TOP SECRET~~
~~FROTH~~

May 1953

GEEWHIZZER I - IV

The GEEWHIZZER (AFSAF-112, ELECTROMECHANAGRAMMER) is a weighting device used with a 405 or 407 TABULATOR to slide a stretch of cipher text (originally 10, later 12 and then 16 letters) against the rest of the message, selecting and summing weights according to the resulting digraphs. Four models were built successively. The first, in 1941, was merely a set of rotary switches in a small box and was probably the first IBM relay gate. The second was a set of wire contact relays mounted in a 60 x 34 plugboard cover. The third, of heavier construction, was a 3'H x 2'L x 2'D gate, mounted separately to avoid vibration. The fourth or NEW GEEWHIZZER, often erroneously called Model II, is really Model IV. It is electronic, supercedes the first three and has additional functions.

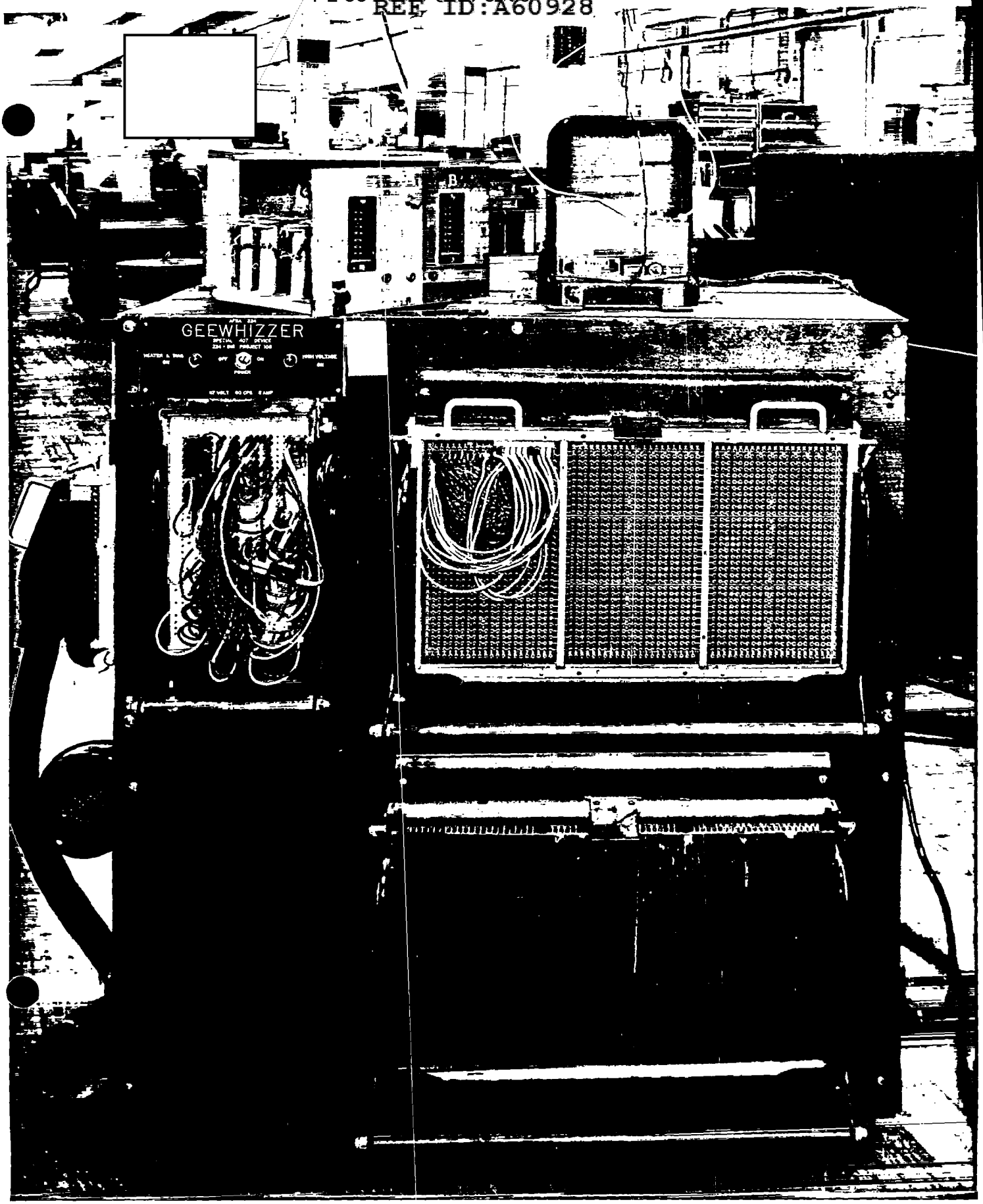
In operation, the particular set of letters chosen, usually the first of text, are plugged on a 405 or 407 TABULATOR and the cipher message read from cards (from tape or cards in Model IV) together with associated sets of log weights of each particular letter, considered both as initial and final half of a digraph. These weights, 0 through 9, and later 00 through 50, are totalled and listed, while all totals above a preset threshold are wired to print in a separate column to facilitate locating the best answer. Model IV has a 32 x 32 pluggable electronic matrix, can do Fourier weighting and is currently at work setting messages in a special case of B-211

GEEWHIZZER I - IV (Cont'd.)

usage where five wheels and a part of the indicator are known.

The tiny first model is still in storage at Arlington Hall Station in Room 1501-A. The second and third have been dismantled. The latest device is 4'H x 4'L x 2'D and has a speed of 2 or 3 cards per second. Location is at Arlington Hall Station in Room 1600-A.

Ref: M.A.C. Outline #1
Mrs. D. Blum
Mr. J. Powers
Mr. S. Thorne



GEE-WHIZZER IV
AFSAF 112
NEW or ELECTRONIC GEE-WHIZZER.
On top, at left is the original
GEE-WHIZZER I or ELECTROMECHANAGRAMMER

~~TOP SECRET CANOE~~

May 1953

GREEN ANALOG

The GREEN ANALOG is a relay device for completely reproducing any function of the Japanese GREEN machine, a 6-wheel cipher device, never used operationally. The analog was built by F Branch, of Army, completed in February 1946, after World War II ended, and delivered to the museum.

Input is by keyboard or tape reader head, and output is to a teletype page printer or tape punch. The 25-point rotors and their complex stepping were simulated by relays. Although rotor wiring was fixed in the two captured converters, four 8 x 20 plugboards allowed for changes. The system used 45 plain text characters and 100 cipher text digraphs, including variants.

The analog measured 6'H x 5'L x 2'D plus a page printer, keyboard, tape reader head and punch. The GREEN converter itself was portable, typewriter size, and never came in for much use. The analog is still in the museum, in NSA-18, stored in the attic of Building 20 at Naval Security Station.

Ref: NSA-354B files
Mr. D. Dribin
Mr. F. Mayol
Mr. S. Snyder

~~TOP SECRET CANOE~~

May 1953

HAGELIN MESSAGE SETTER

The HAGELIN MESSAGE SETTER (AFSAF-38) is a relay operated wheel-setting device which [redacted] Two units were built by Army, the first, by WDGAS-74, was delivered 29 October 1949, and the second (AFSAF-38A), by NSA-354B, on 15 December 1950. There are plans for a third equipment to replace the now worn out first unit. In such a machine, [redacted]

There are four major components, a storage portion consisting of relays and condensers, a comparison circuit for matching key and cipher text, a maze circuit which interprets the comparisons by phases and a control circuit which checks for required conditions and controls the machine accordingly. In operation, [redacted] signs. Counters show the digits of key in the machine. Means is

HAGELIN MESSAGE SETTER (Cont'd.)

provided for manual stopping. In unit II there are provisions for six choices [redacted]

Unit I, a table-top apparatus, measures one cubic yard plus tape reader. Unit II measures 6'H x 2'L x 2'D . Both units are still in Room 2208-A at Arlington Hall Station, but the older one is unused. Tests are made at a rate of 6 to 10 characters per second.

Ref: NSA-354B File
Miss B. Church
Mr. N. Christopher
Mr. W. Cole
Mr. F. G. Mayol

HAGELIN MESSAGE SETTER (Cont'd.)

provided for manual stopping. In unit II there are provisions for six choices [redacted]

Unit I, a table-top apparatus, measures one cubic yard plus tape reader. Unit II measures 6'H x 2'L x 2'D . Both units are still in Room 2208-A at Arlington Hall Station, but the older one is unused. Tests are made at a rate of 6 to 10 characters per second.

Ref: NSA-354B File
Miss B. Church
Mr. N. Christopher
Mr. W. Cole
Mr. F. G. Mayol

~~TOP SECRET CANOE~~

May 1953

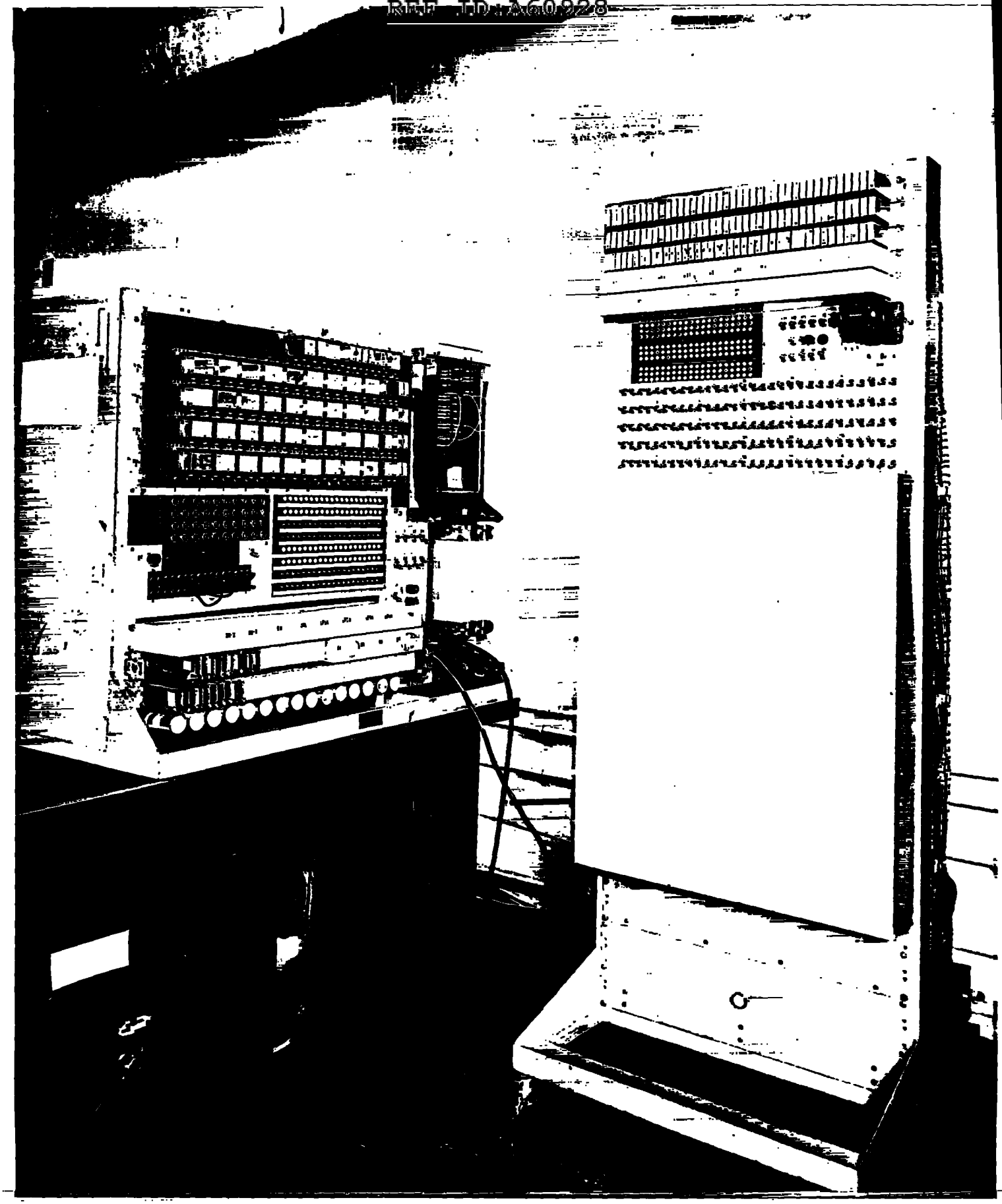
HAGELIN PARITY STREAM GENERATOR

The HAGELIN PARITY STREAM GENERATOR (AFSAF-46) is a relay operated table-top key generator which [redacted] Application is to the HAGELIN C-38 and similar machines. It was built by Army and delivered on 28 February 1950.

[redacted] and output is supplied either directly as an input to the HAGELIN MESSAGE SETTER and/or to a tape punch. Wheel starting positions are set up by push buttons. Lamps indicate the wheel positions at all times.

The device is a table-top model and measures 2'H x 3'L x 2'D. Rate of operation is 6 to 8 characters per second. It is currently in use at Arlington Hall Station in Room 2208-A, in conjunction with the HAGELIN MESSAGE SETTER.

Ref: TO/A 12
NSA-354B Files
Mr. H. Christopher
Mr. F. Nagel



HAGELIN PARITY STREAM GENERATOR
(loft) AFSAF 46
and
HAGELIN MESSAGE SETTER # 2 or
HAGELIN [redacted]
TEST DEVICE
AFSAF 38A

TOP SECRET
FROTH

May 1953

HECATE

HECATE (AFSAF-91, CXDD or HAGELIN CRIBDRAGGER) is a special purpose high speed electronic cribdragger for solving C-38 type HAGELIN messages by exhaustive trials. Two equipments, Serial 1 and 2, were built for Navy by Engineering Research Associates, now part of Remington Rand, the first delivered 1 April 1948 and the second on 16 May 1950. A SATYR is used with each as auxiliary equipment to [redacted] The name HAGELIN CRIBDRAGGER was recently applied to the subproject 351-411, and the term HECATE to 351-411-51 to be sure the subproject covers the full cribdragger field and not a specific equipment.

The machine in general requires [redacted] keys. At a hit, the machine stops to permit hand recording of each possible window setting it finds. Four brief tests on a SATYR will establish the wheel pattern and setting of the two excluded wheels whose patterns are usually known.

Both models are now in operation at Naval Security Station in Room 20103. Dimensions of the tape unit are 6'H x 4'L x 3'D ; and of the analytic section, 6'H x 17'L x 3'D . Operation is at the rate

HECATE (Cont'd.)

of 75,000 trials per second, each window setting being tested in about fourteen microseconds.

Ref: TO/A - 17
NSA-3023 Files
Mr. D. Hogan
Mr. J. Stapleton
Mr. L. Wheatley

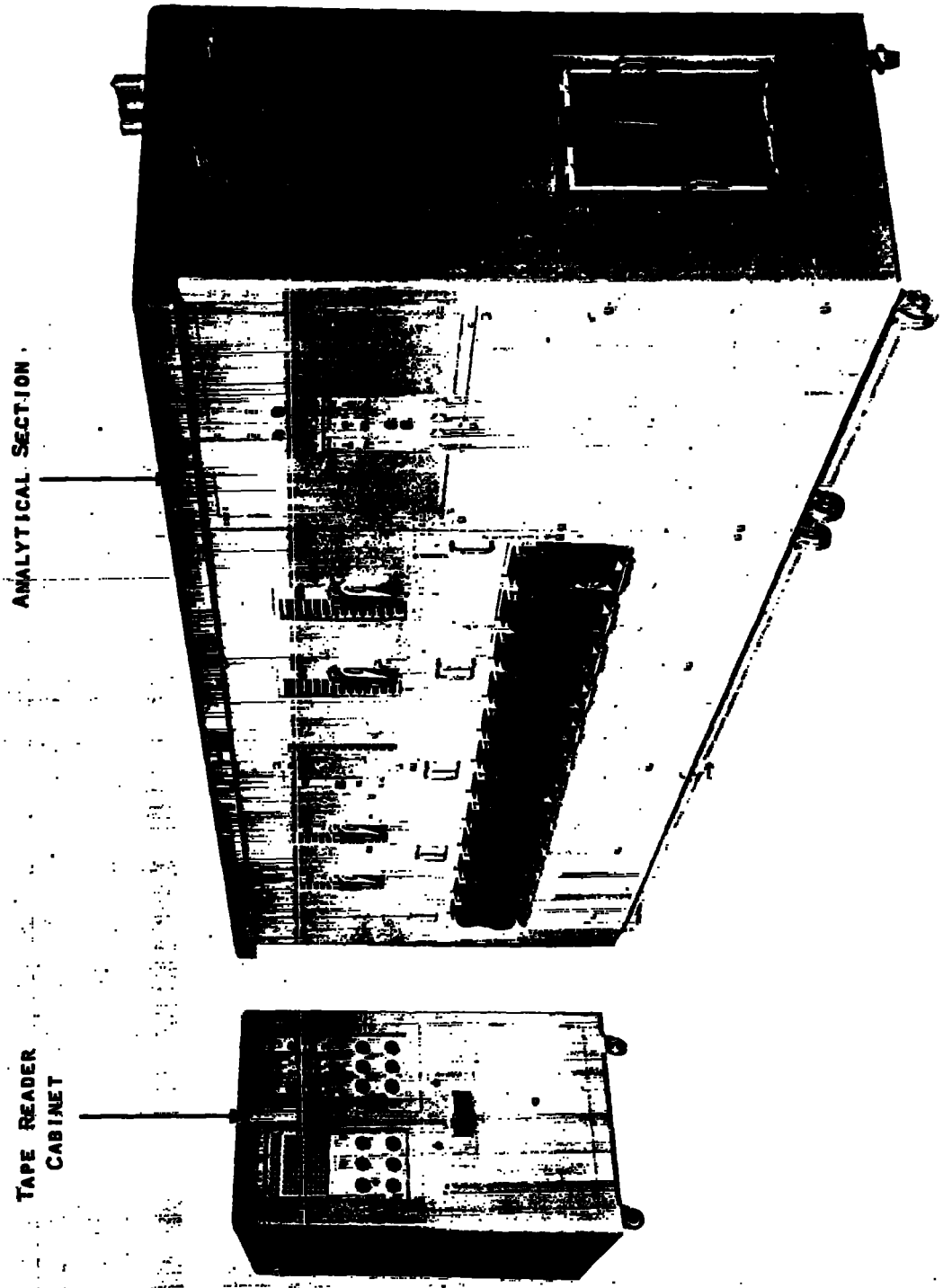


Figure 1-1. Hecate, Serial 1 Equipment, Model CXDD

HECATE
AFSAF 91
HAGELIN CRYPTOGRAPH, CKD

TOP SECRET

FROTH

May 1953

HELLCAT I

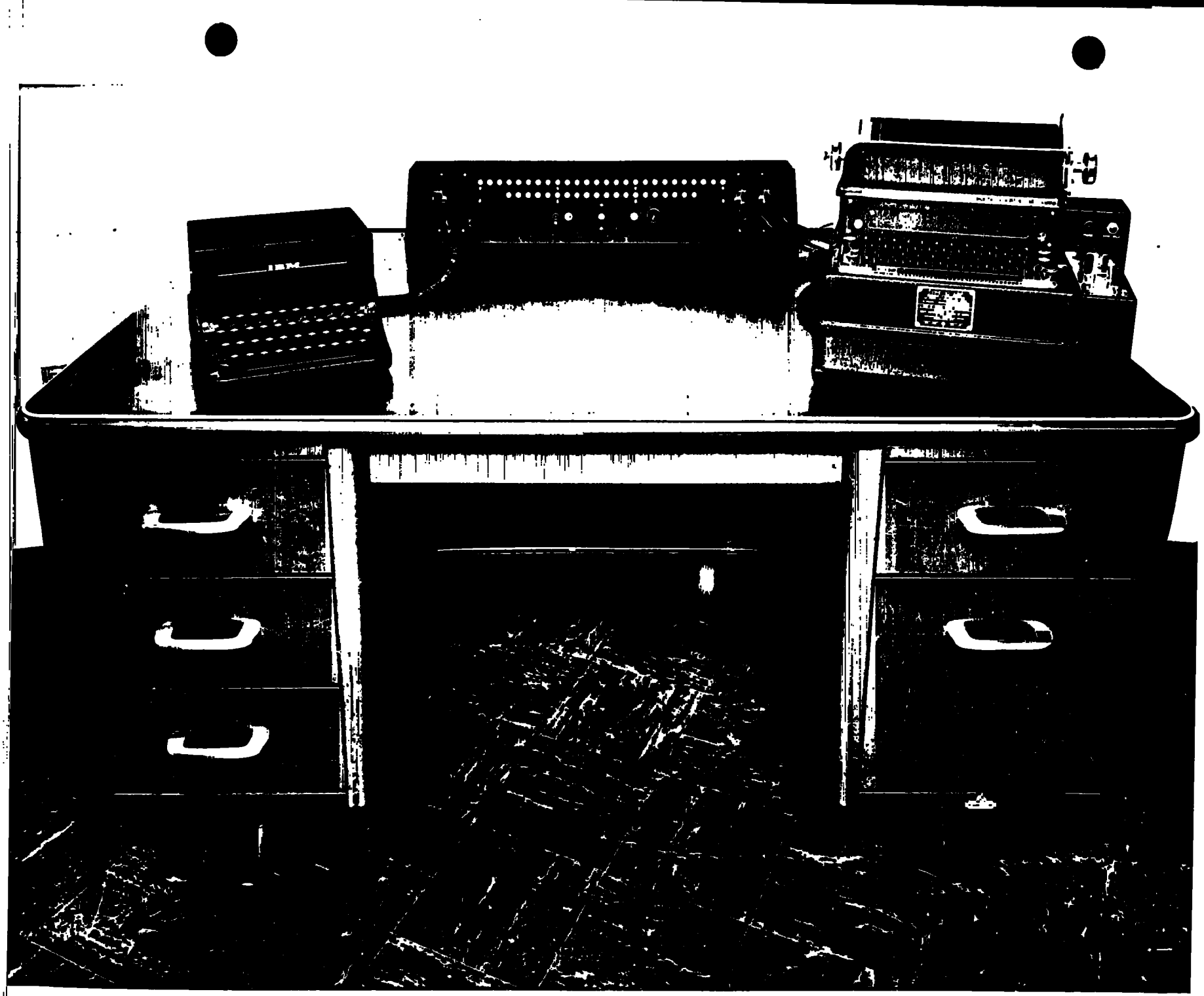
HELLCAT I (originally ELKET for ELECTRONIC KEY TESTER, and also called MATTHEW, JR., DEF 59, AFSAF-D/59) is a desk-side deciphering device and key tester, relay operated, with provision for up to 26 mixed alphabets. It is a general purpose version of DMD, and in some functions resembles MATTHEW more than it does HELLCAT II. The one model ordered was built by NSA-354B for NSA-23 and was delivered in February 1953.

When a set-up switch is thrown, up to 20 letters of key or text may be entered in the relay memory via a ring circuit which acts as a counter and a storage control. Given 26 random alphabets of 26 letters each, set up on a 34 x 60 plugboard, the machine applies assumed key or plain against cipher and derives possible plain or key. Output is to a regeneration typewriter. The ring circuit position, and therefore the particular alphabet and key being used, is shown by lights.

It is 3'H x 6'L x 1'D , designed to fit under the overhang of an executive-type desk. Operation rate is 6 to 8 characters per second. Alphabetic and numerical substitution is possible. It is now located at Arlington Hall Station in Room 2522-A.

Ref: TC/A 8/50
NSA-354B Files
Mr. N. Christopher
Mr. F. Lagol
Mr. K. Polloy

[redacted]



HELLCAT I
AFSAF D59
MATTHEW, JR
formerly ELKET,
ELECTRIC KEY TESTER

CONFIDENTIAL

May 1953

HIGH-SPEED TELETYPE TAPE READER

The HIGH-SPEED TELETYPE TAPE READER (AFSAF-D/63 or CHADLESS TAPE READER) is a high speed, mechanical teletype tape reader. Enough unassembled parts and reading-head assemblies (the novel element) to permit NSA-35 to assemble twenty-nine of these readers, was received from Teletype Corporation in May 1953. Development by NSA-35 of a pair of experimental CHADLESS READERS, one mechanical and the other photoelectric and pneumatic (The PALLY READER), was discontinued when this model was introduced.

Its function is simply to read data from Chadless (or non-Chadless) tape at higher speeds than earlier devices, and will be used as input to numerous equipments.

Rate of operation is from 100 characters per second up to 240 characters per second. Its size is tiny, 5"H x 6"L x 6"D . These readers are being put to use in various locations.

Ref: Mr. R. Bronder
Mr. J. Deutsch
Mr. J. Russell

~~CONFIDENTIAL~~

May 1953

ICKY I

ICKY I, (TETRAGRAPH II or CXCL, called TESSIE by Army personnel), was a general purpose 35mm photoelectric comparator and tetragraph tester built for Navy by Eastman Kodak Co., in 1943. A total of three units was built, the first two being delivered to Navy and Army respectively in October and November 1943. It replaced TESSIE SS, Navy's original tetragraph tests and is superceded by Army's TESSIE II (AFSAF-11).

The four original cameras were small and simple (about 25 pounds), merely transferring data from punched tape to 35mm film. BRUTE I, developed by Eastman Kodak Co., and received in June 1944, provided a greater concentration of information on the film and complicated identification data. It measured 4'H x 3'L x 6'D and was never used operationally. Two new and more flexible cameras, BRUTE II, Serial 1 and 2 (M.A.C. Outline #60), were delivered in March and May 1948. Each is a double camera and exposes film at a rate of over 6 characters per second from cards, or 10 characters per second from tape. Size is 5'H x 3'L x 9'D .

The machine compared two films on which literal or numerical text was represented as clear rectangular spots in a field 30 levels deep together with identification data. The search was for either polygraphic repeats or high I.C. Through a gate 35 characters wide, the films were automatically compared, one held in place and the other drawn past at 3500 frames per second. The "slow" film was moved

~~CONFIDENTIAL~~

ICKY I (Cont'd.)

up as many as 30 frames at the end of each pass by the "fast" film. When the proper number or pattern of letters was found, a neon light flashed and the machine stopped to permit a hand record of the visually represented data.

Size of the machine was 4'H x 2'L x 2'D and rate was 3500 comparisons per second. It was modified by Eastman Kodak Co., in 1948, but was still considered unreliable and so was dismantled. Army's variation of this device, built in 1945 is called TESSIE II or AFSAF-11. Plans for an ICKY II (CXNR) were drawn up then abandoned.

Ref: CIT paper 6
CIT paper 48
M.A.C. Outline #3
Mr. G. Kier
Mr. J. Stapleton
Mr. L. Wheatley

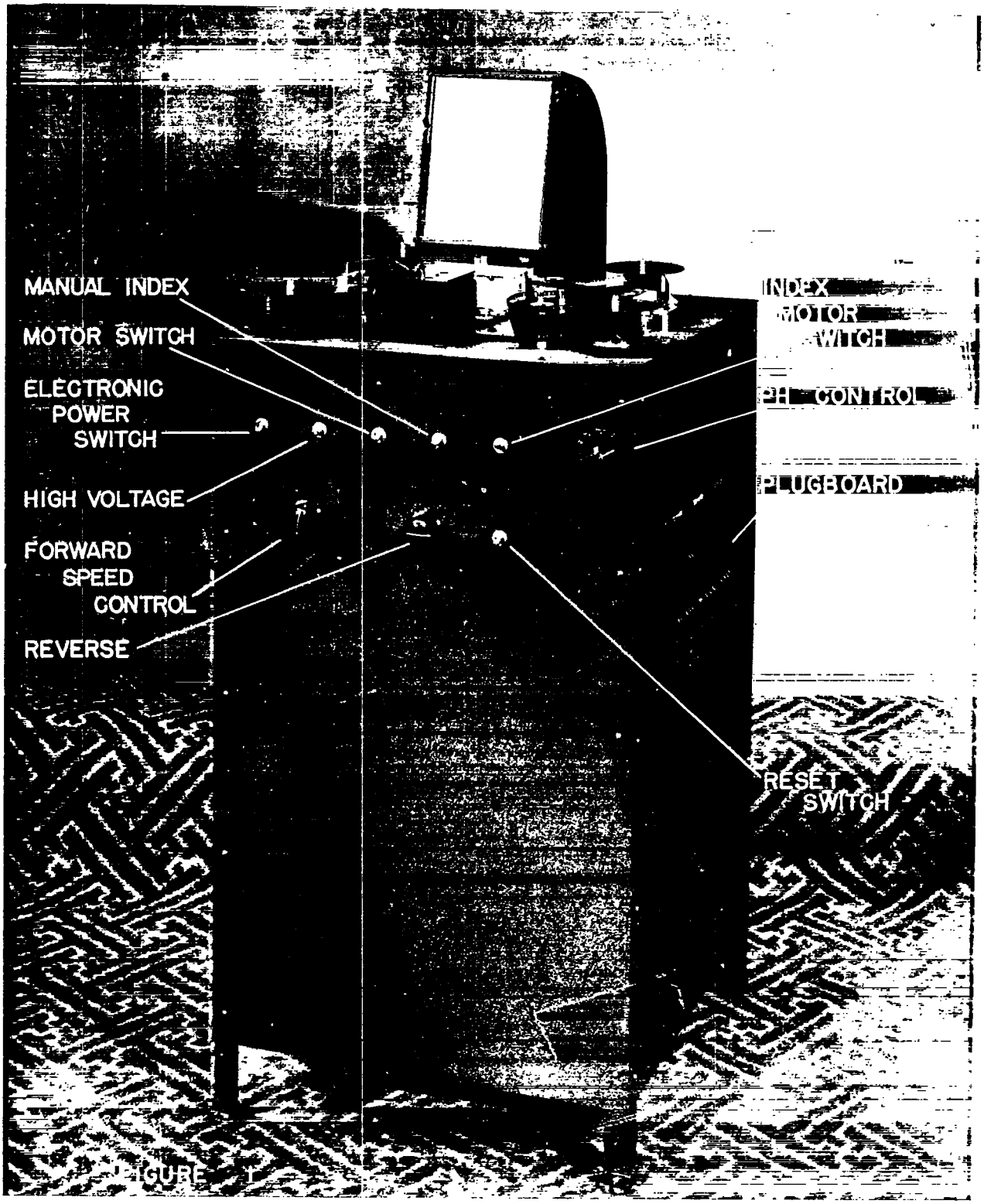

MANUAL INDEX
MOTOR SWITCH
ELECTRONIC POWER SWITCH
HIGH VOLTAGE
FORWARD SPEED CONTROL
REVERSE
INDEX
MOTOR
WITCH
CONTROL
PLUGBOARD
RESET SWITCH

FIGURE 1

ICKY I
AFSAF 103
CXCL, TETRAGRAPH II
ambiguously called TESSIE by some

~~SECRET~~

May 1953

IDA

IDA, (from Isomorphic Depth Analysis, AFSAF-1-X, CONNIE-1-X, DEF-52, AFSAF-D/52) is essentially a stripped-down CONNIE, a special purpose electronic tape comparator for isomorphic pattern search. The AYE-AYE (AFSAF-D52/10, XFN), the associated tape punch for patternizing tape, was completed by NSA-224 in June 1950. The first breadboard model IDA was ready shortly thereafter, and the second, an operational model, was finished in 1951.

The machine counts monographic coincidences of isomorphic repeats over a span of 10 to 12 characters. Two patternized loop tapes are read by a pair of photoelectric readers at 5000 characters per second. AYE-AYE uses 3 frames on the pattern tape to indicate the location of each repeat found in the preceding 12 characters of text. It considers a particular character and punches a hole in level 1 to 5 of the first frame if a repeat is found in the first five preceding characters; in level 1 to 5 of the second frame, for a repeat found in the sixth through the tenth preceding characters. These are pluggable. The character itself is punched into the third frame. Addition of 1, 2, or 3 characters to one tape causes a precession of corresponding step-size between tapes. Each result is in the form of a confirmation or conflict. These are weighted and summed. All totals over a preset threshold are recorded on a 517 REPRODUCER PUNCH.

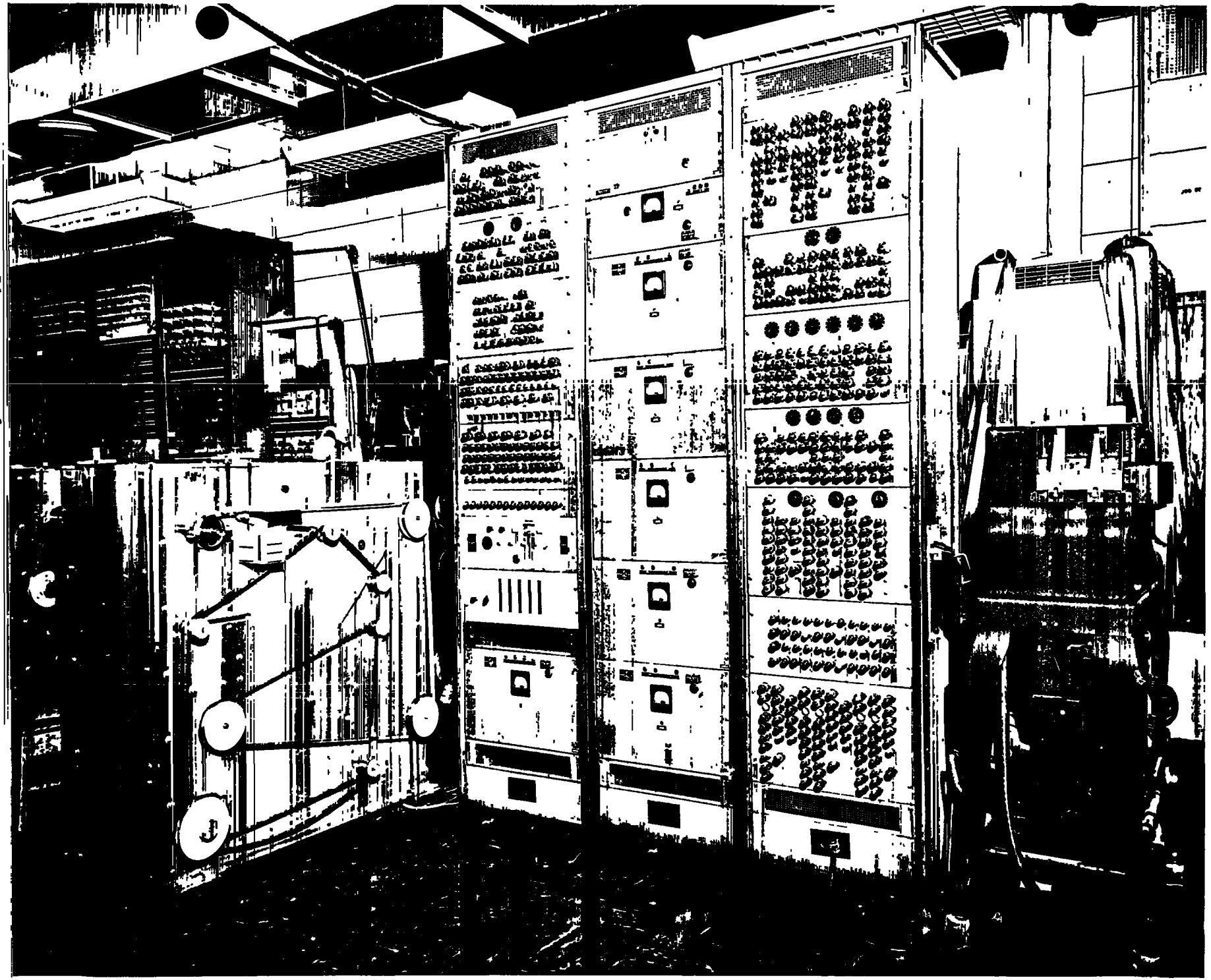
Size of the comparator is 7'H x 6'L x 2'D plus two tape readers

~~CONFIDENTIAL~~

IDA (Cont'd.)

5'H x 4'L x 2'D each and 517 PUNCH. IDA is now in operation at Arlington Hall Station in Room 0411-B. Comparison time on an average pair of tapes is five to twenty minutes.

Ref: Mr. W. Cole
Miss M. Hobbs
Mr. T. McGuire
Mr. J. Powers



IDA
AFSAF D52, Isomorphic Depth Analysi
with CONNIE reader input (left) and
IBM 517 REPRODUCER output

~~TOP SECRET CANOE~~

May 1953

IMITRAM

IMITRAM (MARTINI spelled backward) was a relay analog of the LONGFELLOW [redacted] SHARMANKA type. It was built by Navy in 1948 from a cannibalized VIPER to serve as a companion machine to MARTINI which it completely duplicates except that it has a backward stepping feature. Its purpose was to exploit a fund of knowledge about message endings.

The machine automatically followed in reverse the prescribed key cycle and rule of motion, stopping at ambiguous points to permit the operator to choose which path it should take. Frequent use was made of it as a handtester. Input was by tape or keyboard; output was to a regeneration typewriter.

Size was the same as for MARTINI, 6'H x 4'L x 4'D and rate was six to eight characters per second. It has been dismantled.

Ref: Mr. H. Campaigne
Mr. T. Hollcroft
Mr. J. Stapleton

~~TOP SECRET CANOE~~

May 1953

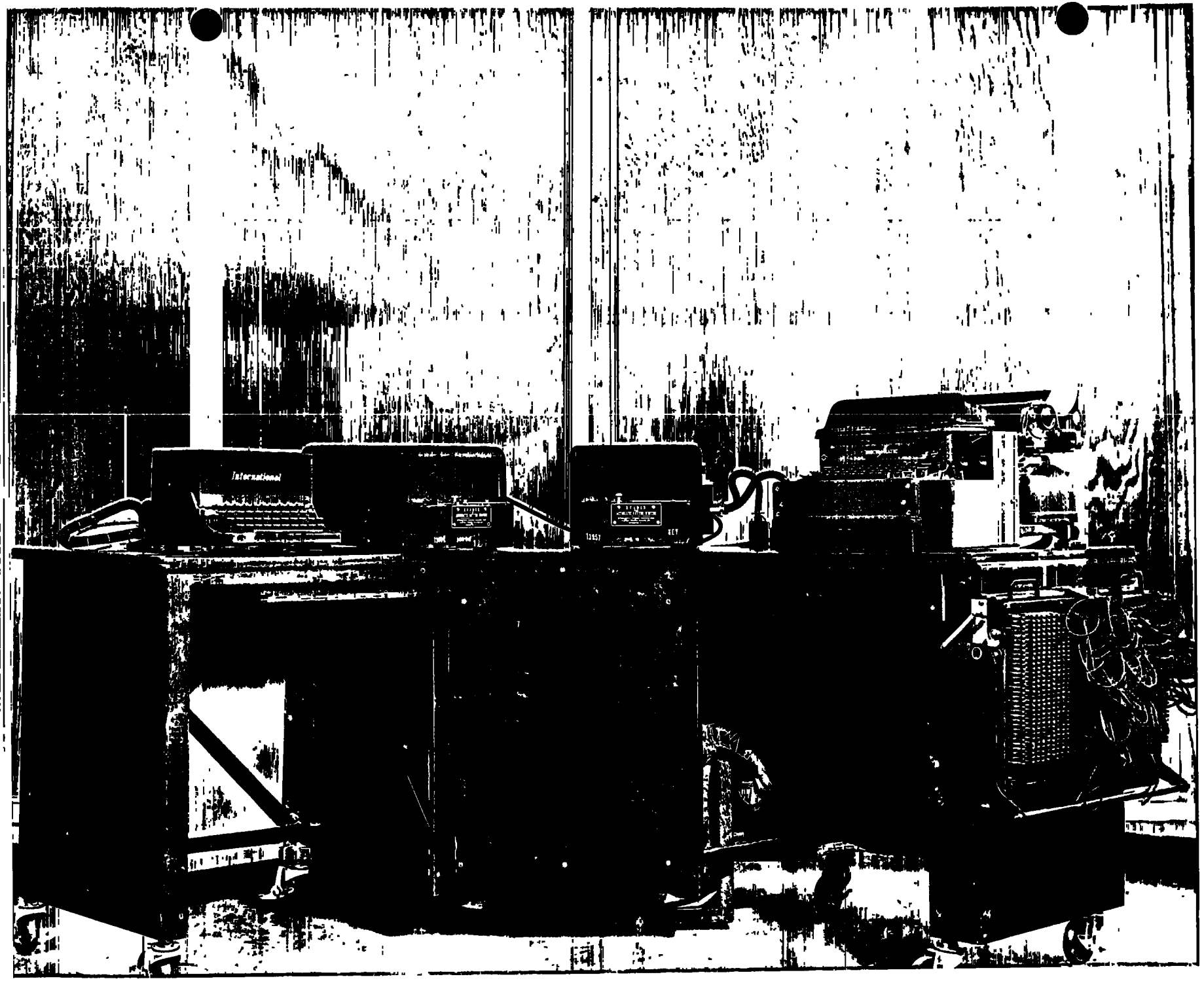
JMA DECIPHERING MACHINE

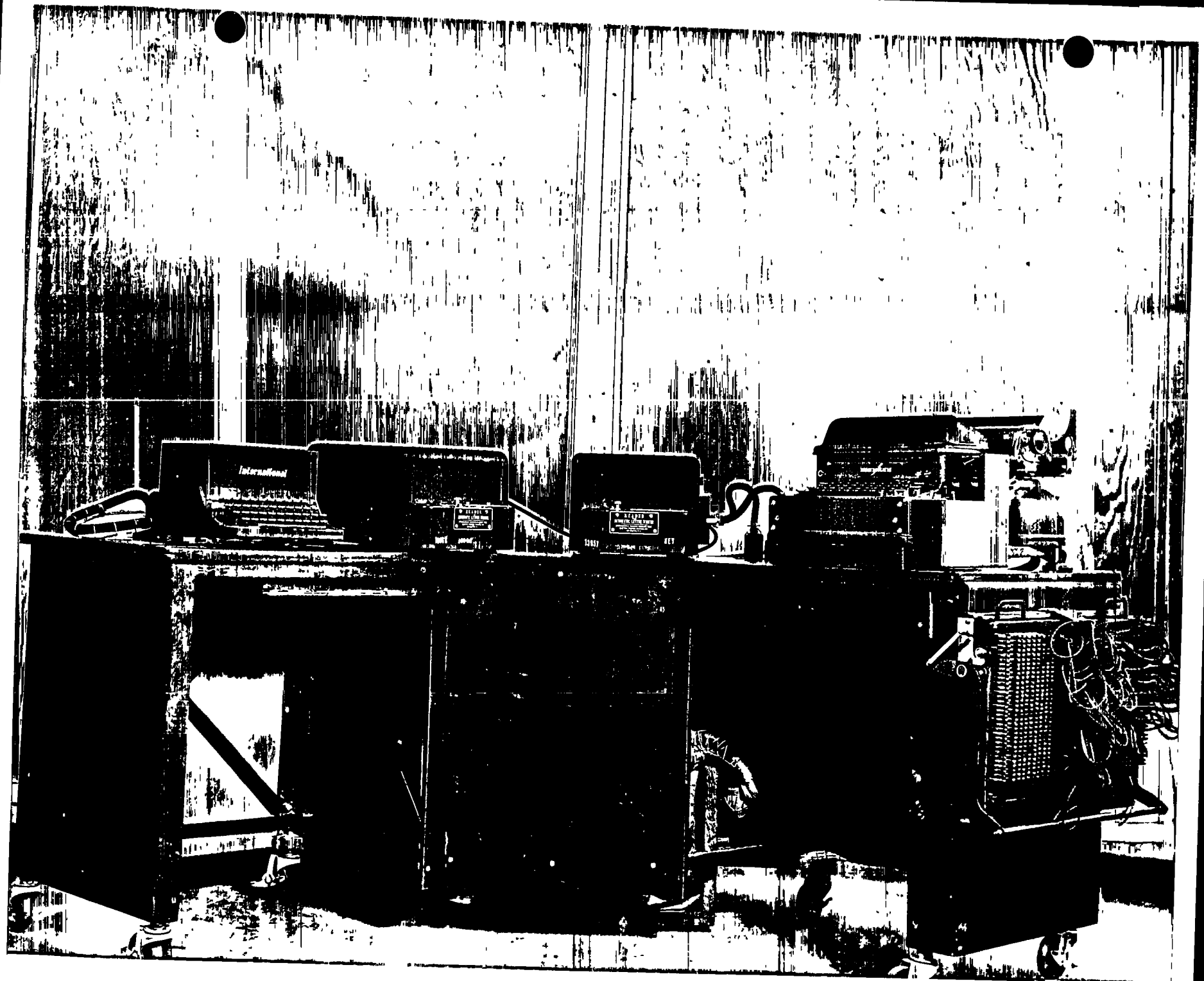
The JMA was a relay-operated deciphering device, deriving its name from the Jap Military Attache system it was built to attack. Originally designed to perform a process equivalent to sliding alphabet strips to find the proper substitution alphabets according to running key, later modification permitted deciphering by any of 26 unrelated alphabets. It was built by Army in 1942 and replaced by MATTHEW.

The machine is best understood when visualized as a 26 x 26 square where an electric typewriter operated to select a letter wired to the left margin (usually according to cipher text) while a synchronized tape-stepper selected a letter (from running or cyclic key) wired to the top of the square. The value found at the intersection of such a row- and -column selection was determined as a certain value according to a plugboard wiring. Thus the machine added any given key value to a corresponding cipher value and gave a predetermined answer.

It handled a 26 character alphabet, used a double tape reader for input and regeneration typewriter and/or tape punch for output. By reversing the role of key and plain or of key and cipher, the JMA could perform enciphering and be used for placement or test purposes. It operated at typist speed and has been dismantled. The 26 x 26 matrix was housed in a CXCO dolly 2'H x 4'L x 3'D with teletype tape reader, IBM keyboard and regeneration typewriter.

Ref: M.A.C. Outline #2
Mr. S. Snyder





JMA DECIPHERING MACHINE

TOP SECRET

FROTH

~~TOP SECRET CANOE~~

May 1953

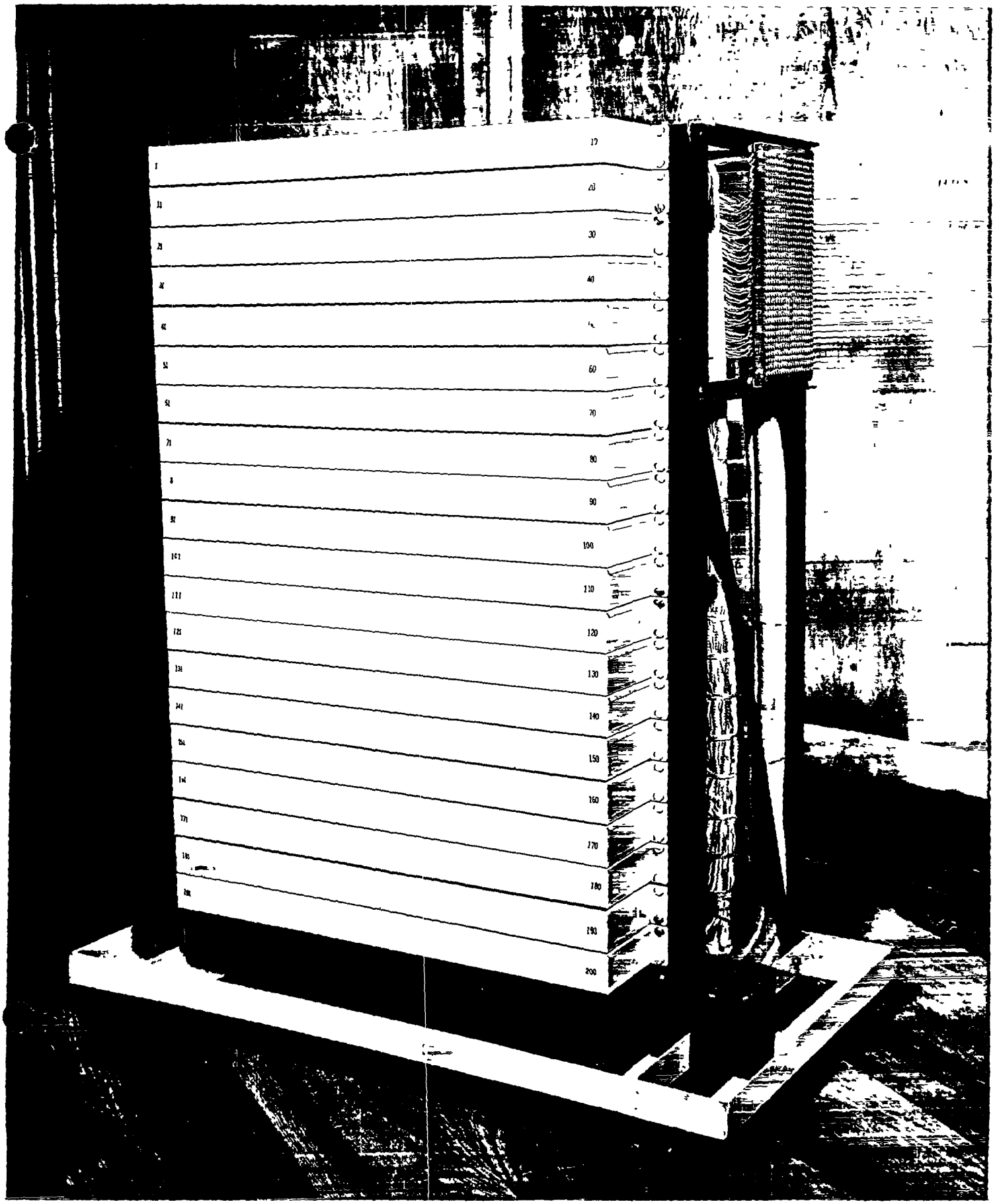
J-SQUARE UNITS

The term J-SQUARE designates a family of 23 equipments whose basic function was code decipherment and recognition. To these probably should be added the three LIMITED SELECTORS and the two CODE RECOGNITION UNITS. All units were built by Army's F Branch, now NSA-354B, and operated in conjunction with an IBM 405 TABULATOR or a 517 PRE-SENSING PUNCH. The 32 x 32 ALPHABETIC SUBSTITUTION UNIT (5'H x 6'L x 3'D) was built by F Branch in 1947 as a logical extension of the 10 x 10 numerical J-SQUARE UNITS, and is still in use at Arlington Hall Station in Room 1700-A.

In general, these devices simulated a 10 x 10 Jap Army cipher square and operated to strip probable additive from a given number of cipher text groups, matching the resulting possible plain groups against a list of high frequency groups set up on a plugboard. It printed and/or punched any recognized groups, together with appropriate collateral notations. All operated at tabulator or tape punch speed, 80 or 100 cards per minute. A listing of equipments, with dates and dimensions is attached. They are all dismentled.

Ref: NSA-354B files
Mr. F. Mayol

~~TOP SECRET CANOE~~



J-SQUARE UNIT
For decipherment and recognition

TOP SECRET

FROTH

~~TOP SECRET CANOE~~ May 1953

LDM

The LDM (LONGITUDINAL DIFFERENCING MACHINE) was a tape differencer consisting of an IBM tape reader (SIGTOT) modified to read either one or two tapes. Used in connection with a small relay unit, it could difference on modulus 2 either consecutive Baudot characters in one tape or characters from two tapes. It was built by Army Security Agency in 1944 for teleprinter cipher systems such as TUNNY.

The modified reader translating one or two tapes was connected to a relay unit. In the unit were three sets of five relays, each corresponding to the five bauds in the characters. Two sets were operated from the reader when two tapes were being read, with the third set governing the other sets. The third set was operated by the combination of the two and in turn operated a regeneration typewriter and/or punch as desired. When only one tape was being read, the third set of relays controlled the alternate switching of characters to the first and second set. Output of the first relay set at each step was the difference of the two characters being held.

Ordinary 5-level tape was used, at a speed of 10 characters per second. Results were accurate, faster than by hand, and could be expressed in print, in tape, or in both. It has been dismantled.

Ref: M.A.C. Outline #5

~~TOP SECRET CANOE~~

May 1953

LIMITED SELECTOR

The LIMITED SELECTOR (and TRANSFER ATTACHMENT) was a code recognition and deciphering device used as an aide in working additive depths. The first model built marked the start of a large family of deciphering devices, including all the SELECTORS, the CODE RECOGNITION UNIT and all of the J-SQUARE devices. Three LIMITED SELECTORS were built by Army's F Branch, with delivery dates of 24 December 1943, 4 February 1944, and 26 February 1944.

The first model received four consecutive cipher groups from the TABULATOR, stripped off key and sent the resulting possible plain groups back to be printed if it recognized among them one of the high frequency groups set up on 3 plugboard panels. Models 2 and 3 contained an 8 x 20 plugboard and additive groups plugged on it were stripped from cipher text (received from the TABULATOR four groups at a time). Also, the 60 x 34 plugboards were the removable slide type, not fixed as in the first model.

The first model was 6'H x 5'L x 2'D , the plugboard being mounted out from the side of the two frames. Both of the later models measured 6'H x 7'L x 2'D and mounted the panels between the two frames. All operated with a 405 TABULATOR at 80 cards per minute.

A LIMITED SELECTOR TRANSFER ATTACHMENT (4'H x 2'L x 2'D) was completed on 3 August 1944, providing a relay unit for transferring 480 leads to the LIMITED SELECTOR, thus permitting the code recognition

LIMITED SELECTOR (Cont'd.)

unit to scan two sets of code groups. All are now dismantled.

Ref: NSA-354B files
Mr. F. Mayol

~~RESTRICTED~~ May 1953

MAISIE

MAISIE (AFSAF D74) is a magnetic card file and look-up device, a general purpose decoder of smaller capacity than was planned for KATY, a similar equipment. Three models are being built by International Business Machine Corp., two for NSA and one for ASA. The first is completed and being tested, with delivery due in June 1953.

Capacity of the two magnetic drums in tandem is about 245,000 characters, or 511 tracks of 480 characters each. This amounts to five to ten thousand code groups and meanings. Each ten to seventy characters in length. Input and output is a 407 TABULATOR which reads up to ten 5-character code groups from a card, prints each, and, via electronic look-up circuits, finds and supplies for printing purposes the corresponding meanings from the drums.

Size of MAISIE is 5'H x 6'L x 4'D , plus 407 TABULATOR, which prints 150 lines per minute. It will be located at Arlington Hall Station, Room 1600-A.

Ref: Mr. J. Deutsch
Mr. E. Fleming
Mr. J. Powers

~~RESTRICTED~~

~~TOP SECRET CANOE~~

May 1953

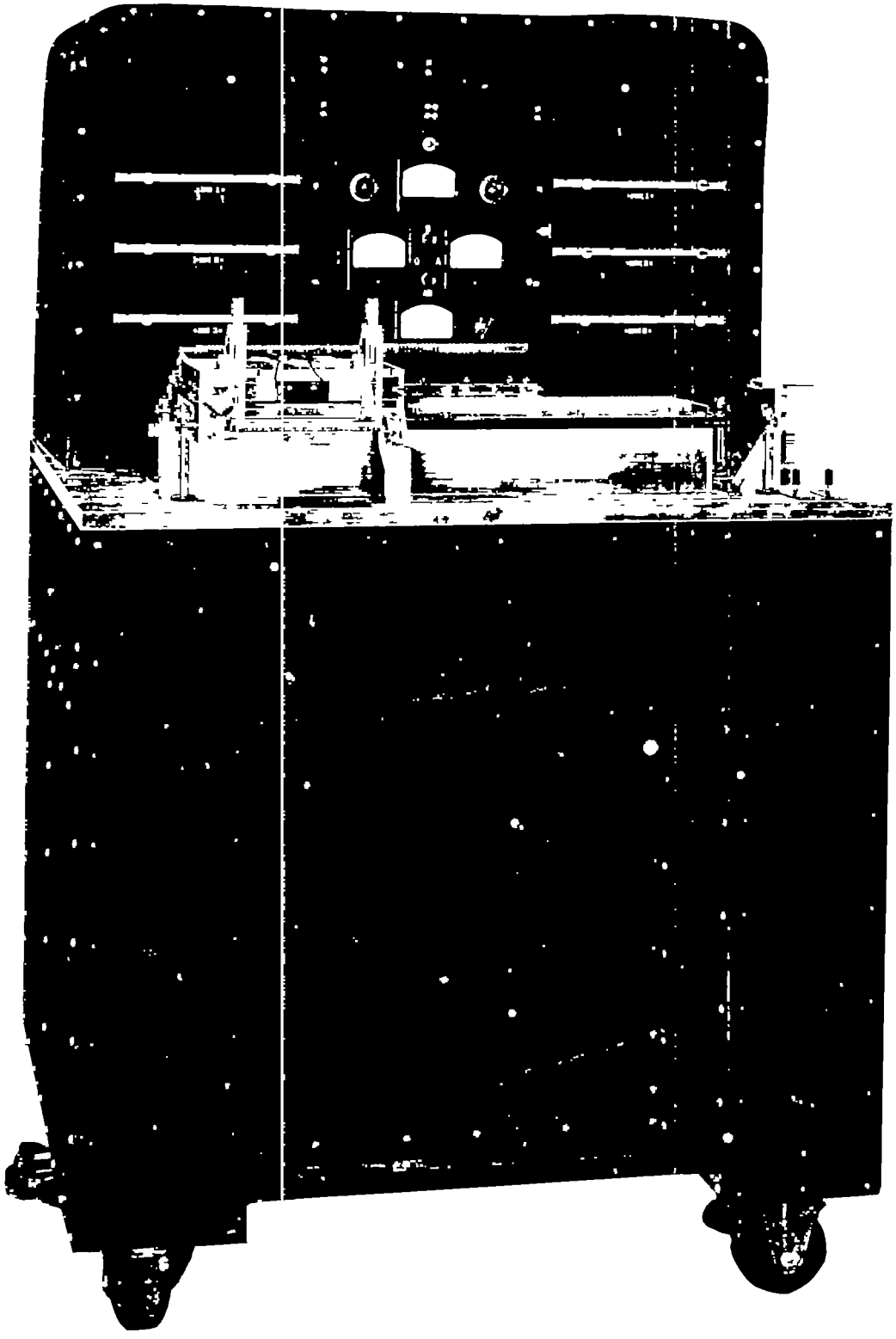
MAMBA

MAMBA, (CXLT) was a message setting device which compared digital information, setting enciphered code or additive by recognition of plain code. Two were built for Navy by National Cash Register Co., and delivered on 15 December 1944, arriving after the specific problem had died.

Input was by specially coded IBM cards. Numerical key data, usually + , 0 or - weights, was placed in fixed reading positions, while cipher in another IBM card deck was moved through a reading gate slide-run fashion, one position at a time, and compared. The "scanning" feature of the code (even division by three of code groups) was the test being made. The message tested was usually known to be on a particular additive page. Reading of cipher was done by 2400 brushes (10 digits in 80 columns in three cards), which could make contact through the reading head only through punched holes. The device also had a weight summing arrangement which in effect totalled the number of circuits completed and stopped the machine when a preset threshold was exceeded. Recording of hits was done manually.

Original intended to be a desksized simplification similar to COPPERHEAD, it measured 5'H x 3'L x 3'D and tested four positions per second, or one card per minute. Later devices made it obsolete, so it was dismentled.

Ref: CIT paper 4
NSA-064 files



MAMBA
C:LT, N-2000

TOP SECRET

~~FROTH~~

~~TOP SECRET CANOE~~

May 1953

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

MARTINI

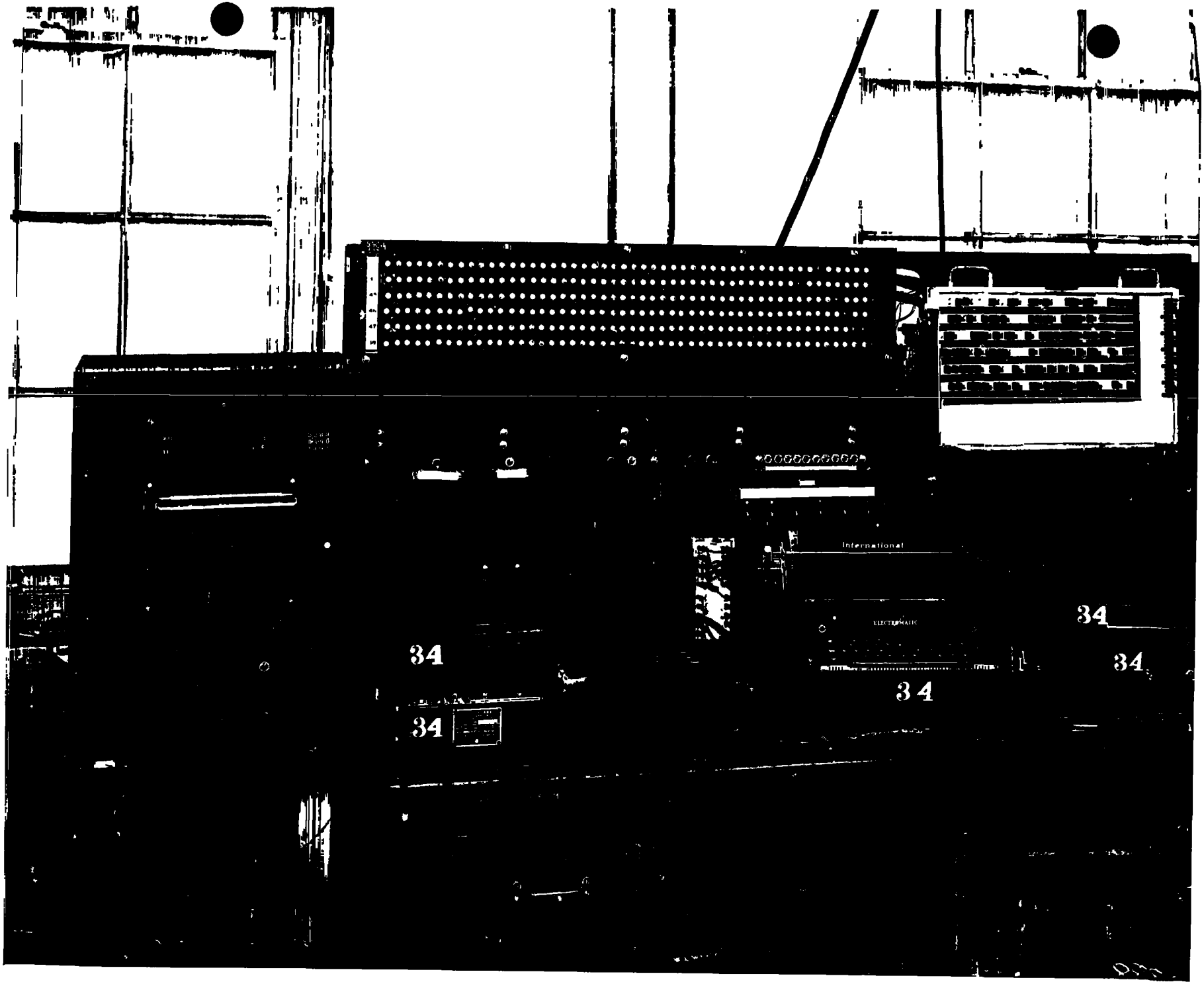
EO 3.3(h)(2)
PL 86-36/50 USC 3605

MARTINI (XFN) was a Navy relay analog for LONGFELLOW, the [redacted] and comparable in function to the Army's TAN ANALOG. It was built by Navy (Lt. Kilham's project) in 1948 from parts cannibalized from PYTHON. INITRAM was a companion machine which stepped in reverse through the key cycle in order to exploit weaknesses in message endings.

The machine was tape fed and simulated with relays the action [redacted] and MARTINI and INITRAM were accordingly retired.

Wheel patterns had to be known, but wheel plugging (selection of the two wheels to be read) could be found by trial and error. The machine, now dismantled, measured 6'H x 4'L x 4'D . Rate of operation was 6 to 8 characters per second.

Ref: Dr. H. Campaigne
Mr. C. Higgins
Mr. J. Stapleton



MARTINI
XEN
and also INITRAM,
identical in appearance

May 1953

McSNOYD, I and II

McSNOYD, (AFSAF-D75) analogous to Navy's O'MALLEY, is an electronic cross products sum computer. Model I, in breadboard form, was built by NSA-351C in August 1950. McSNOYD II, an operational model, is due to be completed in April 1953. In June 1951, an electronic BINARY-DENARY CONVERTER was designed and incorporated into McSNOYD I and gave a printed record on a regeneration typewriter. The CONVERTER was incorporated into McSNOYD I and was also used in reverse as input to ABNER, Serial 1.

McSNOYD's function is to compute and sum the cross products of two sets of digital values fed in on tape at about 200 characters per second by a modified double headed AFSAF-25 READER. The machine recognizes plus and minus numbers. Output circuit to the CONVERTER is through a 32 x 32 plugboard. Fifteen binary digits are expressed as five decimal numbers for print-out, originally by a regeneration typewriter, and later by an M-10 Navy BOMBE PRINTER.

Size is 5'H x 6'L x 4'D . McSNOYD I, already dismantled operated at ten digits per second; Model II, located at Arlington Hall Station in Room 0220-B, operates at 100 products per second. The BINARY-DENARY CONVERTER measures 6'H x 2'L x 2'D , and is pulsed at 200 KC per second.

Ref: NSA-03 Files
Mr. J. Deutsch
Mr. W. McElvy
Mr. J. Russell

MERCURY

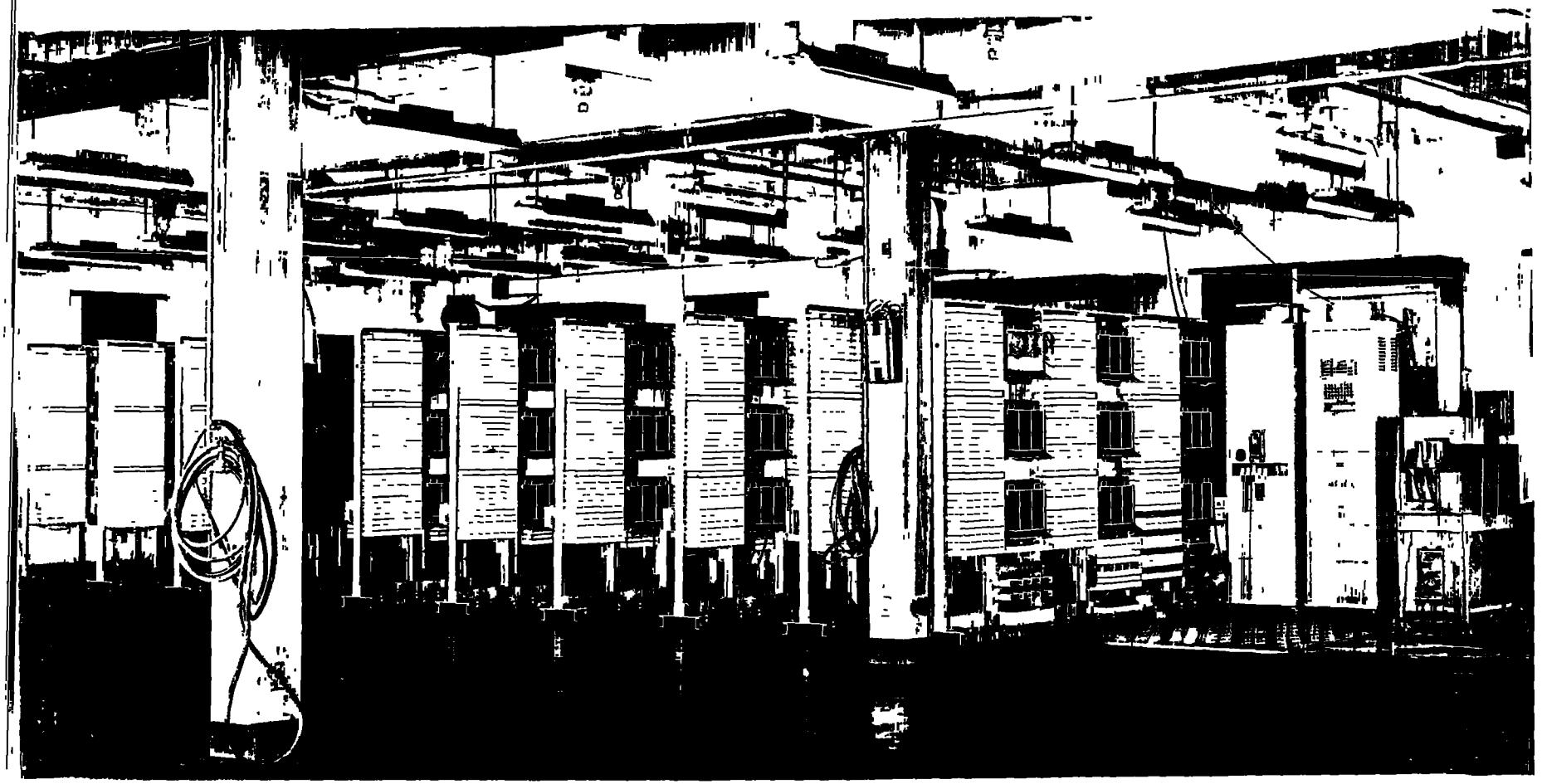
MERCURY (CXMO, FULL SELECTOR DEVICE) was the Navy countorpart of the Army SLIDE-RUN machine, a relay-operated group-scoring device for placing messages against key in additive-enciphered digital code systems. Essentially it was a 10,000 group catalog with provision for assignment of weights (0 to 19) to each group. The one model built dated from June 1945 and was designed for research into weighting methods. It was later expanded from 4 to 5 digit, plus a 100,000 group catalog by effectively building 10 such machines in tandem.

The device was relay operated and consisted of an 077 COLLATOR for card input, a selector and weighting unit, an electronic adding machine and storage unit. An electronic ring counter was used in totaling weights. Data was supplied one group per card (originally four-digit only) and the COLLATOR selected all cards whose total of weights exceeded a preset threshold. In effect, MERCURY dragged cipher against additive, made a weighted frequency count of resulting possible plain, matched the overall total against a threshold and selected a deck of cards containing all "hits" which exceeded it. When no key was known, an attack based on weighting and matching of cipher differences (of two messages in depth) with code group differences was possible. The machine was also capable of a GEEWHIZZIN type usage against transposition systems where digraphs showed sufficient frequency variation to be statistically significant.

MERCURY (Cont'd.)

The original four-digit model was 7'H x 14'L x 2'D , plus COLLATOR. When it was expanded to accommodate five-digit, additional additive racks were attached, in effect producing ten four-digit MERCURYS in tandem. The equipment then took up most of a room, measuring about 7'H x 40'L x 2'D . It operated at four cards per second.

Ref: NSA-18133 Library
Brief Descriptions of RAM Equipment
CIT paper TS 52 "MERCURY"
CIT paper 84
Mr. J. Powers
Mr. J. Stapleton



MERCURY
FULL SELECTOR DEVICE
CXMO, N-2900

May 1953

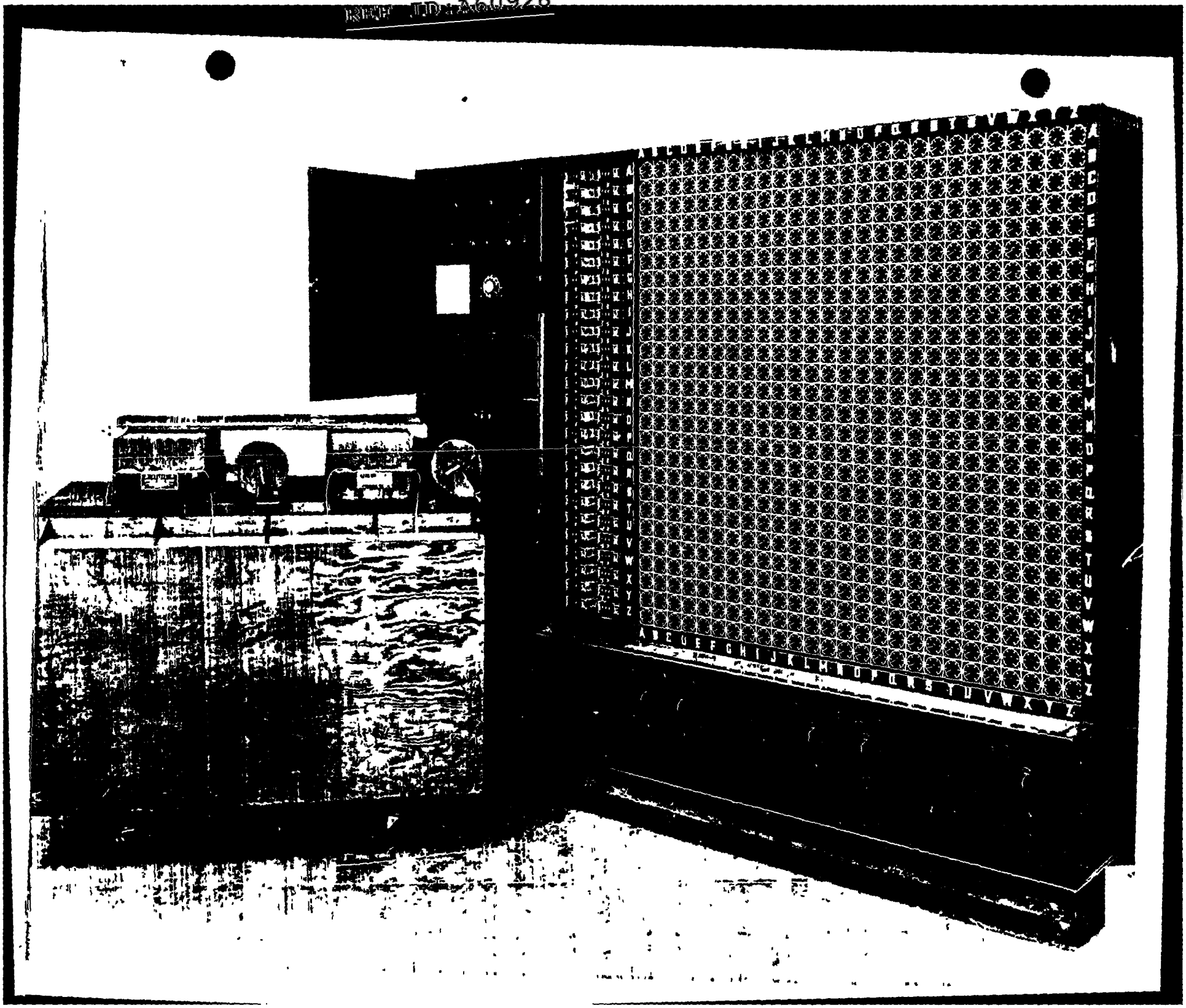
MIKE

MIKE (CXMi, NCR DIGRAPH COUNTER) was a versatile monograph and digraph counter, replaced in July 1949 by ALCATRAZ, a faster, bigger and more flexible counter. The contract was let to National Cash Register in October 1943 and delivery was made to Naval Communications Annex in April 1944.

The machine was basically two units. One was an 8' x 8' counter board containing 52 "visual" counters with 999 capacity for row-column totals, and 676 dial counters with 50 capacity for digraph counting. The other unit was a double-headed reader and associated plugboard. A single impulse from each of two standard tapes is fed from the reader to a matrix, combined into a digraph and sent to (1) a particular dial counter and (2) the two associated Veeder counters for row and column totals. Results were read visually from the board and copied by hand. Plans to use a 70mm camera to photograph the counters were never carried through.

The device replaced manual counting and a slow "MATTHEW M-26" run, handling up to 26 x 26 separate scores. Army Security Agency's CONDENSER FREAK was more flexible and faster, but not so dependable as MIKE. Eight characters per second was the rate, and size was 6'H x 7'L x 2'D plus two 8' x 8' counter boards.

Ref: GYA Report
Mr. J. Stapleton



MIKE
CXMM, N-910
NCR DIGRAPH COUNTER

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

May 1953

MISTRESS

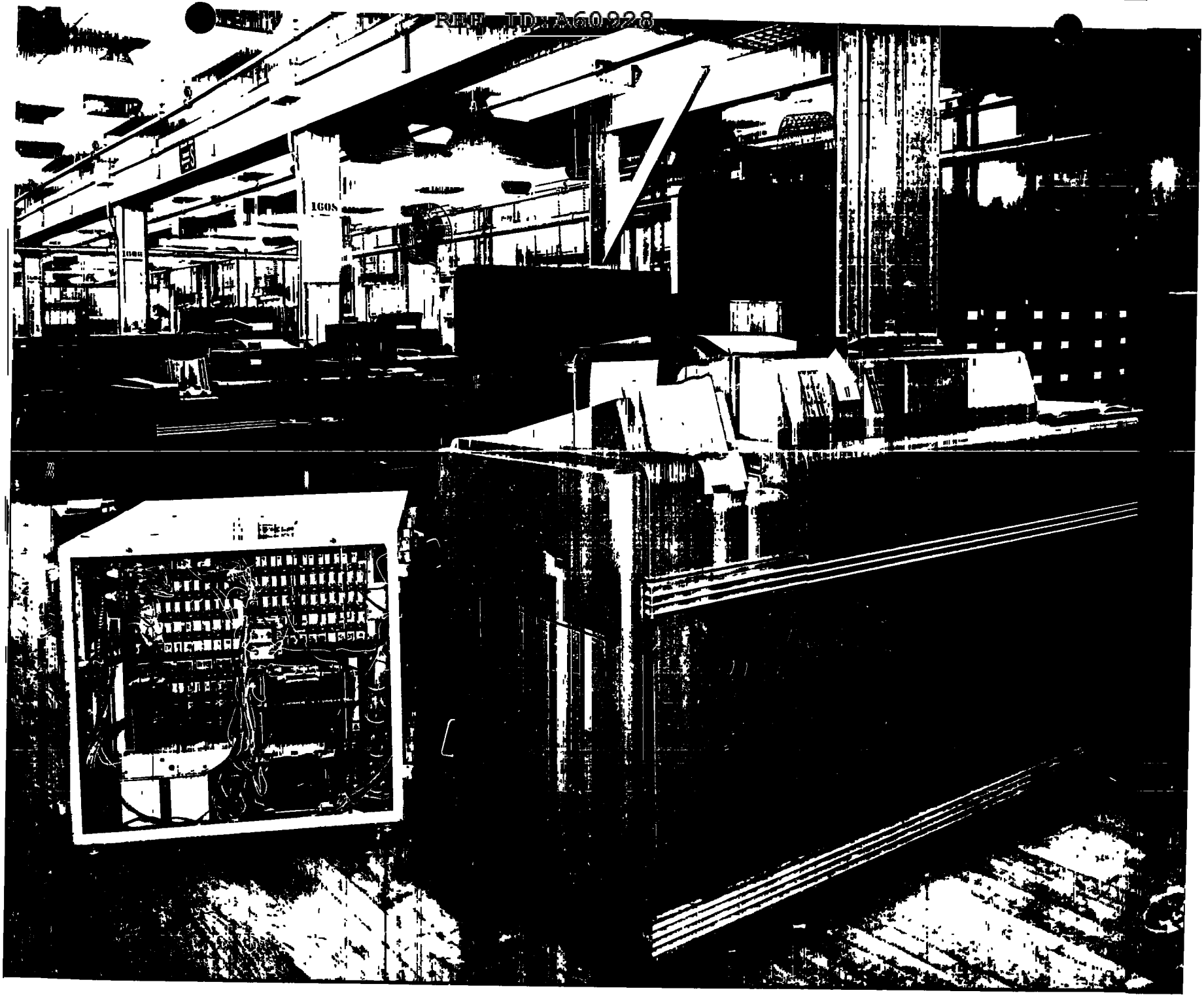
MISTRESS (AFSAF-D73A) is a special purpose repeat search device, a relay gate used in conjunction with a modified 407 TABULATOR. The purpose is to find messages with a significant number of group repeats, as in the case of accidentally unenciphered code message. One model was built by NSA-224, and began operating in June 1952.

The device reads 120 characters from cards, (24 pentagraphs or 30 tetragraphs) and treating one half at a time, intermatches every group to find repeats. 78 comparisons are made in about one second and the TABULATOR prints a line of twelve pentagraphs or fifteen tetragraphs after each set of matches. In addition, a marginal digit showing the number of repeats found in the line printed. Weighting of hits (0-9) is done by plugboard and blank group hits are discounted in this manner. The message print is a by-product.

The device measures 3'H x 3'L x 3'D and is used by NSA-22 at Arlington Hall Station in Room 1600-A. It is designed to consider text as tetragraphs automatically while pentagraphic matching must be set up by plugboard. Listing rate is 75 cards per minute or two TABULATOR card cycles per test.

Ref: Mr. N. Andrews
Mr. J. Powers

~~CONFIDENTIAL~~



MISTRESS
AFSAF D73A
with IBM 407 TABULATOR

~~TOP SECRET CANOE~~

May 1953

M-8

The M-8 (AFSAF-108, XBL) is a deciphering device built on a converted ECM (SIGABA) frame, able to simulate ENIGMA wheel stepping and used chiefly as an analog for higher than hand speed decryption and cryptanalytic testing. Starting in 1943, about thirteen such equipments were built, varying a good deal as to type. It replaces the so-called PAPER MACHINE, a set of cardboard strips in slots in a cardboard frame for tracing circuits and reproducing wheel motion.

The device uses regular two-sided ENIGMA wheels; some can be tape operated. The widest usage is to assist work on the BOMBE or other special machines. Many were incorporated in larger equipments such as HYPO, for example, to produce ENIGMA key as needed.

Its size is negligible, slightly over 1'H x 1'L x 1'D ; it usually operates at tape reader speed, 6 to 8 characters per second and is found in various locations and sections, three at Arlington Hall Station in Room 2050-A.

Ref: CIT Paper TS-4
LCDR R. Greenwood
Mr. J. Stapleton

~~TOP SECRET CANOE~~

M-8 DEVICE HERER
(Sometimes called G.G.)
A Converted SIGABA plus
CXC[illegible] re-encryption typewriter

May 1953

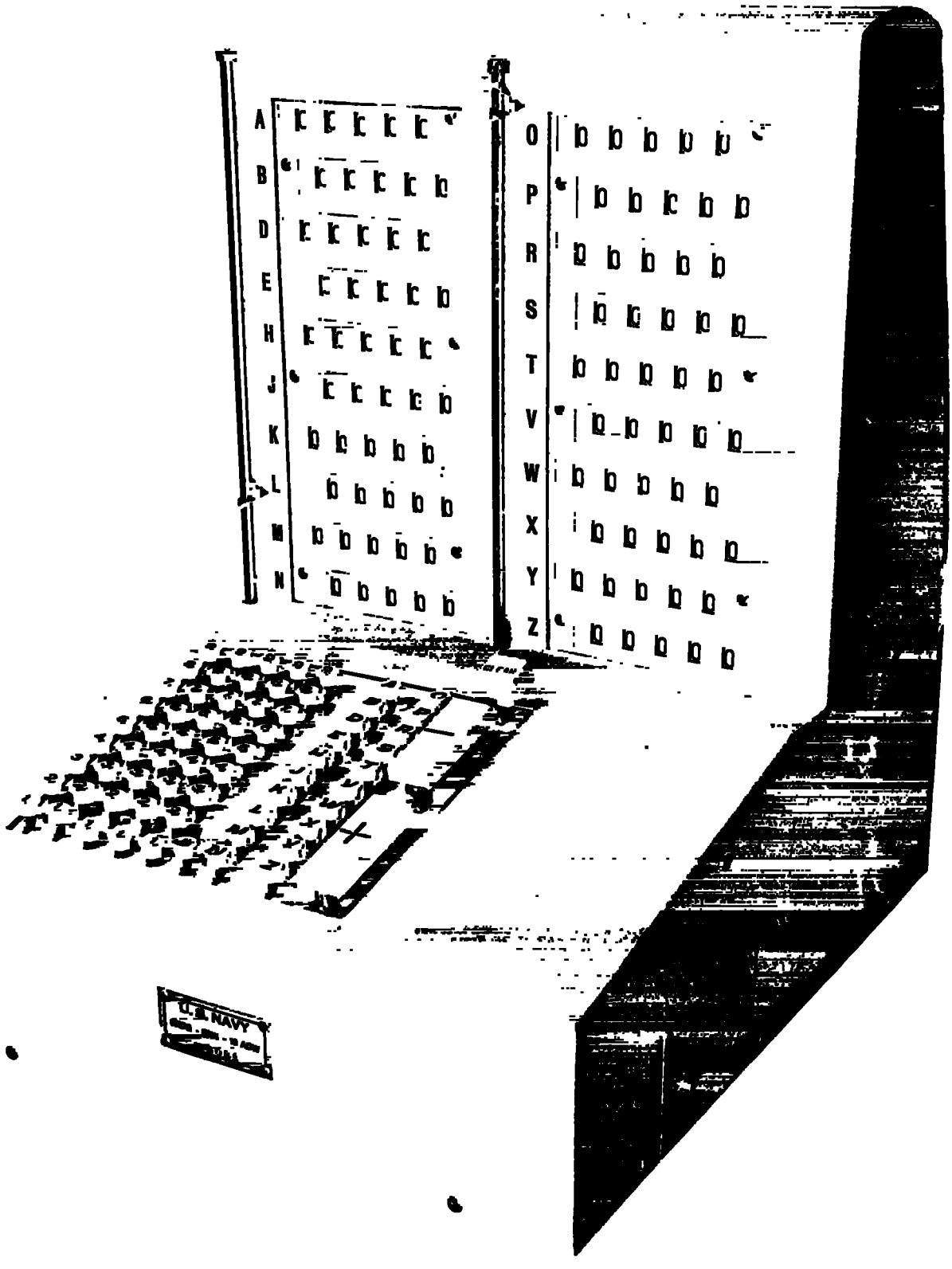
NCR DIFFERENCING CALCULATOR

The NCR DIFFERENCING CALCULATOR (AFSAF-118, ADDITIVE CALCULATOR, JEEP) is a desk-top device built in quantity in 1942 by National Cash Register Company for Navy, and in the following year for Army, used either for stripping probable additive from cipher groups in depth in search of high frequency code groups, or to difference such groups in depth to find probable relative additive. Two, now obsolete, were operated by hand, but most are motor driven and perform non-carrying addition or subtraction on 5-digit or smaller groups for up to twenty groups in depth.

Each calculator has twenty rows of five windows and into each row a pentagraph or shorter group may be set. Any additive or minuend may be tried against this column of groups, using non-carrying arithmetic, or a pair of groups may be differenced. The machine can perform twenty calculations simultaneously, retaining the original entries for further tests.

Operation is at the rate of up to one cycle per second. The device facilitates hand solutions, but is unsuited to large scale add stripping or square conversions stripping. It can be used to add further messages to a depth. An NCR DIFFERENCING CALCULATOR is about 2'H x 1'L x 2'D . Most operating divisions have a few in their possession, still available for use.

Ref: M.A.C. Outline #13


A
B
D
E
H
J
K
L
M
N
O
P
R
S
T
V
W
X
Y
Z
U.S. NAVY

NCR DIFFERENCING CALCULATOR
AFSAF 118
CXDG, JEEP, ADDITIVE CALCULATOR
M-4 MACHINE

~~CONFIDENTIAL~~

~~TOP SECRET CANOE~~

May 1953

PINK ANALOG

PINK ANALOG was a relay device which [redacted] the functions of the [redacted] PINK traffic. Navy's counterpart to this equipment was called RICKY. Two units were built by Army, the first in April 1946 the second in November 1947.

The device had a keyboard or tape reader input; output was to a regeneration typewriter. [redacted] All wheel positions were shown by lights. Plugging and pinwheel starting positions had to be known. A print of either component could be had if desired.

The system was [redacted] and some work has been done on the backlog of traffic. Dimensions of the machine were: 6'H x 2'L x 2'D , plus keyboard, typewriter and reader. Serial 1 was dismantled and Serial 2 was sent to the museum and later disposed of for lack of space.

Ref: M.A.C. Outline #55
Mr. F. Mayol
Mr. J. Raisch

~~TOP SECRET CANOE~~

~~SECRET~~
~~SECURITY INFORMATION~~
~~RESTRICTED~~

~~SECRET~~

May 1953

PLUTO

PLUTO (AFSAF-30, the CYCLE ANALYZER) is a special purpose generating device with computing elements, designed to study cycle structures generated by regularly or erratically stepping rotors. It was built by Sylvania Electric Products Inc., of Boston, Mass., for NSA-34 and delivered in July 1951. It simulates a variety of rules of motion by rotors of up to $2^7 = 128$ points and performs counts and studies on resulting cycles. Not strictly analytic, it merely determines the nature and length of cycles, sub-cycles and lead-in sequences from any given starting point, thus permitting study of key generation.

In operation, a particular rule of motion is set up by properly interconnecting basic components of the frames. A starting point is selected by means of Remington Rand cards; results are displayed on neon lights. Three comparator units function as memories and stop the machine when a selected setting is reached. Automatic search for a setting repetition is built in to stop the machine at a coincidence and indicate the length of the cycle tested and the length of the lead-in sequence. It is capable of continuous performance and was recently modified to make automatic the recognition of certain convergence situations.

It consists of 28 frames arranged in two parallel banks, each 6'H x 40'L x 2'D , plus a 6'H x 9'L x 4'D power supply. Rate of operation is dial controlled, ranging from 500 to a million pulses

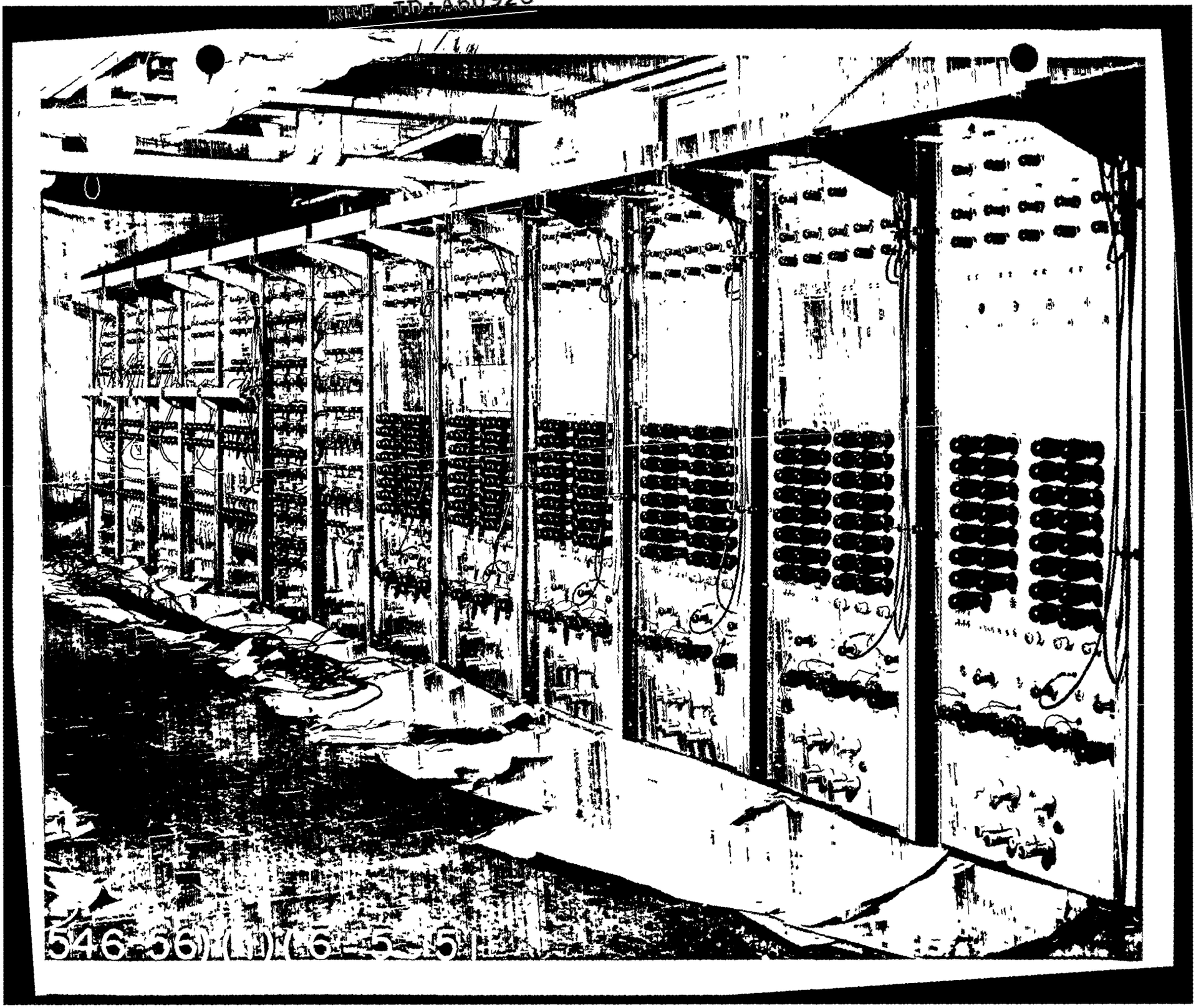
~~RESTRICTED~~
~~SECRET~~
~~SECRET~~

~~SECRET~~

LEAD (Cont'd.)

or settings a second. Location is at Naval Security Station in Room 20105. In many respects its circuitry is identical with WHIRLWIND, Sylvania's electronic computer.

Ref: NSA-34 Files
Mrs. A. Andrews
Mr. W. Erskine
Mr. R. Moulton



PLUTO
AFSAF 30
CYCLE ANALYZER

May 1953

PREPUNCH VERIFIER

The PREPUNCH VERIFIER (AFSAF-D67) is a tape verifier, a modification of CXCO letterwriting equipment which checks the accuracy of two typings of 50 characters before punching the sequence into tape. The one model was built by NSA-354 in October 1952. It has not passed its tests nor been put to operational use.

Designed for 5-level tape only, the device stores a line of 50 characters in an equal number of relays, then matches this letter by letter with a second typing of the same text. At a wrong stroke, the keyboard locks, and correction in relay storage or key stroke must be made before typing can proceed. Carriage return at the end of the line starts the automatic tape punching process and sets up the machine for the next line. Input is by keyboard only, and output is to tape only. Although very useful, the machine really has no cryptanalytic function beyond avoidance of garbles from processing.

CXCO keyboard and tapepunch are mounted on the usual CXCO dolly 2'H x 5'L x 3'D , with relay equipment contained inside. Typing input is at a rate up to 5 characters per second and output is at 10 characters per second. It is located at NSS in Room 4177.

Ref: Mr. J. Deutsch
Mr. J. January
Mr. J. Stapleton

TOP SECRET CANOE

May [illegible]3

PURPLE ANALOG

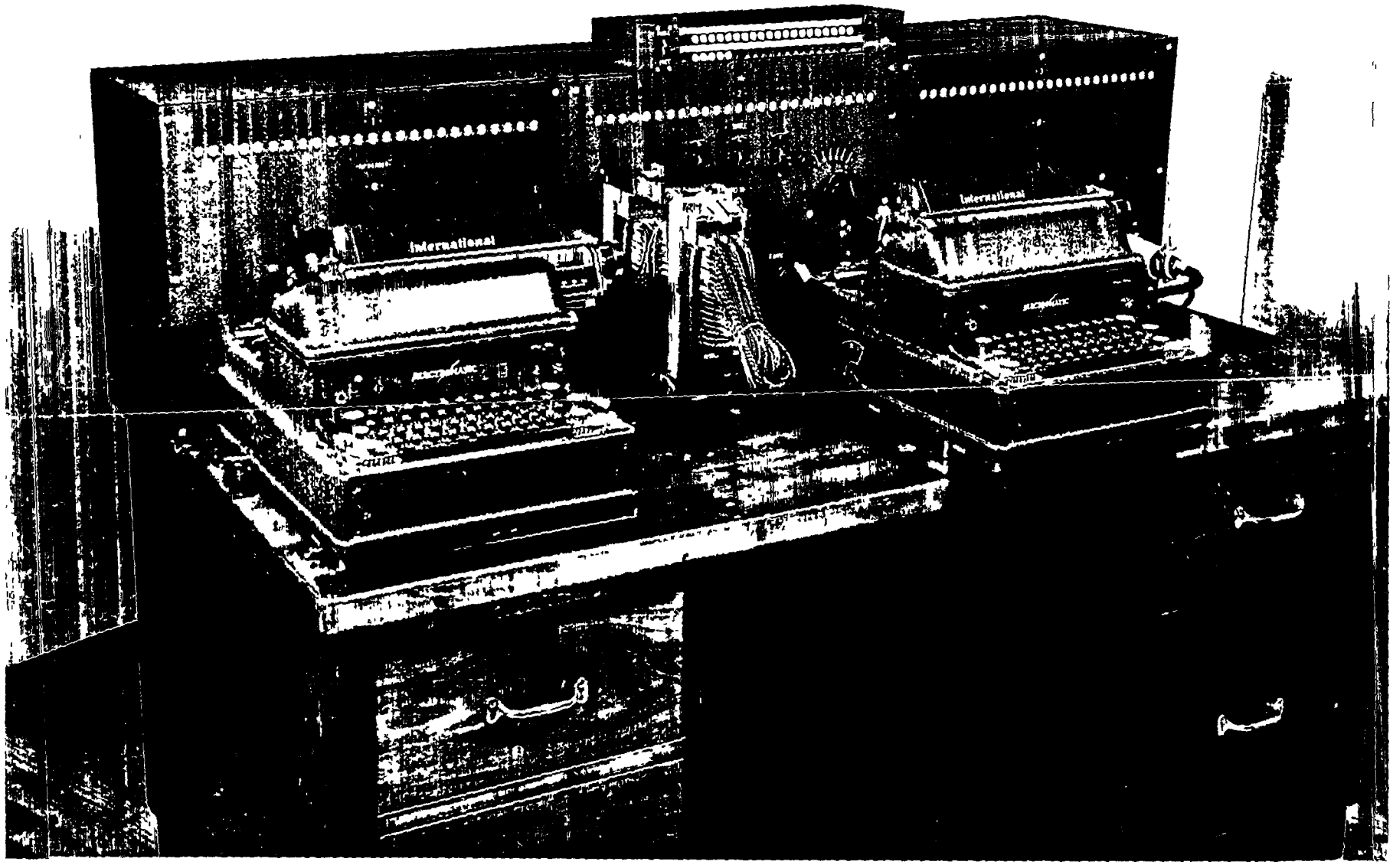
The PURPLE ANALOG is a relay device, simulating the Jap "B" MACHINE or HEIWOKI cipher device which produced PURPLE or Jap diplomatic traffic. (The "A" MACHINE, producing RED traffic, preceded this system and was read by manual methods with no special machine aids.) Between 1941 and 1945 a total of eight analogs were built by Army and Navy, each offering improvement, but no basic change. The equipment supercedes hand methods and a primitive handtester called SILLY SUE for tracing enciphering circuits through three of the four wheels.

As the Japs had done in the original device, the analog enciphers a selected six letters of the alphabet through a single "6" wheel and the remaining twenty letters through three "20" wheels, with stepping provided automatically. All four are 25 point wheels, simulated by rotary selector switches. It was used chiefly for deciphering.

The device, measuring 11"H x 34"L x 11"D, plus keyboard for input and regeneration typewriter for output, is normally placed on a low table or desk. Two models are now in existence, one of which was used recently in the OTP DEVICE and the SCRAMBLER for key study purposes.

Refs: U.S.A.C. Outline #13
NSA-34 Files
Mr. D. Marston
Mr. L. Wheatley

TOP SECRET CANOE



PURPLE ANALOG
for HINOKI, or the Jap "B" MACHINE
Last Navy model

~~TOP SECRET CANOE~~

May 1953

PURPLE DUDBUSTER

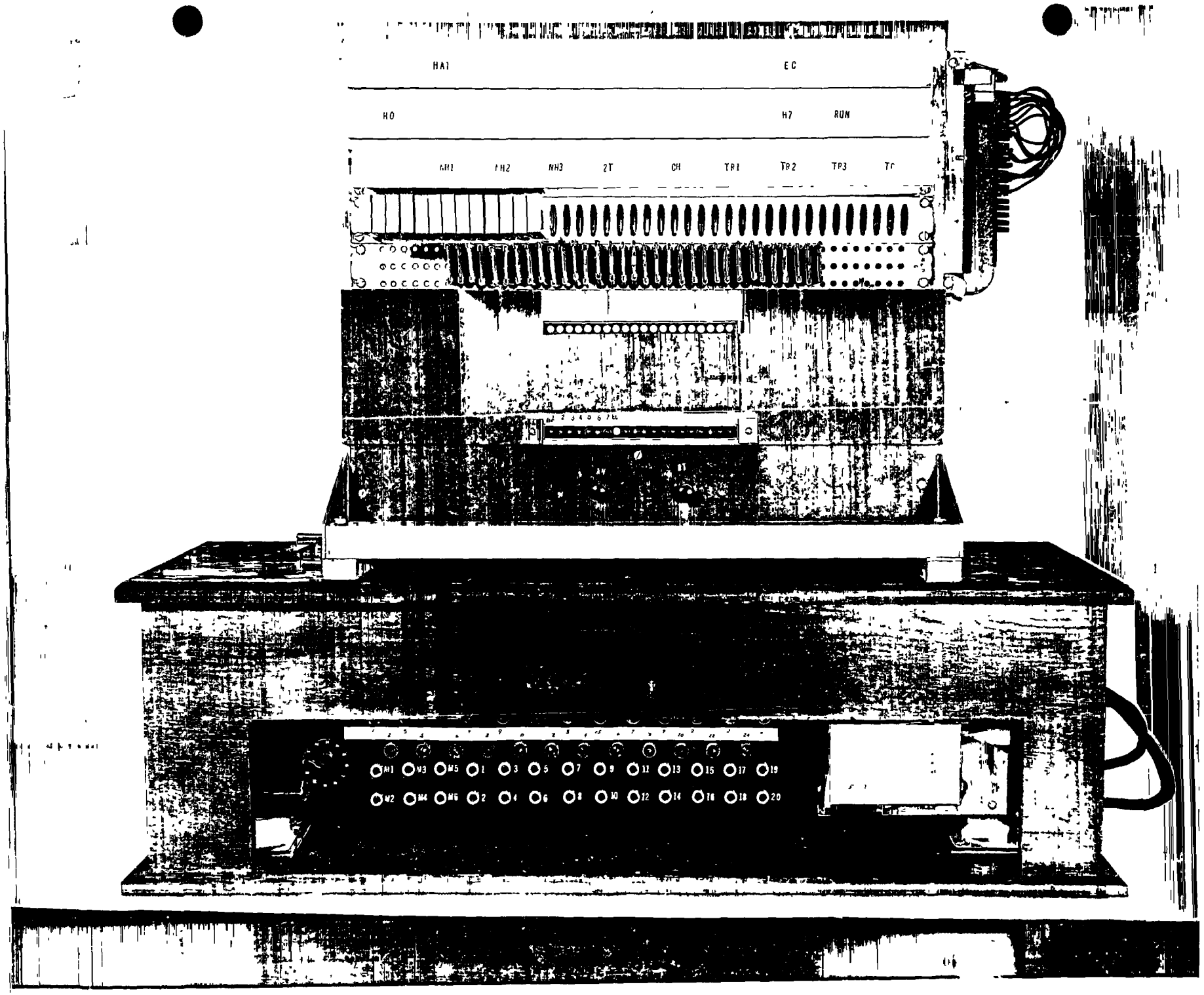
The PURPLE DUDBUSTER was an electrical cribtester made from a modified PURPLE ANALOG and used to find the stepping order and settings of the three wheels which encipher the 20-letter portion of the alphabet in Jap Diplomatic traffic. It was employed after the "6" letters, enciphered on a single separate wheel, had been recovered and when plain and cipher steckering were known. It was built by Army in 1945 and operated at AHS until VJ day, when it and its running mate, the PURPLE ANALOG, were retired to the museum.

One model of the ANALOG was modified for automatic stepping and plugged to decipher text to be analyzed (i.e., recognized) by sets of rotors. Starting at position 111 and arbitrarily selecting one fast - medium - slow order, the machine was set in motion. At the point the first plain-cipher pair was satisfied, the machine considered the second pair, and so on through the full crib until a contradiction occurred. In that case the next position is assumed and the process repeated. A total hit would probably be the true one, and could readily be verified so as to end or continue testing.

Average time for obtaining solution was 35 minutes, one wheel order run taking 18 minutes. Initial plugging and setting time was negligible.

Ref: M.A.C. Outline #44
Mr. E. D. Marston

~~TOP SECRET CANOE~~



PURPLE DUDBUSTER

May 1953

ROBIN I and II

ROBIN (CXOR, AFSAF-D/54 and AFSAF-D/54-1) is a photoelectric comparator for matching tapes round robin. It was designed by 3520 and built by Engineering Research Associates, the first two (known as ROBIN I or AFSAF-D/43, being delivered in November and December 1950. Thirteen more called AFSAF-D/54-1 through -13 have since been built. The original pair and the 13th ROBIN of the second group, still crated, are now stored.

In operation, two teletype tapes usually of 15 to 20 thousand characters each are fed past a dual tape reader, scanned photoelectrically at a rate of 5 thousand characters per second and compared at effectively 50 thousand characters per second. The threshold for a hit is a preset straight line criterion. ROBIN generates its own step-function criterion (ratio between expected coincidences and number of comparisons) as it matches each new message overlap, and punches a card or not whenever a message break in either tape passes the reader. Counting is actually character by character, with dits ignored. Message identification and overlap information causing the required high monographic coincidence are punched in binary form into a card by a 517 REPRODUCER PUNCH. A logical extension of CONNIE, it uses similar and additional circuitry. An optional "bonus" circuit weights consecutive monographic hits, thus tending to select polygraphic coincidences.

Dimensions are 7'H x 12'L x 2'D , plus reader, punch and power supply. Complete matching between two 20,000 character tapes take

ROBIN I and II (Cont'd.)

about two and a half hours. All twelve are operating at AHS in Room 0221-B. At present there is considerable doubt as to ROBIN's theoretical ability to distinguish statistically between random and causal situations as it was designed to do.

Ref: Mr. J. Deutsch
Mr. D. Hogan
Mr. J. May

May 1953

SATYR

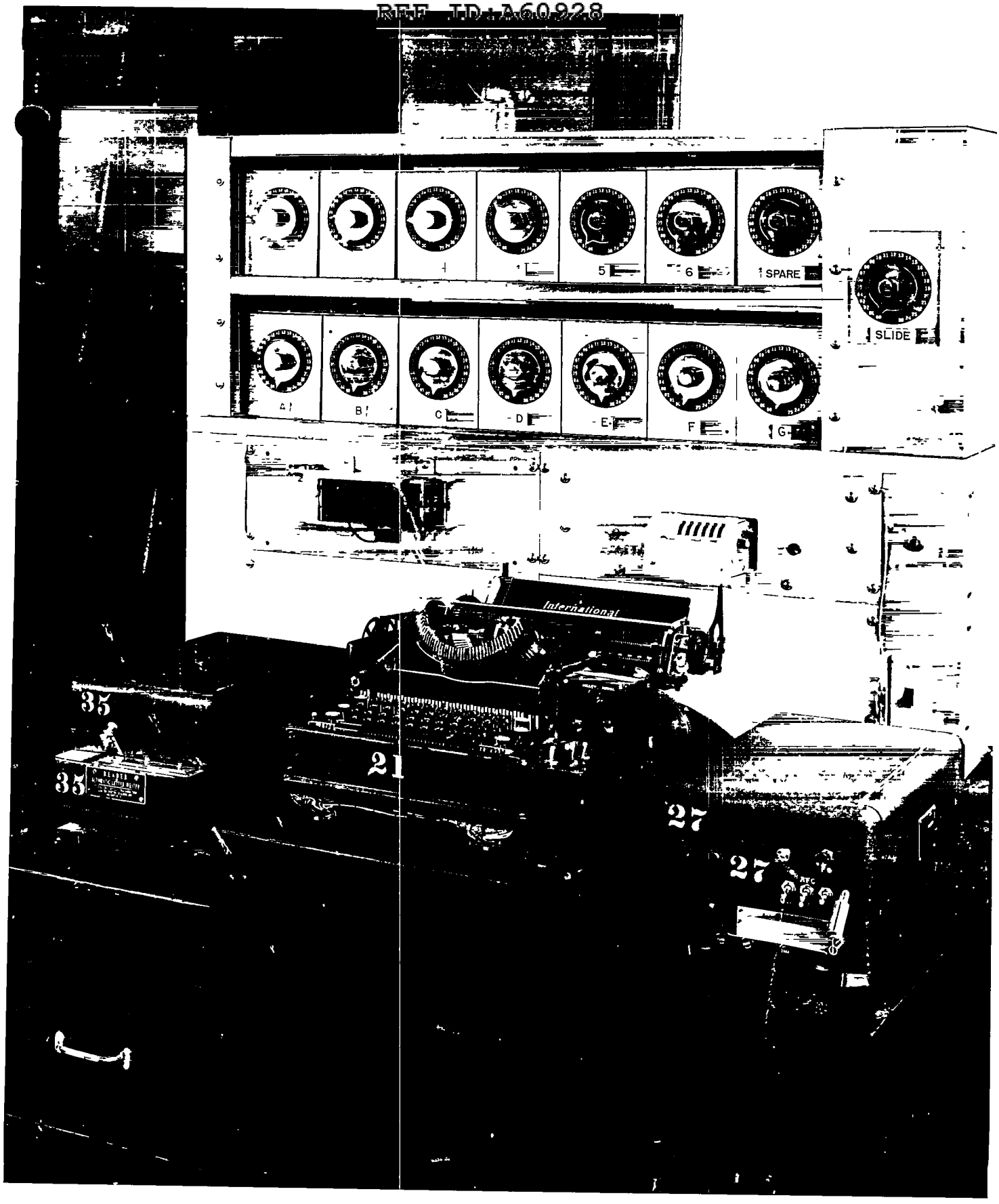
SATYR (AFSAF-102, GXDA) is an electrical analog of a cipher device known variously as the HAGELIN C-38, CSP-1500 or M-209. It is used for enciphering or deciphering traffic and for various cryptanalytic processes such [redacted] testing suggested settings in conjunction with HECATE and WARLOCK I and other special operations. It generates all or part of the entire 6-wheel cycle of about 101 million elements. Serial 1 was built by National Cash Register Co., and Navy in late 1944 and is now dismantled. Four others of a different model, followed shortly, but all are basically identical. Army's ELECTRICAL HAGELIN ANALOG C-38 (refer to M.A.C. Outline #32) is a comparable machine, slightly faster, using relays instead of actual Hagelin wheels. The SATYR HEAD (AFSAF-102/10) is a specially developed pattern generator which punches the 6 wheel patterns into tape. It was developed by Navy in 1944 at the same time SATYR was.

Each machine consists of (1) twenty-two 26-point switches (6 for kick, 15 for overlap, 1 for slide), (2) a converted set of HAGELIN wheels, (3) a keyboard for input and (4) an 8 x 20 plugboard to make both input and output pluggable. The input contacts of the plugboard are connected to the switch-relay units, including the slide, and back again to the output contacts of the plugboard. If all switches are set at "off", the input impulse goes through unchanged. A given switch-relay is operated as many times as there are active

[redacted] Both input and output may be by either tape or typing.

Dimensions vary only slightly between the two models, averaging about 4'H x 4'L x 3'D plus a keyboard, a regeneration typewriter, a reader and a punch, all usually set on a nearby desk or stand. The early model was the larger. Three machines are located at Naval Security Station, two of which are in Room 20103 with HECATE. The fifth is at USNCML in St. Paul. Operating speed is 6 characters per second. SATYR permits analytic study of any one element or combination of elements of the C-type HAGELIN.

Ref: M.A.C. Outline #7
CIT-TS 51
Mr. K. P. Cook
Mr. J. Stapleton



SATYR II
AFSAF 102
CXDA, N-2500

TOP SECRET
FROTH

May 1953

SETTING GENERATOR

The CIPHER MACHINE SETTING GENERATOR (AFSAF 35, CMSG) is a relay operated testing device which can simulate fifteen rotors of up to 80 positions, each stepping according to almost any rule of motion. Its aim is to facilitate such cycle studies as were conducted under the ANANERATCH project by reproducing successive wheel positions of most known cipher machines. The one model was built by NSA-352 on 14 May 1951.

The function of AFSAF 35 is to generate all successive rotor settings possible in any cycle, recording: (1) after each stepping cycle, (2) after selected cycles only or (3) on all or selected wheel positions only. Results may be in printed or punched tape form and may include stepping instructions. It has application to such problems as KOKET, notched ring or wired rotor machines and permits study of rules of motion, rotor wiring and key generation. Set-up of notch pattern, rule of motion and order of wheel print is by plugboards and initial setting is by pushbutton. There are two reading positions for each of the 80 wheel-positions.

Size is 6'H x 15'L x 3'D plus CKOO equipment and power supply. Rate of operation is 35 steps per minute, or up to 210 steps without printing. It is used operationally at FSS in Room 17114.

Ref: Mr. K. Rhodes
Mr. C. Schierlmann
Mr. R. Scheppiehl

May 1953

SLIDE-RUN MACHINE

SLIDE-RUN MACHINE (AFSAF-39 AXAB/1, IBM #931, CODE RECOGNITION UNIT) was a relay deciphering and message setting device, used to place 4- or 5-digit messages against a bank of recovered key, by either non-carrying or "square" arithmetic. Brute force searches up to seventeen groups were also possible. Eight 4-digit machines and one 5-digit machine were built by F Branch of Army between early 1944 and 1946. It was superceded by SKATE and SLED.

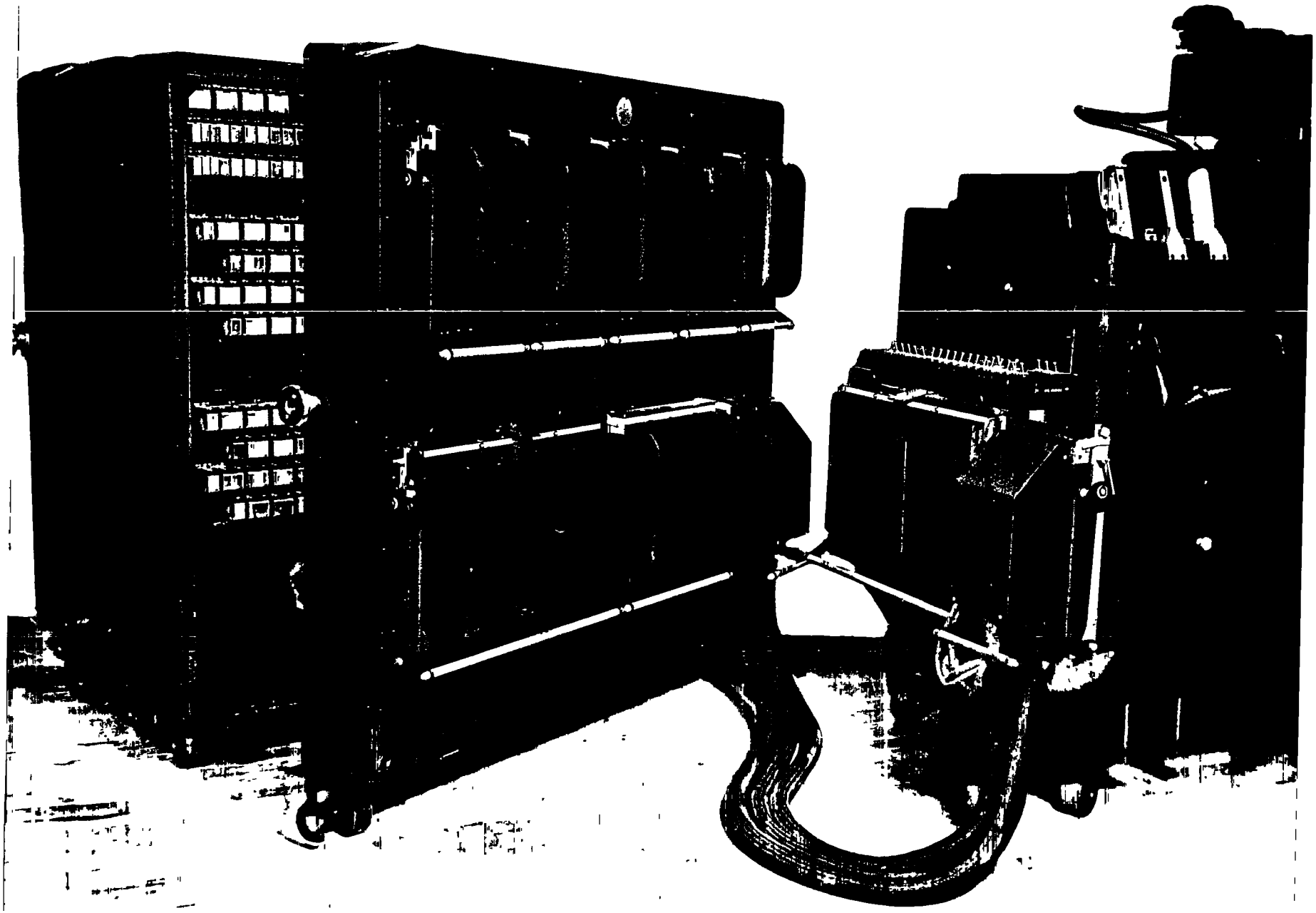
A 405 TABULATOR read 17 consecutive groups at a time to this gate which employed counters and relays to strip an equal length of key from the groups through appropriate deciphering squares. At the same time it matched resulting possible plain groups against a selected set of 100 high frequency groups set up on a plugboard. At a hit, the TABULATOR printed a record of the line, indicating by a dit to the right which groups were recognized. It was adaptable to three-digit traffic also.

A weighting device was included in the later models, with a toggle switch to set the threshold. The DECIPHERING UNIT, built shortly after the first SLIDE-RUN MACHINES, was basically similar but minus the recognition elements. Both are of the J-SQUARE family of deciphering machines. Dimensions were 5'H x 7'L x 2'D. An ELECTRONIC CIRCUIT BREAKER (5'H x 2'L x 2'D) was built by AS-92 in 1947, increasing the SLIDE-RUN MACHINES rate from 80 to 150 cards per minute. All models are now dismantled and replaced by the SKATE

SLIDE-RUN MACHINE (Cont'd.)

and SLED equipment.

Ref: M.A.C. Outlines #4
NSA-354B files
Mr. F. Mayol
Mr. J. Powers



SLIDE-RUN MACHINE
AFSAF 29
with CODE RECOGNITION UNIT
AXAB/1 IBM 931

~~TOP SECRET CANOE~~

May 1953

SUPERSCRITCHER

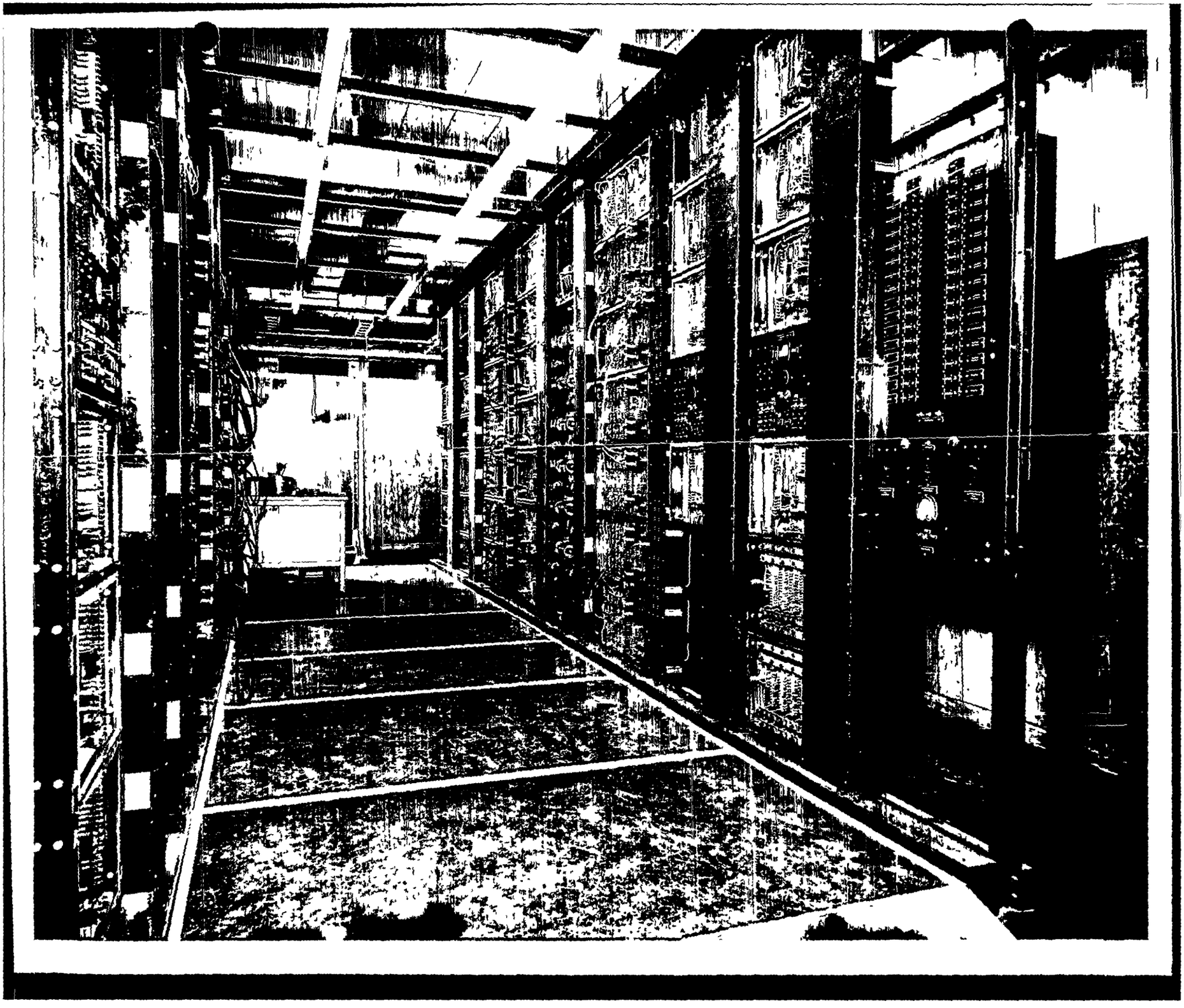
The SUPERSCRITCHER, (AFSAF-18), was an electronic cribtoster, analogous to Navy's DUENNA, designed to attack ENIGMA traffic. The first model was completed by F Branch in 1945 shortly after VE day, and replaced the now dismantled AUTOSCRITCHER. In December 1951 modifications were completed to permit its use as a low speed BOMBE (it tested serially, not in parallel, as does the BOMBE) and it became operational in 1952 in solution of [redacted] traffic (fixed reflector plugging) for a brief time.

Its function was to make successively all possible stecker assumptions in conjunction with all possible reflector pluggings, testing each setting through a menu (selected pairings of plain and cipher letters) and sensing contradictions and non-contradictions in circuitry. Requirements were a 200 to 600 letter crib (and therefore a menu of about 20 pairs) and known rotor wiring, to find stecker, reflector plugging, wheel order and window setting. The menu was set on a plugboard and results were in the form of a printed list of possible window settings.

It consisted of two rows of frames, each 10'H x 20'L x 2'D , with nine bays or frames to a row. It used actual rotors and 2075 tubes, testing at the rate of 10 to 15 KC. It was dismantled in 1952.

Ref: Mr. J. Deutsch
Mr. E. Flemming
Mr. J. Raisch

~~TOP SECRET CANOE~~



SUPERSCRITCHER
AFSAF 18
ELECTRONIC SCRITCHER
SEQUENCE TESTER

~~TOP SECRET CANOE~~

May 1953

TUNNY DRAGON

The TUNNY DRAGON, (or GEHEIMSCHREIBER CRIBTESTER) is a relay device built by F Brarch of Army on 14 August 1944 and delivered to GCCS in England in October for use

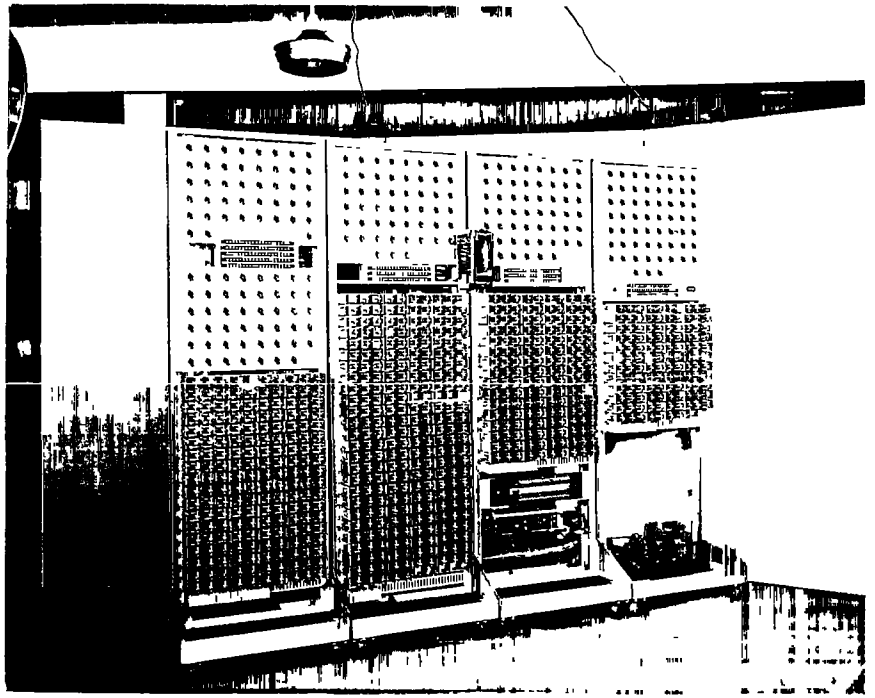
[redacted]

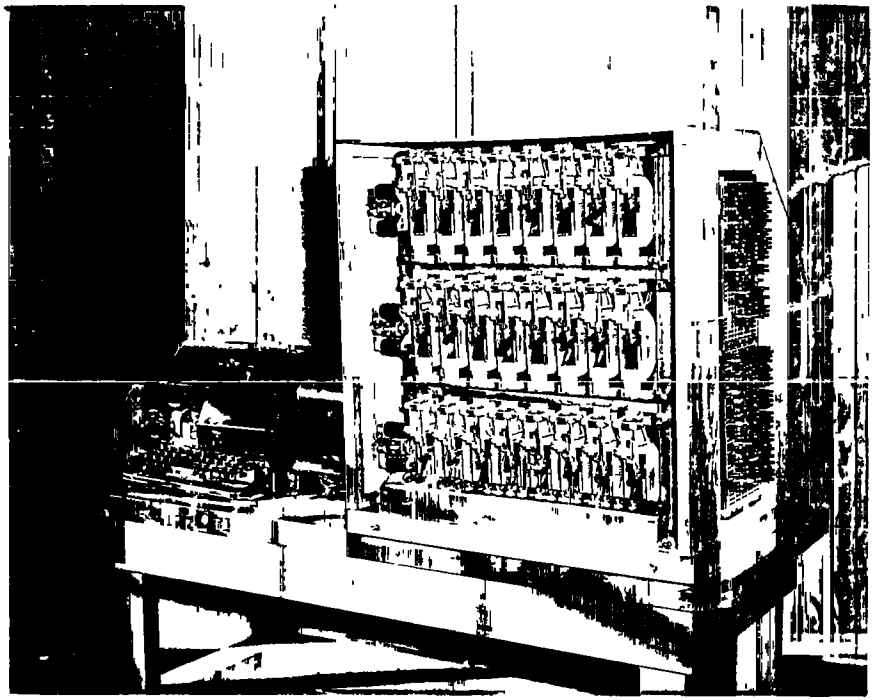
When a match occurs at one or more levels, the machine recognizes the match and stops, indicating wheel position by lighting appropriate lamps. The operator then records necessary data for further testing.

Tape preparation required 20 minutes; plugging the crib, 5 minutes; setting rotor switches, 20 minutes. The DRAGON compared 6 tape positions per second and was faulty but effective. The problem ended with World War II and the DRAGON has since been dismantled. Size was 7'H x 9'L x 2'D .

Ref: M.A.C. Outline #21
Mr. E. D. Marston

~~TOP SECRET CANOE~~





TJNNY DRAGON (left)
and an earlier model
[illegible]EIMSCHREIBER CRIBTESTER (right)

May 1953

WIRED WHEEL HANDTESTER

The WIRED WHEEL HANDTESTER (called HEBERN HANDTESTER in H.A.C. Outline #8) was an electro-mechanical testing device applicable to all such wired rotor cipher machines as SIGABA (called ECM or ELECTRIC CIPHER MACHINE by Navy), ENIGMA or ASAM-7. Built by ASA in 1946, it was one of a series of simple handtesters.

It consisted of two rotor baskets to handle both ordinary and pluggable rotors, two panels and three or four plugboards. The device provided a means of assembling up to twenty 26-point rotors with fixed or pluggable wiring. A panel of pushbuttons and lights was provided for encipherment and another for decipherment. Basket endplates were wired to plugboards for complete flexibility. All rotor motion was controlled by hand. The output of the first ten wheels (one basket) could be connected to an optional fourth plugboard or to the input of the second ten wheels.

Operation was limited to the user's speed. Size was 1'H x 1'L . It was sent to the museum, and has probably been dismantled.

Ref: H.A.C. Outline #8

May 1953

5202 COMPARATOR, MARK II

The 5202 COMPARATOR, MARK II (AFSAF 41) is a high-speed general purpose IC comparator, photoelectrically matching large volumes of text on 35mm film. The MARK II was built by Hogan Laboratories, Inc., formerly known as Radio Inventions, Inc., and delivered to AFSA in 1952. Its basic purpose is calculation of IC (ratio of coincidences to comparisons) between two fields in a 35mm film. Testing covers a range of ratios between 1/40 and 40/1 coincidences with a very small tolerance in sensitivity. AFSAF 40 is the associated camera and storage unit, and accepts any tape input.

The film is divided into a high and a low field each 40 levels deep and is viewed in a gate 600 frames wide, permitting a match between two blocks of up to 24,000 characters. Three circuits are provided for recognition of coincidence, one for straight high IC above a set criterion (in the form of a step function which the machine successively computes at each setting), another for measuring light difference between the two film fields, and a third for recognition of blackout or no coincidence. At a hit the machine stops, the operator makes exact alignment manually and reads the IC total from an electronic counter of 999 capacity. Weighting of results is possible.

Film is exposed at a rate of 1000 frames per minute, and comparisons are made at up to 5000 overlaps per second. MARK II has increased accuracy (a few percentage points of error), greater

5202 COMPARATOR, MARK II

flexibility and speed and a wider gate (600 as against 500) than MARK I. The MARK II camera measures the same as MARK I, 4'H x 6'L x 3'D . The comparator is 5'H x 4'L x 3'D . Location is at Arlington Hall Station in Room 0320-B.

Ref: Mr. J. Deutsch
Mr. E. Fleming
Mr. D. Marston
Mr. J. Raisch

~~SECRET~~

Brief Descriptions of Analytic Machines
Second Installment

NSA-34
NSA-35
12 March 1954
Wheatley, LeRoy H

The project of writing these Brief Descriptions of Analytic Machines has been transferred from NSA-34 to NSA-35 since publishing the first installment, so this and subsequent installments will be under their joint sponsorship. This second installment consisting of eighty-five equipments or topics is now ready for publication. An additional thirty-four have been written in rough draft and are in the process of proofing, review, etc. Some twenty-two equipments remain to be written up. This figure includes the small backlog list and all equipments being planned to date, and may be reduced somewhat by research and changes of plans.

When the whole set of approximately 200 briefs has been published, a small number of re-issues will be sent out to correct errors and bring facts up to date. There will also be a glossary, index and table of contents compiled for the complete set. It is intended that such an index constitute the most complete existing list of Agency machinery, past and present. Reproduction at the Photolab, NSA-81, of 8 x 10 prints of most of the equipments is proceeding and will be sent out presently. Comments, criticisms and corrections on this work are invited; the extension is 563 at Arlington Hall Station.

March 1954

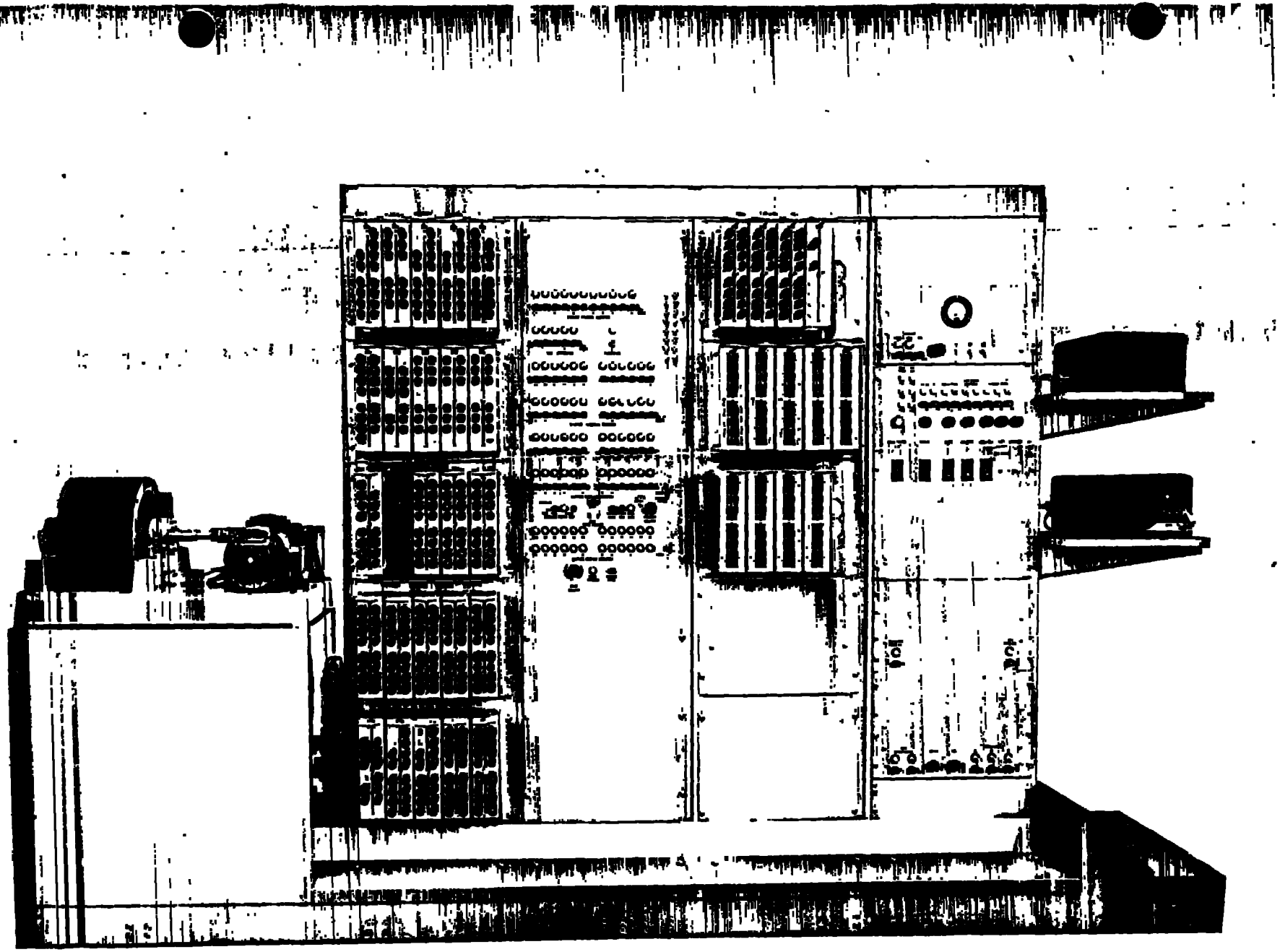
ABEL

ABEL (XFF) is a relay computer for low-speed parallel-type computation, including arithmetical and other logical processes. Built by Navy in 1949, it was the first of the Agency-sponsored computers to operate. It is an analog of ATLAS I, and contains no analytic orders.

It is a parallel computer, operating on the full 24 bits of a word simultaneously. Input of both data and program (sequence of orders) is by CXOO tape reader and not under program control; output is to a CXOO regeneration typewriter and tape punch. Programming of a problem is much the same as for ATLAS I and uses a one-address system. Memory storage is on a 24-channel (later a 48-channel) magnetic drum with a 2047 word capacity, each word consisting of 24 binary bits or digits. Pushbuttons provide for manual insertion into or reading from the registers. The 48-place accumulator, operating in conjunction with the control section of the machine and the 24-place auxiliary Q-register, performs all computations.

Overall size is 7'H x 14'L x 2'D plus associated equipment. Rate is 10 orders per second. It was transferred to Office of Naval Research and is in operation at George Washington University.

Ref: Technical Library
NSA-34 files
Mr. K. P. Cook



ABML
XFF
Analog to ATLAS I

March 1954

ABNER

ABNER (AFSAF-32 is Serial 1 and AFSAF-D53 is actually Serial 2, not a different machine as numbering implies) is a serial electronic digital computer especially designed for such cryptologic problems as key generation, frequency counts, coincidence and equality counts, slide routines, modular arithmetic, writing on widths and others. Designed and built by Army, the Serial 1 machine began operation on 1 June 1952. Delivery of Serial 2 is expected from Technitrol Engineering Company by February 1954. BAKER (AFSAF-D89) was a relay computer analogous to ABNER whose programs it was built to test.

The machine operates serially on the individual bits or digits of a word, starting with the least significant. Most instructions employ four addresses. The machine can distinguish between numbers by size or sign. Programming (listing of orders in sequence) is relatively simple and is normally coded in decimal instead of octal notation as for most Agency computers. There are 19 ordinary and 12 special analytic orders available on the machine.

Input is by (1) punched tape, photoelectrically read on a Ferranti reader at up to 315 characters per second; by (2) punched cards on a collator at 240 or 120 cards per minute and by (3) magnetic tapes at about 2500 characters per second;

ABNER (Cont'd.)

all under program control. Output includes these three plus an Anderson-Nichols line printer (AFSAF-44B) at 300 characters per second, - 7½ lines of 40 characters each. One, and eventually four 7-level magnetic tapes of 720,000 character capacity serve as input, output and intermediate storage. The peripheral ABNER CONVERTER UNIT provides ready interchange between media.

The control unit receives orders from the memory and operates the memory, arithmetic unit and input-output devices accordingly. The arithmetic unit consists of five registers or loops of electric delay lines constantly circulating the information. One of these, the accumulator, may be used to retain the results of arithmetic processes.

The memory consists of 1024 words contained in 128 mercury delay lines each storing eight 45-bit words plus 3 associated non-textual bits for control of synchronism. Being under program control, the magnetic tapes constitute auxiliary memory. A console permits manual control for interruption, insertion and verification.

Pulse rate is one megacycle and access time cannot exceed 336 microseconds, resulting in from 440 to 20,000 arithmetic operations per second. The main cabinet measures 7'H x 24'L x 2'D and, together with console and other units, requires about 630 square feet (2-1/2 bays) floor space. Potentially one of the most versatile and valuable equipments yet conceived, Serial 1 is in operation at Arlington Hall Station in room 0310-B.

Ref: T/CA 10/53
Mr. J. Hyduke
Mr. P. Johnson
Mr. J. Rixse

MARCH 1954

ALCATRAZ

ALCATRAZ (AFSAF-92, CXLQ) is a digraph frequency counter with a 36 x 40 counter array, with two rows and two columns of totals counters. It was built by Engineering Research Associates under task 7 in July 1950 and replaces MIKE (CXMM). BABY ALCATRAZ (CXMH, 6 x 6 CB), developed by ERA under task 11, LEO, is a 36-cell frequency counter, one thirty-sixth the size of ALCATRAZ and now in use at Naval Security Station in room 4152. Its special line-printer, type 10 AVN, prints out results eleven groups to a line, exactly half the 22 group capacity of the type 10 AVR printer developed at the same time for ALCATRAZ. In July 1950, Commercial Controls Corporation delivered a card-reader unit, BEAR (AFSAF-93, CXOL), permitting input from IBM and RemRand cards at 4 per second as an alternative to the usual CXCO double-headed 6-level tape reader input.

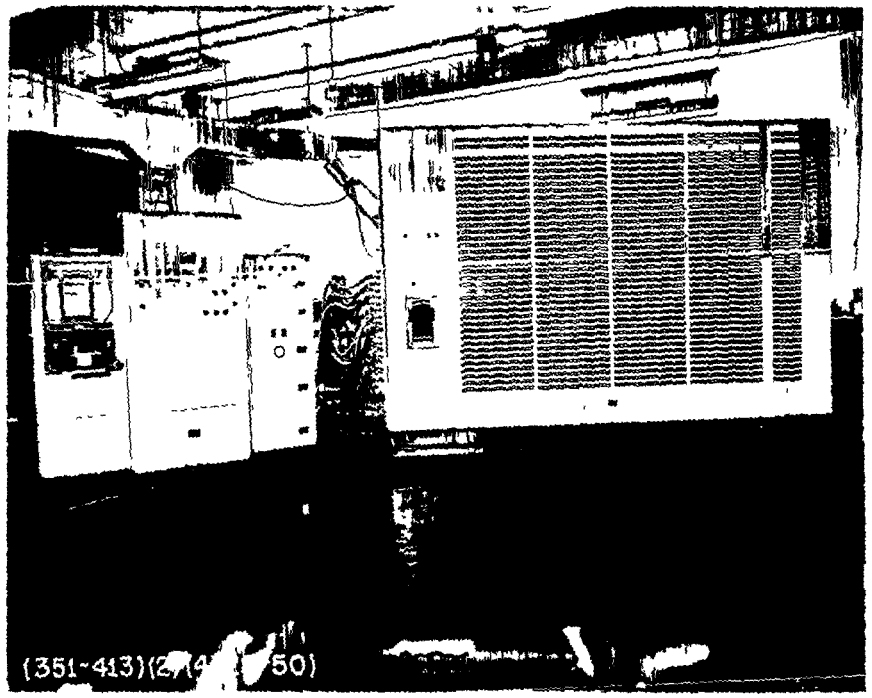
The machine is an improvement over MIKE in that results are printed as well as visual, cell counters have a 3-digit capacity, total counters have a 5-digit capacity, 6-level tapes may be used to operate the 36x 36 translation matrix. The control contains a double-headed CXCO tape reader, matrix input plugboards, the 36x36 translation matrix and the distributive cyclometer. The two counterbanks are fed by 36^2 or 1,296 wires from the translation matrix. Printed output contains cell totals, row and column totals and the overall frequency count.

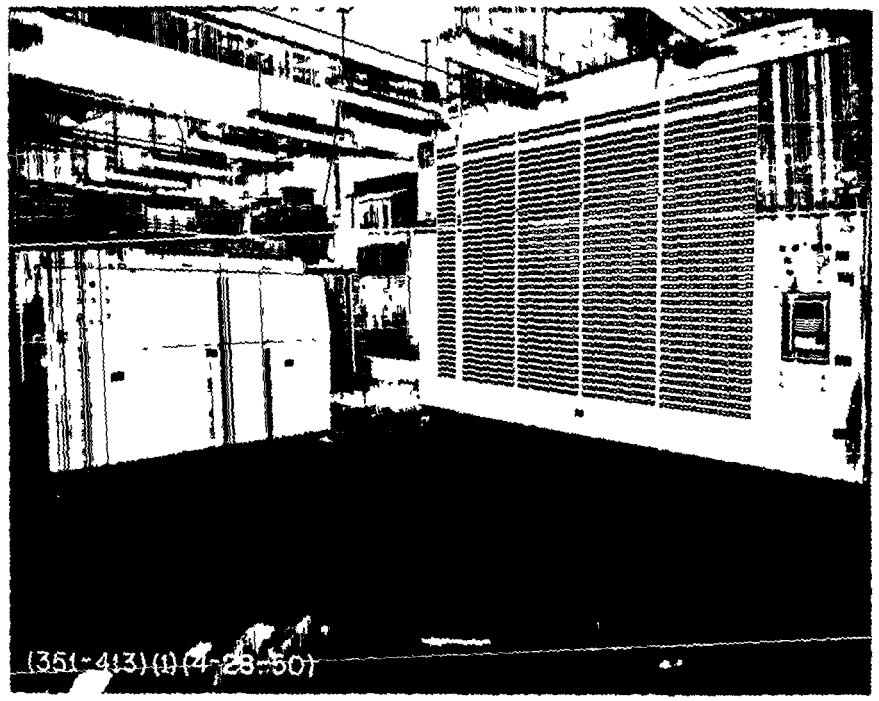
ALCATRAZ (Cont'd.)

Control and printer each measure 6'H x 6'L x 3'D, and the two counterbanks 8'H x 12'L x 4'D. Rate is up to 16 characters per second. It is at Naval Security Station in room 4152.

Ref: Instruction Manual (R531.1/775)

T/CA 8/51 Report
Mr. D. Hogan
Mr. J. Stapleton





ALCATRAZ
AFSAF 92
CXLQ

~~CONFIDENTIAL~~

March 1954

ASAY-7 ANALOG

The ASAY-7 ANALOG was a relay device to simulate the function of the ASAY-7 ciphony device. It operated with a 513 REPRODUCER to generate key for a security study. Section WDGAS-92 of Army built it in early 1948.

The ANALOG was developed to permit study of cipher resulting from use of random noise generated key, and produced 50,000 elements of key. Motion of the 4 key-producing wheels was simulated by cyclic offset of pattern in cards, including dilation (repetition) of key. Thirty wire contact relays were used according to the same principles as the TAN KEY GENERATOR. Results were checked by doing the job twice.

Size was 3'H x 2'L x 2'D plus a 513 REPRODUCER and rate was 100 cards per minute. It was dismantled shortly after the study was completed.

Reference: Mr. S. Thorne

March 1954

ATLAS I

ATLAS I (AFSAF-70, CXMX) is a parallel type electronic computer to perform basic arithmetic processes and able to make conditional decisions on the basis of size and sign, modifying its own program of orders. Under Task 13, Engineering Research Associates delivered Serial 1 in December 1950 and Serial 2 in May 1953. The model is available commercially under the name ERA 1101 COMPUTER. NSA-35 built ABEL, a relay analog, in November 1949, which has since been transferred to George Washington University.

Several peripheral equipments have been developed: a pair of special tape punches, a HIGH-SPEED TAPE COMPARATOR consisting of two POTTER READERS (AFSAF-25) and a comparing unit, and a trio of rather non-descript devices known as OCTAL KEYBOARD, 8 KEYS, 2 OCTALS PER FRAME (AFSAF-D65), a CONTROLLER-OCTAL-TAPE-REPRODUCER-CONVERTER (AFSAF-D66), a TAPE PUNCH VERIFIER (AFSAF-D67) and a CONTROLLER-OCTAL-TAPE-REGENERATOR-CONVERTER with no AFSAF number. In addition, two equipments are under construction: BUNNY (AFSAF-D70/11), which is a high speed tape reproducer to insert seventh level pattern, and CENSOR (AFSAF-D70/10), a tape checking device.

Operation is in parallel, simultaneously handling all bits of a word, a binary number. This makes for faster operation but more complex machinery. Each order employs one address. Data

ATLAS I (Cont'd.)

is read in from 7-level punched paper tape on a photo-electric reader at 144 characters per second, and is not under program control. Output is to a CXCO regeneration typewriter and tape punch. The control unit interprets orders read from the drum (a repertory of 42 is now available) and operates the machine accordingly. The magnetic drum memory is divided into $2^{14} = 16,384$ boxes or memory locations, each of which holds a 24 binary digit word, which may be either a coded order or datum. The arithmetic unit consists of a 48-bit accumulator or A-register, a 24-bit Q-register and a 24-bit X-register. These together perform computations as required by the controls. Special orders have been added, including a random order, probably the most novel feature on the machine.

The drum revolution time of 17 milliseconds indicates that, without planning, each instruction will take that long. But with careful planning, placing the instructions and relevant data where they will be immediately available when needed, the time per order can be lowered to as little as one percent of a drum revolution, or, at times, one fifth of one percent. The care needed to accomplish this is considerable.

Physical size of the main machine is 7'H x 40'L x 2'D plus reader, control panel and auxiliary equipment; this requires

ATLAS I (Cont'd.)

over a thousand square feet of floor space. Pulse rate is 400 kilocycles per second and access time ranges from 32 micro-seconds up to 17 milliseconds (1 drum revolution). Both are in operation at Naval Security Station in room 4152.

Ref: NSA-34 Files
Mr. E. Burke
Mr. D. Hogan
Mr. P. Johnson

ATLAS I
AFSAF 70, CXMX, ERA 1101

March 1954

ATLAS II

ATLAS II (AFSAF-70A, AFSAF-70B) is an electronic parallel-type computer with all the functions of ATLAS I but with additional types of memories which result in greater speed and capacity. Serial 1 was delivered by Engineering Research Associates, now a subsidiary of Remington Rand Corporation, in September 1953. Serial 2, actually a model change, is expected by August 1954. The machine is available commercially under the name of ERA 1103 COMPUTER. Auxiliary equipment is the same as for ATLAS I, the ERA 1101 COMPUTER.

Operation is in parallel - all bits of a word (number) are operated on simultaneously. Word size is 36 bits, 6 for address and 30 for two 15 bit addresses or data. Initial input is by 7-level paper tape read photoelectrically at 144 characters per second. Four magnetic tapes under program control during operation serve as input, output and an auxiliary memory. In addition, a CXCO regeneration typewriter or tape punch is available for output. In addition to the intermediate speed magnetic drum memory which holds 2^{14} or 16,384 words and the magnetic tapes just mentioned, there is a primary high-speed electrostatic storage (Williams tubes in serial 1, AFSAF-70A, and magnetic cores in serial 2, AFSAF-70B) capable of storing 2^{10} or 1,024 words. Both the electrostatic and drum memories are fully addressed. The arithmetic unit consists of a 72-bit accumulator, a 36-bit X register and a 36-bit Q-register. The control unit functions the same as in ATLAS I. Programming, or sequencing of orders, uses a 2-address system and is not very difficult.

ATLAS II (Cont'd.)

Several special orders, such as modular arithmetic, a scale factor order and repetition, are built in routines. This last one in particular is the outstanding feature which differentiates the machine from other computers and contributes most to its cryptologic usefulness.

The device consists of 6 cabinets each measuring 7'H x 18'L x 2'D, plus peripheral equipment, and requires about 1200 square feet of floor space. Pulse rate is 500 kilocycles per second. Access time for electrostatic storage is about 12 to 18 microseconds, and for data on tape or drum is not great since one drum revolution takes 34 milliseconds. It operates at Naval Security Station in room 4152.

Ref: Lt. E. Friend
Mr. D. Hogan
Mr. P. Johnson

March 1954

BABY OPHIS

BABY OPHIS (AFSAF-D57A) is a WIRED WHEEL ANALOG designed to simulate with relays almost any rule of rotor motion for five rotors of up to 32 points each. It was constructed by NSA-35 in April 1953 to test rotor settings and cycles under various rules of motion.

Considerable flexibility of control is provided. A tape, often one from the AFSAF-35 SETTING GENERATOR, controls rotor stepping through a plugboard. CCM and classic Enigma motion are built in. Certain comparisons are possible, including a feature permitting carrying plain text through a couple of rotors, while carrying cipher text back through the others and making comparison between the two results.

It is a baby only in number and size of rotors when compared with OPHIS, its dimensions being 6'H x 5'L x 3'D . Rate of operation is 6 to 8 pulses per second. It is now located at Arlington Hall Station in room 2050-B.

References:

NSA-354B files
Mr. N. Christopher
Mr. F. Mayol
Mr. K. Polley

March 1954

BAKER

BAKER (AFSAF-D89) was a low-speed parallel relay computer to perform the same mathematical operations and analytic functions as ABNER. It was built by NSA-35 in February 1953 and used mainly to test programs for ABNER.

Input was a standard CXCO tape reader and output was to a CXCO regeneration typewriter and tape punch. The magnetic drum memory operated at 440 RPM and had a storage capacity on either half of the drum of 1024 words of 45 binary bits. Either half could be used independently. There were four 45 bit registers, the Q, X, X-bar and Y, and a 90 bit accumulator. All but three of the orders were handled in paralled fashion; that is, all bits were operated on simultaneously. A 10-bit address system and a 4-address code similar to that for ABNER was used. Control was similar to that in ABNER.

The machine, arranged in an "L", measured 6'H x 20'L x 2'D plus power supply. The timing control clock in BAKER made 10 cycles a second yet there was no basic pulse rate. Multiplication and division required 4 seconds at most; addition, subtraction and comparison needed 1/3 of a second. It has been dismantled.

Ref: Mr. B. Baker
Mr. K. P. Cook
Mr. J. Deutsch

March 1954

BRUTE FORCE DEVICE

The term BRUTE FORCE DEVICE (AXHB/1) refers by general usage to the IBM gates and processes (and rarely to the several other machines of comparable function) designed to search through cipher text and find a type of coincidence known variously as a brute force hit, a copperhead hit, a double hit, a double repeat, a two-point hit, a red (point) hit, or a pattern hit, - this last in only one of its several meanings. Briefly, the required condition is that two pairs of repeated groups exist, either between two parts of a message or between pairs of messages, and further, that these repeats be in phase and at equal intervals. ICKY I and COPPERHEAD did a comparable job.

The first such gate, the BABY BRUTE FORCE DEVICE, described in M.A.C. Outline No. 24, operated in connection with a 405 TABULATOR. Four successive models were built by army section WEGAS-92 between 1942 and 1944, all designed to find double repeats at any interval from 1 to 9, in 3- , 4- , or 5-character traffic. The JUNIOR BRUTE FORCE DEVICE, for use with a 407 TABULATOR, superseded this and increased the span of search to 12 pentagraphs, numeric only. It was also needed with a special plugboard for reducing test to pattern and called PATTERN BRUTE FORCE DEVICE. In this connection 110 relays of a general purpose gate were rewired and used with a 797 COORDINATING REPRODUCER to punch patterns into cards at 100 yards per minute. It was called PATTERN PUNCHING DEVICE. The term FULL BRUTE FORCE applies only to a process on IBM equipment where search is made through the full length of the message for this type of coincidence.

BRUTE FORCE DEVICE (Cont'd.)

Operational time depends on the job; the 405 TABULATOR matched cards at 150 cards per minute and listed at 80 per minute; the 407 currently used is faster, matching and listing at 150 cards per minute. This type of search is most efficient on 5-character traffic. The last, BABY BRUTE FORCE measured 1'H x 2'L x 1'D, in a plugboard cover, and JUNIOR BRUTE FORCE was 3'H x 3'L x 1'D. The former is dismantled, and the latter is in operation 82, 1700-A in Arlington Hall Station.

Ref: M.A.C. Outline No. 24
Mr. J. Hyduke
Mr. J. Powers
Mr. W. Sharp
Mr. S. Thorne


B


B
START
STOP
FINAL TOTAL

JUNIOR BRUTE FORCE

AXHB/1

March 1954

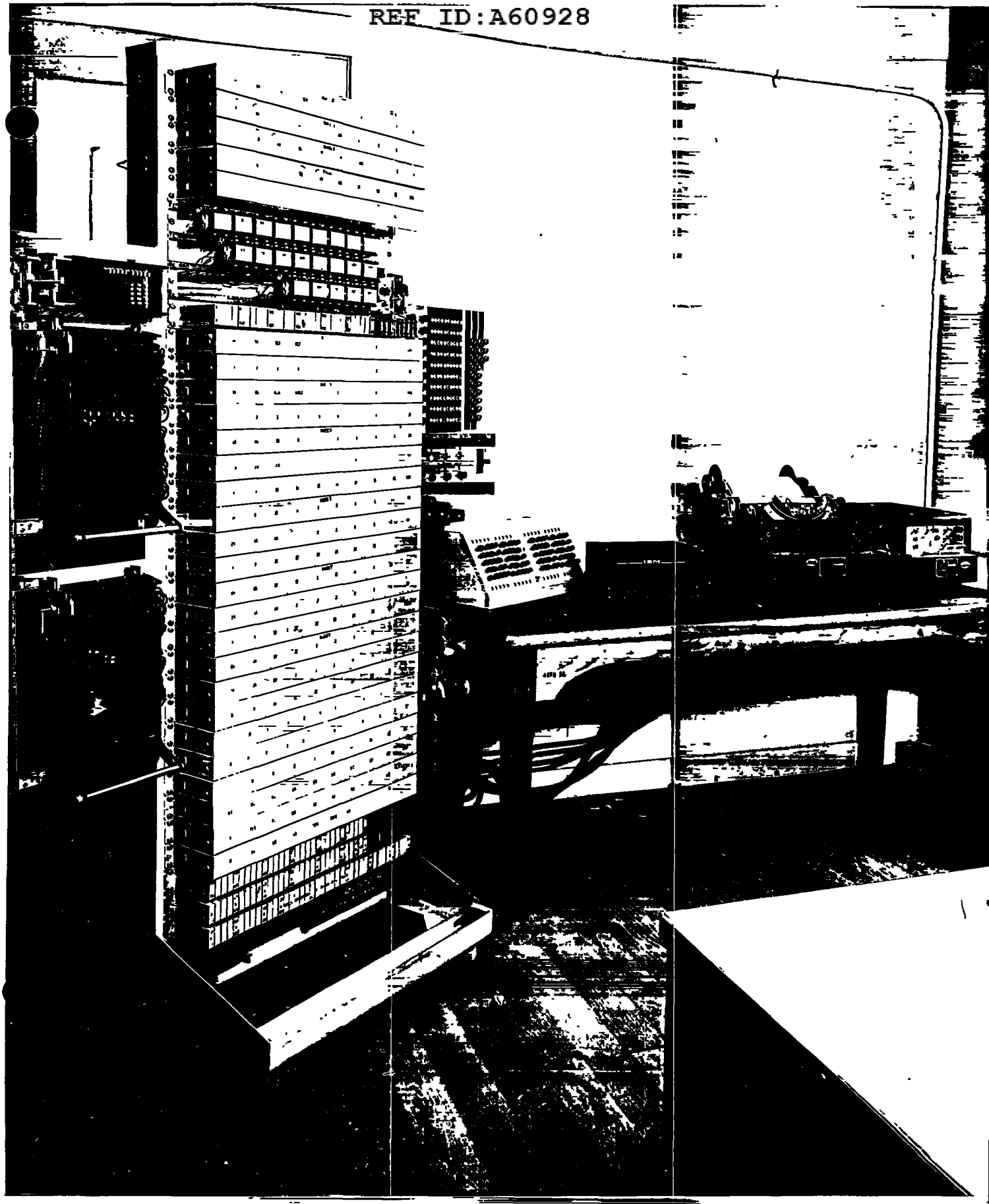
B-211 ANALOG

The B-211 ANALOG (AFSAF-36, AXOQ/1 and /2), comparable to Navy's RICKY, refers to a set of relay devices to simulate completely the functions of both [redacted] and [redacted] modifications of the HAGELIN B-211 cipher device. The first, for the [redacted] problem, was built by Army in 1944. Then two PINK ANALOGS (AXOQ/1 and AXOQ/2, [redacted] ANALOG) were built for the [redacted] the first delivered in April 1946. Three models for the [redacted] were built in 1949, 1951 and 1953. Although basically no different cryptographically, variations include selector switches in earlier models and relays in later ones [redacted]

In all of them rotor wiring is set on a plugboard, and stecker by pushbuttons or on plugboards, with lights to show wheel positions. Input is by tape or keyboard and output is to a CXCO regeneration typewriter. Some may be used as a whole or effectively as either of the component halves to produce enciphered, deciphered or fractionated text.

Operation is at 8 characters per second and size is about 6'H x 3'L x 2'D . Three are dismantled, but the last three [redacted] type are used operationally at Arlington Hall Station in room A-2208.

Ref: Completion Report, AFSA Technical Document #35
Mr. F. Snyder



March 1954

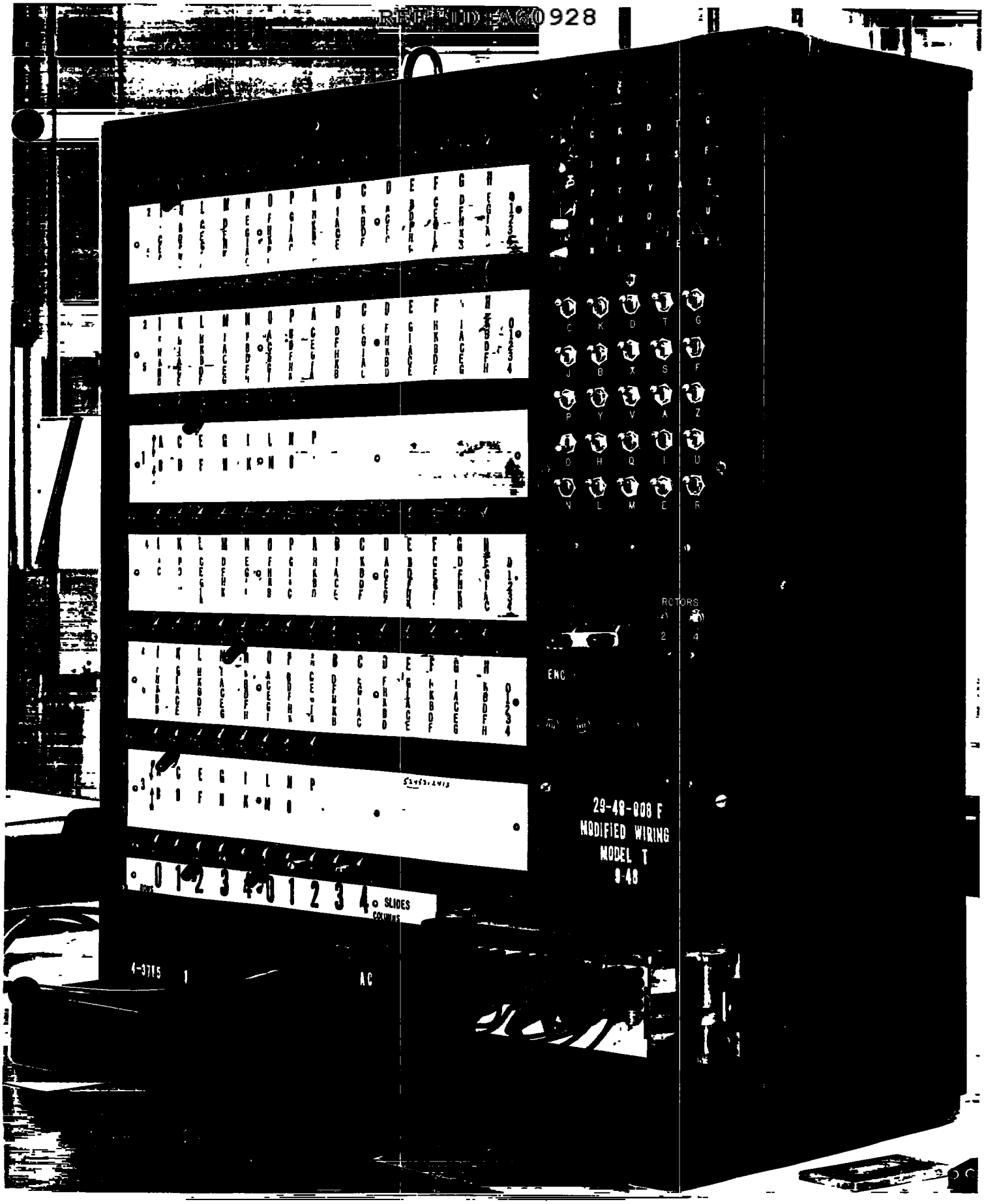
B-211 HANDTESTER

The B-211 HANDTESTER (AFSAF-119, AXO4/1) is an electrical circuit testing device able to produce the effect of the commutators and rotors of the HAGELIN B-211 cipher machine. The first was built by Army, WDGAS-74, in January 1947 (see M. A. C. Outline No. 8) and is now dismantled. Three later models, delivered in February and July 1947, use switches to accomplish the fractionation.

An analyst or trained clerk may use the device to test wheel settings, fractionate text to obtain either of both components, decipher and encipher messages, and recover slide and motion pattern. All wheel motion is by hand. Cipher is introduced by switches and plain text values are read from lights, or vice versa by resetting a switch. All steckering is now provided for in a single switchboard.

Rate of operation depends on the operator and the job. The device is much more rapid than using charts or the cipher machine itself. All three are now in operation at Arlington Hall Station in room 2407-A [redacted] handling both model T and model M wiring. Size is 3'H x 3'L x 1'D.

Ref: M.A.C. Outline No. 8
Mr. H. Collins
Mr. F. Mayol


29-48-008 F
MODIFIED WIRING
MODEL T
9-48
ROTORS
ENC
SLIDES
COLUMNS
AC

B-211 HANDTESTER
AFSAF 119

TOP SECRET

FROTH

March 1954

CALL 35 DEVICE

The CALL 35 DEVICE (AFSAF-114, MOD 35 GATE) is a relay gate which operates with a 797 COORDINATING REPRODUCER to convert [redacted] intercept call-signs to their corresponding Baker-Volume book number. It was built by NSA-22 in March 1951.

The device consists of two complete units for sender and receiver call signs, and [redacted] Input is by card and output is the sum in decimal form and corresponding book number. [redacted]

Its size is 3'H x 3'L x 2'D. All computation occurs between card cycles so the rate of 100 cards per minute results in 200 call sign decipherments per minute. It is in use at Arlington Hall Station in room 1200-A.

Ref: Mr. S. Thorne


CALL 35

CALL 35 DEVICE
AFSAF 114
MOD 35 GATE

TOP SECRET

FROTH

March 1954

COLERIDGE KEY SUBSTITUTION DEVICE

COLERIDGE KEY SUBSTITUTION DEVICE is a twice-used term. Navy informally constructed a device of that name in 1947, a collection of plugboards used for a few months and dismantled when DEMON arrived. It merits no write-up. In 1948, NSA-82 built informally for Army the electrical COLERIDGE KEY SUBSTITUTION DEVICE (KEY DERIVATION for COLERIDGE) described here, [redacted] a hand-operated decipher, hand-tester and key checker. In general, it parallels OBOE (which likewise was called KEY DERIVATION for COLERIDGE) and PICCOLO (AFSAF-37).

This device consists of a keyboard for input and a lampbank or CXCO regeneration typewriter for output. Pressing 2 key in succession representing key and cipher in either order produces a possible-plain character in the form of its [redacted] A switch permits enciphering.

Rate is up to 6 or 8 characters per second and size is insignificant, only special wiring and lamps on the back of an IBM keyboard, plus CXCO regeneration typewriter. It is available, but stored at Arlington Hall Station in room 2058-B.

Ref: Miss K. Blank
Mr. W. Lutwiniak
Mr. E. Marston
Mr. J. Stapleton

March 1954

COLUMN ARRANGING DEVICE

The COLUMN ARRANGING DEVICE (AFSAF-113, COLUMN ARRANGER) is a specialized relay device used with a SELECTIVE PUNCH, later with a 797 COORDINATING REPRODUCER, to prepare a table of relationships based on two sets of digits with a mod 5 or 6 range. Model I was built by Navy in 1949, an independent part of the NC-8 AUTOMATIC CIRCUIT CHANGER, and simply arranged pentagraphs in ascending or descending order, 0 to 9 . Model II, also by Navy in 1949, and Model III, by NSA-22 in December 1950, operate with a 797 REPRODUCER.

[redacted]

tetragraph. Column selection order is pluggable. Input, therefore, is two tetragraphs and output is a list of pentagraphs or hexagraphs which are searched by other equipments for isomorphism in either of the two components.

Size is 4'H x 3'L x 2'D and rate is 100 cards per minute. Model I was dismantled. Model II and later Model III were built into the same gate with GLID and the SUBSTITUTION DEVICE. It is available for use at Arlington Hall Station in room 1700-A.

Ref: Mr. W. Hopper
Mr. J. Hyduke
Mr. F. Smith
Mr. S. Thorne

March 1954

COMPUTERS

The general purpose electronic computer can perform at high speeds a number of arithmetic and logical operations. The results can be retained internally for later use or they can be used to control the computational procedure to follow. This control is made possible by the computer's ability to discriminate and to modify its own instructions. The Agency is concerned with 6 types, or a total of 10 or 11 machines, each described under one of the following headings: ABEL, ABNER, ATLAS, BAKER, EDPM (IBM 701) and NOMAD.

Information can be transferred to and from a computer by means of magnetic tape, perforated paper tape, punched cards, or electric typewriters. Most computers use more than one of these mediums and several use all. Some machines, particularly those which employ magnetic tape, are capable of accepting input during operation; others require that all data needed for a computation be loaded into the computer before operation is started.

In addition to input-output equipment a computer has three main components: the control unit, the arithmetic unit, and the memory. This last is divided into cells and in each a unit of information, either an instruction or a datum, may be stored. In order that stored material may be located and used, addresses are assigned to the memory cells. The control unit on receiving an instruction from the memory directs the arithmetic unit to perform the operation

COMPUTERS (Cont'd.)

indicated by certain bits (binary digits) of the instruction. Other bits specify the location(s) in the memory of the operand(s). When the operation has been completed and if the instruction has not called for a jump to some other part of the memory, the control unit of most computers takes as its next instruction the contents of the memory cell following that which contained the instruction just used, and the cycle is repeated. However, some computers do not depend on this sequencing, but rather each instruction includes the address of its successor. This device is characteristic of the so-called four-address computers.

The greatest restriction to computation speed is the access time of the memory, i.e., the time required for a memory cell to release its contents to the arithmetic unit or the control unit after the latter has called for the information. This fact has motivated the search for faster memories and as a consequence there has been a progression from the slow static electro-mechanical relay memory through the medium speed cyclic memories of the magnetic drum or acoustic delay lines to the present high-speed static storage made up of electrostatic storage tubes. The magnetic core matrix may constitute an even faster memory in the near future. Magnetic tapes are now being used for auxiliary storage, but their speed-limiting mechanical features preclude use as a primary memory.

Computers can be further distinguished by the manner in which the arithmetic is performed. Machines which operate on each bit

COMPUTERS (Cont'd.)

separately are called serial computers; those which handle all bits simultaneously are called parallel. Parallel computers tend to be faster, but their construction is considerably more complex.

Ultimately the design of a computer becomes a function of the work it will have to do. Input-output equipment must be adequate to handle the necessary data without unduly holding up computation, and the computer itself should be fast and flexible enough to provide practical solution for the problems to which it is to be applied. Specialization in the order code is one means by which the potentialities of a computer can be extended, and this has been done to varying degrees in the machines being used and to be used by NSA, principally ABNER.

March 1954

COUNTING DEVICE FOR CARD-OPERATED TYPEWRITER

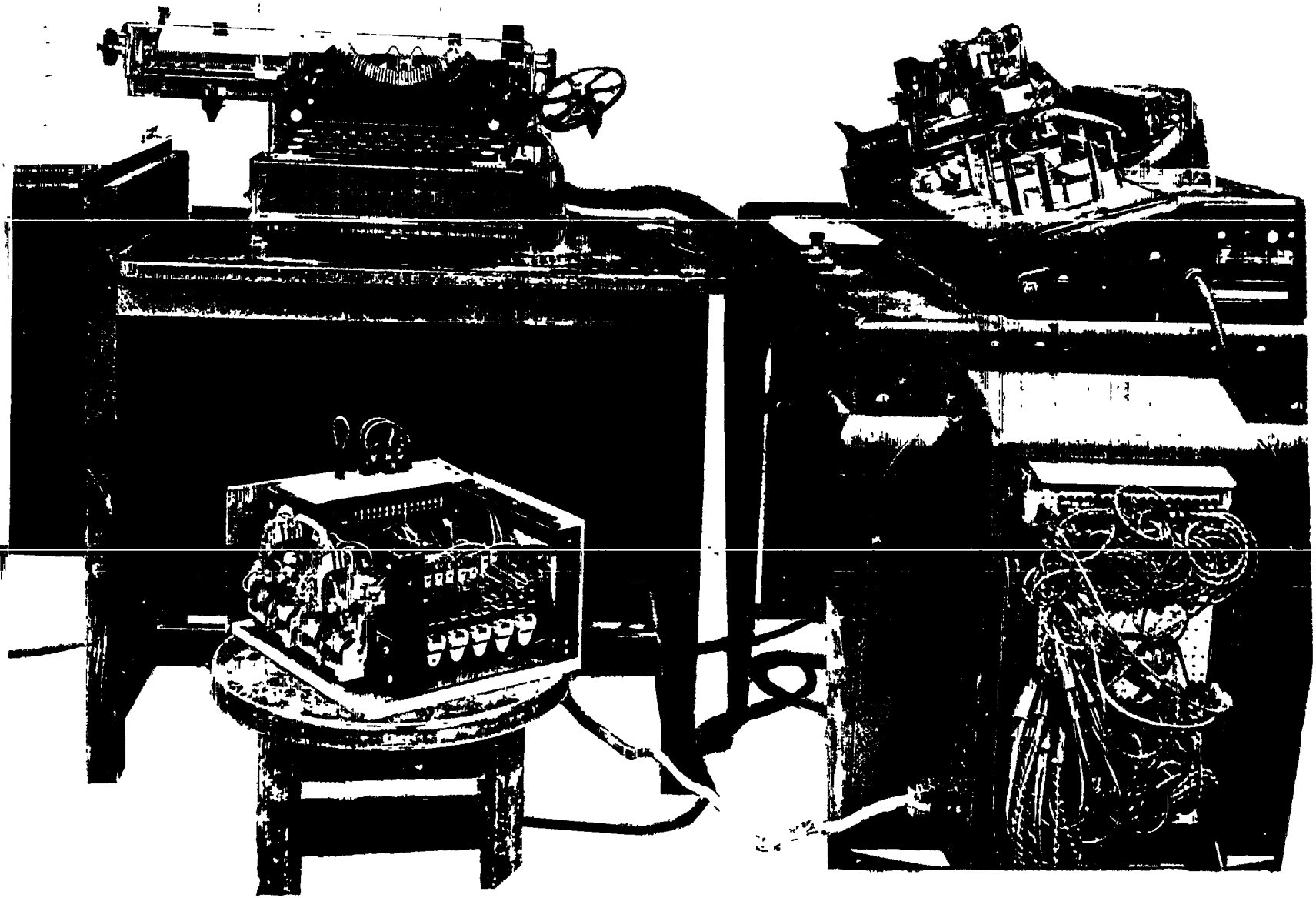
The COUNTING DEVICE was a relay gate which, by counting the strokes of an 058 CARD-OPERATED TYPEWRITER, served to break the text into required lengths. It was built by WDGAS-92 in 1948. A similar job was done by a set of TRANSPOSITION DECIPHERMENT CIRCUITS, a machine modification and not a device in itself, which were built into an 040 TAPE-TO-CARD PUNCH for use with traffic on tape.

The COUNTING DEVICE, consisting of seven relays, was used for deciphering simple columnar transposition messages in which length of column varied. It counted strokes of the typewriter, at most 99, and when a predetermined critical value was reached, it halted the card feed, operated the carriage return, reset the counters, and started the cycle again.

Size was 1'H x 1'L x 1'D plus an 058 CARD READER and a CXCQ regeneration typewriter. It operated at 8 to 10 characters per second and has been dismantled.

Ref: Machine Branch Annual Report, 1948
Mr. S. Thorne

COUNTING DEVICE for CARD OPERATED TYPEWRITER



COUNTING DEVICE
for CARD-OPERATED TYPEWRITER

MARCH 1954

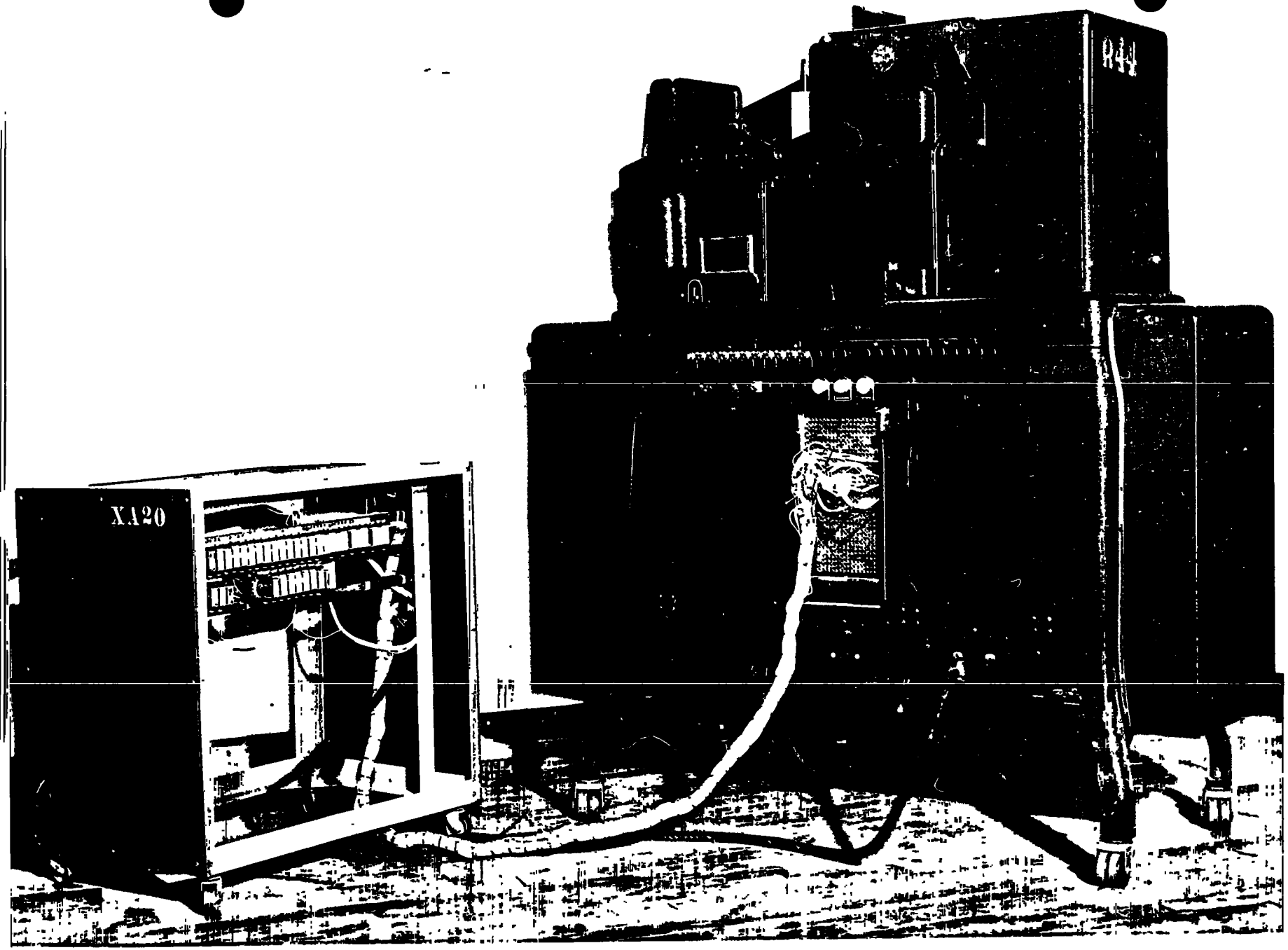
CYCLIC DELAY KEY GENERATOR

The CYCLIC DELAY KEY GENERATOR (CD KEY GENERATOR) was a special purpose relay gate used with a 513 REPRODUCER to produce key for study purposes according to prescribed control. MARK I was built by Army, section WDGAS-92, in late 1948; MARK II, a similar generator, was completed in late 1949 by simply rewiring MARK I.

Both models used the same rules of motion. The first had five 16-point wheels, and the second had eight. Key in parity form was calculated in two ways. The first used mod 2 addition to combine selected points on the 5 (or 8) wheels. The second used a formula involving storage in IBM cards of as many as five elements of key. Starting points for all wheels were put into cards, and wheel settings were continuously recorded to facilitate cycle study.

The gate measured 3'H x 3'L x 2'D and operated with a 513 REPRODUCER at 100 cards per minute. It is now dismantled.

Ref: Machine Branch Annual Report, 1949
Mr. S. Thorne



CYCLIC DELAY KEY GENERATOR

CYCLIC DELAY KEY GENERATOR
C.D. KEY GENERATOR

March 1954

DECIPHERING MACHINE

The DECIPHERING MACHINE (SPECIAL DECIPHERING DEVICE, Project 1049) was a relay deciphering device intended to incorporate the functions of several special purpose devices into one generalized machine. It was built by F Branch of Army in September 1945 and paralleled in part functions of MATTHEW and similar devices.

Two control units, each with CXCO tape reader and keyboard for input and a control panel, operated with a relay unit which performed the actual deciphering processes, Results went to a CXCO regeneration typewriter for page printing. It could do 1) monoalphabetic substitution through a plugboard, 2) plain text reproduction, 3) polyalphabetic decipherment for cycles of 2 to 5, or 4) decipher literal or digital codes of up to 5 characters. Although superior to hand methods, the machine was slow and not so flexible as expected.

Each of the two control units was set on desks together with tape reader head, keyboard and CXCO regeneration typewriter and measured 2'H x 2'L x 1'D. The relay unit was 6'H x 2'L x 1'D. Rate was 6 to 8 characters per second. It was dismantled and replaced by the 797 COORDINATING REPRODUCER and various faster equipments.

Ref: MAC Outline #27
Mr. N. Christopher

March 1954

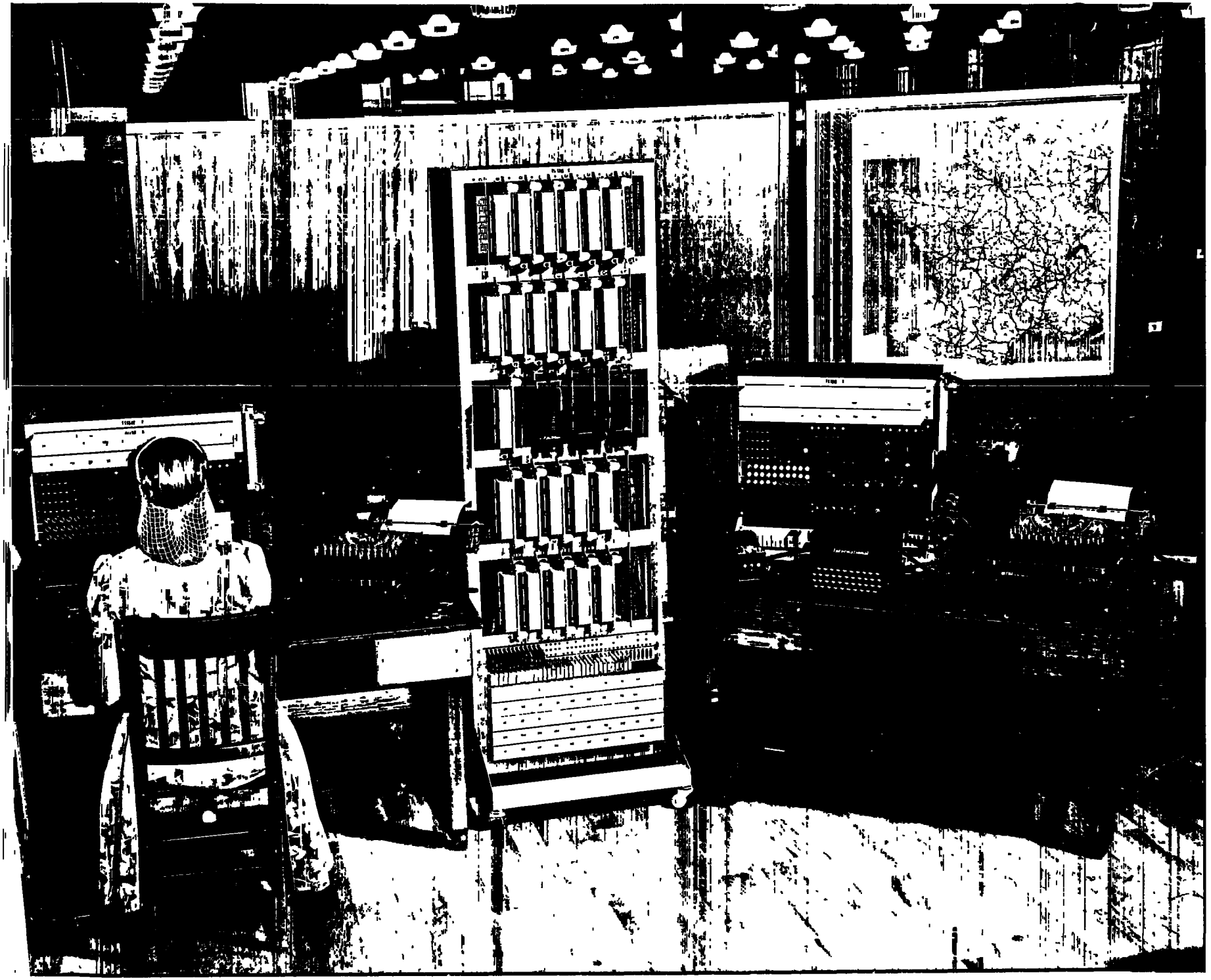
DECIPHERING UNIT

The DECIPHERING UNIT was a relay deciphering device used with a 405 TABULATOR to apply numerical key to traffic through an enciphering square. The first of four was built by Army in early 1944 and deciphered twenty cipher positions simultaneously using one of fifteen squares set up on interchangeable 8 x 20 plugboards. The second, built by International Business Machines Corporation, was actually four smaller units each handling five groups. These were wired in tandem and used for slide-runs in conjunction with the SLIDE-RUN MACHINES. Two more, further modifications of the first, were built and used by Army.

A cipher and a key digit were entered from the TABULATOR into a pair of counters in the gate. The key counter energized a row of 10 cells, one in each column of the enciphering square plugboard. The cipher counter did the same in a particular column and the cell thus selected emitted the deciphered value to the TABULATOR.

The device was like a SLIDE-RUN MACHINE, but lacked the recognition elements. The first and the last two were 5'H x 8'L x 3'D; the four units of the second model were each 4'H x 2'L x 2'D. All are now dismantled. A unit could handle up to 2200 messages per day and operated at 150 cards per minute.

Ref: Mr. J. Powers



TOP SECRET FROTH

March 1954

DMD

DMD (AFSAF-D60, DESK MODEL DECIPHERER) is a special purpose handtester, part relay and part electronic, to decipher messages in the Czech system [redacted] The first model was built by NSA-35 and delivered in April 1952. It parallels several other equipments such as MATTHEW and HELLCAT I and II.

Using 26 alphabets of 26 characters each, the device assumes key (or plain) against cipher and derives possible plain (or key). It has a 26 x 26 non-pluggable matrix. Input is by keyboard and output is to a CXCO regeneration typewriter. 25 of the alphabets are inversely related to the plain (or key) sequence, which is the 26th alphabet.

Size is 2'H x 6'L x 2'D. Speed is about 1 character per second. It is located at Arlington Hall Station in room 2520-A.

Ref: T/CA 8/50
Mr. N. Christopher
Mr. E. Fleming
Mr. J. May

TOP SECRET FROTH

REF ID:A60928

DMD
AFSAF D60, DESK MODEL DECIPHERER

~~SECRET~~

March 1954

DUDBUSTER

The DUDBUSTER (ARLINGTON DUDBUSTER) was a relay-type analog of the ENIGMA cipher machine, designed to set messages, i.e., find window settings, by using a statistical test rather than a crib. An earlier model, using thirty-six 003 frames (basic units of the Army BOMBE), was built in 1943 by F Branch but was discarded in 1944 in favor of a two-frame model.

The 16 lowest frequency letters of the language were plugged through a frame to a 52 segment distributor controlling 52 counters. The frame then ran through a machine cycle of 26^3 settings, enciphering the set of low frequency letters at every possible setting. These sets were stored and matched with 52 cipher letters represented on a plugboard. Occurrence of less than 19 coincidences stopped the machine. The second frame, running 52 settings behind produced the possible plain text and printed it on a CX00 regeneration typewriter.

Set up time was about 15 minutes, and operating speed was 40 tests per second. Size was 8'H x 4'L x 2'D. It has been dismantled.

Ref: M.A.C. Outlines No. 15.

MARCH 1954

DUENNA

DUENNA (CXLU, N-1500) is a high speed two-wheel bombeing device to recover reflector plugging, window settings and steckering as used in YELLOW ENIGMA,. given only rotor wiring. It considers crib-vs-plain pairings and tries all intervening scrambling circuits possible to find one with no conflicts. Five such machines were built for Navy by U.S. Naval Computing Machine Laboratory, the first being delivered in November 1944. The Army AUTOSCRITCHER and SUPERSCRITCHER and the British GIANT are comparable equipments. Plans for a pair of BOMBE-type cribtesters to be called MONA were dropped in favor of DUENNA, which would do the same test using 2 wheels where MONA would have used one.

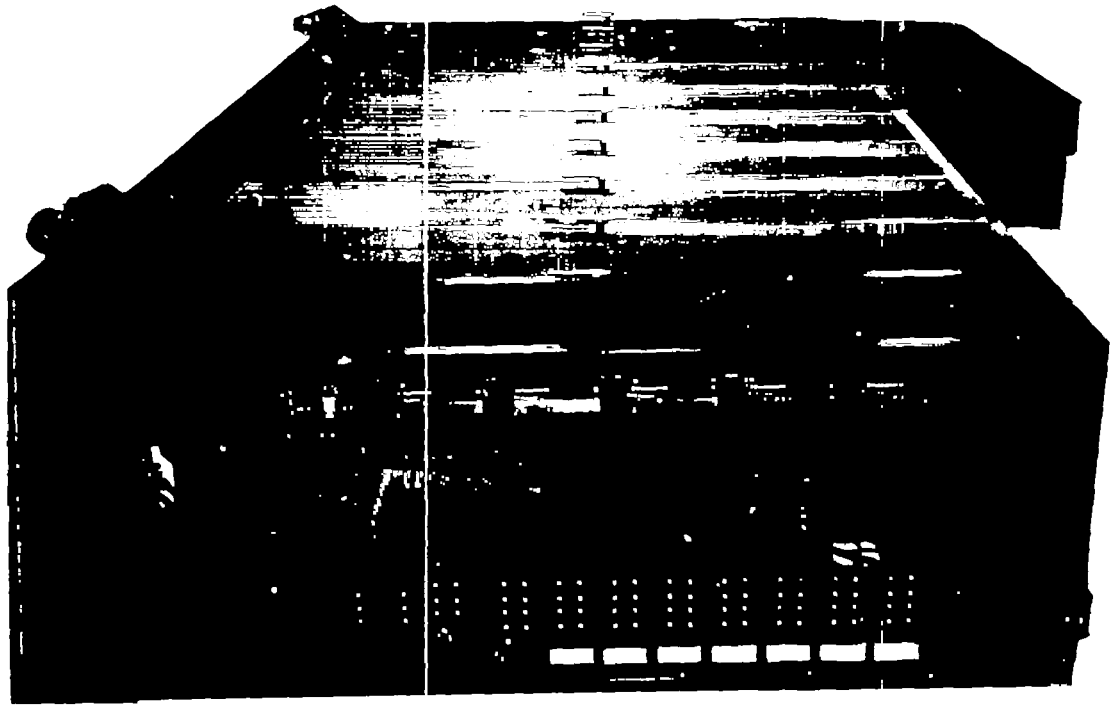
The machine consists of two separate units, a wheel unit housing four wheel-banks and an electronic unit. It exhaustively makes all possible stecker assumptions for 2 or 3 high frequency letters, testing each against a 100 or more letter menu, (cribs vs cipher pairings). Two wheels are sufficient because it is assumed that there is no slow wheel turn-over, so reflector and slow-wheels may be considered as an unchanged unit. Motion pattern is considered through menu set-up and wheel order through programming runs (up to 56 in some systems to cover all combinations). Results are on teledeltos paper in a square diagram.

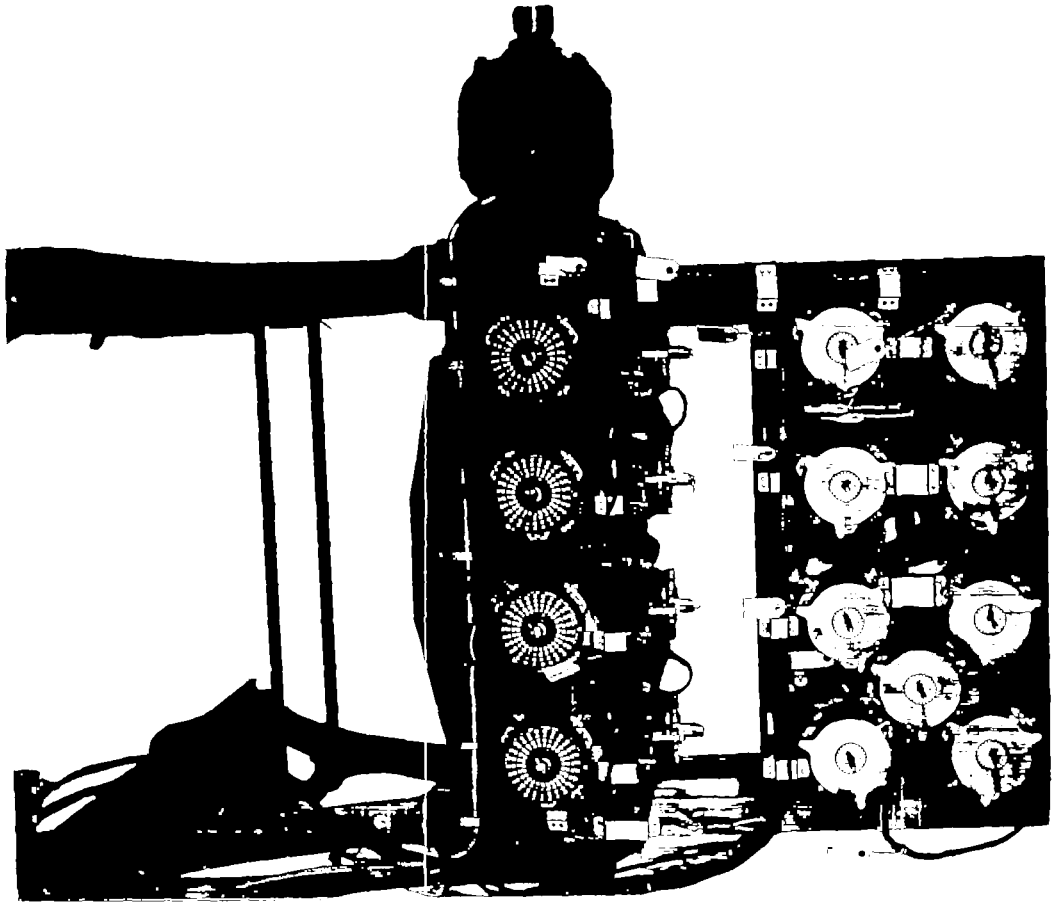
The electronic unit measures 8'H x 14'L x 3'D plus a wheel unit

DUENNA (Cont'd.)

and a blower unit. Rate is about 20 minutes to test each assumption. All five are stored at U.S. Naval Computing Machine Laboratory in St. Paul, Minnesota.

Ref: Technical Library
CIT paper TS-39





DUENNA
CXLU, N-1500

TOP SECRET
FROTH

March 1954

EMBRYO OPHIS

The term EMBRYO OPHIS (AFSAF-D57B and D57C, ALPHABET GENERATOR) refers to a relay device designed to cimulate wired rotor encipherment under a wide variety of motions. Its main use is for cycle study or decipherment purposes. NSA-82 built the first two (one is AFSAF-D57C, card operated; the other is AFSAF-D57B serial 2, tape operated) in December 1952. NSA-35 completed the third (AFSAF-D57B, serial 1, also tape operated) in January 1953.

The card-fed EMBRYO OPHIS operates with a 513 (later a 519) REPRODUCER, while the other two use CXCO equipment. All have three 30-position wheels and pluggable internal stepping control. Two of these could be connected in series to provide 6-wheel operation. Notch pattern and rotor wiring are set on a plugboard.

Size for all three is about 3'H x 2'L x 2'D, plus teletype tape reader and CXCO regeneration typewriter or 513 REPRODUCER. Rate is respectively 360 or 100 characters per minute. The first is in use in NSA-82 in room 1700-A; the other two operate in room 2059-B.

Ref: NSA-354 files
Mr. N. Christopher
Mr. S. Thorne

March 1954

FIRECRACKER

FIRECRACKER (AFSAF-121) is an electronic or relay cribtester used to find possible settings in Jap Purple Diplomatic traffic where a particular crib could have been enciphered. The first was built by NSA-35 in August 1953 and a second, a relay equipment, in October 1953.

Five letters of plain text and the corresponding five letters of cipher are set on 10 dials which range from 1 to 20, since only the letters steckered to the three 20's wheels are involved. The 6's letters must be considered separately Motion is controlled by plugboard. Three electronic matrices, analogues of the old PURPLE ANALOG wheels, step automatically through the full cycle of both encipher and decipher, or approximately 36,000 settings. At any point where the crib fits the cipher text the device stops to permit recording of the setting shown in lights. The device can be hand stepped.

Size is 4'H x 2'L x 2'D and rate is about 600 tests per second. They are located at Arlington Hall Station in room 1067-A

Ref: Mr. T. McGuire
Mr. P. Oyer
Mr. K. Polly

March 1954

FIRE ENGINE

FIRE ENGINE (CXCQ) was an "inverted"BOMBE, a modification of the standard N-530 machine and similar in all respects except that relative speeds of the wheel levels were interchanged. A total of eight were so modified by Navy in 1944.

The job accomplished is the usual BOMBE job, - given rotor and reflector wiring to recover stecker, rotor order and window settings, - but additional information is used to shorten the run. The position of the fast and slow rotors are interchanged, permitting setting up a machine to take advantage of (1) known fast wheel positions, or of (2) known medium wheel motion (called an H-Hoppity run), thus shortening the runs. This cannot be done conveniently on the standard N-530 or N-1530. Wiring of the slow rotor in such runs represented the combined effect of the slow rotor and the reflector plate.

Size, speed and external appearance of the machine remained unchanged by the modification. Dimensions were 7'H x 9'L x 3'D and 26^4 = 456,976 tests were made in about 20 minutes. All eight are now dismantled.

Ref: CIT-TS-14
NSA-34 files
Mr. J. Stapleton

March 1954

FOUR-POSITION ALPHA GATE

The FOUR-POSITION ALPHA GATE (32 x 32 ALPHABETIC SUBSTITUTION UNIT, FOUR-POSITION 32 x 32 MATRIX) is a general purpose relay deciphering device which operated with an NC-4 SELECTIVE PUNCH, and later with a 797 COORDINATING REPRODUCER, doing summing and differencing on mod 1 to 32 simultaneously for four positions. It was built by Army, section WDGAS-92, in October 1946, and modified in 1950 to operate with a 797 COORDINATING REPRODUCER.

The machine, a logical extension of the 10 x 10 J-SQUARE equipment, is designed to combine a pair of tetragraphs to produce a final tetragraph in one machine cycle. There are four plugboards, a pair of 20 x 34 plugboards for coordinate control, a 40 x 34 plugboard for matrix control, and an 8 x 20 plugboard for substitution. The groups being combined may come from the same or different cards.

It measures 5'H x 6'L x 3'D and operates at 100 cards per minute. Location is at Arlington Hall Station in room 1600-A.

Ref: Mr. N. Andrews
Mr. S. Thorne

March 1954

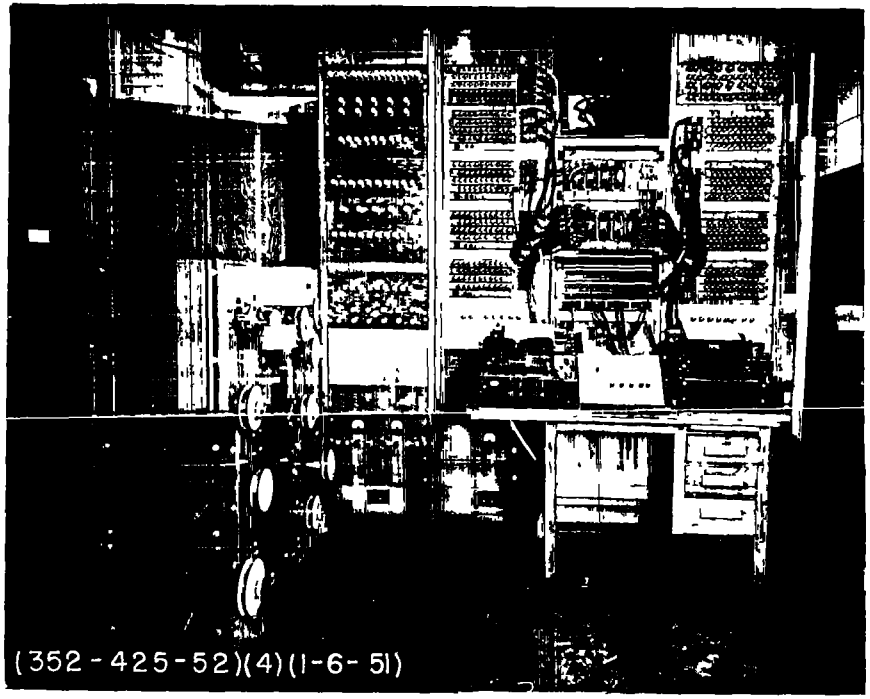
FREAK II

FREAK II (AF3AF-31, AXIC/1, ELECTRONIC FREAK, orginally MONOGRAPHIC FREQUENCY COUNTER) was an electronic frequency counter for making high speed monographic and digraphic frequency counter for making high speed monographic and digraphic frequency distributions of up to 32 character text of great length. Of two planned, F Branch of Army built one experimental breadboard model in January 1950. The device counted characters in 5-level tape and furnished an overall total.

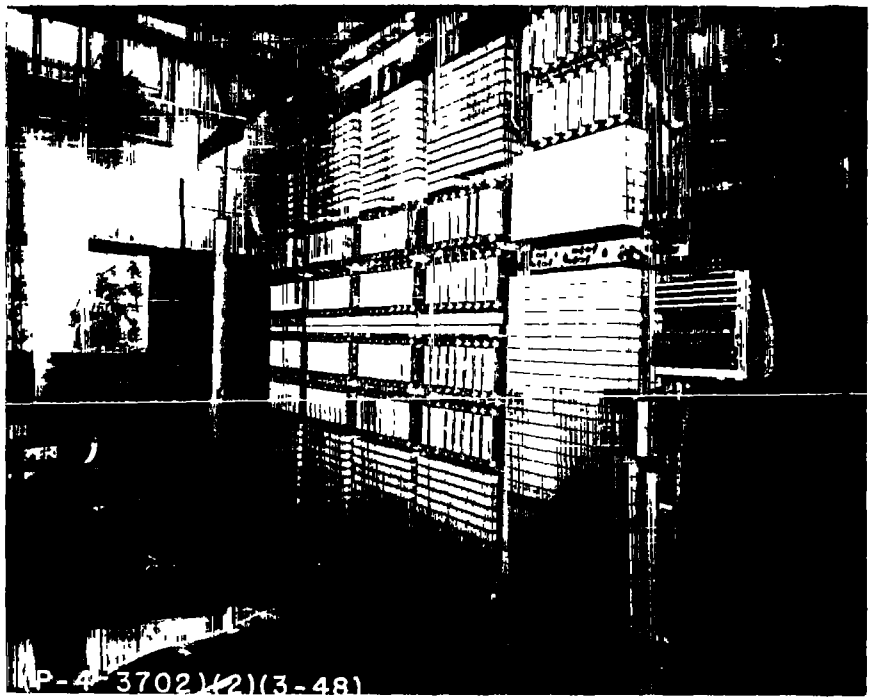
Input by a CXCO tape reader or alphabetic keyboard was connected through 32 pluggable leads to any of 40 resettable mechanical counters, each with 5 decimal place capacity. Seven of these served as spares and one was for the overall total. Results were typed on a CXCO regeneration typewriter. One function was to check the accuracy of tapes.

Rate was 10 characters per second and size was 5'H x 3'L x 2'D plus typewriter and keyboard. It was basic and simple in operation and has been dismantled.

Ref: Completion Report, May 1952
M.A.C. Outline#47
Mr. W. Cole
Mr. J. Russell
Mr. C. Schierlman



(352-425-52)(4)(1-6-51)



(P-4-3702)(2)(3-48)

FREAK I (right) AFSAF 24
The FREAK, MULTIPLE FREQUENCY COUNTER,
RELAY FREAK, CONDENSER FREAK
and
FREAK II (left) AFSAF 31
ELECTRONIC FREAK, MONOGRAPHIC
FREQUENCY COUNTER AXIQ/1

~~SECRET~~

March 1954

FREQUENCY DISTRIBUTION DEVICE

The FREQUENCY DISTRIBUTION DEVICE was a relay device used with a CXCO tape reader, 405 TABULATOR and a 513 SUMMARY PUNCH to make mono-alphabetic frequency distributions on limited spans of text. It was built by Army, section WDGAS-2, in 1949.

The device used a set of 32 counters to keep individual totals. A special character in the tape set off a totaling, listing and/or punching cycle and also reset the counters for the next distribution. Totals were usually recorded by the SUMMARY PUNCH.

The gate measured 3"H x 3"L x 3"D and rate was 150 characters per minute. It is now dismantled.

Ref: Machine Branch Annual Report, 1949
Mr. S. Thorne

March 1954

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

[redacted] KEY GENERATOR

[redacted] KEY GENERATOR was a relay analog of a [redacted] number-stamping device to produce one-time pads for the [redacted]

A makeshift desk-model, set up hastily by F Branch of Army in late 1944 for use in the operating section, used a CXCO regeneration typewriter output. The second operated with a 513 REPRODUCER. Work was begun in April 1945 on a companion equipment, the DEVELOPMENT NUMBER CONVERSION UNIT, and terminated in May because of the War ending. It was a relay-type manual substitution device (6'H x 2' L x 2'D) to mechanize conversion of key numbers (representing step point of five numbering wheels) to development numbers with results read from a bank of lamp.

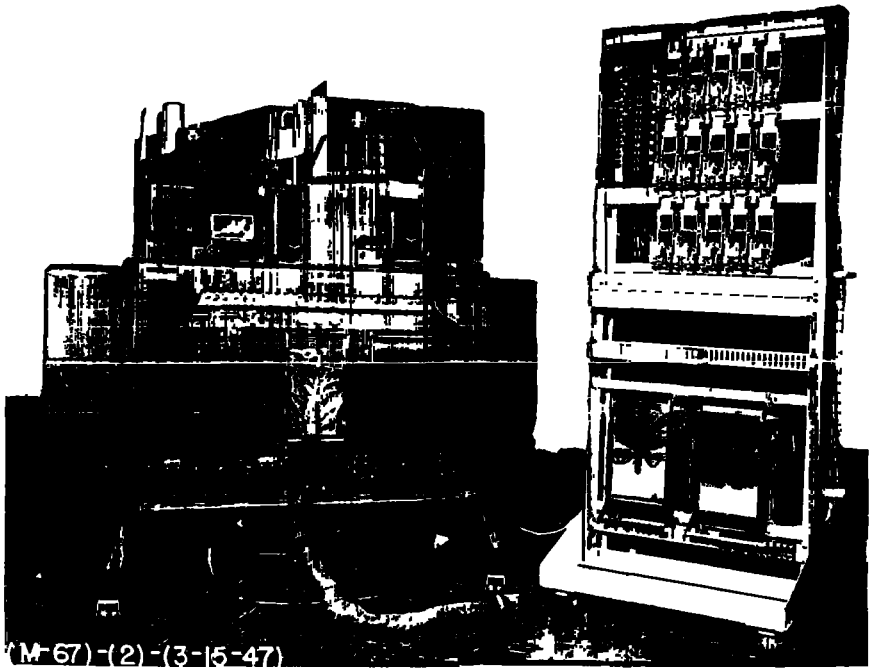
As in the original [redacted] device, the analog contained 48 units of

[redacted]

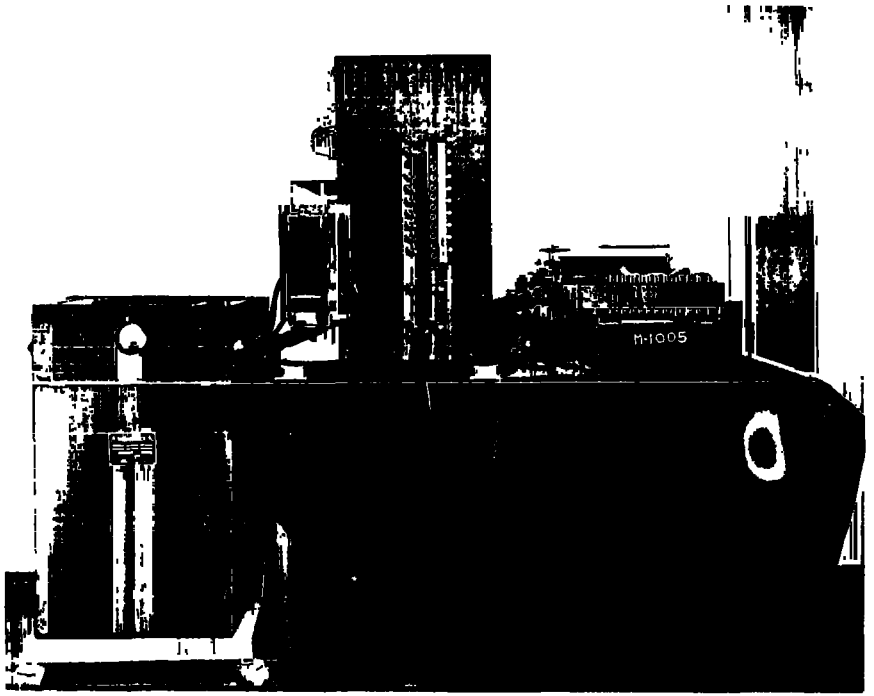
The desk model measured 4'H x 3'L x 1'D and printed at the rate of 6 to 8 key digits per second. The IBM model produced 80 lines of key digits per minute and measured 6'H x 2'L x 2'D. Both are dismantled.

References:

Mr. D. Dribin, Mr. B. Getchell, Mr. F. Mayol



(M-67)-(2)-(3-15-47)



[redacted] KEY GENERATOR
card-operated (left) and
Keyboard operated (right)

MARCH 1954

GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE

The GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE (AFSAF-110 and 100A, SELECTOR GATE, 100 RELAY GATE) is a relay device to increase selector capacity of any base machine connected with it. Army, section WDGAS-92, originally built two in 1947. A third was constructed in 1950 and a fourth (AFSAF-110A), containing its own power unit, in 1951. They replace International Business Machine Corporation's AR and RC gates (called 797's, miscellaneous equipment) which were rental equipments used to do similar jobs.

These are versatile devices and do a wide variety of jobs, requiring special internal wiring or only plugboard changes. A 40 x 34 plugboard makes all contacts interchangeable, and an 8 x 20 plugboard allows comparisons on numeric material. The gate itself does no computations.

One modification late in 1947 was called the SINGLE WHEEL CHAINING TEST. It operated with a 405 TABULATOR and a teletype tape recorder to determine [redacted] It has been dismantled.

Model I of a ROUGHNESS TEST DEVICE was set up in 1949 and Model II in July 1952. The device read 32-character text by a

GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE (Cont'd.)

double-headed tape reader or from cards by a 407 TABULATOR. Characters were distributed at 150 or 600 per minute to the counters in the TABULATOR arranged to provide two-digit counters for 32 categories and a four-digit counter for totals. The result recorded on the TABULATOR or a 517 SUMMARY PUNCH, was a frequency count of the text or of character differences and was limited to six digits. Model I was dismantled but Model II is in operation at Arlington Hall Station in room 1700-A.

Another modification was the HAGELIN SETTING LOCATION DEVICE in 1949. It operates with an 077 COLLATOR to [redacted] Rate was 240 cards per minute. It has been dismantled and superceded by AFSAF-12 and other comparators.

An interesting cryptographic use was made of one of these gates in March 1950, called the ALPHABET CONSTRUCTION DEVICE (ALPHABET CONSTRUCTION CIRCUIT). It operated with a 513 REPRODUCER to create randomized alphabets. Characters were read from tape by a single-headed teletype reader, TDX, at 600 per minute and the REPRODUCER punched each letter into a card as it occurred initially and ignored all subsequent occurrences until the 26th character appeared. Re-set and repetition were automatic.

The ALPHABET CONSTRUCTION PLUGBOARD was set up by NSA-22 in 1950. The counters of a 405 TABULATOR were used as mod 2 tube counters, with 5 and 0 for plus and minus. Each pulse added 5, non-carrying arithmetic. A ring of counters was set up and stepped by KOKEN motion. A Baudot character was formed from readings at 5 selectable points.

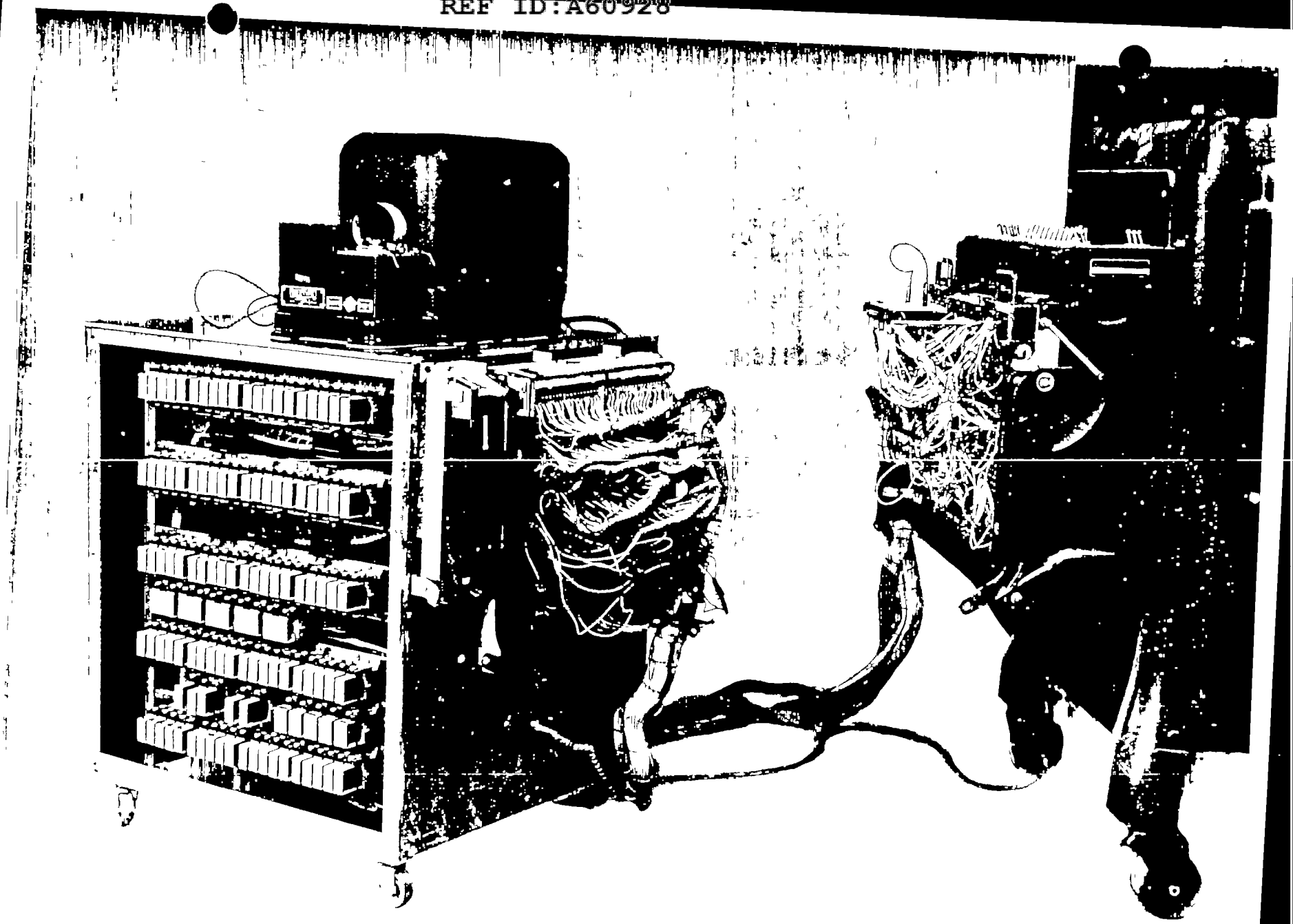
GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE (Cont'd.)

A count was made to determine the number of settings required to construct all 2^5 or 32 possible characters. The end product was a listing of the complete KOKEN development, together with the character each setting produced and, at the last setting, the total number of settings. It has been dismantled.

Another KOKEN - type usage is the relay analog called the 59-KOKEN DEVICE, wired in September 1952. It operates with a 407 TABULATOR to produce and record binary wheel settings for security study purposes. It completely simulates the key generation of the original 59-stage device at a rate of 75 settings per minute and is still in use at Arlington Hall Station in room 1700-A. Sixteen selectable points for motion control and sixteen for key are read at each setting and combined in the gate using mod 2 addition, Boolean addition, multiplication, double delay and dilation (standing for one pulse). In addition, pluses and minuses in key are counted and the excess between totals indicated.

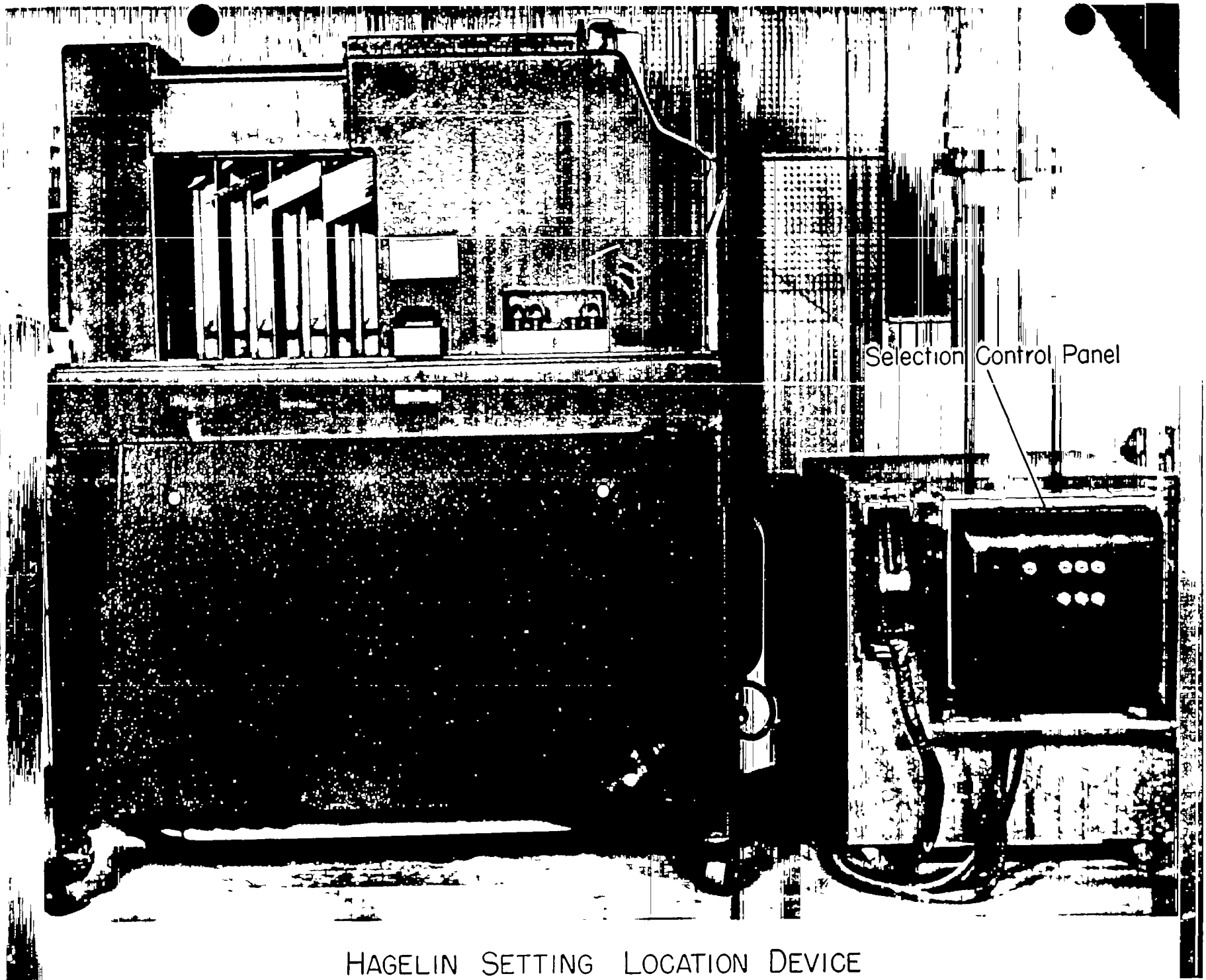
These gates measure 3'H x 3'L x 2'D and are available for similar special jobs. They are Arlington Hall Station in room 1700-A in NSA-22.

Ref: Machine Branch Annual Report, 1949
Mr. O. Algren
Mr. A. Duncanson
Mr. W. Erskine
Mr. J. Powers
Mr. S. Thorne



SINGLE WHEEL CHAINING DEVICE

SINGLE WHEEL CHAINING DEVICE
a special usage of
GENERAL PURPOSE 100-WIRE CONTACT
RELAY GATE



HAGELIN SETTING LOCATION DEVICE

A'ELIN SETTING LOCATION DEVICE
a modified
GENERAL PURPOSE 100 WIRE CONTACT
RELAY GATE

MARCH 1954

GLID

GLID (AFSAF-113, Group Length Indicating Device) is a relay gate first used with an NC-4 SELECTIVE PUNCH, and later with a 797 COORDINATING REPRODUCER to indicate by appropriate card punches the length of a selected field. It was built by Navy in 1949 and adapted for use with the 797 in the following year. The device eliminates tedious card sorting methods to determine length of punched field.

The device reads a selected set of columns in a deck of cards, determines which is the last column containing punching, and punches an indication of this into the same or a different card. Also, this length indication may be used to control feeding of blank cards into a collator in preparation for an offset slide of groups. The selected field tested may contain single blank columns, but not double or greater spacing. One use is in making rhyming dictionaries which require reverse sorting of irregular length entries.

GLID is built into the same frame with COLUMN ARRANGER GATE and the SUBSTITUTION DEVICE. Size is 4'H x 3'L x 2'D and rate is 100 cards per minute. It is located at Arlington Hall Station in room 1700-A.

Ref: Mr. W. Hopper
Mr. S. Thorne

~~CONFIDENTIAL~~

March 1954

GOLDBERG

GOLDBERG (AFSAF-90) is a high speed general purpose comparator and scoring device, with magnetic drums, designed to compare 2 or 3 streams of data. It does coincidence and frequency counts, cribdragging, wheel stripping, transformations, pattern and round robin searches, weighting, distribution matching and calculation of certain statistics. Engineering Research Associates under task 9 delivered the one model to Navy in September 1949. It replaces the 70mm COMPARATOR and various others. Serial 2 of SIGMAGE (AFSAF-28) was tried with GOLDBERG to limit the number of print-outs, but with indifferent success.

A double-headed seven-level tape reader puts data onto one of the two magnetic tape coated drums, usually while the other is being analyzed. A drum has 32 tracks of 4740 cells each and memory has 6 positions of storage for each track. Using the elements of the comparator unit (input translators, 36 x 36 matrix and 4-position counters), an nC2 calculator and various control components, all flexibly inter-connected, the machine does various counts, weightings, matches and calculations. It can apply an upper and/or lower criterion to each of the 36 counters and the nC2 calculator which computes $\Sigma fi(fi-1)$ for any of the 36 counters. Attaining a criterion at the end of analysis produces a print-out of counter totals and certain other data at a rate of 3 seconds per line. There are 38 four-digit numbers and 1 eight-digit number to a line.

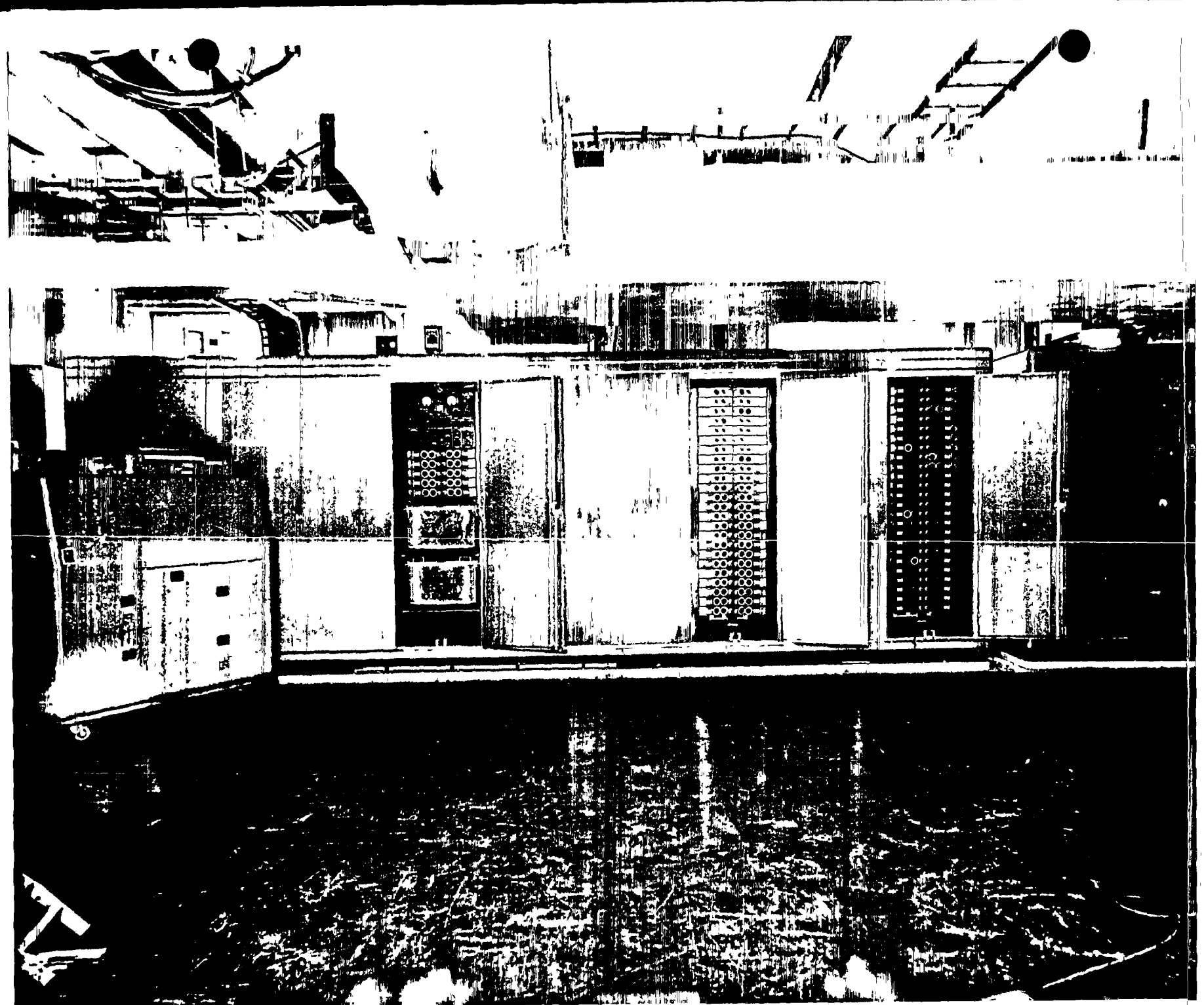
~~CONFIDENTIAL~~

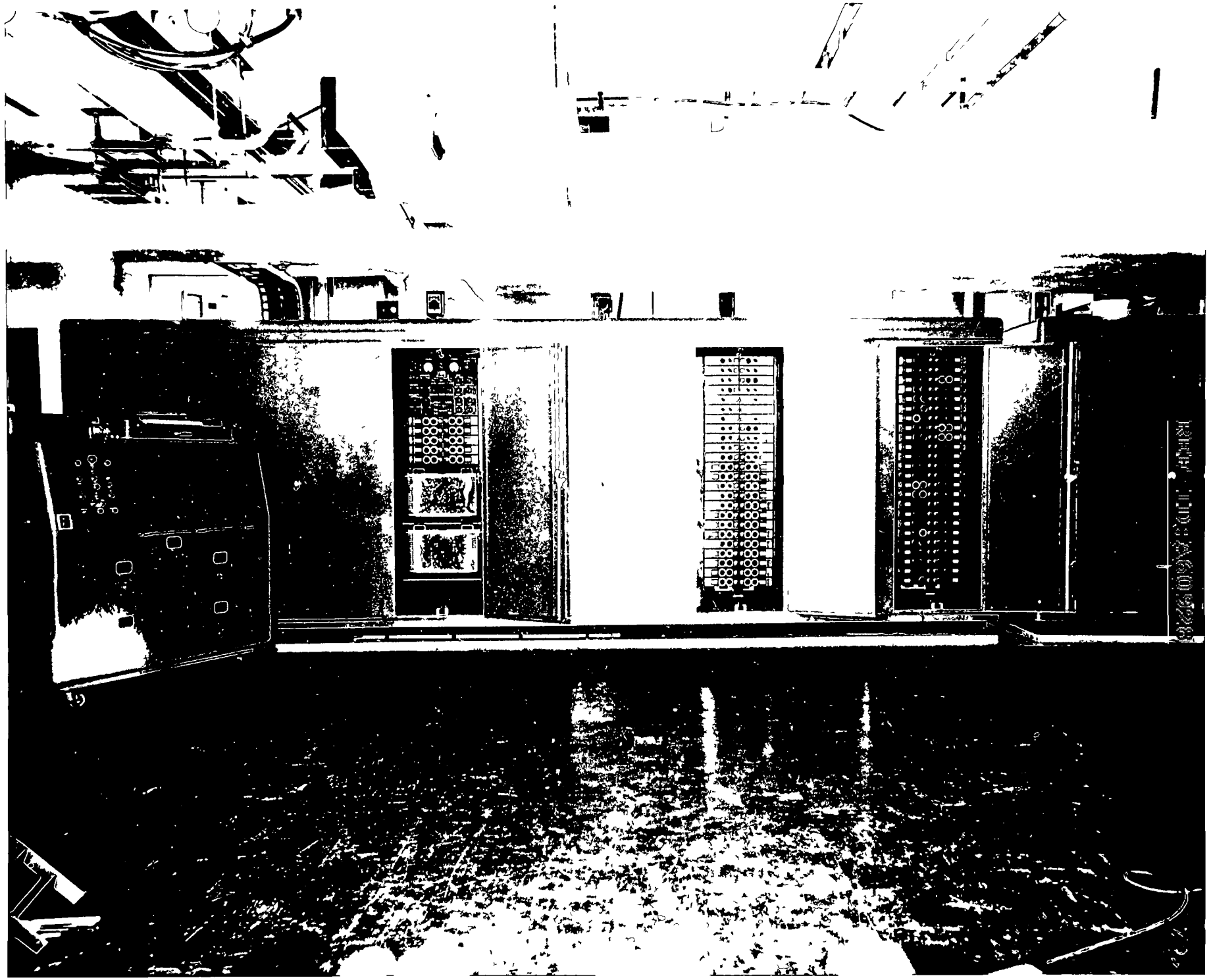
GOLDBERG (Cont'd)

Size of the machine is 9'H x 25'L x 3'D plus console and printer. Character rate is 20,000 comparisons per second; bit rate is 20KC. It operates at Naval Security Station in room 20105. Plans for a GOLDBERG II (CXOT) were dropped when it was found ATLAS II would do all the required functions.

References:

Mr. D. Hogan
Lt. F. Sperberg
Mr. J. Stapleton





GOLDBERG (AFSAF 90,
ERA task 9)

GOLDBERG (AFSAF 90,
ERA task 9)

March 1954

GRANDDAD

GRANDDAD (CXCQ, N-800, DOUBLE BOMBE) is actually two N-530 BOMBES with common drive, and consists of 32 ENIGMA frames. Given rotor wiring, reflector plugging and a crib, it can find rotor order and stecker (end-plate plugging). Eight were ordered from National Cash Register Company, but five were cancelled. Two were delivered in late 1944 and one in early 1945.

Operation is the same as for a standard BOMBE, except a crib of up to 32 letters may be used, instead of only 16 letters. It tries all possible stecker combinations until it finds one which satisfies the menu (crib-vs-cipher letter pairings), when it stops, prints a record and continues testing.

A 3-wheel run takes 50 seconds; a 4-wheel run takes 20 minutes. Dimensions are 7'H x 20'L x 3'D , or slightly less than twice as long as a standard BOMBE. All three are stored at Mechanicsburg, Pennsylvania, along with the rest of the BOMBE equipment.

Ref: Cdr. R. Greenwood
Mr. C. Higgins
Mr. R. Nothnagel
Mr. J. Stapleton

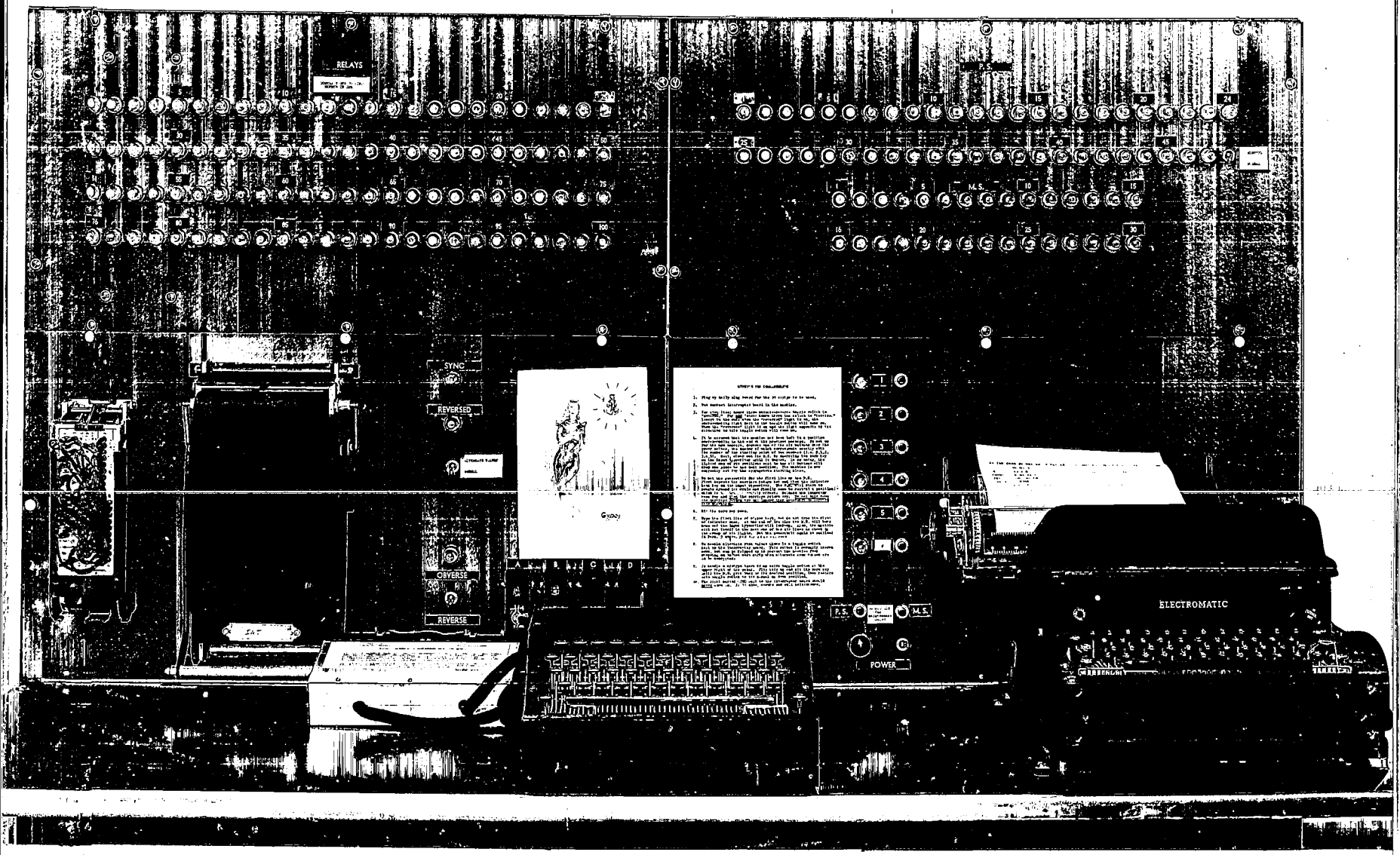
GYPSY

GYPSY (CXMR) was a relay strip cipher analog to mechanize routine decryption of JN-87 traffic. Two were built by National Cash Register Company of Dayton, the first delivered to Navy in 1945. Plans to send the second to FRUPAC at Pearl Harbor never materialized.

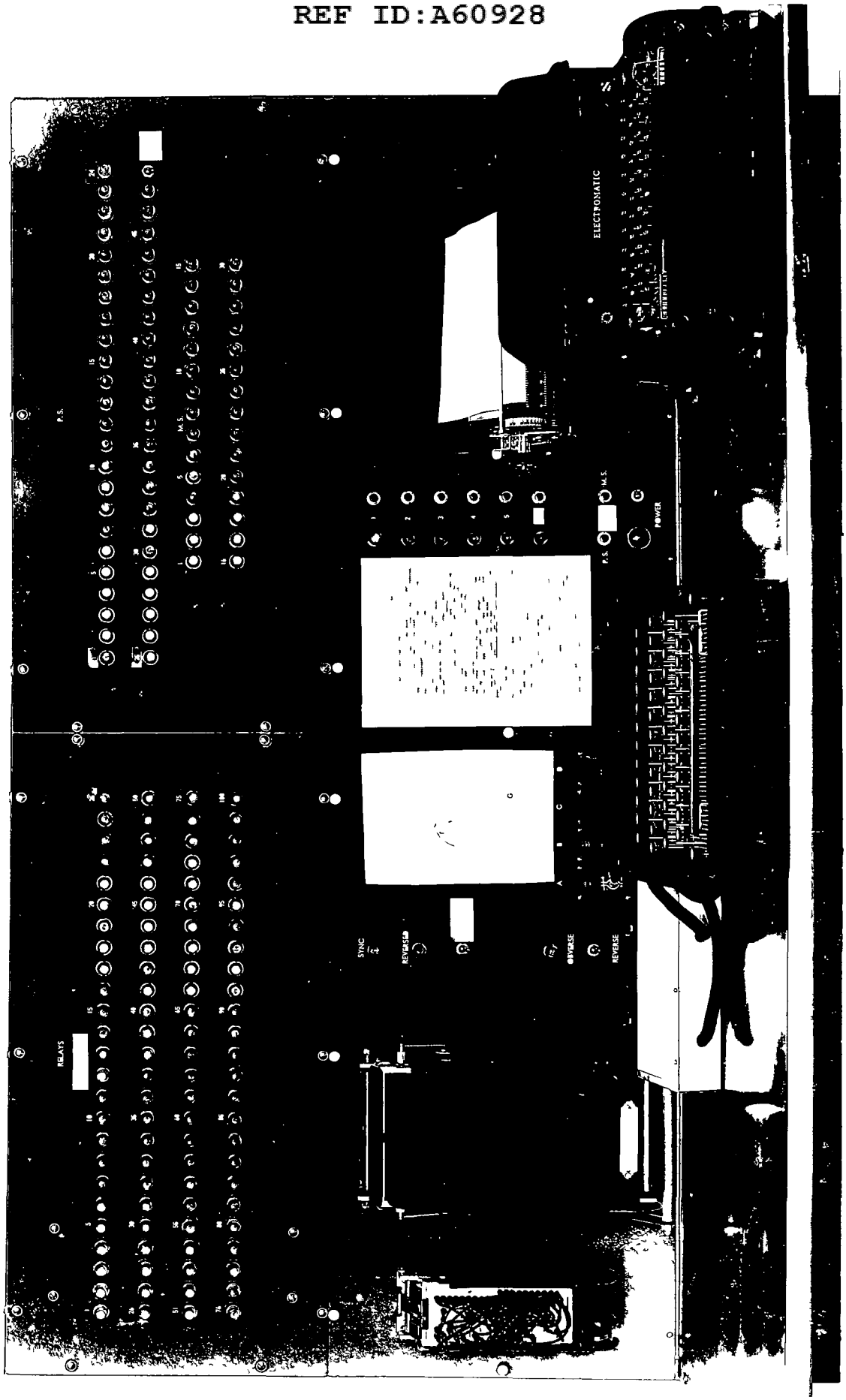
Thirty strips represented by plugboards were chosen daily from the 100 two-sided strips available, taking care of pre-arranged omissions and reversals (interrupter pattern) in the plugging. A set of switches took care of other variables. Input for cipher text was a 48-Kana keyboard and output for plain text was to a CXCO regeneration typewriter, both being mounted on a metal shelf across the front of the machine.

Size of the control unit was 5'H x 5'L x 2'D plus 5 cabinets 6'H x 2'L x 2'D. Rate was at 6 to 8 characters per second. They have been dismantled.

References:
CIT paper 32
CIT-TS-25, 30



REF ID:A60928



GYPSY
CAIR,N-1450

March 1954

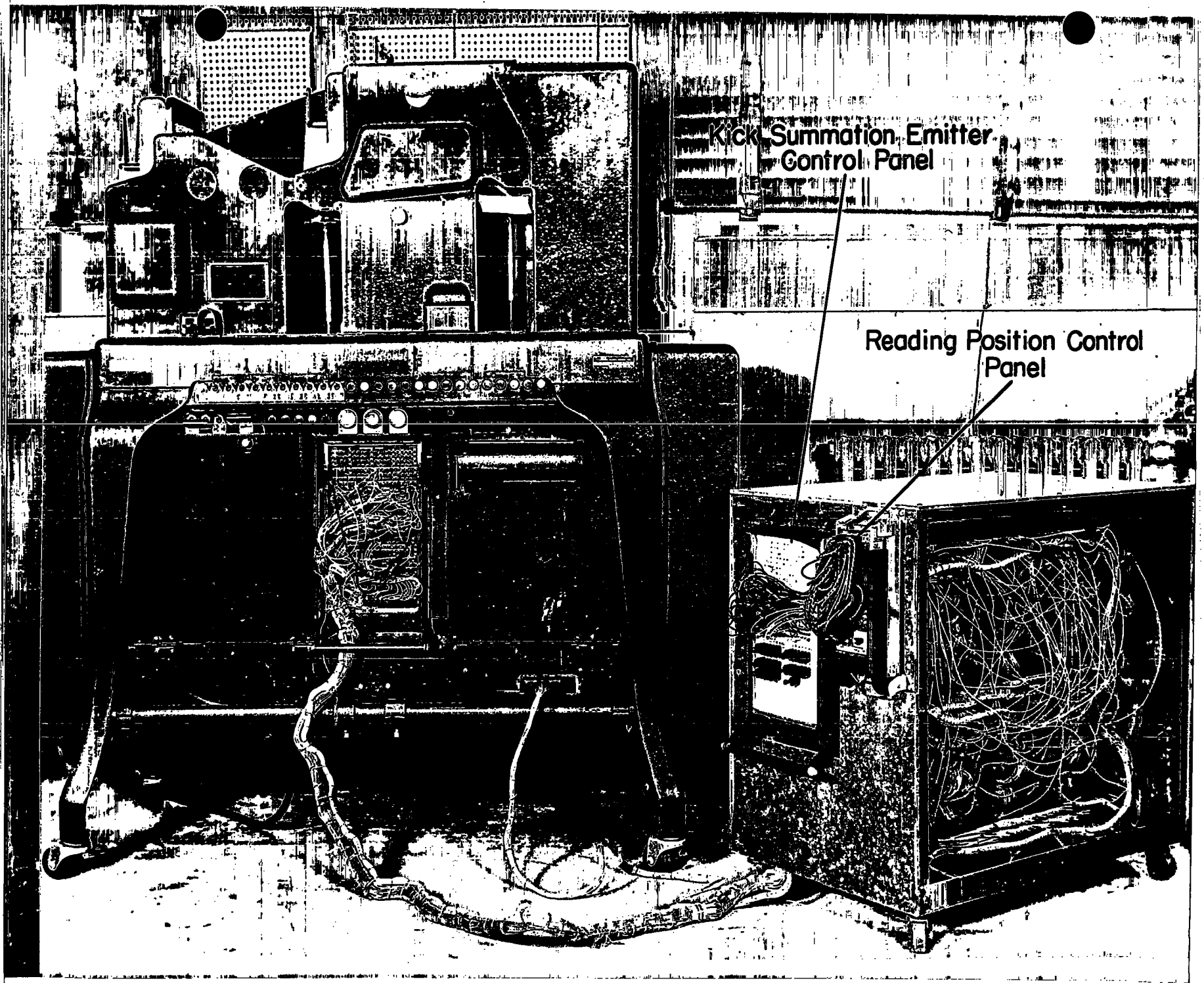
HAGELIN KEY GENERATOR

The HAGELIN KEY GENERATOR (no AFSAF No.) is a relay gate used with a 513 REPRODUCER for the simultaneous production of 6 elements of alphabetic key from the patterns of six HAGELIN wheels. One model of TAN ANALOG left idle by the disappearance of LONGFELLOW traffic was modified to simulate HAGELIN pattern wheels and completed by Army, section WDGAS-92, in April 1949.

The patterns of the six wheels are recorded on six levels of an IBM card, and wheel motion is represented by a horizontal cyclic offset. Plugboards select the appropriate positions for reading and translate the sums of the "kicks" or offsets into alphabetic key. Data is read in by a 513 REPRODUCER which also punches results into cards. There are checking circuits to help accuracy.

Size is 2'H x 3'L x 2'D plus a 513 REPRODUCER and rate is 600 elements of key or 100 cards per minute. It is at present in storage at Arlington Hall Station in Room 1700-A.

Ref: Interim Report JPAG No. 5812, IT-Ø61
Machine Branch Annual Report, 1949
Mr. J. Powers
Mr. S. Thorne



HAGELIN KEY GENERATOR
with IBM 513 REPRODUCER

MARCH 1954

HAGELIN [redacted] TEST DEVICE

The HAGELIN [redacted] DEVICE (AFSAF-38A, ODD KICK DETECTION DEVICE) is a relay gate used with a 519 REPRODUCER and a CXCO tape reader to test [redacted] wheels. It was built by Army, section WDGAS-92, in November 1949.

[redacted] are read from tape by a CXCO reader, stored consecutively and offset by gang punching into seccessive columns and levels of an IBM card, after [redacted] Agreements and disagreements are recorded by the 519 REPRODUCER and listed on a 407 TABULATOR, permitting the analyst to study the ratio of such [redacted] About 800 or more characters of cipher are needed.

The device measures 2'H x 2'D. Rate is 100 cards per minute. It is still available for use at Arlington Hall Station in room 1800-A.

Ref: Mr. S. Thorne

March 1954

HELLCAT II

HELLCAT II (AFSAF-D59A) is a relay hand-tester and deciphering device which combines two letters at a time to produce cipher or plain. Only two of the four units planned were built, NSA-35 delivering them in June 1953. The remaining two were cancelled.

The keyboard input is located on a desk nearby and the memory (a relay storage unit), adder unit coder and ring circuit are all enclosed in a small table 2'H x 2'L x 2'D mounted on casters. A CXCO regeneration typewriter sits on top and serves as output. Twenty characters, usually key, are typed on the keyboard, converted to a corresponding number in the coder and stored in one of the twenty storage cells in the form of five-level Baudot impulses. The ring circuit controls the level of storage used. Cipher text via the keyboard is then combined with the stored key by means of an adder unit, a set of 15 relays which add characters by pairs, modulo 26. The output, reconverted to letters, is page printed on the typewriter.

The device will have no plugboards as in HELLCAT I. Its rate of operation is up to 6 or 8 characters per second. It is located at Naval Security Station in room 1323.

Ref: Mr. N. Christopher

March 1954

HOYLE

HOYLE (no AFSAF #) is a relay decipherer to mechanize decipherment of Playfair cipher messages. The one model was built by NSA-82 in July 1953 as a desk-top crypto-aid.

Input is by keyboard; output is to a CXCO regeneration typewriter. The first keystroke stores the initial half of a playfair digraph in the relay unit and the second stroke starts the analyzing sequence which results in printing a pair of plain text equivalents according to the plugging of a square. Dimensions of the square at present are 6 x 6 , but this could be modified to a smaller rectangle with but little difficulty.

Size of the relay unit is 1'H x 2'L x 2'D plus keyboard and typewriter. Rate is up to 6 or 8 characters per second. At present the device is in storage at Arlington Hall Station in room 1500-A.

Ref: Mr. S. Thorne

March 1954

HYPO I - III

HYPO (CXEA) is a 35 mm photoelectric film comparator used as a statistical GRENADE to locate starting point of traffic from an ENIGMA with known reflector, stecker and wheel order. Eastman Kodak Company delivered to Navy a pair of HYPO cameras in 1943 (325 target capacity, 4'H x 8'L x 3'D) and a pair of projectors in late 1943 and 1944. A third camera and card reader pair, built jointly by Eastman and International Business Machines Corporation, arrived in 1945 and is called Serial 1 (of Model II). A fourth camera called Serial 2 (of Model II) remains undelivered, stored in Rochester. Both have 676 target capacity. Navy built two more projectors. The first, called Model I with complete disregard for the earlier model, was mostly the work of Lt. Steinhart, and was finished in 1946. Model II was finished in 1952. A special equipment called LETTERWRITER SUBSTITUTION TRANSFERRING DEVICE was developed to make automatic substitution in preparing message tapes.

The card-reader and camera operate together to produce a master and a cipher film. The master film contains a graphic representation of all possible encipher links through the reflector, slow and medium wheels for the full alphabet in the form of digraphs. The message film consists of cipher text deciphered through the stecker substitution and the fast wheel, then combined with 3 or more high frequency letters to produce digraphs which are merely

HYPO I - III (Cont'd.)

input-output pairings. The projector matches the two films photographically to find the point of maximum coincidence, stopping automatically to permit hand recording at a hit. There are 30 frames in the gate and 5 columns of 26 possible spots per frame. The ICKY II Camera (CXNR) can be used to produce HYPO film.

The equipment tends to be bulky, the smallest item being the original projector, 4'H x 2'L x 2'D and the largest the readers for Model I and II, 6'H x 7'L x 3'D . Rate of comparison is about 10,000 items per second. The two latest cameras and readers are in use at Naval Security Station in room 20209. The latest two projectors are in room 20210. All the earlier equipments have been dismantled.

Ref: Brief Description of RAM Equipment
CIT paper 33, 61
CIT-TS 9, 21, 24, 34
Mr. G. Kier
Mr. J. Stapleton

March 1954

I. C. MACHINE

The I. C. MACHINE (AFSAF-7 and -8, CXCM, I. C. PROJECTOR) is a general purpose photoelectric comparator designed to match two portions of text on photographic plates at every overlap and locate either the point of maximum Index of Coincidence (I.C. = Number of coincidences divided by number of comparisons) or the several positions where I.C. exceeds a pre-set threshold. Eastman Kodak Company built 6 for Navy, the first in August 1942. Two were diverted to Arlington Hall in 1943 together with the Vane Camera (AFSAF-6) and the I.C. Plate Camera (AFSAF-9) for photographic text onto plates. One (AFSAF-7) was modified in 1947 to handle 35mm tape; the Lucite Rod Camera (AFSAF-10) produced the film for it.

Two lengths of text are photographed onto 1" x 4" glass plates as a 30 x 600 field of clear spots on an opaque background. A clear balance track of length proportional to text length and identification data are also added. The plates are placed in the projector gate and slid past each other as light is beamed through them. Light from matching clear spots (indicating text coincidence) is weighted by a photoelectric cell and matched against output of another photoelectric cell receiving light from the overlapped balance tracks (exactly proportional to overlap of texts being compared). When the ratio (I.C.) of these two currents exceeds a pre-set amount, a neon light flashes and the operator hand records

I. C. MACHINE (Cont'd.)

the setting. Only one other machine, the 5202 COMPARATOR MARK II, has such a wide gate, 600 frames. This is restricted to 128 frames when film is used. The device handles numerical or literal text and is completely general in usage, but experience has shown that I.C. studies must not be used indiscriminately to build up depth on unknown traffic.

Size is negligible, less than 1'H x 1'L x 2'D and an average effective rate of comparison is about 1000 matches in 4 or 5 seconds, or 1500 frames per second when film is used. In spite of extensive redesigning by the manufacturer the equipment has not been as useful as hoped, so all but two, one for plate and one for film, have been dismantled. Both of these are stored in the attic of building 20 at Naval Security Station.

Ref: M.A.C. Outline #12
C.I.T. papers 1, 1A, 71
Mr. J. Stapleton
Mr. L. Wheatley

March 1954

KEYFINDER

KEYFINDER, (AFAB/2, AUTOMATIC COLUMN STRIPPING UNIT, NUMERIC KEYFINDER) was a digital key tester or depth tester, used with a 405 TABULATOR to try probable key against an overlap column. Six type 931 SLIDE-RUN gates were built by and rented from International Business Machines Corporation in 1944, and two were converted to a KEYFINDER by section WDGAS-92. The first one, in 1945, was dismantled and the second built in 1948. It continued in use until replaced in December 1949 by SKATE and SLED equipments. Navy used a combination of IBM equipment and MERCURY to do the same job.

The original plan was to apply the full 10,000 keys possible in a 4-digit system to all groups in an overlap column 3 to 20 deep. Instead, the machine assumed successively 95 high-frequency groups at each group in an overlap column up to 20 deep, applied key thus derived against the remaining groups in the column and tested resulting possible plain groups against a recognition bank of 300 high-frequency groups.

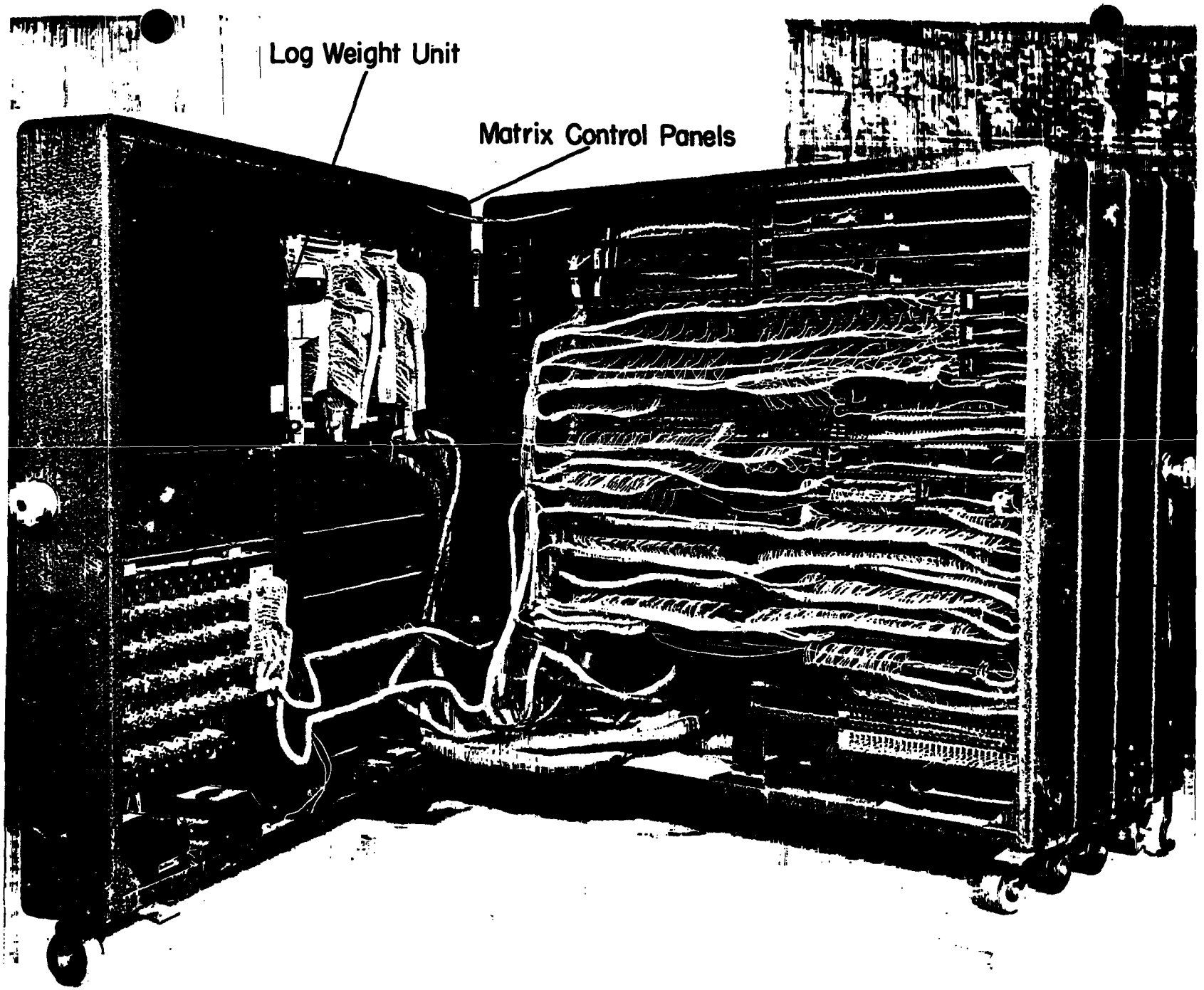
Later, two 5-position 10 x 10 matrices were added making the use of cipher, crib and key more flexible. This modification, made in 1948, further changed its capacities from 4 digit only to 3, 4, or 5-digit, set depth limits at 3 to 16 , permitted from 93 to 192 high-frequency crib assumptions, and from 300 to 1500 groups in the recognition unit. A log weighting feature ranging

KEYFINDER (Cont'd.)

from 1 to 7 was also provided. Input and output were still through the 405 TABULATOR, and record was made of all keys for which the number of recognized groups exceeded the preset threshold. The first model contained 5 channels to accomplish simultaneous decipherment through 5 random squares. This feature was eliminated on the later model, since only the defunct Jap Army used "square arithmetic" keyings. Weights and recognition groups were set up on plugboards.

The gate itself consisted of five leaves or frames, hinged together and measured 5'H x 6'L x 3'D plus a 405 TABULATOR. Cards were read at 150 per minute, giving up to 20 x 150 = 3000 tests per minute. All special circuitry was removed and the gate returned to International Business Machines Corporation.

Ref: Machine Branch Annual Report, 1946
M.A.C. Outline No. 18
Mr. J. Powers
Mr. S. Thorne



KEY FINDER

KEY FINDER
NUMERIC KEY FINDER, AXAB/2,
AUTOMATIC COLUMN STRIPPING UNIT

March 1954

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

KEY SYNTHESIZER

The KEY SYNTHESIZER (STURGEON KEY SYNTHESIZER) is a pattern generator which prints out [redacted] It applies to [redacted] traffic produced on the German-built on-line teletype cipher device and was built by NSA-22 in 1950.

[redacted]

for identification.

The machine consists of an IBM keyboard, a 1'H x 1'L x 1'D combiner unit and a CXCO regeneration typewriter. Rate is 6 to 8 characters per second. It is in operation at Arlington Hall Station in room 2048-A.

Ref: Miss V. Collins
Mr. G. Stahly

March 1954

LETTERWRITER EQUIPMENT

The term LETTERWRITER EQUIPMENT (AFSAF-96, CXCO PERFORATED TAPE EQUIPMENT) refers to a unit of three standard commercial machines for processing 7/8 inch perforated paper LETTERWRITER tape and also for 11/16 inch teletype tape. Serving as a two-way link between information printed in page form and in mechanically-readable perforated form, the CXCO provides input or output for a large number of the analytic machines. It is not Agency developed and not analytic in the strictest sense, but is included here because it is so completely adaptable to a number of the analytical processes or auxiliary to others, and because punched tapes and cards still handle the greatest part of all data during processing.

Several hundred such sets or units, composed of READER, REGENERATION TYPEWRITER and PUNCH, plus various minor items such as the the junction box (chime box), pulse counter, etc., have been procured since April 1942. Such units, originally produced by Electromatic Typewriter Corporation, an IBM subsidiary, are now produced by the independent successor, Commercial Controls Corporation, under the commercial name of Flexowriter.

Versatile MATTHEW and many other machines are logical modifications and extensions of this equipment. For straight production of page copy from tape, the cheaper COPY MACHINE (a REGENERATION TYPEWRITER minus the tape-punch control) is often used. A similar special

March 1954

LETTERWRITER EQUIPMENT (Cont'd.)

purpose PUNCH CONTROL TYPEWRITER with no solenoids and only 5 translator bars under the keys, operates a tape punch and cannot be reader-controlled to do tape-to-print work.

Rate of operation ranges from 4 to 12 characters per second. The three pieces are usually mounted on a 2'H x 5'L x 2'D dolly, with the READER and PUNCH, each 1'H x 1'L x 2'D, placed on either side, and the REGENERATION TYPEWRITER in the center. Such units are found in various locations. Faster readers, writers and punches are being sought and found, so eventually the equipment may become obsolete, but is most useful at present. 15-level tape equipment (CXCO-2), developed through commercial companies, is now available. All CXCO EQUIPMENT in the Agency has been redesigned and improved recently and is now called CXCO-1.

Ref: CIT paper 34, 62, 63
M.A.C. Outline No. 46
Mr. R. Nothnagel
Mr. J. Russell
Mr. J. Stapleton

LETTERWRITER EQUIPMENT
AFSAF 96
CXCO PERFORATED TAPE EQUIPMENT
including tape reader, regeneration
typewriter and tape punch

~~CONFIDENTIAL~~

March 1954

MATRIX GATE

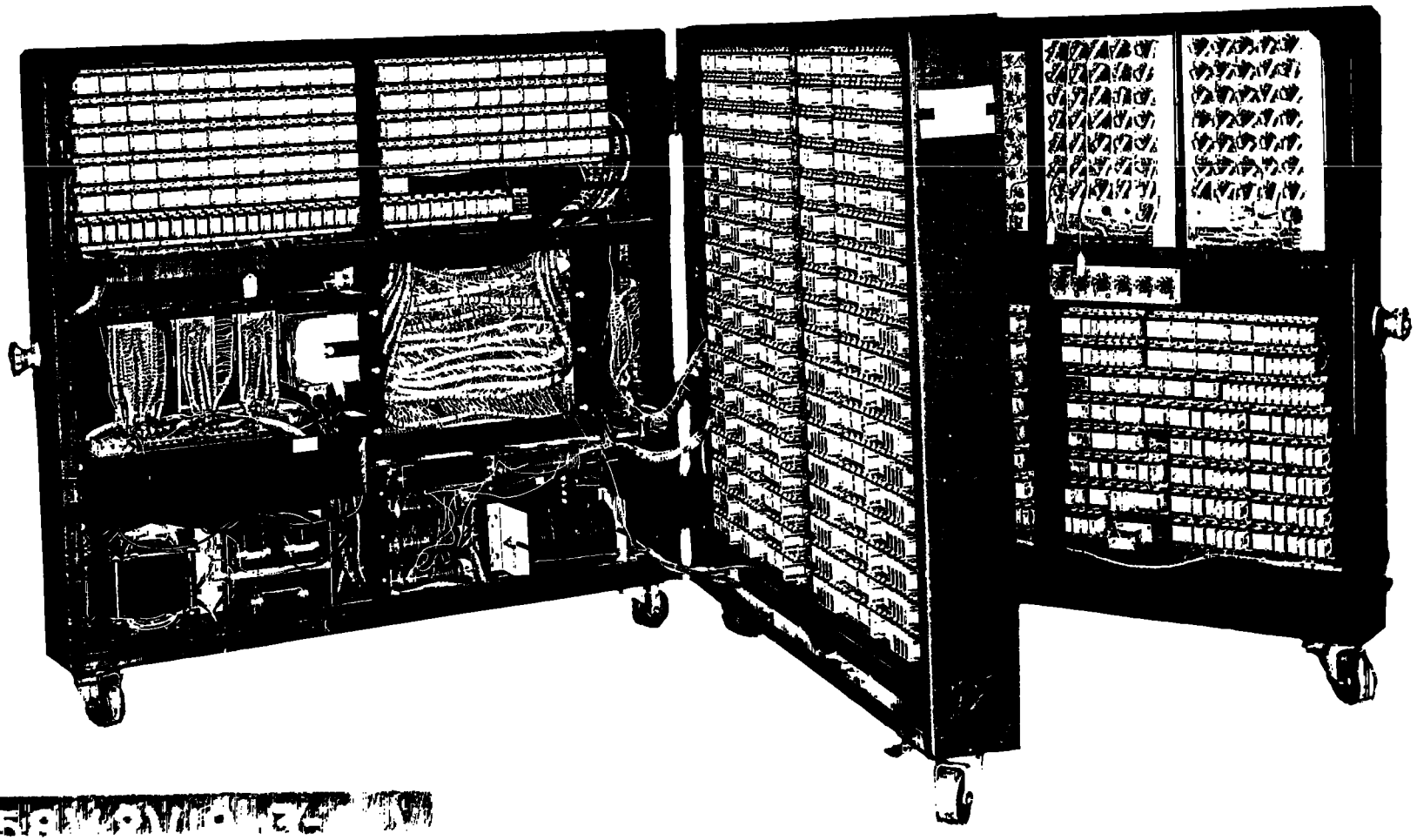
The term MATRIX GATE (AFSAF-104, 798 SUBSTITUTION GATE) refers to one of a set of relay devices used with 797 COORDINATING REPRODUCERS to perform various substitutions on 5 and 10 characters of text. All twelve were purchased from International Business Machines Corporation in 1951. The J-SQUARES and the FOUR-POSITION ALPHA GATE are predecessors to this equipment and MATTHEW does a comparable job.

Six are for alphabetic data, with pluggable 32 x 32 matrices. Of these, four handle 5 characters at a time and two handle 10 characters. The six numeric ones have 10 x 10 pluggable matrices, four of which handle 10 characters at a time, and two of which only 5 characters. The numeric gates can do normal, false, or minor differencing. Each has its internal power supply but can not operate independently. Results are checked by double computation.

Sizes range from 5'H x 5'L x 3'D for the large 10 position numeric down to 3'H x 4'L x 2'D for the small frame, 5 position 32 x 32 alphabetic. All operate at 100 cards per minute and are now in use at Arlington Hall Station in the four A-building wings of Section NSA-82.

Ref: Mr. O. Algren
Mr. J. Powers
Mr. S. Thorne

~~CONFIDENTIAL~~



MATRIX GATE
AFSAF 104E
IBM MATRIX SUBSTITUTION GATE
10-position, 32x32

MARCH 1954

MATTHEW

The term MATTHEW (AFSAF-104, 104B, CXCX) covers a family of general purpose substitution and comparing devices, used for differencing and combining two punched paper tapes character by character on any modulus up to 26 using non-carrying arithmetic. About 9 models of such equipment were built. The first (CXCX, MATRIX MACHINE, M-26) by Navy in January 1943, had a fixed 10 x 10 matrix mounted in a CXCO LETTERWRITER dolly, with the usual CXCO reader, regeneration typewriter and punch set on top. Later models include a 10 x 10 pluggable matrix, a fixed and a pluggable 26 x 26 matrix, and a pluggable 32 x 32 matrix (AFSAF-104), this last in an upright relay rack. The latest model is a pair with a 36 x 36 pluggable matrix (AFSAF-104B) built into old PYTHON-VIPER frames set on a a desktop. LUKE and JOHN are specialized modifications and the several IBM MATRIX GATES are card-operated equipments having identical functions. The output of a 10 x 10 pluggable MATTHEW was connected to a 10 x 10 FREQUENCY COUNTER and called MATTHEW-SIMON, BASE 10. Matthew replaced Army's JMA DECIPHERING DEVICE and other substitution devices as well.

Basically, the device consists of two readers or a double head reader, a relay matrix, a CXCO regeneration typewriter and a tape punch. Input is by keyboard and tape, or two tapes and output is to a regeneration typewriter and/or punch. Thus the machine can

decipher literal or numerical text, or can combine two tapes accordint to almost any rule of combination. Plugboards make substitution possible on input or output.

The dolly housing the relays of early models measured 2'H x 5'L x 3'D. An upright or rack-type MATTHEW measures 6'H x 2'L x 1'D. The newer desk-top models measure 4'H x 5'L x 3'D. Operation is a 6 to 8 characters per second. They are located at various places, for example, the desktop MATTHEW is at Arlington Hall Station in room 2054-B, and the two of the latest models at Naval Security Station in room 4152.

Ref: MAC Outline #5
CIT paper #95
Mr. R. Bronder
Mr. F. Mayol
Mr. J. Stapleton

March 1954

NOMAD

NOMAD (AFSAF-D81 through D88) will be a system of high-speed electronic mass-data-handling equipment with all the capabilities of a computer, but with design emphasis on its huge data handling capacity rather than on computations and operations on individual terms. A typical use will be a large-scale sorting job which it will accomplish 100 to 300 times faster than current IBM equipment. The idea of such a machine was suggested in 1946 and studies of mass data handling methods, started by Navy in February 1949, led to a contract on 7 September 1951 with Raytheon Corporation for one operational model due January 1956.

Eight pieces of peripheral equipment, 4 for tape and 4 for card, will convert data onto 6-level magnetic tape at a rate of 240 characters per second from punched tape, or more than 320 characters per second from cards, or 85 per second from chadless tape. There will be two units to convert magnetic tape to page copy on a 407 TABULATOR. Information on these magnetic tapes will be read in and out at a rate of 14,000 characters per second. A CXCO tape punch will be provided for output of brief, infrequent answers.

In the main machine, 4 PITS, Primary Internal Tape units, will each store 10^9 bits in the form of 36-bit words on 36-level magnetic tape. This is equivalent to about 2 million IBM cards per PIT. In conjunction with automatic monitor registers, four

NOMAD (Cont'd.)

magnetic core buffers will act as interim storage, each accepting up to 128 words from its associated PIT and feeding it into the main memory and computation units as needed. The high speed memory will be a unit of 36 magnetic core matrices, 32 x 32 , having a constant access time of 20 microseconds and a 1,024 word capacity. There will be an auxiliary drum memory with a $2^{14} = 16,384$ word capacity. The control section will use 3-address instructions, each consisting of a 6-bit order code and three 10-bit addresses. Both program and data will be handled in the main memory. There will be special cryptanalytic orders to facilitate such character manipulations as modular arithmetic, masking transfer, automatic repetition and jump orders based on distinguishing between numbers on the basis of size, sign or pattern.

Repetitive operations on large sets of words will be at a rate of up to 50,000 words per second for short stretches or 14,000 for continuous operation. The main machine will occupy 5,000 square feet of floor space, and the peripheral equipment, 2,000 square feet. It will be delivered at Ft. Meade, Maryland. Potentially one of the most useful of all the machines, it is also the most expensive (4 to 5 million dollars) and the largest.

Ref: Mr. D. Hogan
Mr. J. Hyduke
Mr. J. Powers
Mr. S. Snyder

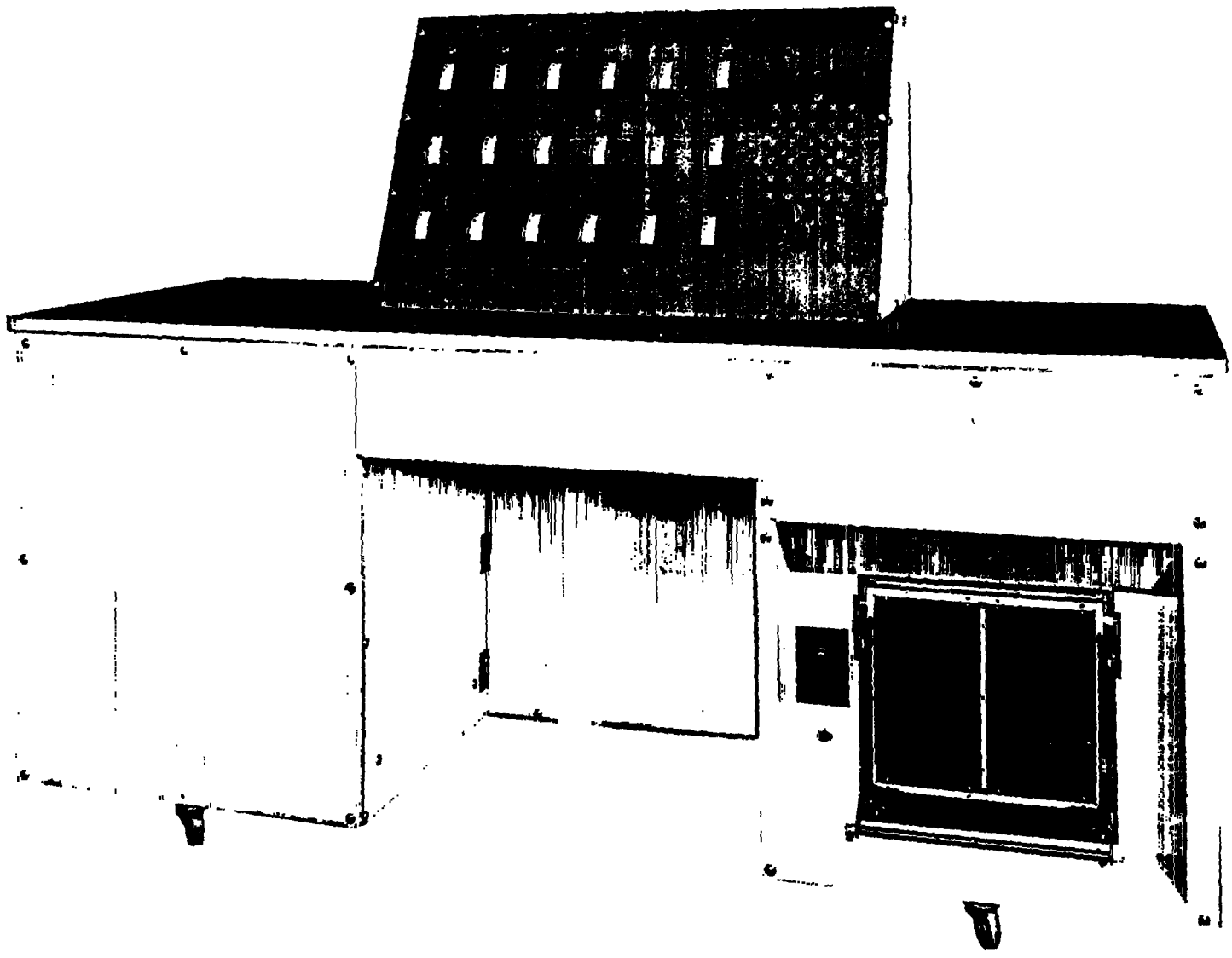
March 1954

OBOE

OBOE (XFE, also called KEY DERIVATION for COLERIDGE, a term also applied to the COLERIDGE KEY SUBSTITUTION DEVICE) was a special purpose relay cribtester for COLERIDGE isomorphic depths of two. It was built by Navy in 1948 and has been superceded by PICCOLO (AFSAF-37). Earlier, Navy cancelled plans for FLUTE, a cribtester which was to have been a prototype to OBOE.

The device was desk-like in arrangement and measured 5'H x 6'L x 3'D . Operation was at the operator's own speed. It has been dismantled.

Ref: M.A.C. Outline #62
Mr. J. Eachus
Lt. R. Marmet



OBOE
AFSAF 37A
KEY DERIVATION for COLERIDGE

SECRET

March 1954

O'MALLEY

O'MALLEY (AFSAF-95, CXMY) is an electronic digital calculator for finding sums of cross-products. The card reader and relay sections were built for Navy by Commercial Controls Corporation and the electronic section by Engineering Research Associates. The one model was delivered in December 1948.

The machine applies to problems requiring sums of products, such as flagging, inversion of large circulant matrices or matching frequency distributions with a known universe. The reader-printer is simply a two-card feed mechanism to handle multiplier and multiplicand decks, as well as the printing mechanism, control panels and plugboards. Each card holds as many as 35 signed four-digit numbers.

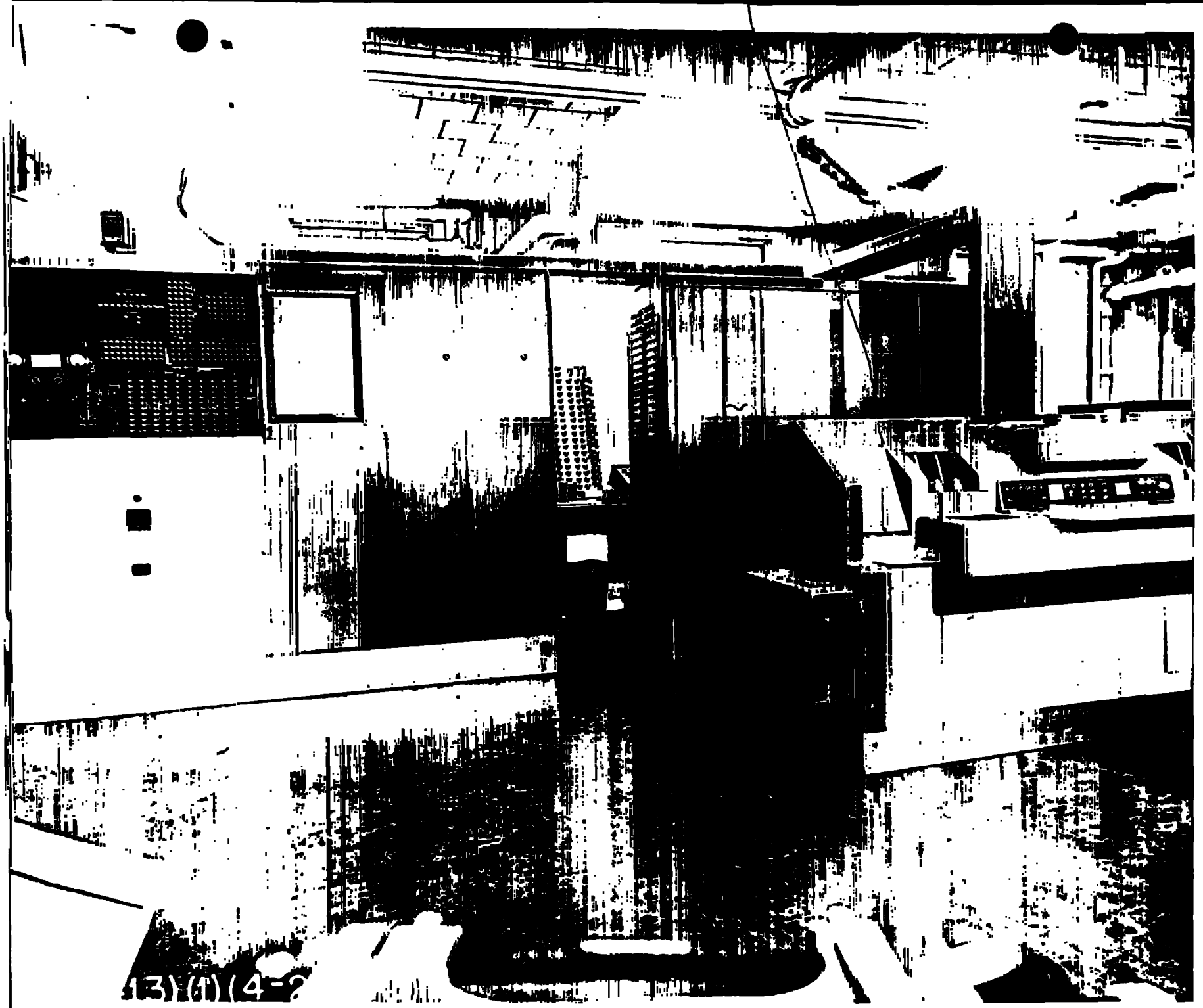
The relay unit stores values read from the cards and the resultant sums of products. An electronic unit scans these values, feeding them by pairs into counter rings and adding their product into a 10-ring accumulator of 10^{10} capacity. These sums transfer to the reader-printer for recording. Special coding is used in the cards, and output is in printed form only. Negative numbers are expressed as the complement of 10 .

Input is at the rate of 80 pairs of cards per minute and print-out is one line of 30 characters per second (20 characters for identification and a 10-digit answer). Each answer is computed

O'MALLEY (Cont'd.)

and returned in 425 milliseconds. Size is 2 cabinets totalling 6'H x 17'L x 2'D plus reader-printer console 4'H x 5'L x 3'D, requiring 16' x 32' floor space. It is now at Arlington Hall Station in room 1530-A.

Ref: Mr. D. Hogan
Mr. J. Stapleton



13(1)(4-?

MARCH 1954

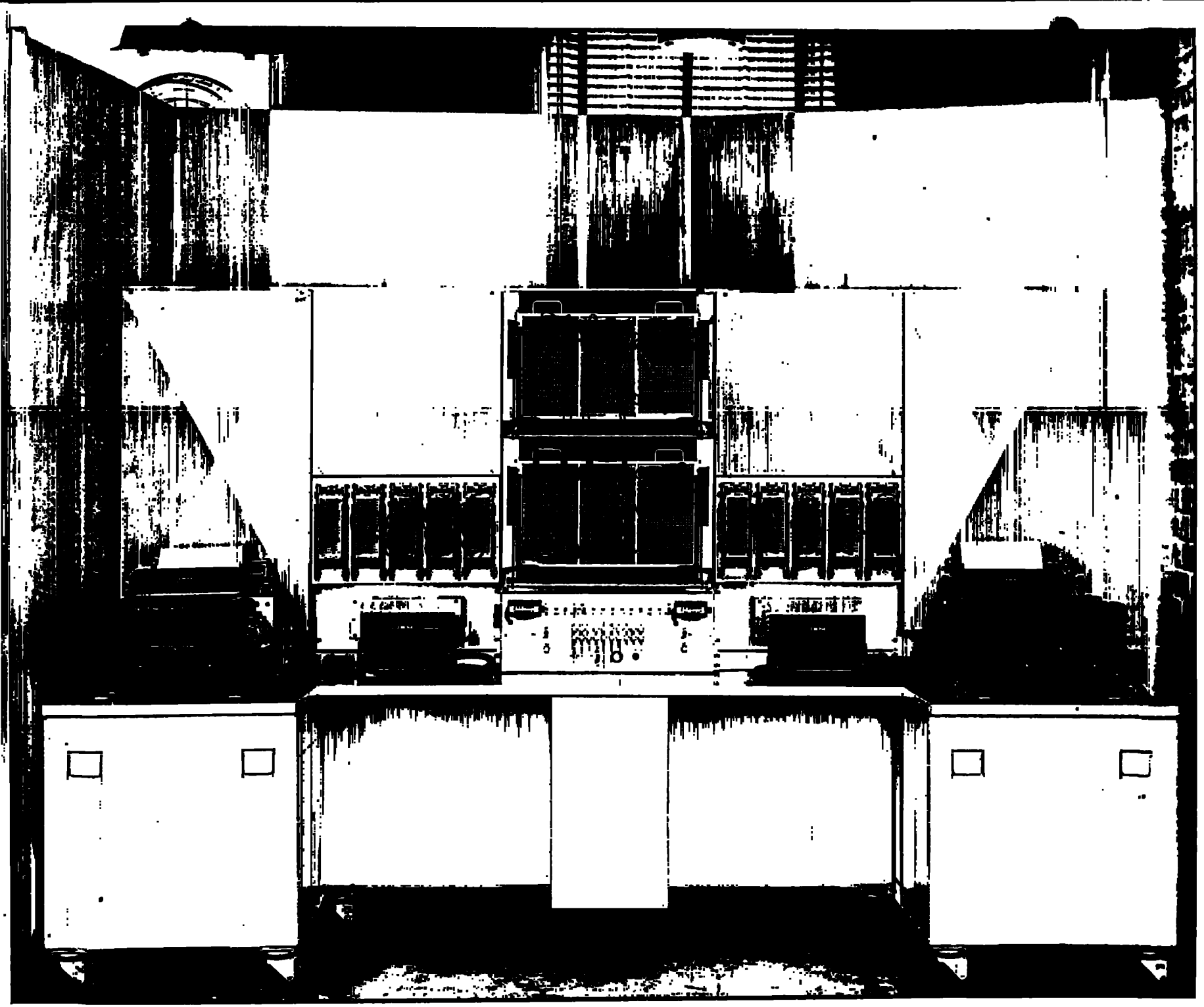
OPHIS

OPHIS (AFSAF-D57) is a generalized wired-rotor relay analog, a general purpose substitution device designed to duplicate the function of any wired rotor machine of up to ten 36-position rotors. A contract with Engineering Research Associates for its construction was cancelled and NSA-36 built it instead. It was delivered in October 1953 and is used to aid in studies of wired rotor cipher devices. An OPHIS COMPARER (Project 352-419-50-0) was completed in January 1953 to operate with OPHIS and later with BABY OPHIS to count instances where input to a maze comes out at the same position.

The machine can be used as a 10-rotor device or as two 5-rotor devices. Tape or keyboard input is provided for both sections. It contains a completely pluggable relay wired-rotor analog in which stepping can be controlled by internal elements or by tape. It can do enciphering and deciphering, using two 60 x 34 plugboards, and ten 8 x 20 plugboards, making all elements pluggable.

It consists of a U-shaped table 3'H x 10'L x 3'D backed against five racks of relay equipment, 6'H x 10'L x 2'D. On either arm of the U is a tape reader, tape punch and CXOO regeneration typewriter which limit the speed to 6 or 8 characters per second. It is located at Naval Security Station in room 17114.

Ref: NSA-34 files
Mr. N. Christopher
Mr. W. Erskine
Mr. R. Sengpiehl



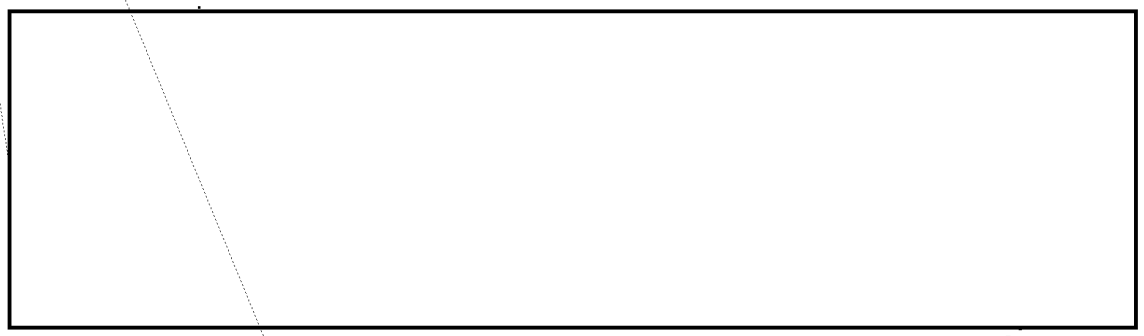
OPHIS
AFSAF D57

SECRET

March 1954

PICCOLO I -IV

PICCOLO (AFSAF-37) is a special purpose relay cribtester and decipherer for applying cribs through a given substitution to a pair of isomorphic COLERIDGE messages. Four models were built, the first by NSA-35 and later ones by NSA-22, one each year from 1948 to 1951. Serial 2 of model IV was completed in September 1952. These supercede the Navy OBOE and the planned FLUTE prototype.



For each setting tried, the machine automatically prints out 20 letters of possible plain on a CXCO regeneration typewriter. Models III and IV have provision for [redacted] and have special typewriters which print [redacted] if desired.

The first two units were table-top size, 1'H x 3'L x 3'D. Later ones are relay racks, 5'H x 3'L x 2'D plus typewriter. Model I has been stored and model III has been dismantled, but the remaining 2 models, II and IV, are often referred to as models II and III. There are now 3 PICCOLO's in use at Arlington Hall Station in room 2054-B. Rate is 6 to 8 characters per second.

References:
Mr. N. Christopher
Mr. G. Lockhart
Mr. F. Mayol
Mrs. L. Pokorski

~~CONFIDENTIAL~~

March 1954

PRESENSING PUNCH

The PRESENSING PUNCH was a modification of a 517 REPRODUCER PUNCH or SUMMARY PUNCH, a completely general input-output device which operated with other equipments to do digital enciphering and deciphering using arithmetic or substitution, on up to five digits at a time. It was a rental equipment developed in 1944 for the Army by International Business Machines Corporation and made substitutions at a higher rate of speed than any previous IBM method. Navy's NC-4 COORDINATING REPRODUCER replaced both it and the NC-3, and was itself replaced by a MARK II model (AFSAF-43), now called the 797 COORDINATING REPRODUCER.

The machine had two sets of 80 reading brushes and one set of 80 punch magnets plus 20 digit-selectors. Key and cipher were fed in from one deck. The extra set of brushes, installed one cycle before the punching stage, permitted computations to be punched into the same card from which the base information came or into a new deck. With auxiliary equipment the machine could encipher or decipher and punch a record of the results, all in one cycle. In itself, it does no computation, serving only as a base machine.

It measured 4'H x 3'L x 2'D and operated at a rate of 100 cards per minute. All have been returned to International Business Machine Corporation.

Ref: Mr. O. Algren
Mr. J. Hydnke
Mr. S. Thorne

~~CONFIDENTIAL~~

March 1954

PURPLE KEY DEVICE

The PURPLE KEY DEVICE was a temporary connection of the PURPLE ANALOG and a 514 REPRODUCER used to develop alphabets in the machine cycle. It was set up by NSA-82 in March 1953 for a one-time job.

On the strength of studies of [redacted] the retired PURPLE ANALOG was gotten out of storage and put into working order. It was run through its full cycle of 25^3 or 15,625 positions. (The three 25-position "20's" wheels only, since the "6's" wheel is always considered separately) and the resulting encipher-decipher alphabets catalogued on other equipment for decryption and study purposes.

Analog size was 1'H x 3'L x 1'D plus a 514 REPRODUCER. Rate was 100 cycles per minute. Although now dismantled, it would be easy to re-combine the pair of equipments if needed.

Ref: Mr. S. Thorne

RATTLER

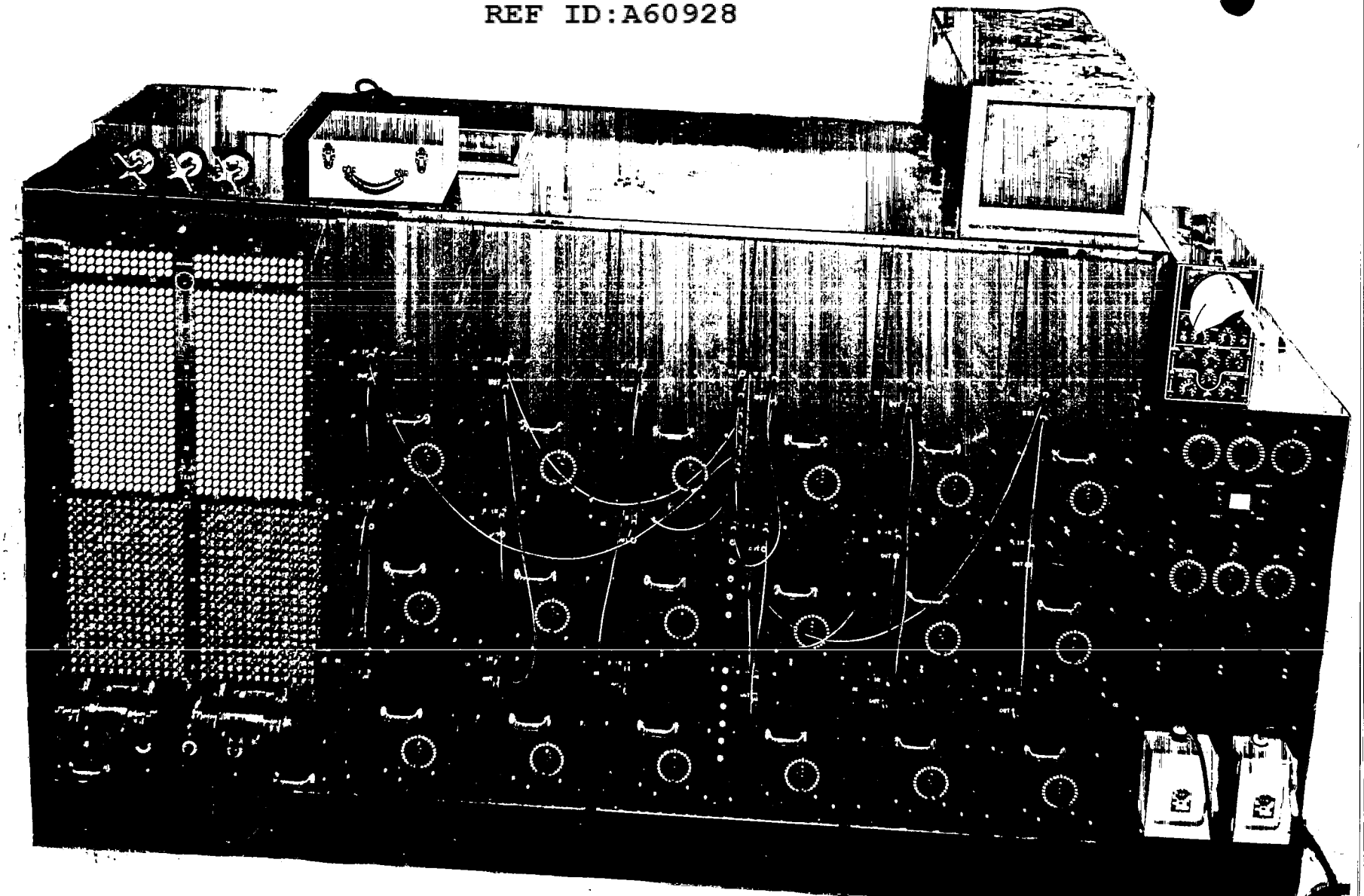
RATTLER (CXLS) was a relay analog for the Japanese JADE machine (a telephone selector cipher device producing JN-157 traffic) to recover starting points through exhaustive trial. National Cash Register Company built three for Navy, the first in May 1944. Plans to send one to Pearl Harbor were cancelled and it was eventually dismantled. The other two were modified in October 1944 to apply interchangeably to either 5-wheel VIPER or 3-wheel PYTHON problems. Auxiliary equipment included a cable continuity checker, a relay checker, a test oscillator and plugboard test. There was an unimportant tape-operated pre-punch verifier built for Navy about 1946 which was called RATTLER for a short while.

The machine tested a 5 or 6 letter crib against cipher through a full cycle by tracing cipher text through the 3 moving rotors and matching the results for possible circuits. These last 2 rotors were hand stepped between messages and were not interchangeable. The system used 50 characters, 25 each in upper and lower case, with each half enciphering only to itself. There were 25 plugboards, one per letter. Each board, containing the rotor wirings and the 10-day stecker, had 25 inputs and 625 outputs to a detector circuit. At a hit, consisting of 5 or 6 points hot in the same column, the machine stopped to indicate the existence of required circuits and showed the setting on neon lights. Cipher input was by CXCO tape reader.

Size was 7'H x 9'L x 2'D plus tape reader and rate was a full cycle tested in about 10 minutes. They were dismantled.

References: CIT-TS 23 and 33
Mr. J. Stapleton
Mr. H. Stukey

REF ID:A60928



RATTLER
(CXLS, N-1200, N-2200)

TOP SECRET

FROTH

March 1954

ROE

ROE (AFSAF-D98) is a special purpose tape-operated relay deciphering device for STURGEON traffic,

The STURGEON ANALOG supplies both substitution and transposition key tapes, and ROE applies these to cipher. A pair of double-headed readers permit three tape inputs at a time, usually cipher text tape and two key tapes. The resulting plain values are printed out on a CXCO regeneration typewriter. Its present use as a supplement to the ANALOG is limited due to a change in the traffic system from use of one-way tapes to multiple daily wheel settings, thus requiring the ANALOG to do the full job. ROE is still useful for fitting out-of-phase messages in shallow depth, and will be in use again whenever wheel patterns change and must be recovered.

Size is 1'H x 1'L x 1'D , plus two double-headed readers and a CXCO regeneration typewriter. Rate of speed is 6 to 8 characters per second. At present it is stored at Arlington Hall Station in room 2048-A.

Ref: Miss V. Collins
Mr. G. Stahly

March 1954

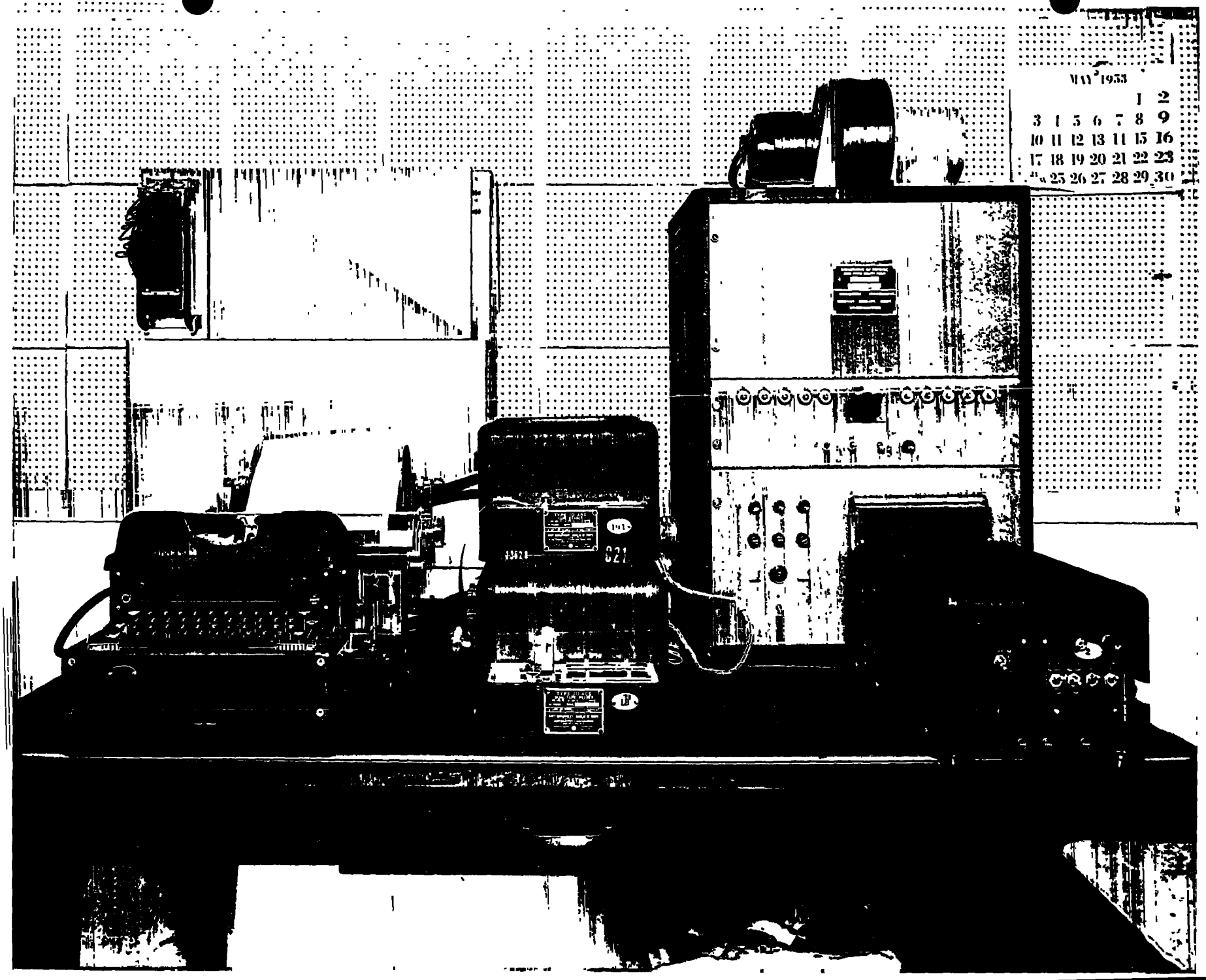
ROSE

ROSE (AFSAF-D55, DEPTH-READING CRIBDRAGGER) is an electronic cribdragger for depths of two in STURGEON [redacted] Probably the first electronic desk-top crypt-aid ever built, the single model was built in 1951 by NSA-35.

Up to 20 letters of crib are supplied by tape or RemRand cards and two cipher messages in depth are read by a double-headed tape reader. Output is to a CXCO regeneration typewriter and/or tape punch. [redacted] The analyst may then try to read text from these irregular lines. Weight summing is accomplished in binary counters, and printed in decimal form. Wheel patterns and stecker and consequent function must be known.

Input is at the rate of 1 character per 4 seconds and output is at 8 characters. The several pieces of equipment in the unit fit comfortably on a table. It is now in use at Arlington Hall Station in room 2048-A.

Ref: T/CA 15/50
Miss V. Collins
Miss N. Miller
Mr. G. Stahly



ROSF
AFSAF D55
DEPTH-READING CRIBDRAGGER

March 1954

[redacted] KEY GENERATOR

The [redacted] KEY GENERATOR was a relay device which operated with a 513 REPRODUCER as an analog of a [redacted] cipher machine called [redacted] It was built by Army, section WDGAS-92, in April 1947.

The patterns of the [redacted] were represented on six levels of an IBM card and automatically offset by a 26 position class selector to produce the effect of motion. The full cycle of the cipher device could be reproduced in four and sometimes two cycles of the analog.

The device was mounted in the cover of a 20 x 34 plugboard on a 513 REPRODUCER and measured 1'H x 1'L x 1'D. Rate was 100 cards per minute. It has been dismantled.

Ref: Mr. S. Thorne

March 1954

SIGMA

SIGMA (AFSAF-120, TWO-POSITION GATE) is a relay adding device used with 797 COORDINATING REPRODUCER number 35 to do modular addition on two positive numbers read from a card. It was built by NSA-22 in late 1950.

The computation is true arithmetic, and selection of modulus is by an 8 x 20 plugboard. Two numbers from 00 to 99 are compared to find $A \geq B$ or $A < B$. For either case, the selected modulus may be employed before computing $A + B$. Both factors are read from a card and results are punched into the same or a different deck.

Size is 2'H x 3'L x 2'D and rate is 100 cards per minute. It is available but unused at Arlington Hall Station in room 1700-A.

Ref: Mr. S. Thorne

March 1954

SINGLE POSITION COMPARING COLLATOR

The SINGLE POSITION COMPARING COLLATOR was an 077 COLLATOR, rewired to provide 32 separate and distinct comparing positions, all inter-connectable in any desired manner. Three of these were built by Army, section WDGAS-92, in September 1946. In 1949, an 072 COLLATOR was similarly modified to handle alphabetic material.

The first device was used for pattern search in digital material, testing several different patterns simultaneously. The special wiring was through the regular 20 x 34 plugboard, permitting plugging of any pattern(s) of any length up to 32 . Input was by IBM cards, and at a hit the card in question was sorted into a different pocket.

Rate was 240 cards per minute and size was 4'H x 4'L x 2'D. The three modified 077 COLLATORS were recently dismantled but the modified 072 COLLATOR is still available at Arlington Hall Station in room 1600-A.

Ref: Machine Branch Annual Report, 1947
Mr. S. Thorne

MARCH 1954

SLED I

SLED I (AFSAF-72, ALPHABETIC SLIDE-RUN MACHINE) is a general purpose analog computer, capable of a great variety of analytic operations. Two have been bought from International Business Machines Corporation. Serial 1 was delivered in January 1953 and Serial 2 arrived in July 1953. They replace MERCURY, SLIDE-RUN, KEYFINDER, SKATE I and II and other equipments. Plans for one or two SLED II's are still under discussion, but as yet no specifications have been drawn. CONSORT (AFSAF-D72/10, GROUP I.C. ATTACHMENT) has been added to permit making 4- or 5-digit group comparisons and to evaluate an Index of Coincidence of the groups matched over a span of up to 300 characters.

The device is card-operated and has a 48,000 character magnetic drum with revolvers, delay line storage, two pluggable 32 x 32 matrices, a 2000 pentagraph recognition unit, a statistical evaluation or comparison unit, and provisions for weights over a range of 1 to 127 . It is capable of notched wheel or wired rotor decipherment, depth search, keyfinding, crib-dragging, coincidence counts, group I.C. counts, fractionation, chaining and other operations. Operation is controlled, not by program as in most computers, but by interconnecting machine elements and by plugboard wiring. Emphasis on data-handling rather than digital computation and large numbers of simultaneous rather than serial

SLED I (Cont'd.)

operations are the outstanding characteristics of the machine.

Pulse rate is 120 K.C. and drum rate is 3720 RPM , permitting 30,000 decipherments per second and up to 30 million pentagraphic comparisons per second. Physically, the machine is L shaped, each arm being about 7'H x 20'L x 3'D, plus a 797 COORDINATING REPRODUCER. They are in operation at Arlington Hall Station in room 1530-A.

Ref: Mr. J. Hyduke
Mr. J. Powers

March 1954

SKATE I and II

SKATE (AFSAF-71 = CXNQ; AFSAF-71A = CXOS) is a high speed cribdragger for reading depths, slide-run and keyfinder jobs. Both models were built for Army by International Business Machines Corporation and delivered in January and December 1949. They served partly as pilot models to SLED (AFSAF-D72), of which they are only abbreviated versions, and supercede Army's SLIDE-RUN MACHINE (AFSAF-29) and KEYFINDER.

Model I was limited to cribdragging in COLERIDGE traffic, for isomorphic depths of two. Model II is much more flexible and general, able to do cribdragging, slide-runs and keyfinder jobs. All SKATE-SLED equipment uses special input-output devices. A modified 072 COLLATOR is the input and a special 517 SUMMARY PUNCH or a 797 COORDINATING REPRODUCER is the output. Both models try each of 192 cribs in message A ;

Key may be tried offset up to 9 position. Cribs and recognition banks are set on plugboards. Model II has an additional feature, a device for applying weights of 1 to 9 and an accumulator.

Model I measured 7'H x 16'L x 3'D and II is 4 feet lower. The 15 KC pulse rate is the same for both, permitting testing 192 cribs at one position and checking against 2000 recognition groups in .12 seconds on either model in a cribdragging job. Model II

SKATE I and II (Cont'd.)

also does 21,100 decipherments per second, checking each against the 2000 group recognition bank. [redacted] but the latter is in operation at Arlington Hall Station in room 1530-A.

Ref: Mrs. D. Blum
Mr. J. Powers
Mr. J. Russell

SLED I
AFSAF 72
ALPHABETIC SLIDE-RUN MACHINE
CXOA

~~SECRET~~

March 1954

SLOT MACHINE

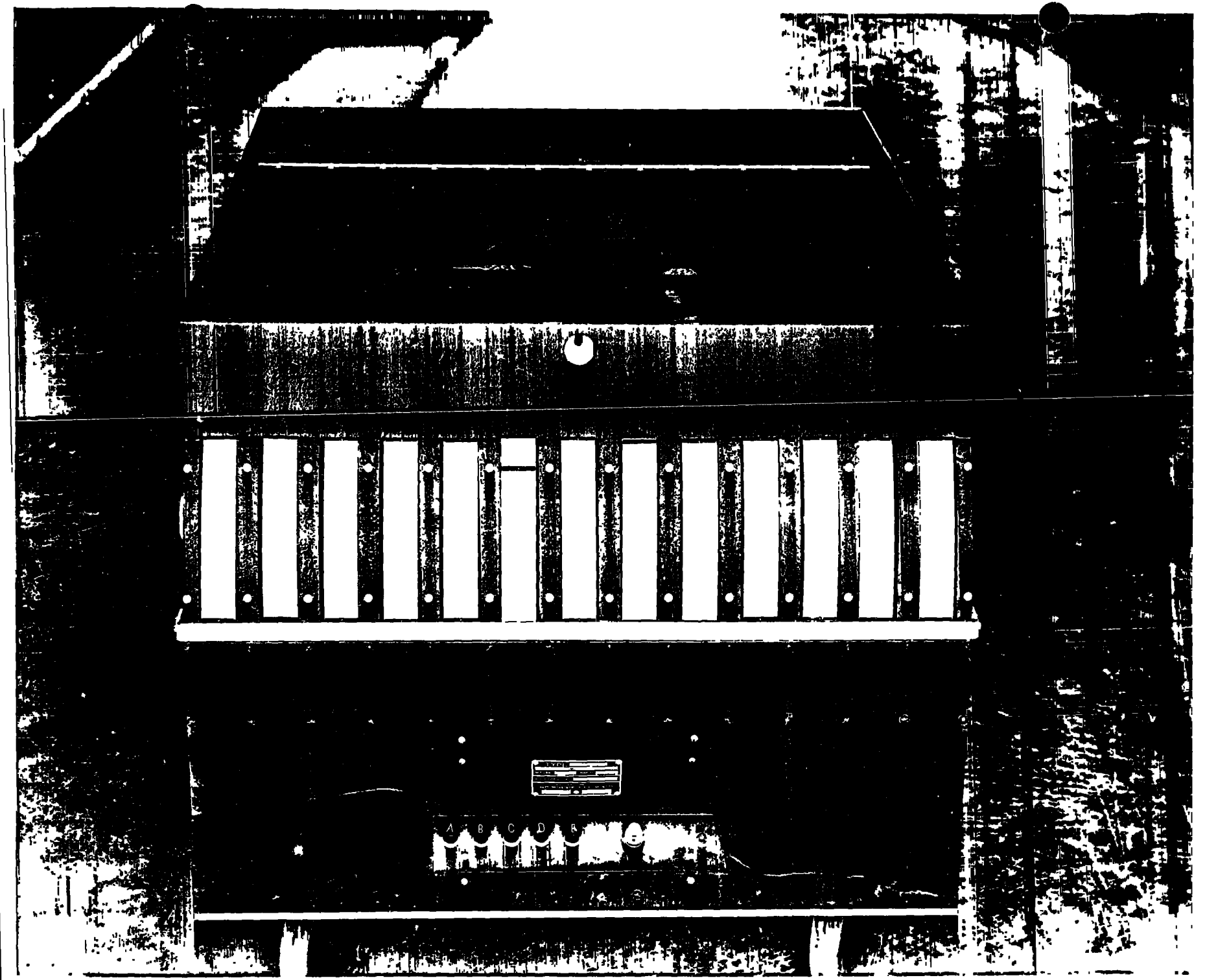
SLOT MACHINE (XEJ, 13-WHEEL DEVICE) was a solenoid operated deciphering device used to remove known key in certain weather systems. It was built by NSA-35 in August 1950 to mechanize tedious hand decipherment. It was planned as a pilot model, but due to its cumbersome operation was the only one built.

The machine contained 13 wheels, each 18 inches in diameter, whose sanded lucite circumference was marked off into 10 equal segments. On this rim synoptic data could be pencilled. Five pushbuttons controlled stepping combinations (motion of sixth wheel equals sum of motion of first and fifth wheel, motion of seventh wheel equals motion of second and sixth wheels, etc.). It permitted use of semi-skilled personnel on a highly skilled job. Operation consisted of inscribing standard synoptic data on the wheels semi-permanently, setting the wheels according to each message in turn and hand copying the data thus aligned in the window slots.

Size was 3'H x 3'L x 3'D and rate was about one operation per second. It operated at Naval Security Station for a while, then was sent to the museum and later dismantled.

References:

Mr. K. P. Cook
Mr. F. Sims



SLOT MACHINE
13-WHEEL DEVICE, XFJ

~~SECRET~~

~~FROTH~~

STORK

STORK (XFA) was a slow-speed relay slide-run device for placing a long crib against cipher by recognizing cyclic key and roughness. The one equipment was built by Navy in November 1949 and was used on COLERIDGE traffic.

Input was a CXCO tape reader. Each of the five bans on the tape was wired to each of five chains of thyratrons which operate a stop circuit when fired by a strong enough current. The device tried a 30-letter crib at successive points, allowed a slide of up to 30 positions, calculated $\sum \frac{n(n-1)}{2}$ roughness statistic and stopped the machine when the statistic exceeded a preset amount. Output was in the form of lights revealing pertinent data.

Size was 7'H x 7'L x 3'D and rate of comparison was 4 to 6 characters per second. It has been dismantled.

Ref: CIT papers #96
NSA-Technical Library
Mr. J. Stapleton

REF ID:A60928

STORK (XFA)

March 1954

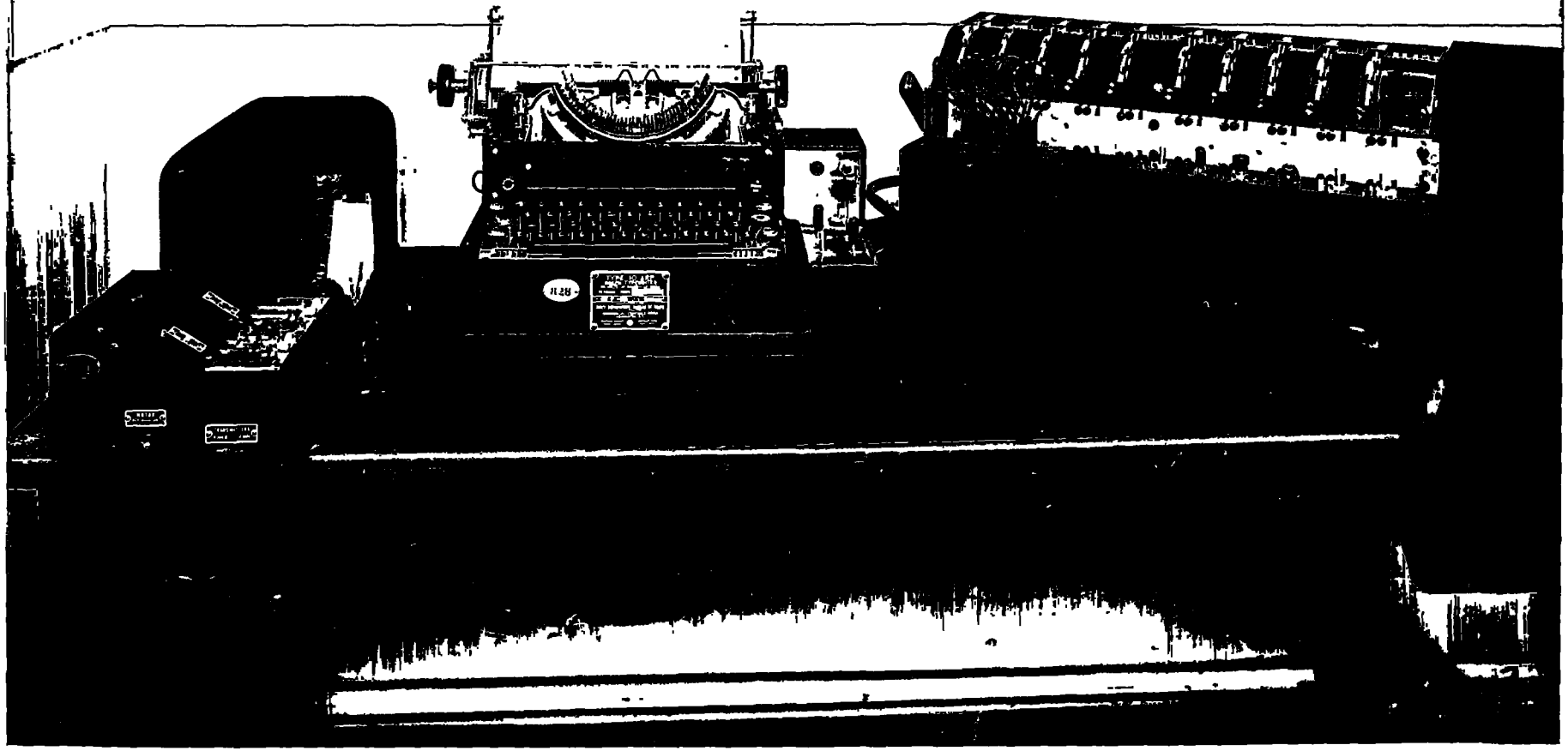
STURGEON ANALOG

The STURGEON ANALOG (AFSAF-106) applies to the German-built STURGEON on-line teletype keying device (SFM T52C, T52D, and T52E) used by the [redacted] A total of 6 was built by NSA-22, the first in December 1949. Three still have the old wheel patterns of [redacted] patterns. All handle types C, D and E and their various wheel patterns.

The analog contains 10 pattern wheels (73, 71, 69, 67, 65, 63, 61, 59, 53 and 47 in length) and the stepping controls as in the original cipher device. As now used, plain or cipher is read on a double-headed teletype reader and output is to a CXCO regeneration typewriter and/or tape punch. A tiny plugboard on the front controls the stecker, determining which 5 wheels are concerned with substitution and which with transposition. A switch permits writing out either type key for study or other use.

Size is 1'H x 2'L x 2'D plus double-headed reader, CXCO regeneration typewriter and tape punch. Rate is 6 to 8 characters per second. All 6 are now in use at Arlington Hall Station, 5 in room 2048-A and the other in room 0413-B for use with IDA.

Ref: Miss V. Collins
Mr. G. Stahly



STURGEON ANALOG
AFSAF 106
for the SFM T52C, D and E

TOP SECRET

MARCH 1954

SUBSTITUTION DEVICE

The SUBSTITUTION DEVICE (AFSAF-113) is a relay gate used with an NC-5 PATTERN PUNCH to perform simple substitution on up to five columns in a card. It was built by Navy in March 1949.

The device will recognize 38 characters, 0 through 12, and A through Z. Substitution for all five positions is controlled by a plugboard but is not unique and independent of other columns. Results are punched into the same card.

The SUBSTITUTION DEVICE is built into the same gate with GLID and the COLUMN ARRANGER. Size is 4'H x 3'L x 2'D and rate is 80 to 90 cards per minute. It is at Arlington Hall Station in room 1700-A and available for use only after some rewiring, since no NC-5 now exists.

Ref: Mr. S. Thorne

TAN ANALOG

TAN ANALOG (AFSAF-48, TAN MACHINE, LONGFELLOW ANALOG) designates a set of relay analogs designed to [redacted] usage in LONGFELLOW traffic, [redacted] Used mainly to generate key, they could also set pattern wheels, decipher and encipher. Traffic included [redacted] but not [redacted] IN POGODA system which was a double-tape on-line usage. At Army, sections WDGAS-74, 76 and 92 built a total of 7 such machines. Navy's two similar analogs, MARTINI AND INITRAM, are described under those headings.

A major component of HIAWATHA (CXNO, a projected wheel setter) was to be an electronic analog of TAN pattern wheels. Work under task 20 at Engineering Research Associates was suspended when the system disappeared and continued under LEO, task 11, as a generalized study of a wheel analog.

In all models it is necessary to [redacted]

The first model in April 1947 by WDGAS-92, consisted of two units. The TAN SETTING GENERATOR (AXIB/1, TAN MOTION GENERATOR) was a small plugboard attachment operating with a 513 REPRODUCER to develop motion patterns only. The first such unit was mounted on a board and a later model in a 20 x 34 plugboard cover.

TAN ANALOG (Cont'd.)

Its working mate, the TAN KEY RECORDER, AXKB/1, TAN KEY REPRODUCER) was a small plugboard attachment to an NC-4 SELECTIVE PUNCH (AFSAF-42) to combine motion and wheel pattern to produce key. Size was 1'H x 1'L x 1'D and rate was 50 keys per minute.

The second model also operated with a 513 REPRODUCER, incorporating motion and key production in one unit. It also was built in April 1947 and added a comparison circuit for checking results. Size was 3'H x 2'L x 2'D and rate was still 50 keys per minute.

In October 1947, three of a third model were finished and all these earlier ones dismantled. Plans for three more were cancelled. Size was 2'H x 3'L x 2'D and rate rose to 100 keys per minute. A circuit was added in 1948 for producing key parity. One of these 3 was made into the MODEL TAN GENERATOR, a reduced version for cycle study to include finding branch points. It contained three wheels of variable size. Later in 1948 this same gate was re-wired and became the BINARY MOTION SETTING GENERATOR, a generalized pattern wheel analog, also for cycle studies. It was dismantled.

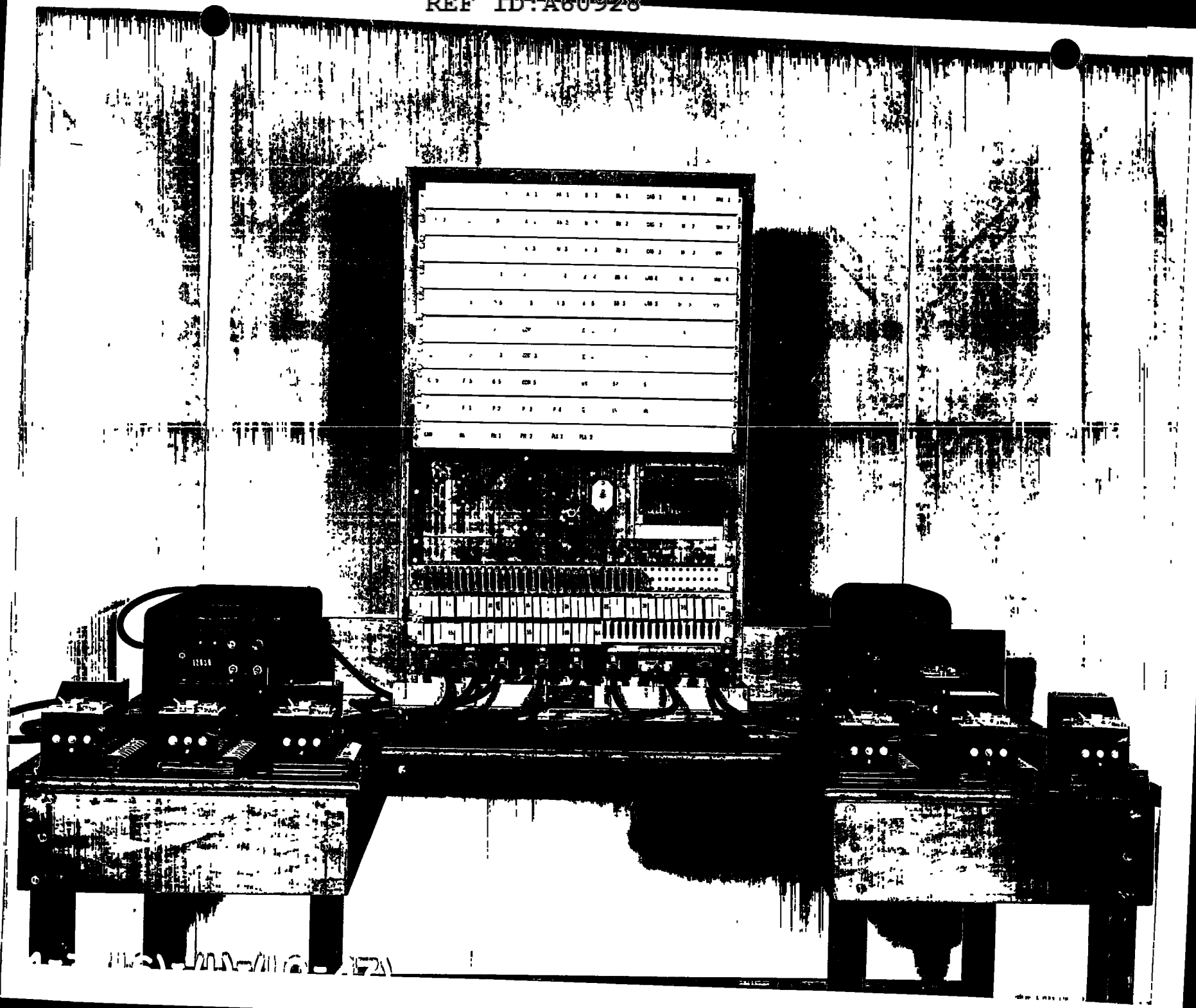
These five machines alone generated about four million digits of key for use in the operational sections. Experience with these led to development of the AFSAF-12 COMPARATORS and the associated AFSAF-13 KEY GENERATOR.

In July WDGAS-74 built a relay TAN ANALOG (LONGFELLOW, LONGFELLOW ANALOG FOR [redacted] which used 6 loop-tapes read on solenoid-operated reader heads to simulate notched wheels. Cipher text could be read in by a TDX reader, with results being punched on a CXCO tape punch. Plans for a second and larger one, called a SEQUENTIAL SETTING TESTER FOR [redacted] were cancelled. Size was 3'H x 3'L x 2'D and rate was about 6 to 8 characters per second.

TAN ANALOG (cont'd.)

In December 1947, WDGAS-76 completed a Tan Analog (AFSAF-48) for key generation and deciphering. The wheels were represented by [redacted] having electrical contacts set around the rim and read by wiper arms. Notch patterns were set on plug-boards, and output was a key tape from a CXCO punch. Size was 5'H x 3'L x 3'D and speed was 5 characters per second. It was later modified to do key generation only and used as an aid to cycle studies. The usual procedure with all these machines was to produce key in tape for use on other equipments. Two of the third model built by WDGAS-92 are now at Arlington Hall Station in room 1600-A, and the model by WDGAS-76 is in the museum. The rest are dismantled.

Ref: E. R. A. Final Report, Task 20
M. A. C. Outline #53
Machine Branch Annual Reports, 1947, 1948, 1949
Mr. F. Mayol
Mr. J. Powers
Mr. J. Russell
Mr. R. Sykes
Mr. S. Thorne



One model of
TAN ANALOG
AFSAF 48
LONGFELLOW ANALOG

~~CONFIDENTIAL~~

March 1954

TERTIARY MOTION SETTING GENERATOR

The TERTIARY MOTION SETTING GENERATOR was a relay device used with a 513 REPRODUCER for simulating [redacted] It was built by NSA-22 in February 1950.

The device operated as [redacted] Wheel settings were recorded continuously on a 513 REPRODUCER in 6 levels of a card. Wheel set-up was controlled at the time of punching the first card. Motion was simulated by cyclic offset within the card.

Size was 2'H x 3'L x 2'D and rate was 100 cards per minute. It was dismantled after the key study was finished.

Ref: Mr. S. Thorne

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

March 1954

TESSIE I

TESSIE I (TESSIE SS, SYMMETRY SEQUENCE MACHINE) is the posthumous designation of a photoelectric film comparator and tetragraph tester built for Navy by Eastman Kodak Company in 1942, and called simply TESSIE with no numeral designation. When ICKY I, a second model tetragraph tester, arrived in 1943, Navy called it ICKY while Army, unaware of TESSIE I, called it TESSIE (AXOE). At that time the original tetragraph tester was modified to do symmetry search only and was then called TESSIE SS or SYMMETRY SEQUENCE MACHINE. The nomenclature problem was further befogged by (1) a third model tetragraph tester (called TESSIE II, AFSAF-11), built by Army in 1945 and by (2) unfruitful plans at Navy for a fourth tetragraph tester to be called ICKY II (CXNR). Film for TESSIE I was made by a 35mm cameras which also supplied ICKY I.

As used for symmetry search, the device consisted essentially of a film advance mechanism and an electronic scanning system. The first character of text on the message film loop actuated a master photoelectric cell which scanned the next 20 letters of text while a mask representing A to Z passed across each position of text. A repeat of the initial character caused a punch in two 70mm tapes, one white and the other black-and-red. These tapes, superimposed in a viewer (a particular device but no nomenclature to identify it) and scanned visually position by position through a triangular guage, allowed the operator to detect blackouts, or a diagonal of red spots indicating the presence of symmetry in the cipher.

~~CONFIDENTIAL~~

TESSUE I (cont'd.)

Size was 6'H x 7'L x 2'D and rate was about 5 minutes to search a pair. The camera was less than a cubic foot in volume. It was tape controlled and ran at 6 characters per second. TESSIE I has been dismantled.

References:

Brief Descriptions of RAM
CIT paper 9
Mr. H. Lofink
Mr. J. Stapleton

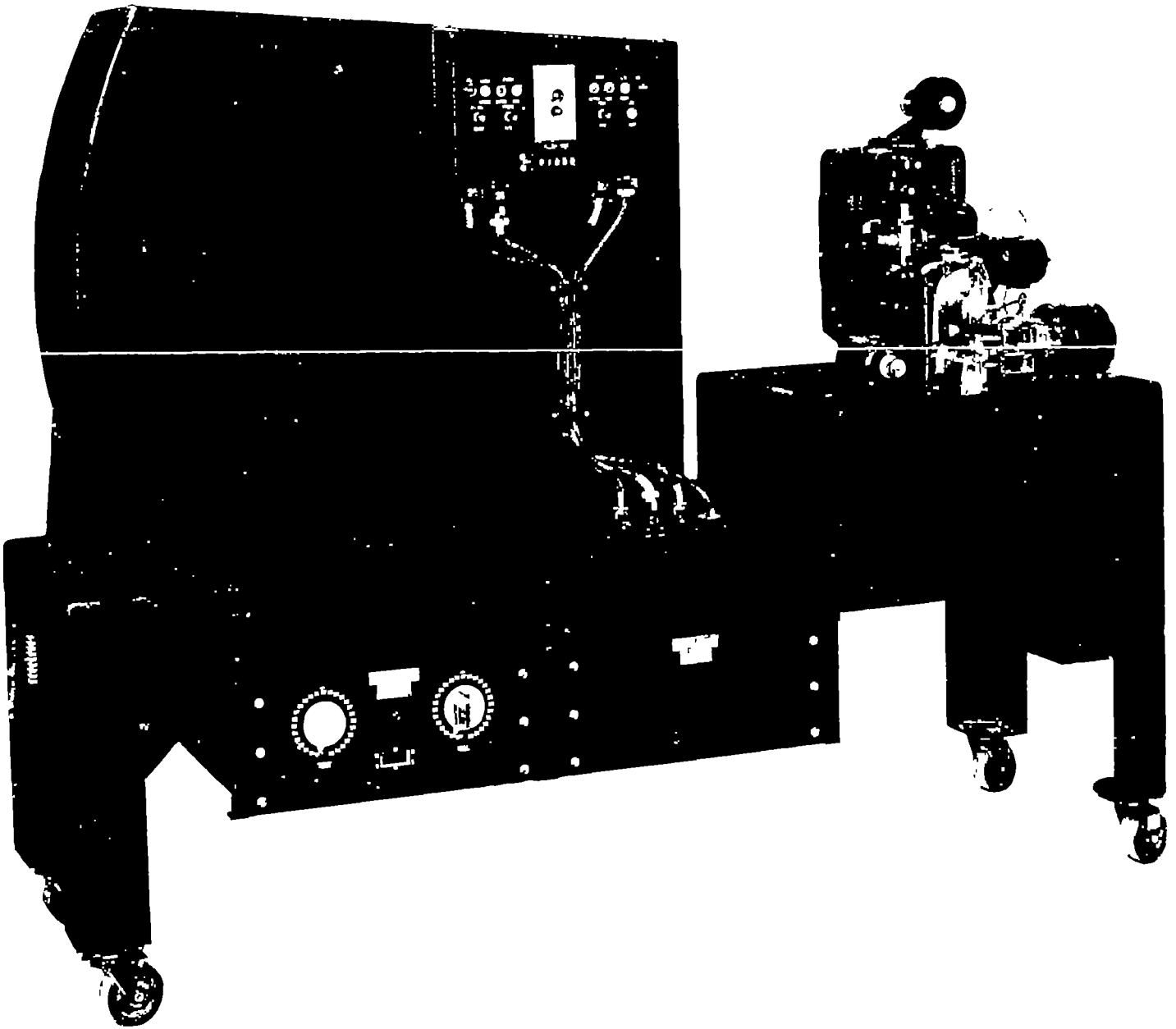


PLATE I - TESSIE SS (Front View)

PLATE I
TESSIE, TESSIE SS
SYMMETRY SEQUENCE MACHINE

March 1954

TESSIE II

TESSIE II (AFSAF-11) is a general purpose photoelectric 35mm film comparator and tetragraph tester. Army personnel added the II after delivery of a pair by Eastman Kodak Company in 1945 to distinguish it from (a) ICKY I which had erroneously called TESSIE and from (b) Navy's TESSIE I (TESSIE SS) of whose prior existence Army seemed unaware. At first, a tiny camera supplied the 35mm film. It was replaced by BRUTE camera and currently by a pair of BRUTE II camera and storage units (AFSAF-5) which concentrate more information and identification data on the film.

The device offers nothing new in principle or function over ICKY I, all modification being merely for operational convenience. Its function is to search for tetragraphic or larger repeats or patterns up to the limit of the 35 column wide gate.

Size is 4'H x 2'L x 4'D. Rate of the motor-driven film is still 3500 frames per second as in ICKY I. Both are located at Naval Security Station in room 20210.

References:

Mr. G. Kier
Mr. H. Lofink

March 1954

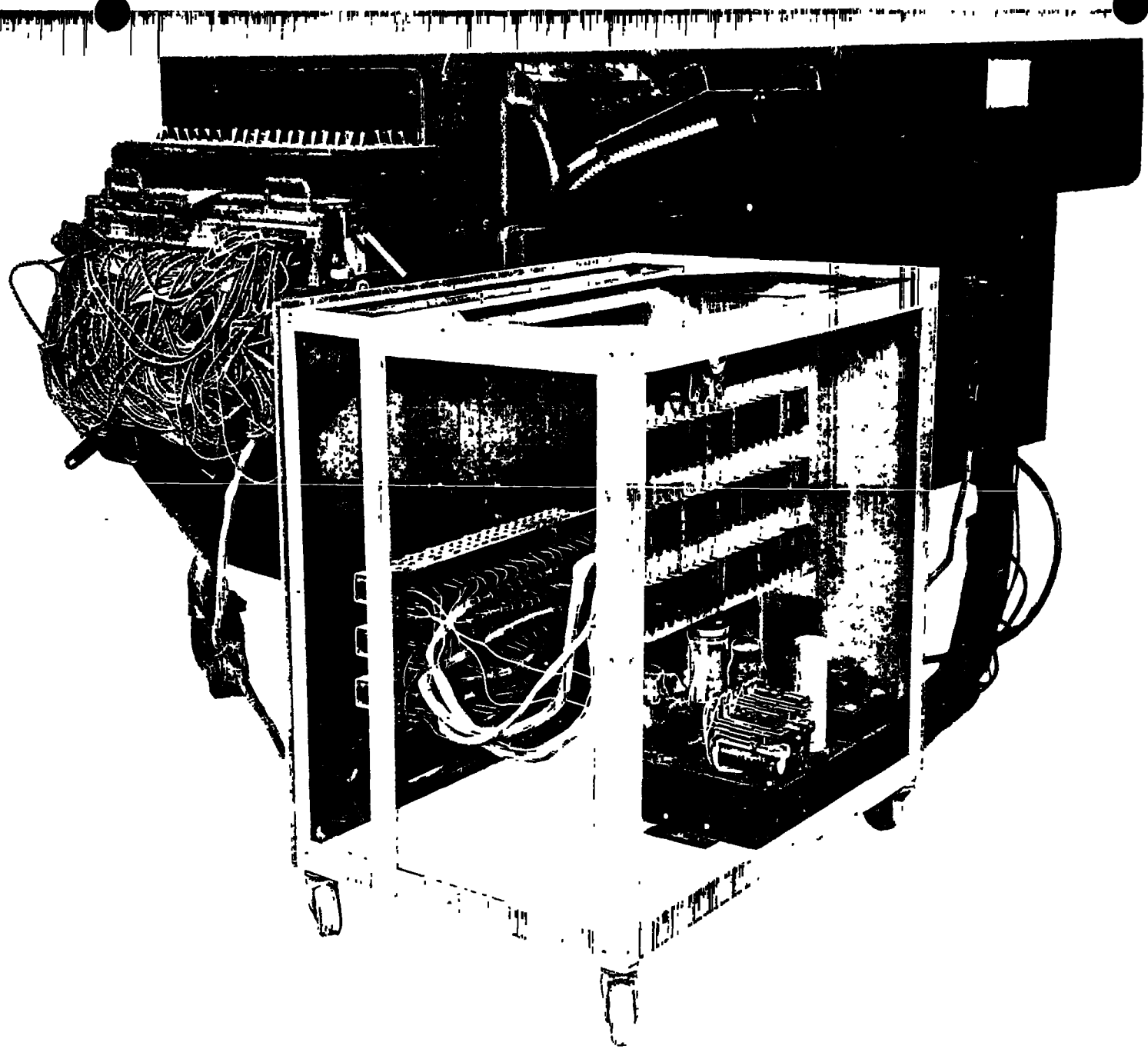
THRESHOLD DISCRIMINATOR

The THRESHOLD DISCRIMINATOR was a relay gate which operated with a 405 TABULATOR to count digits, in effect, and to locate and identify any digit occurring more than a predetermined number of times. It was built by Army, section WDGAS-92, in 1948 specifically for the [redacted] This operation is now done by the 101 ELECTRONIC SORTER and HORACE (AFSAF-116).

The TABULATOR, over a span of 50 columns in a card, sequentially read all punches on the 9's level, 8's level, etc. Occurrence of a given digit was made to increase the voltage of a tube by passing a pulse through a set of from 2 to 15 matched resistors. When a preset voltage value was reached, the tube energized a relay to produce a listing on the TABULATOR of the digit which caused the listing.

Size was about 3'H x 2'L x 2'D and rate was 150 cards per minute. It has been dismantled.

Ref: Machine Branch Annual Report, 1948
Mr. S. Thorne



THRESHOLD DISCRIMINATOR

THRESHOLD DISCRIMINATOR

March 1954

TOPAZ

TOPAZ (CXEK) was the relay analog of a Jap strip cipher system, intended to mechanize decryption of large volumes of JN-11 and JN-25 traffic which never materialized. Two such equipments were built for Navy in March 1945 at US Naval Computing Machine Laboratory.

Up to 50 strips, each 20 digits long, were set up on plugboards and selected 20 or less at a time by switches. Cipher text was supplied by keyboard or tape reader, with the analog automatically applying the key elements, non-carrying. Resulting decoded values were typed in 4- or 5-digit groups as desired on a CXCO regeneration typewriter. Code values for these groups were then looked up by hand. The provisions for 5-digit code were never used. Key could be used either as additive for deciphering or subtractor for enciphering. Internal setup was indicated at all times by a panel of lights. The strip-selection feature and ability to read across the resulting rows made columnar transposition possible on the machine.

The machine measured 6'H x 4'L x 3'D with a metal shelf in front for tape reader, digital keyboard and regeneration typewriter. Rate was 6 to 8 characters per second. Both machines are now dismantled.

Ref: CIT paper 31
CIT paper 43

~~CONFIDENTIAL~~

March 1954

TRACK-IN TEST DEVICE

The TRACK-IN TEST DEVICE was a relay gate used with a 513 REPRODUCER to find branch points for cycle studies. It was built by Army, section WDGAS-92, in September 1949. PLUTO (AFSAF-30) now automatically does this type testing for branch points.

Four wheel-patterns were stored in cards, although only two, the 25 and 23 , were wheels in the usual sense. The two 12 wheels were simulated by fixed plugs. Rules of motion were involved and were, in part: 1) The sign on the 23 wheel two cycles previous determined dilation (standing) of the 25 wheel; 2) The sign on the 25 wheel three cycles previous determined dilation of 23 wheel. The REPRODUCER continuously recorded 23 and 25 wheel settings. The card held 25 positions of key which, by sorting, permitted determination of exact point at which cycles began repeating (i.e., - branch points).

Size was 2'H x 3'L x 2'D plus 513 REPRODUCER, and rate was 100 characters per minute. It was dismantled.

Ref: Mr. S. Thorne

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

March 1954

TRANSPOSITION RECOGNITION DEVICES

TRANSPOSITION RECOGNITION DEVICES (AXEB/1) refers to a set of five relay units developed for use with IBM equipment for anagramming keyed columnar transposition systems. They were built by Army, section WDGAS-92, in the spring of 1946 to replace hand methods. Only one of each was built and all are now dismantled.

The RECOGNITION ANAGRAMMING DEVICE was used with a 513 REPRODUCER PUNCH to search a 4-column field for any of fifty 4-digit recognition groups which were wired on a 20 x 34 plugboard, and to punch a log weight into a card for each group recognized. By an earlier sorting, 5-digit material could be handled. The device consisted of 153 wire-contact relays, measured 2'H x 1'L x 2'D and operated at 100 cards per minute.

The COLUMN SELECTION DEVICE operated with a 513 REPRODUCER to select for reproduction one of ten columns in four fields simultaneously. Selection was controlled by a punch in a master card. The device consisted of 45 wire-contact relays mounted in a 20 x 34 plugboard cover and rate was 100 cards per minute.

The BINARY ARRANGING DEVICE operated with an NC-4 COORDINATING REPRODUCER to inter-compare 5 binary numbers and arrange them in order of magnitude. This rearranged set of 5 was punched back into the card it came from. In 1948, an automatic checking unit was installed. The device consisted of 35 relays mounted in a 20 x 34

~~CONFIDENTIAL~~

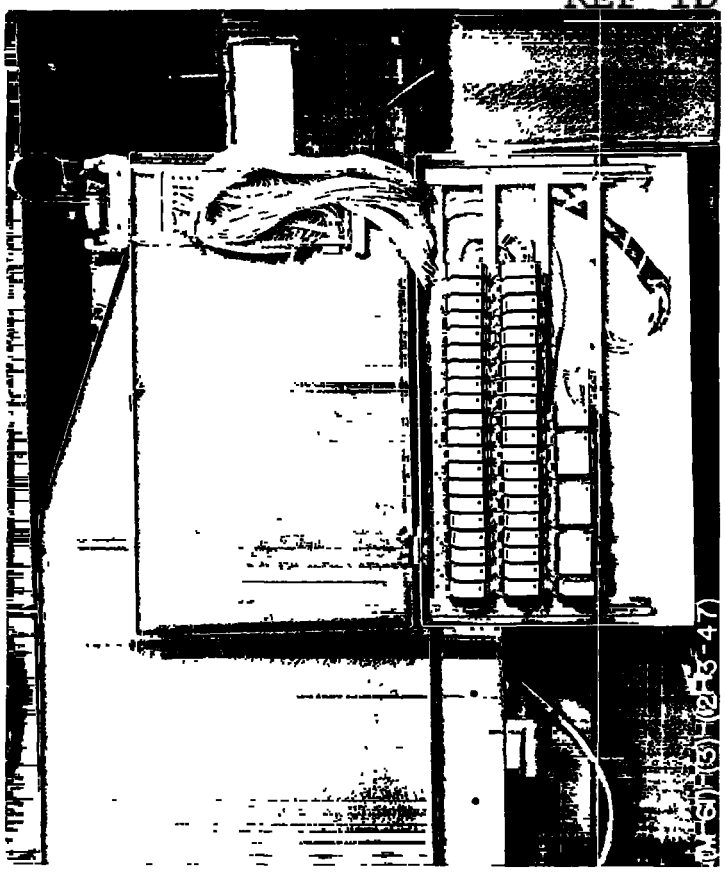
TRANSPOSITION RECOGNITION DEVICES (Cont'd.)

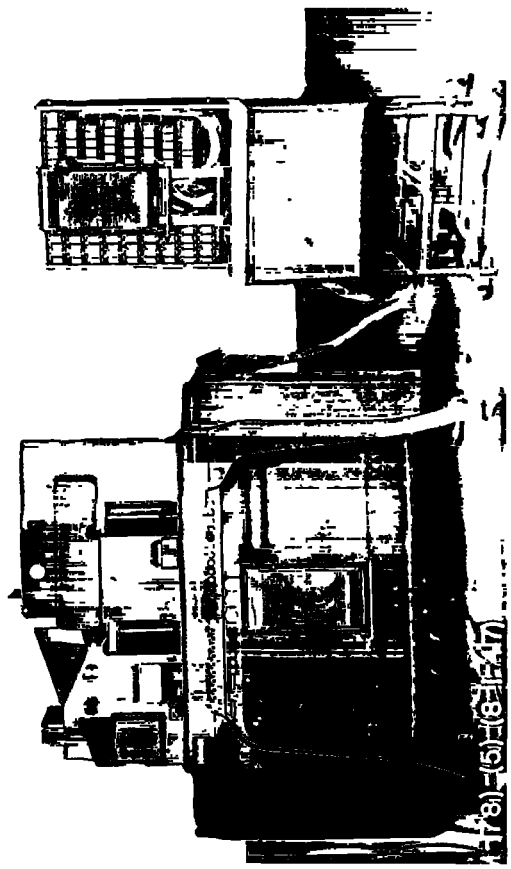
plugboard cover and operated at 100 cards per minute.

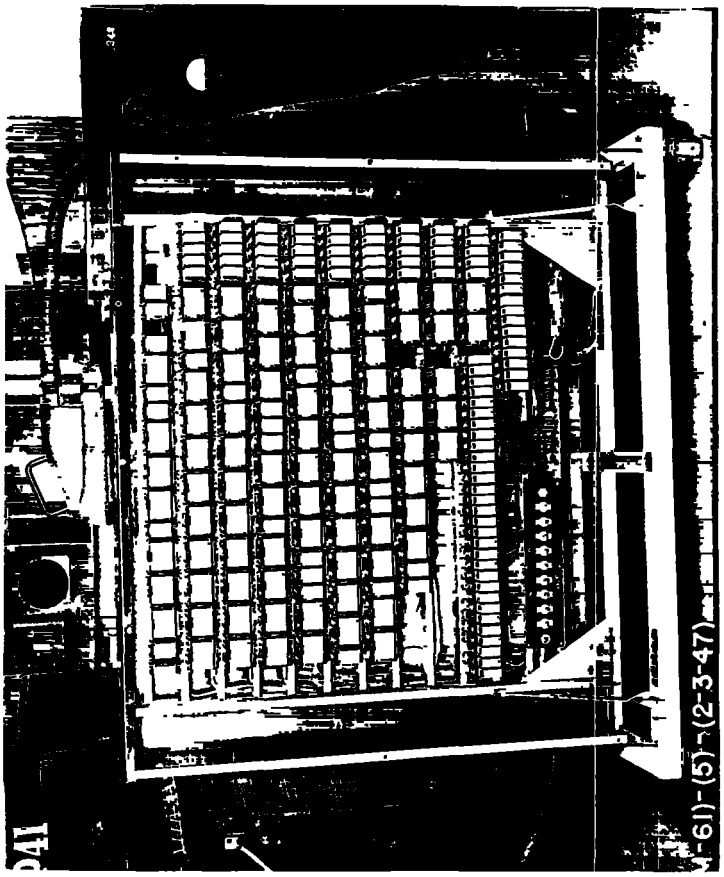
The BINARY DIFFERENCING and CHECKING DEVICE was usually used in conjunction with the BINARY ARRANGING DEVICE just described and an NC-4 COORDINATING REPRODUCER to calculate and check differences among the 5 binary numbers being arranged by the preceding device. It consisted of 38 relays in a 20 x 34 plugboard cover. For checking, the circuit was duplicated and the entire computation done twice. In 1948 these last two were rebuilt, housed in the same 2'H x 2'L x 2'D frame and called BINARY ARRANGING and DIFFERENCING DEVICE. Rate was 100 cards per minute.

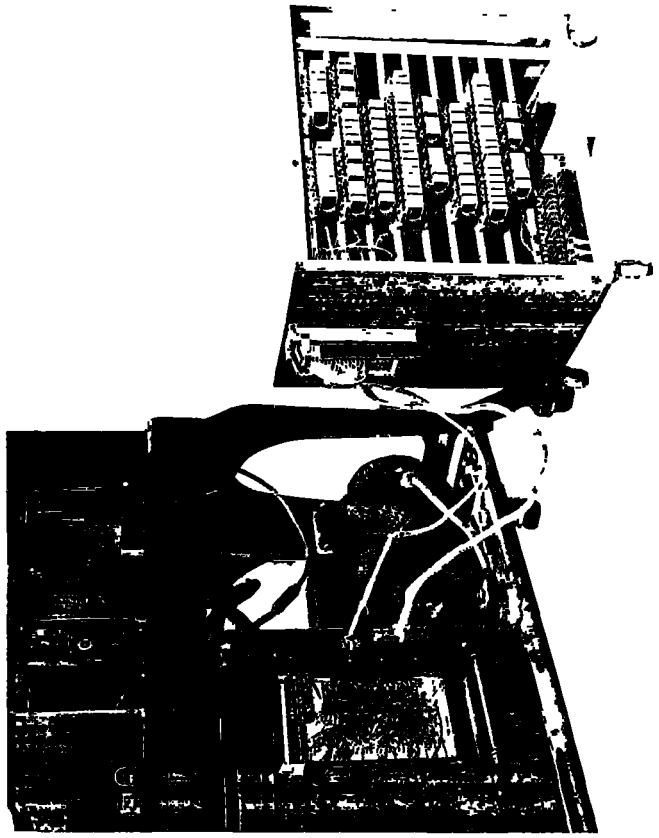
The COMMON SHORT-COLUMN IDENTIFICATION DEVICE was attached to a 405 TABULATOR and a 513 REPRODUCER which could do summary punching. It operated on the differences obtained by the preceding device to determine possible short column lengths common to the four binarily expressed differences. Lengths from 11 to 40 were recognized automatically and cases with no common length were passed over while favorable cases were listed on the TABULATOR. Differences over 255 were arbitrarily considered to have all lengths possible. The device consisted of 201 wire-contact relays and operated at 150 cards per minute. Size was 3'H x 3'L x 1'D. All these equipments have been dismantled.

Ref: Interim Report, JPAG No. 1236, Misc. 050
Machine Branch Annual Report, 1947
Mr. J. Powers
Mr. S. Thorne









TRANSPOSITION RECOGNITION DEVICES
AFEB/1

RECOGNITION ANAGRAMMING DEVICE (PENTANAGRAMMER)	lower right
COLUMN SELECTION DEVICE	upper right
BINARY ARRANGING and DIFFERENCING DEVICE	lower left
SHORT COLUMN IDENTIFICATION DEVICE	upper left

~~CONFIDENTIAL~~

March 1954

VIVIAN I-II

VIVIAN (AFSAF-12, D12B) covers a family of general purpose electronic comparators designed to [redacted] A study contract with Transducer Corporation, indicated that delay line circuits would be superior to magnetic binary circuits in a comparator and this led to VIVIAN I, known orginally only as MDL COMPARATOR, MERCURY DELAYLINE COMPARATOR, ASAF-12 (X-1), now AFSAF-12, or FLYING SAUCER. It was delivered in February 1951 by Technitrol Engineering Company. JENNY (AFSAF-13, PATTERNGENERATOR, ELECTRONIC PATTERN WHEEL) is the external companion key generator, built locally at that time.

A contract with Transducer Corporation in April 1950 produced the second member of the family, a MAGNETIC BINARY COMPARATOR or ASFA-12 (X-2), now AFSAF-D12A, which was only partically completed but never acquired the VIVIAN name. It failed its test and the contract was closed. VIVIAN II (AFSAF-D12B), a second delay line comparator using quartz crystals instead of mercury, is due for delivery by Denver Research Institute in April 1954. Plans were cancelled for a STORAGE TUBE COMPARATOR (AFSAF-49), a logical member of the family of electronic comparators which also never acquired the VIVIAN name.

~~CONFIDENTIAL~~

VIVIAN I-II (Cont'd)

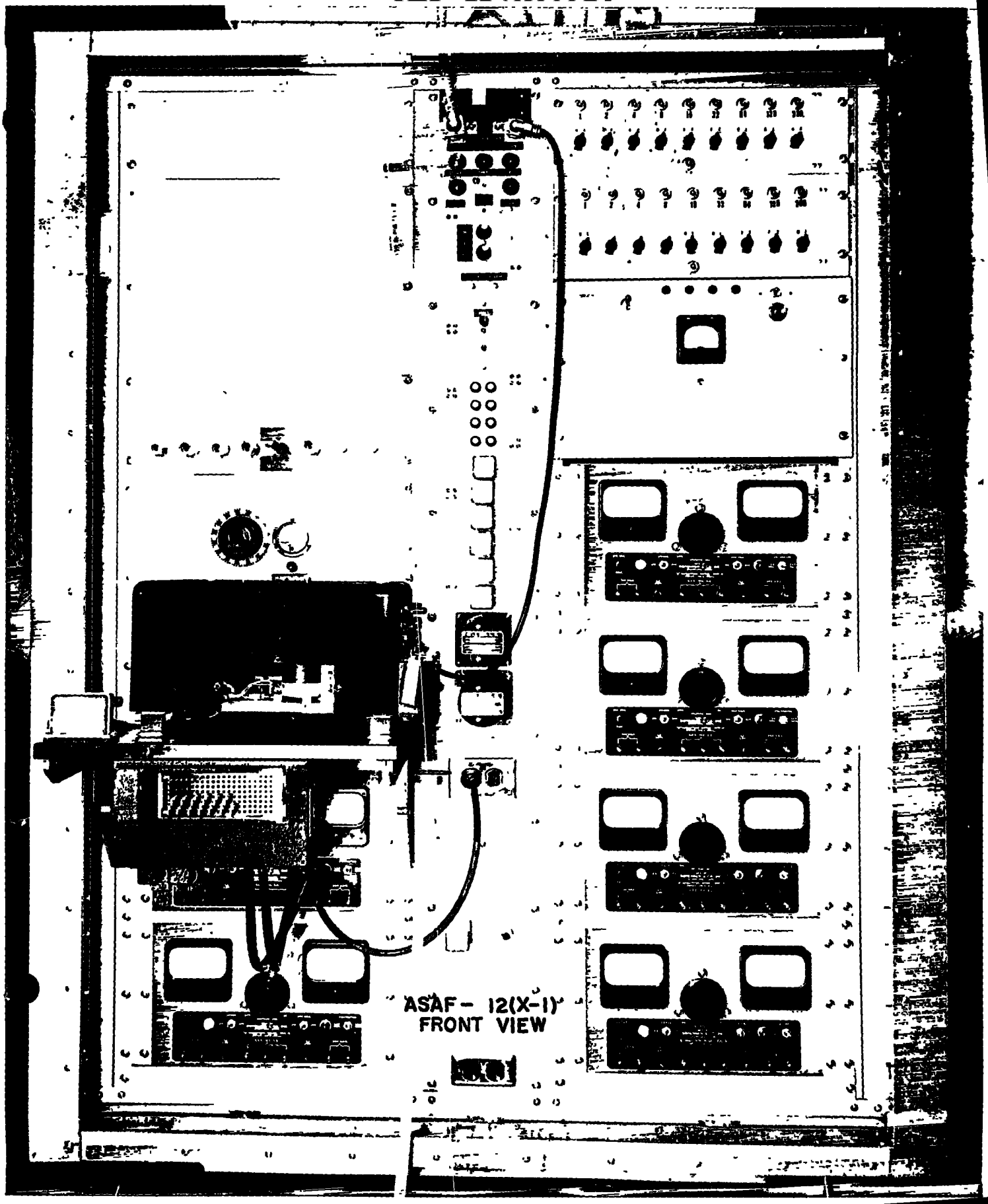
VIVIAN I is finding application to the HAGELIN problem,

[redacted] This sequence is cycled constantly at 2 kilocycles per second pulse rate. The pattern of as many as [redacted] Totals are matched against a preset threshold; when a hit occurs, the machine completes that comparison cycle and stops to indicate on lights for manual recording the interval setting together with the amount of excess over the threshold. The experimental AFSAF-D12A used a locally built pattern generator for input and an AFSAF-44 DIGITAL RECORDER for output.

VIVIAN II has a quartz delay line memory, used JENNY for input and offers several improvements. The most novel is a built-in osciloscope which at a hit displays the memory contents as a 20x25 array of bits on the scope face. New memory circuitry permits making use of short messages for faster cycling, the pulse rate ranging from 2 KC per second for messages 500 long up to 6.8 KC for messages 100 long.

VIVIAN I measures 7'H x 4'L x 2'D and VIVIAN II slightly more. The PATTERN GENERATOR, measures 7'H x 3'L x 2'D. At 2KC pulse rate, a 5-wheel cycle requires from 30 to 45 minutes. Model I is in use at Arlington Hall Station in room 1530-A and model II will operate nearby.

Ref: T/CA 16/51
Mr. W. Davidson
Mr. J. Russell
Mr. C. Schierlmann



ASAF - 12(X-1)
FRONT VIEW

VIVIAN I
AFSAF12 FLYING SAUCER
MERCURY DELAY LINE COMPARATOR

March 1954

WARLOCK I AND II

WARLOCK (AFSAF-D79=CXNK, AFSAF-D80=CXPB) is an electronic message setter capable of high speed decryption and statistical recognition of plain text roughness. Under task 18, Engineering Research Associates of St. Paul, Minnesota, completed Model I in February 1951; Model II is due for completion in November 1953. Model I has a 4-bit weighting matrix or weight shifter developed by Engineering Research Associates under task 24, URSA, and Model II has a similar one for 3-bit weights. The statistical evaluation unit, an accumulator, is completely general and could be built into other equipments.

Model I is specifically for Hagelin.

Output is to a CXCO regeneration typewriter. At a hit, the machine prints out window setting and excess over the criterion. An optional decryption print-out is available at the rate of 5 letters a second.

Model II is completely general, using five 32 x 32 matrices to simulate any wired rotor devices whose wiring and stepping patter are known. Its span is 80 characters, with provisions to use this as two sets of 40 characters. Size of Model I is a pair of cabinets totaling 7'H x 40'L x 4'D plus typewriter and power units occuping 1600 square feet of floor space.

WARLOCK I AND II (cont'd.)

Model II is U-shaped 40'L on an arm and about 6'H x 3'D, occupying 2400 square feet of space. Rate is 100 KC per second for both. The pair are being kept in St. Paul, available for operational use.

Ref: Miss M. Hobbs
Mr. D. Hogan
Mr. J. May

March 1954

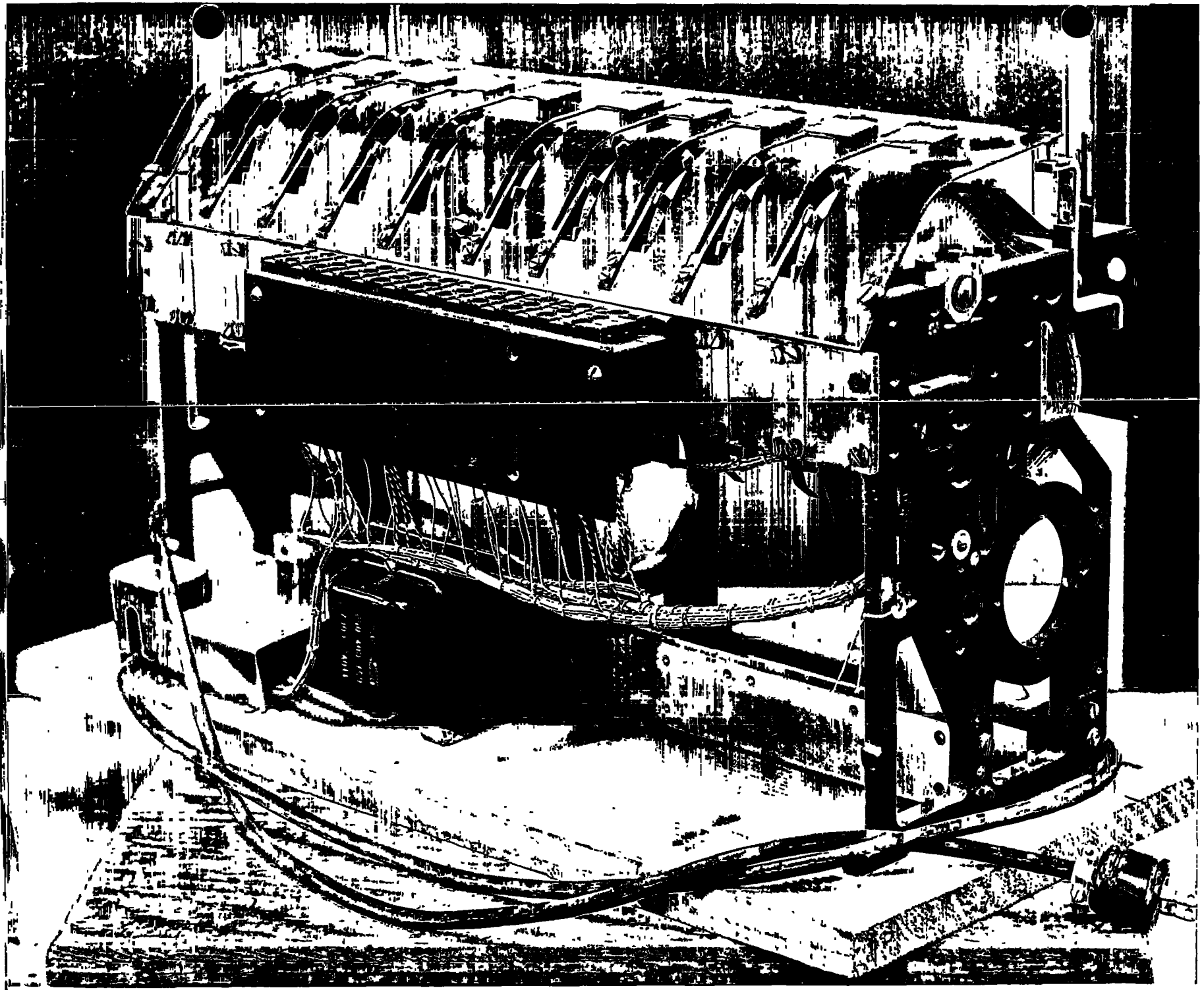
WORK-BACK MACHINE

The WORK-BACK MACHINE was a handtester for [redacted] on the T52C STURGEON, used to find the initial setting when break-in occurred in the middle of a message tape. It was built by NSA-82 in early 1950.

The device mounted 10 notched wheels (73, 71, 69, 67, 65, 63, 61, 59, 53 and 47 long) in a frame, permitting the operator to interplug them so as to control substitution or transportation, and to step them as desired by hand. Lights on the front panel indicated wheel notch activity to assist choice of settings at each branch point.

Size was 1'H x 2'L x 1'D and operation was at hand speeds. It was used at Arlington Hall Station and is now dismantled, its work being done by other devices.

Ref: Miss V. Collins
Mr. G. Stahly



WORK-BACK MACHINE

March 1954

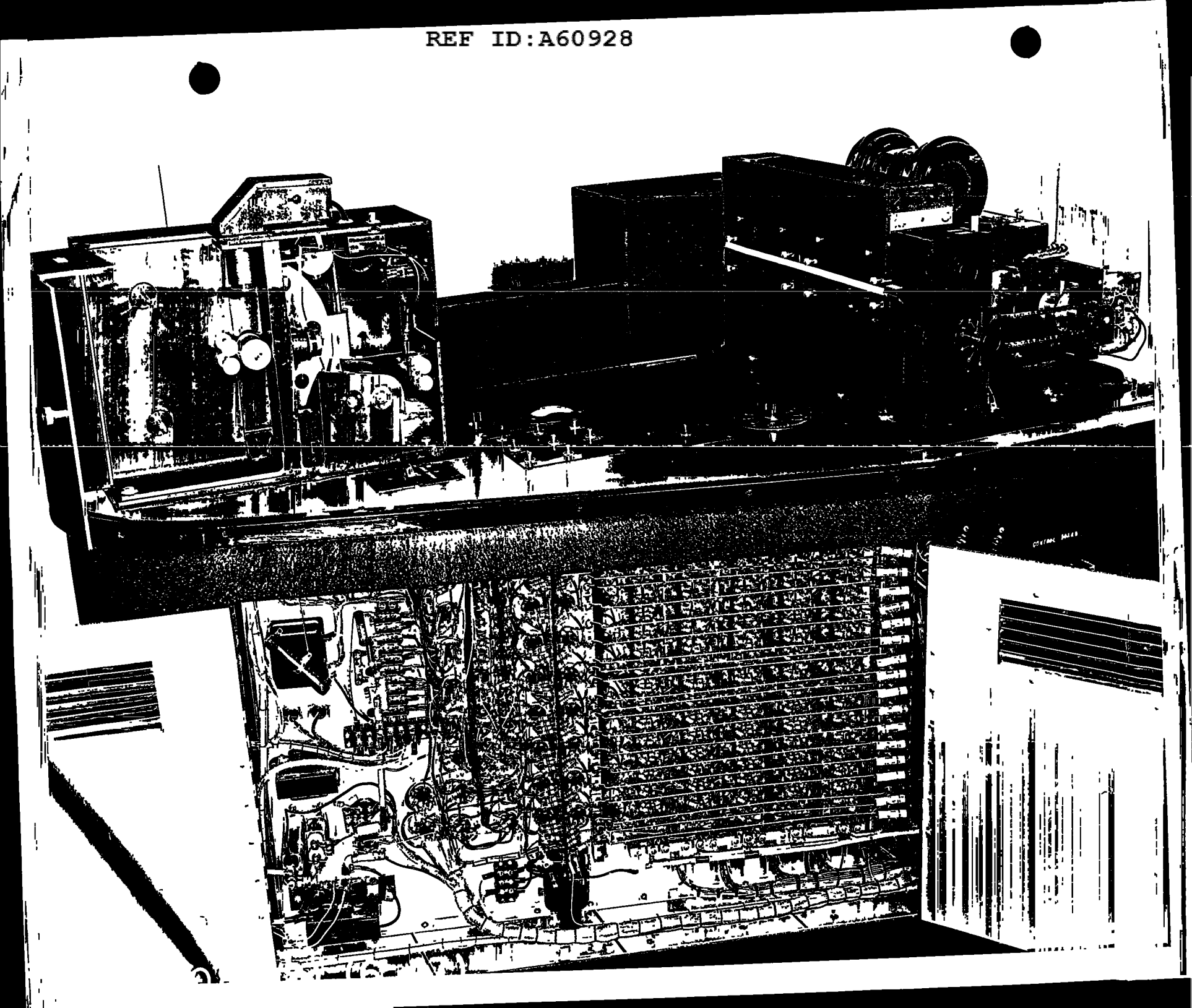
5202 COMPARATOR, MARK I

The 5202 COMPARATOR, MARK I (AFSAF-4, AXGQ/1) is a highspeed general purpose I. C. comparator to match photoelectrically a large volume of text on 35mm film. It was built for Army by Eastman Kodak Company in March 1945 and after satisfactory tests, was transshipped to GC and CS for use on the TUNNY problem for about a year. The associated camera, synchronized with a built-in key generator, is called AFSAF-4/1.

A pair of 35mm films containing literal or digital text is matched in a gate 80 deep by 500 wide. This field is usually considered as two fields of 40 x 500 and matched for high I.C. expressed as a ratio between the two fields. Weighting of scores is possible. Threshold is preset by a dial and at a hit the machine stops, permitting visual study and hand recording of approximate location. The camera was originally tape operated, but later modified to accept cards. Operation with a HAGELIN key generator unit has also been tried successfully.

The comparator measures 5'H x 2'L x 4'D plus a small counter unit and operates at 3000 frames per second. The camera with its built-in generator measures 4'H x 6'L x 3'D and exposes film at up to 635 frames per second. Since its recent overhaul and modification it is now available at Naval Security Station in room 20210.

Ref: MAC Outline #10
The 5202, ANCRAD Technical Paper
Mr. J. Deutsch



5202 GENERATOR and CAMERA, MARK I
AFSAF 4/1 AXGQ/1

CONFIDENTIAL

March 1954

70mm COMPARATOR

The 70mm COMPARATOR (AFSAF-2, CXCN, RAM-4) is a general purpose photoelectric comparator to count coincidence and pattern repeats between two texts punched into 70mm paper tapes. Probably the oldest of the cryptanalytic devices, its conception dates back at least to 1937 when M.I.T. built the BUSH MACHINE (named after Dr. Vannevar Bush), prototype to the 70mm COMPARATOR, and delivered it to Navy upon completion. It was used briefly and stored until 1942, then was used again until the first of the four COMPARATORS (CXCN), built by National Cash Register and Gray Manufacturing Companies, was delivered that year.

The second (AFSAF-2, RAM-4) was delivered to Army in August 1944, along with AFSAF-3, the associated punch. Including the BUSH MACHINE, five comparators and six punches were built. Reed Research, Incorporated, of Georgetown, D.C. delivered SIGMAGE (AFSAF-28, SIGMAGE CONTROL, PRINT SUPPRESSION DEVICE) to Army in September 1949 and a second to Navy in April 1950 for use with GOLDBERG which supercedes the 70mm COMPARATOR.

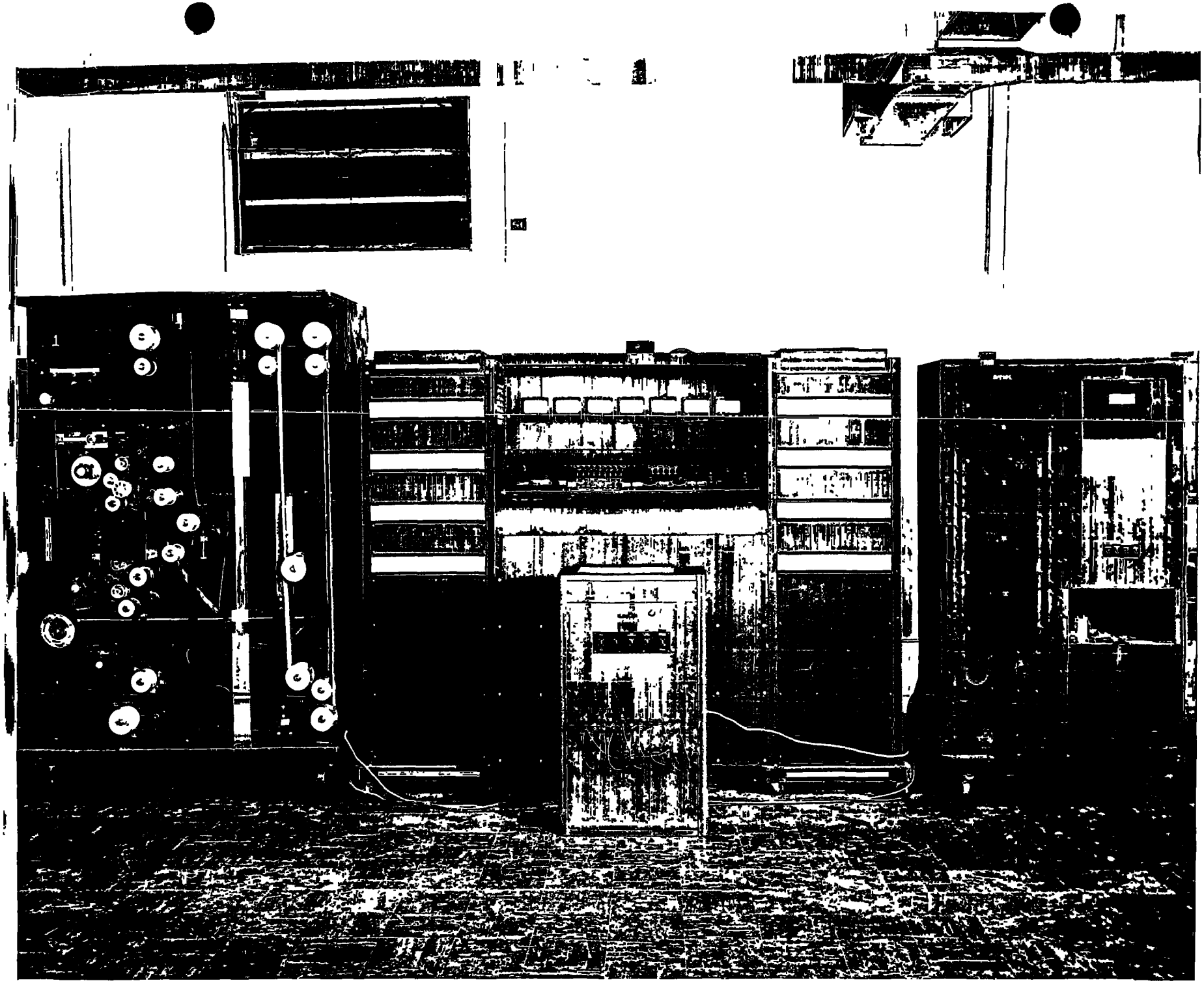
The machine matches two loops of tape, each holding as many as 2000 characters in the form of perforations in any of 32 levels. Required patterns or conditions of coincidence are preset on a plugboard. Twelve photoelectric cells scan the tapes at all offsets through a 10 column wide gate. Originally a record was printed after each cycle, but SIGMAGE permitted setting a threshold

70mm COMPARATOR (Cont'd)

and reducing recording to as few print-outs as desired. An optional circuit provides a means of stopping the machine when a particular event such as a pentagraphic repeat occurs.

Together, the three units which make up the COMPARATOR measure about 7'H x 9'L x 2'D. Comparisons are made at the rate of one offset tested in .4 seconds. All but one are dismantled, and that one is in the museum.

Ref: Brief Descriptions of R.A.M.
C.I.T. paper # 82
Lt. F. Sperberg
Mr. J. Stapleton



70mm COMPARATOR
AFSAF 2
"THE COMPARATOR," CXCN, RAM-4
used with
SIGMAGE (PRINT SUPRESSION DEVICE)
AFSAF 28 (center rear)

March 1954

701 EDPM

The 701 EDPM (ELECTRONIC DATA PROCESSING MACHINE, DEFENSE CALCULATOR) is an electronic parallel computer capable of mathematical and statistical functions. Serial 1, rented from International Business Machine Corporation, arrived in May 1953. There are plans for a Serial 2 in the coming year.

The computer operates in parallel on all bits of a word (digits of a binary number) simultaneously and can distinguish between two numbers by sign or size. Input is from cards by a printer type 711 CARD READER or from one of 4 magnetic tapes, all under program control. Output is to a 716 ALPHABETIC PRINTER and a 721 PUNCHED CARD READER. There are three types of memory storage. Cathode ray tubes provide the primary electrostatic storage holding $2^{11} = 2,048$ words of 36 bits each, with access time of 12 microseconds. Each of four magnetic drums holds $2^{11} = 2,048$ words with access time of 40 milliseconds. Each of four magnetic tapes holds up to approximately 1 million words with recall rate of 800 microseconds. Additional drum and tape units may be added. Various standard IBM equipments provide for interchange of media.

Control is much the same as in ATLAS, with addresses advancing one each time unless specifically altered. The arithmetic unit contains a 38-bit accumulator, a 36-bit M-Q register (for Multiply-Quotient) and a 36-bit memory register serving the same function as

the X-register in ATLAS I. The 36-bit words may be handled effectively as two 18-bit words if desired. There are no special analytic orders. Programming is based on a single address system.

Physically, the machine consists of 12 units ranging from a 3'H x 3'L x 2'D card reader to a 6'H x 7'L x 3'D calculator unit, in total requiring about 1500 square feet of floor space. Pulse rate is 100 KC, affording 16,666 additions or 2,192 multiplications per second. It is in operation at Arlington Hall Station in room 1730-A.

Ref: NSA-82 files
Mr. J. Hyduke
Mr. P. Johnson
Mr. J. Young

~~SECRET~~

Brief Descriptions of Analytic Machines
Third Installment

NSA-34
NSA-35
2 August 1954
Wheatley, LeRoy H.

This third installment consists wholly of photographs. Further Briefs, completed since issuance of the Second Installment, will presently be distributed as Fourth Installment. These 8 x 10 prints total 88 and are to be interleaved with your copy of BDAM. Briefs on the remaining equipments are still to be published, along with some republications and a list of corrections.

The correspondence between prints and Briefs is, in most cases, obvious (a print of ABEL to be filed back of the ABEL write-up). Aside from these there are two categories must be listed.

(1) Prints for which the related Brief is yet to be published, and which therefore are to be held and filed later:

Print	Brief to be published
✓ DEMON	DEMON
✓ DELTA-DOT-CROSS COUNTER	FREQUENCY COUNTERS
✓ HORACE	FREQUENCY COUNTERS
✓ GYP	GYP
✓ HAGELIN C-38 ANALOG (original)	HAGELIN C-38 ANALOG
✓ HAGELIN C-38 ANALOG (serial 5)	HAGELIN C-38 ANALOG
✓ HAGELIN WINDOW SETTING GENERATOR	HAGELIN WINDOW SETTING GENERATOR
✓ M-9 HANDTESTER	HANDTESTER
✓ JOHN	JOHN
✓ MADAME X	MADAME X
✓ Navy BOMBE	Navy BOMBE
✓ PEELER	PEELER
✓ PLAINTEXT RELAY ANALOG	PALLY
✓ PYTHON	PYTHON
✓ TAN KEY GENERATOR	TAN KEY GENERATOR
✓ HORIZONTAL DIFFERENCER	TAPE COMPARATORS
✓ VIPER	VIPER

~~SECRET~~

~~SECRET~~

(2) Prints whose title does not correspond exactly to the title of the related Brief:

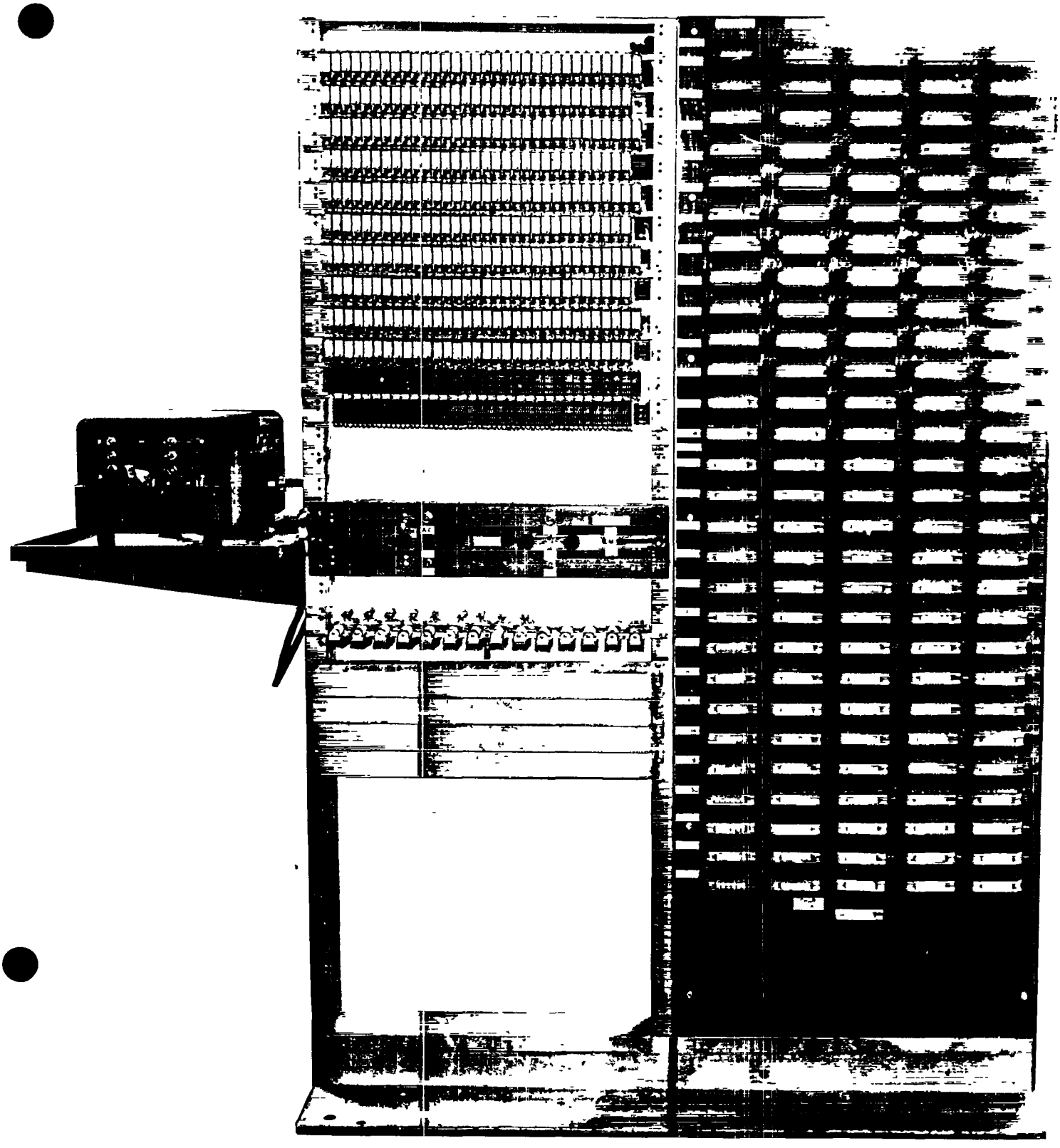
Print	Brief
JUNIOR BRUTE FORCE	BRUTE FORCE DEVICES
HAGELIN SETTING LOCATION DEVICE	GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE
SINGLE WHEEL CHAINING DEVICE	GENERAL PURPOSE 100 WIRE CONTACT RELAY GATE

REF ID:A60928

[redacted]

DEMON II
AFSAF 77
CINS
serial 2

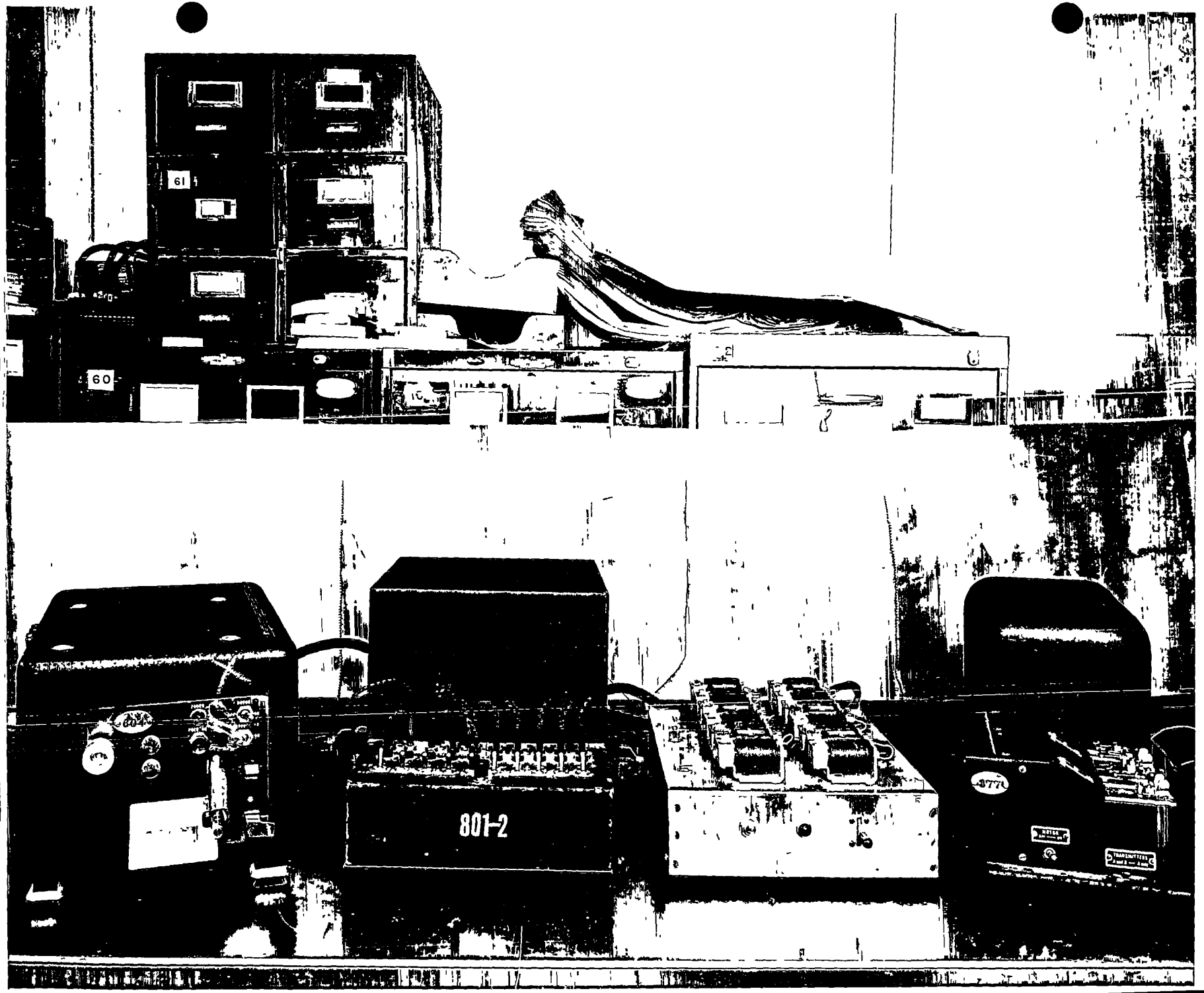
~~CONFIDENTIAL~~



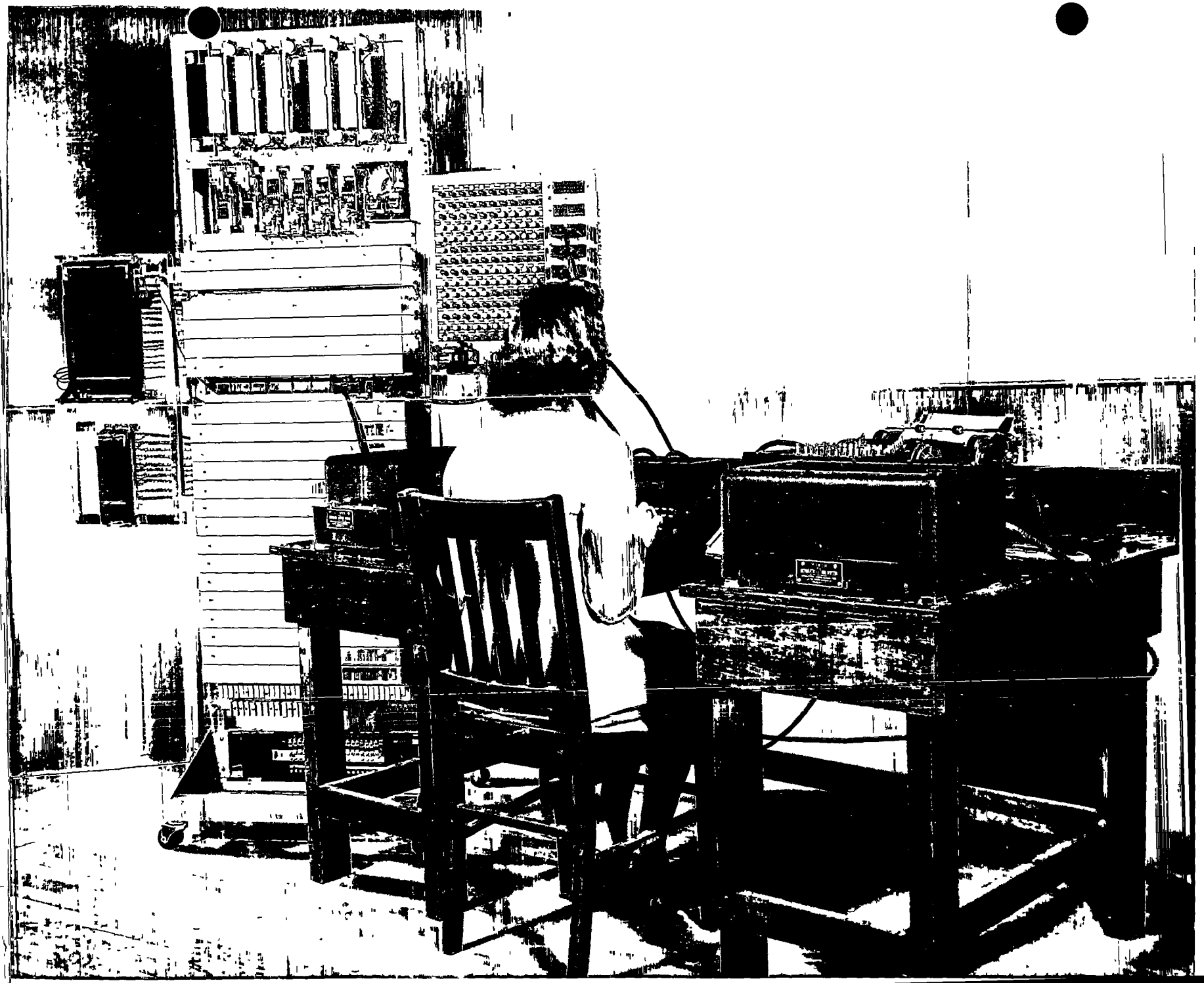
DELTA-DOT-CROSS COUNTER
AFSAF D56
one of the many FREQUENCY COUNTERS


HORACE

HORACE
AFSAF 116
(left) with 407 TABULATOR

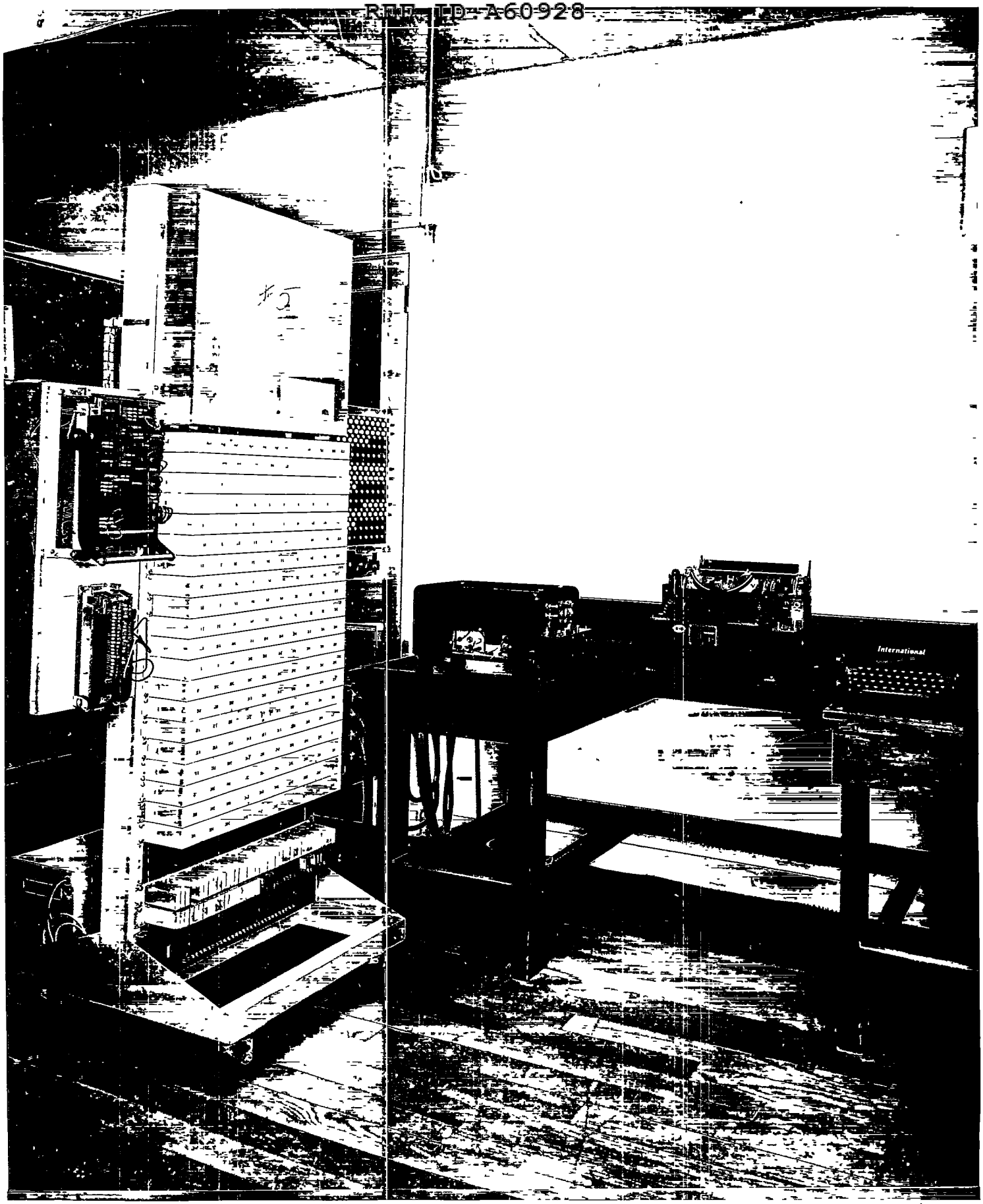


GYP
(originally
KEY COMBINER)
STURGEON model



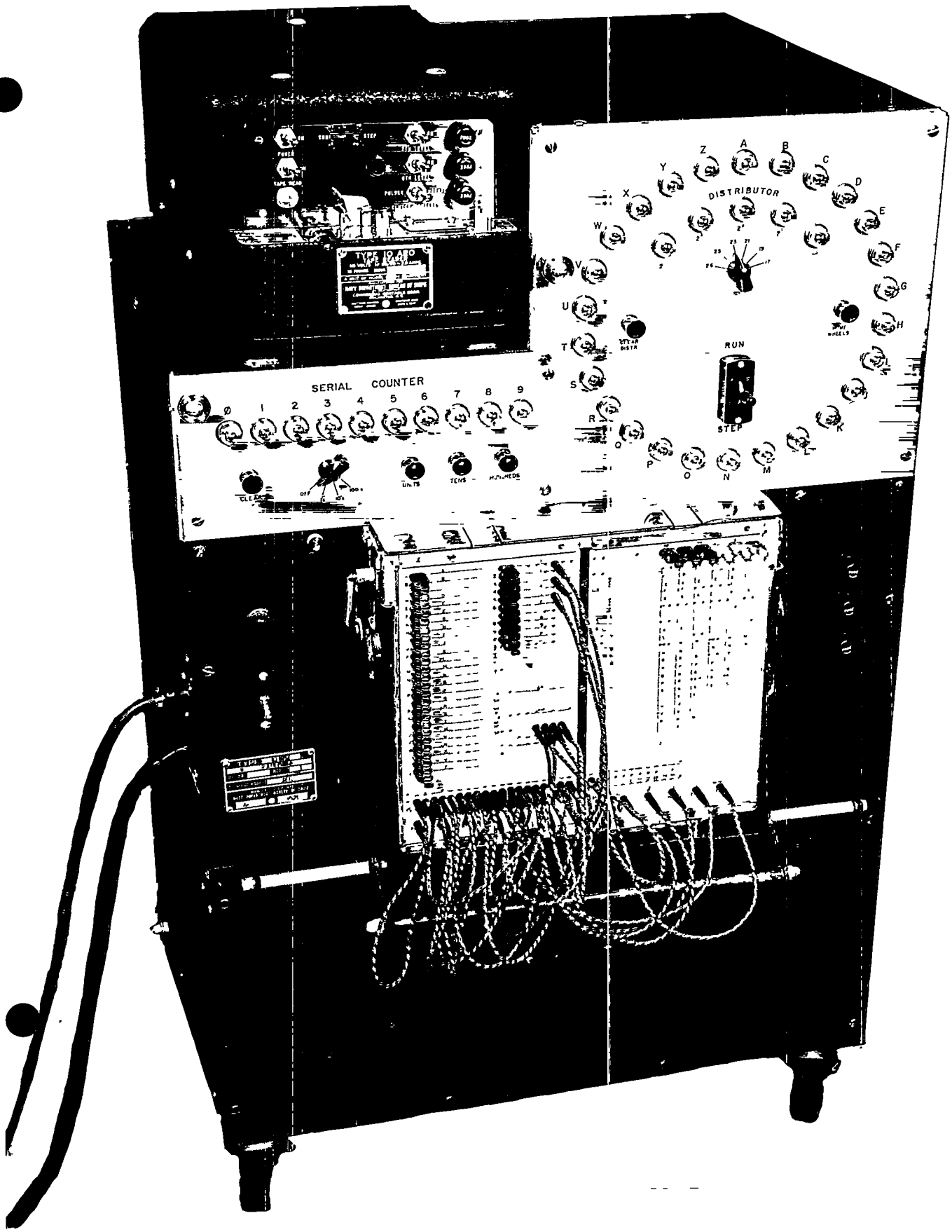
~~TOP SECRET~~

~~FROTH~~

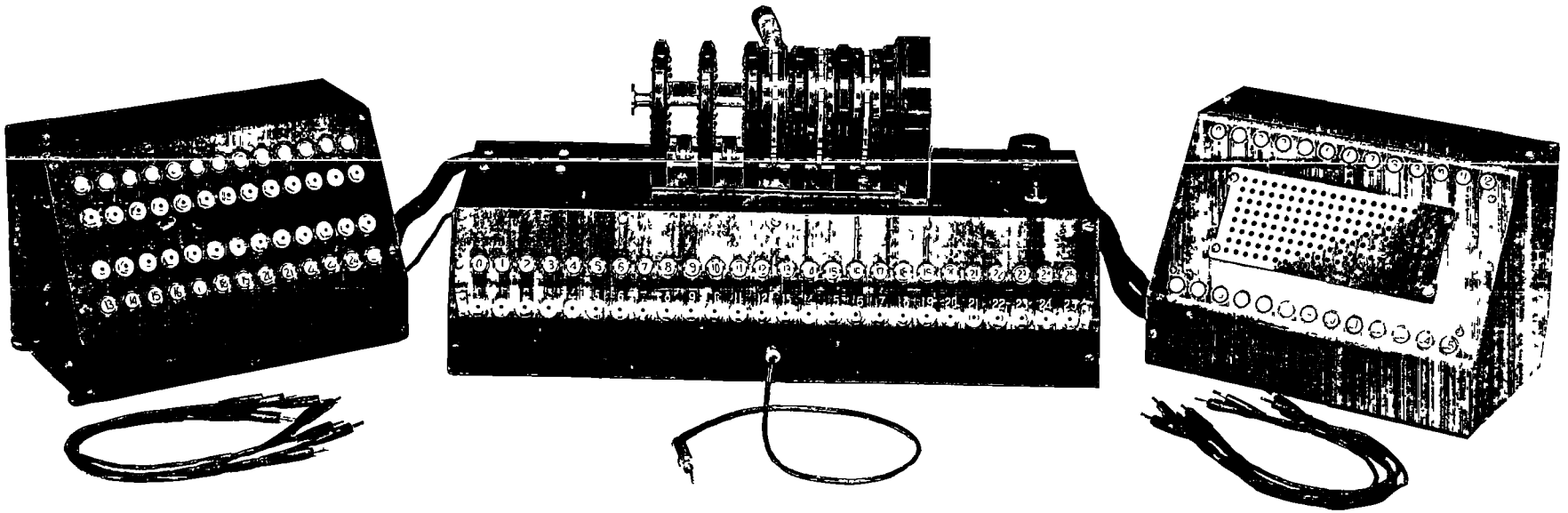


HAGELIN C-38 ANALOG, serial 5
AFSAF 105 ELECTRIC HAGELIN, HAG

TOP SECRET
FROTH

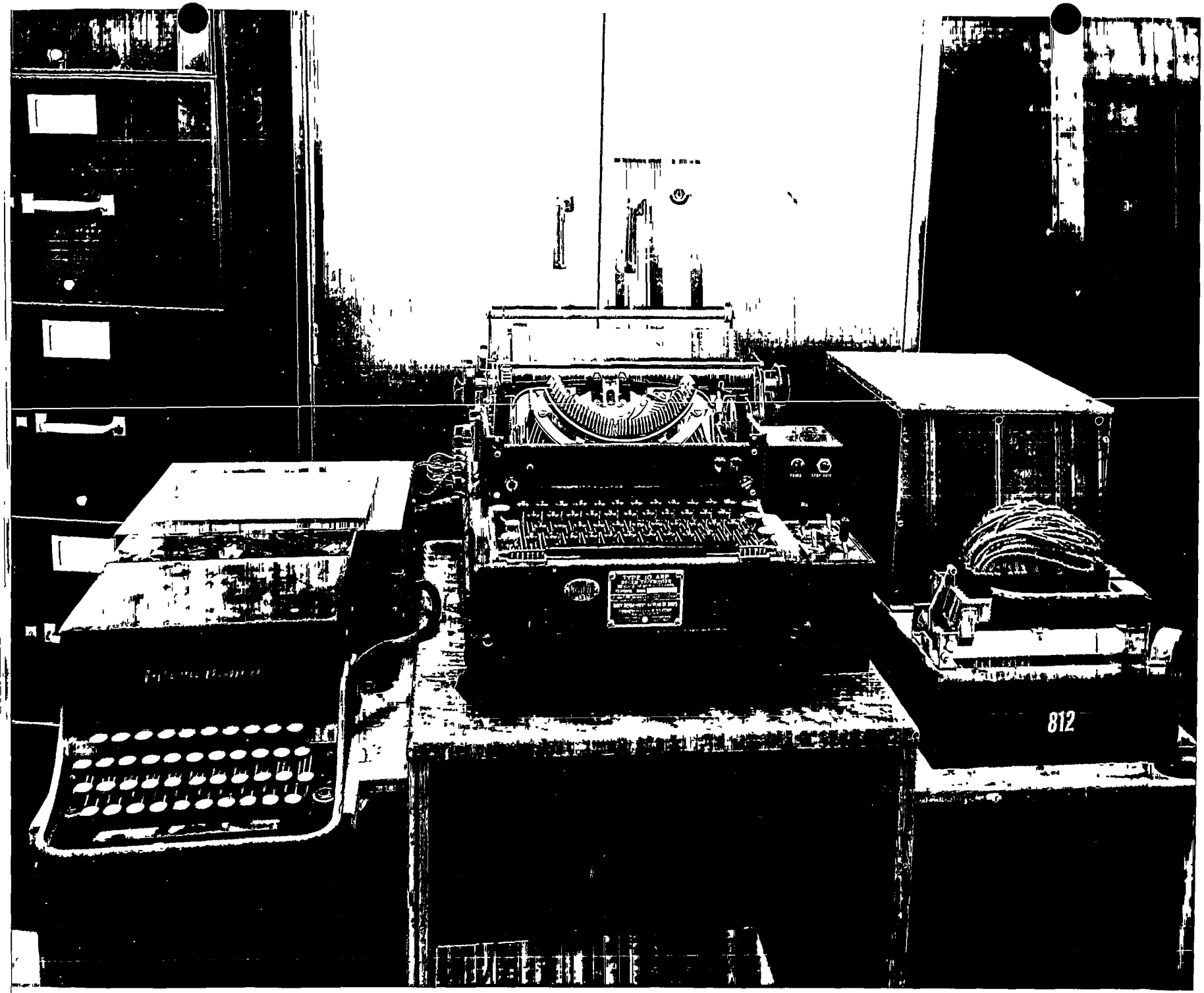


HAGELIN WINDOW SETTING GENERATOR



M-9 HANDTESTER
N-550, N-1800, N-2400
with BOA WHEEL (N-2300)
in third position

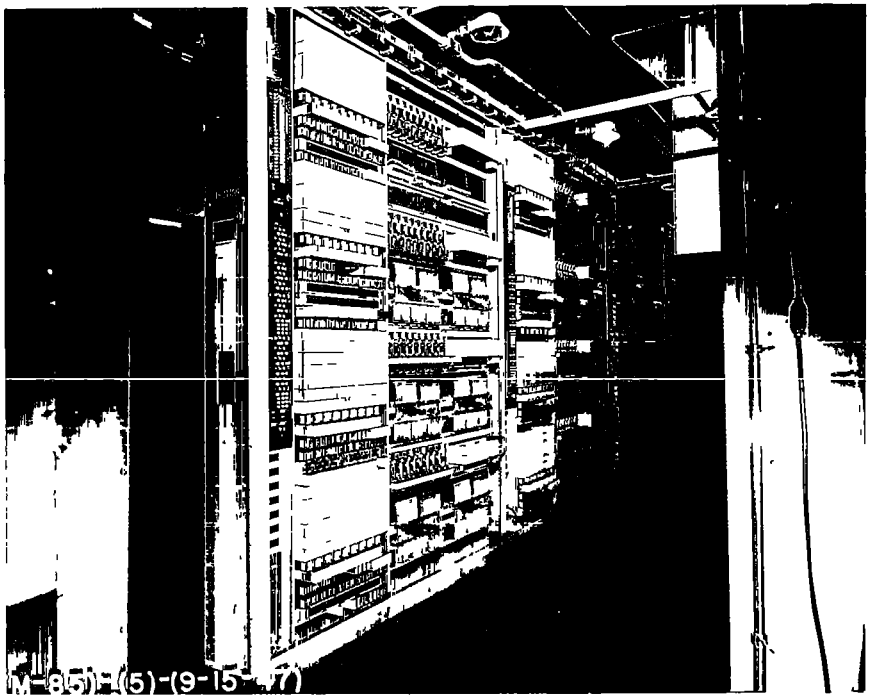

JOHN



KEY SYNTHESIZER
(STURGEON)

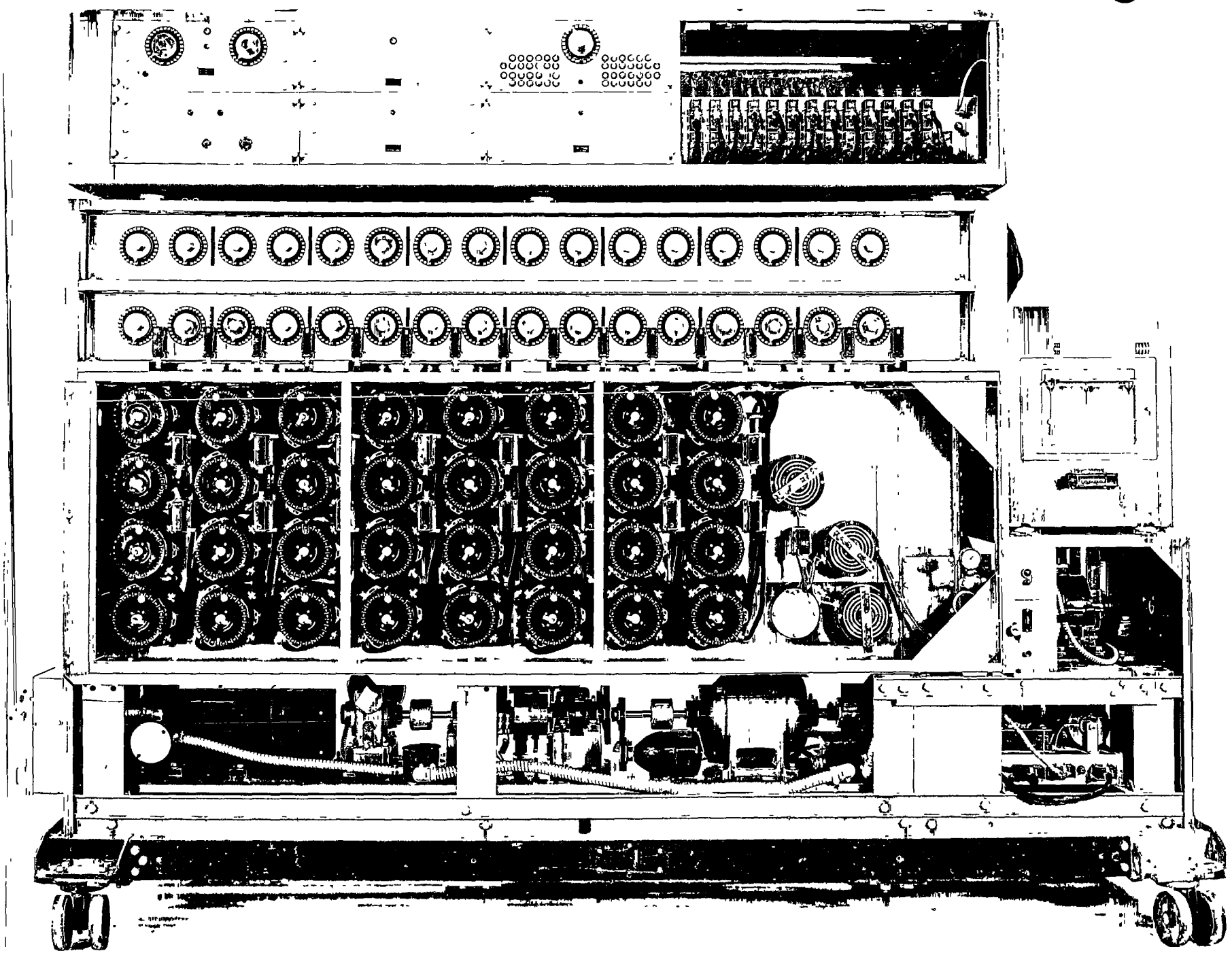
~~TOP SECRET~~

~~FROTH~~

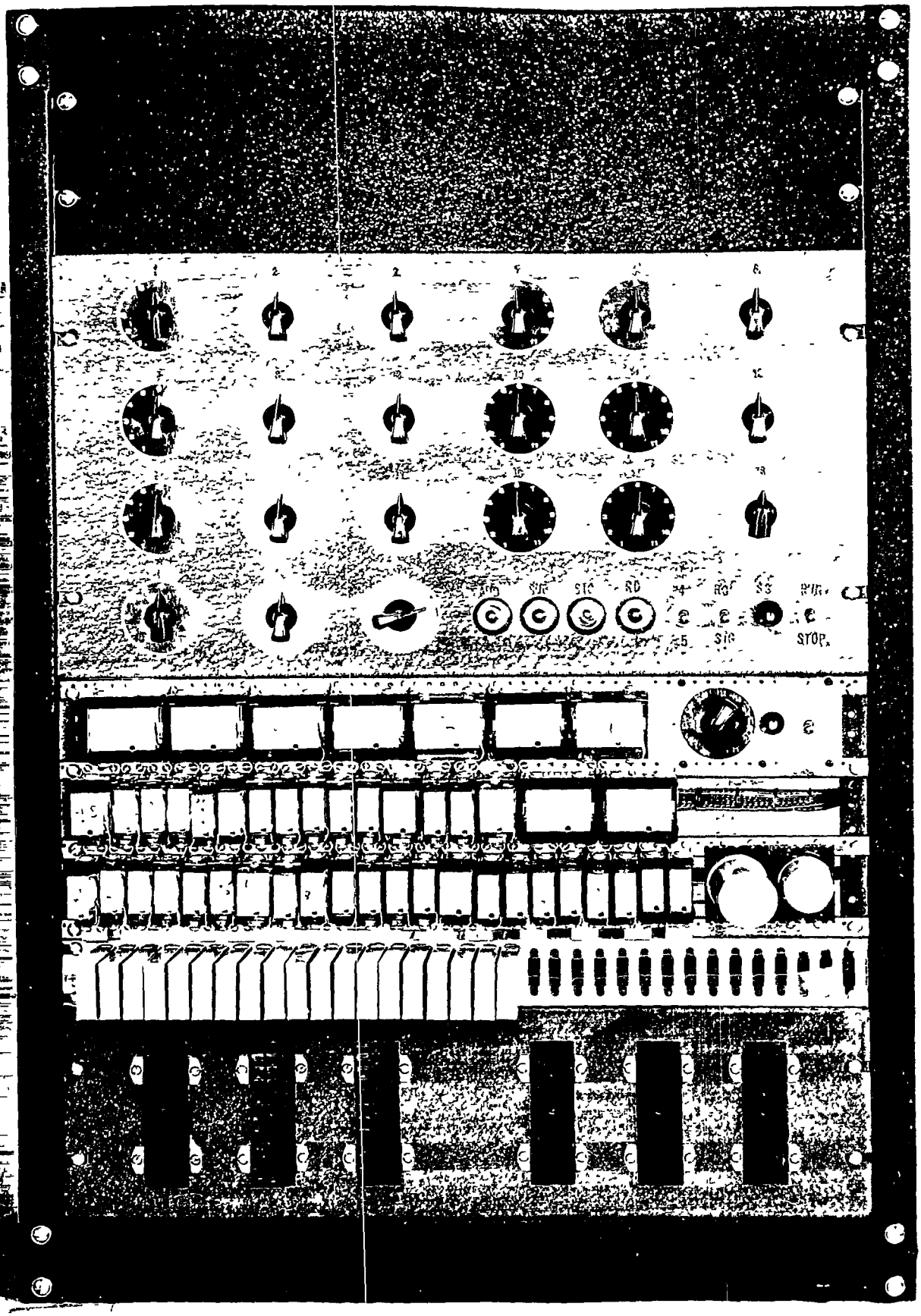


MADAME X
AFSAF 14
ARMY BOMBE, 003 RELAY BOMBE, AXCQ/1
turret controls & printers (left) and
a bay of BOMBE racks (right).

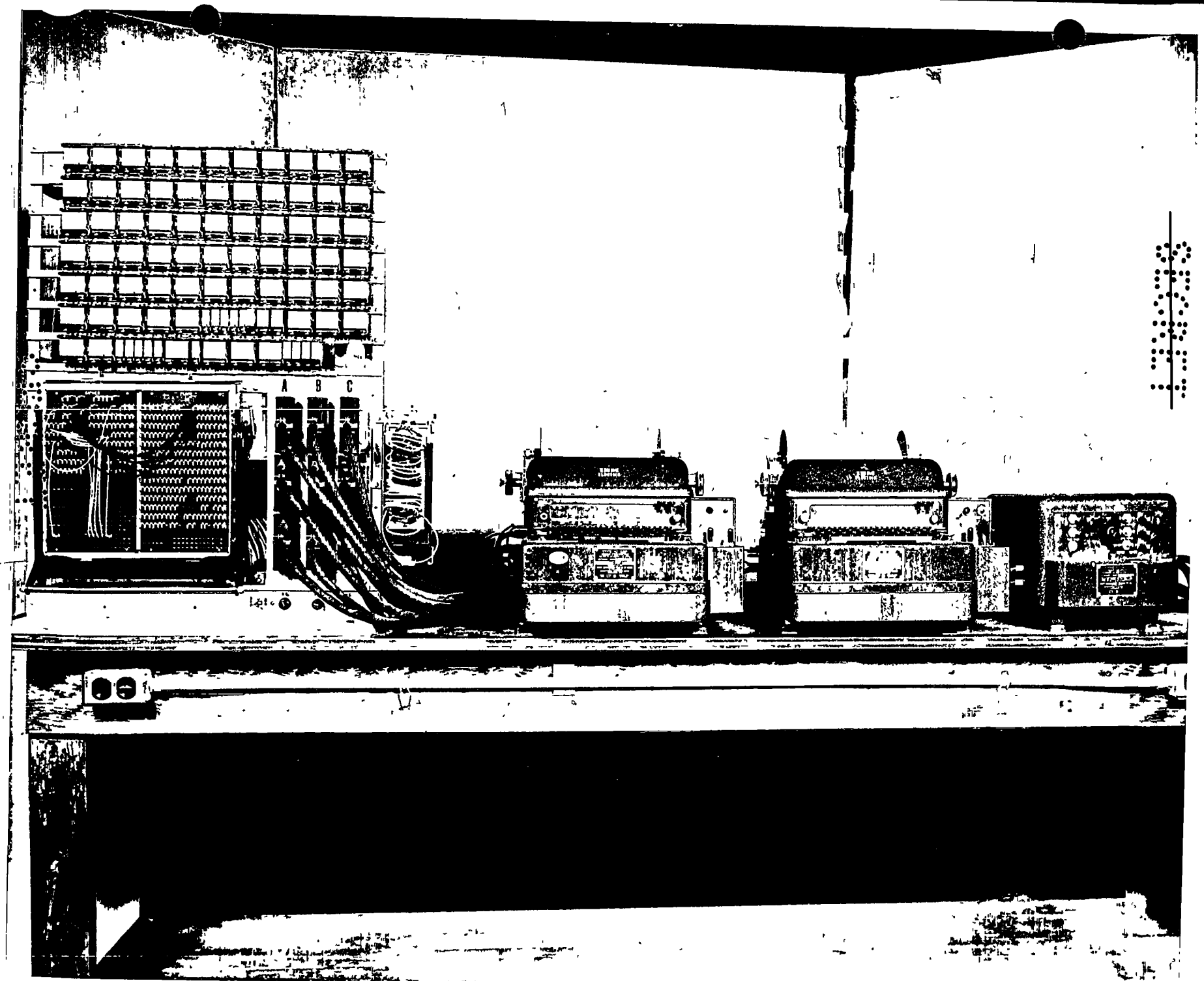
REF ID:A60928



NAVY BOMBE
AFSAF 23, CXNQ, N-1530

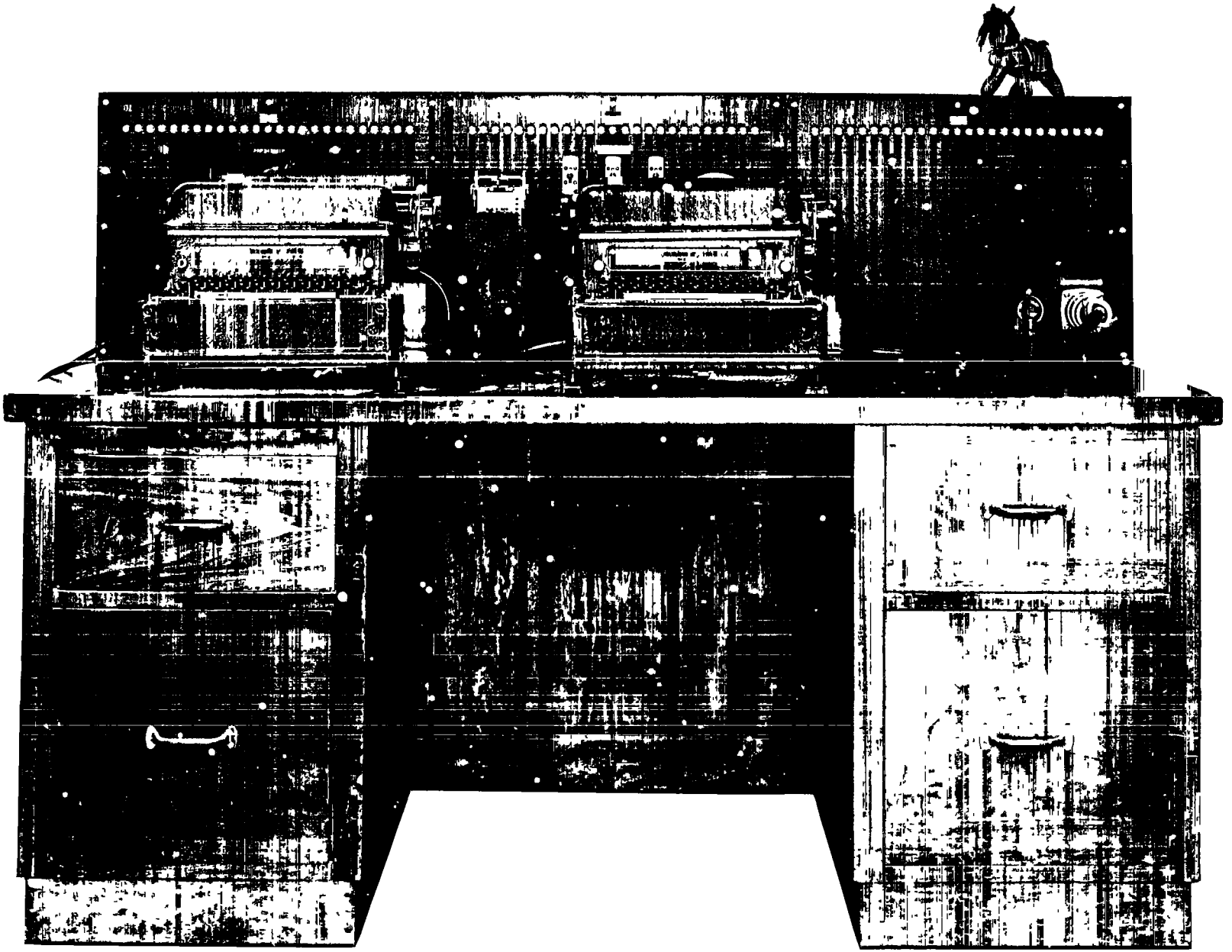


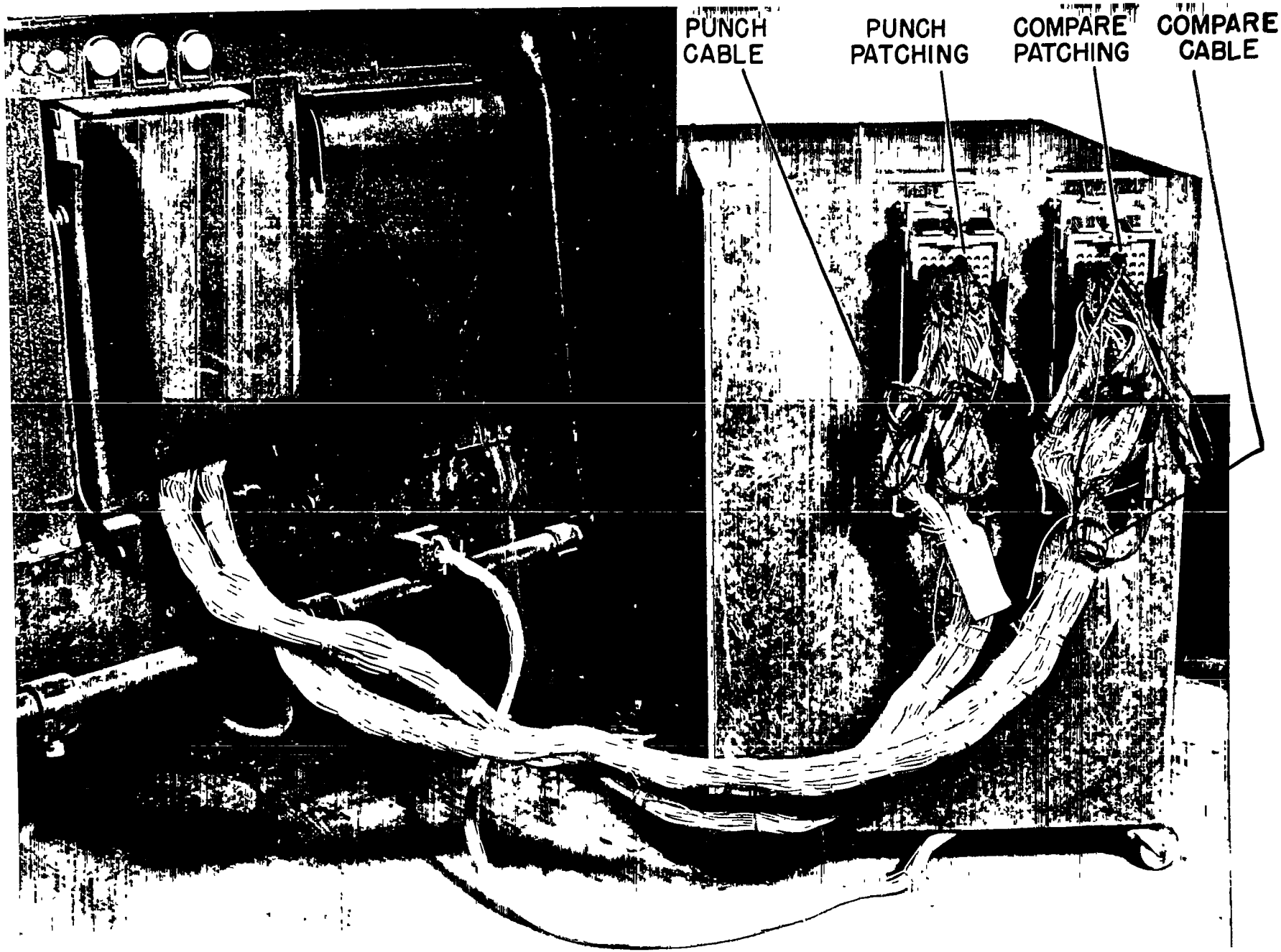
PEELER
AFSAF D 109
(erroneously called HATCHET)



PLAIN TEXT RELAY ANALOG
prototype to CHUMMY (AFSAF D97A)
related to: PALLY equipment

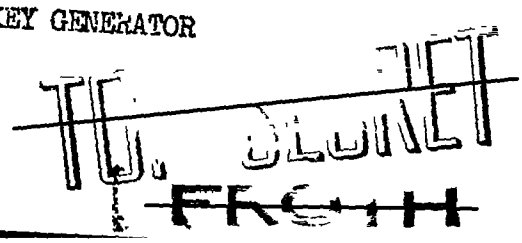
~~SECRET~~





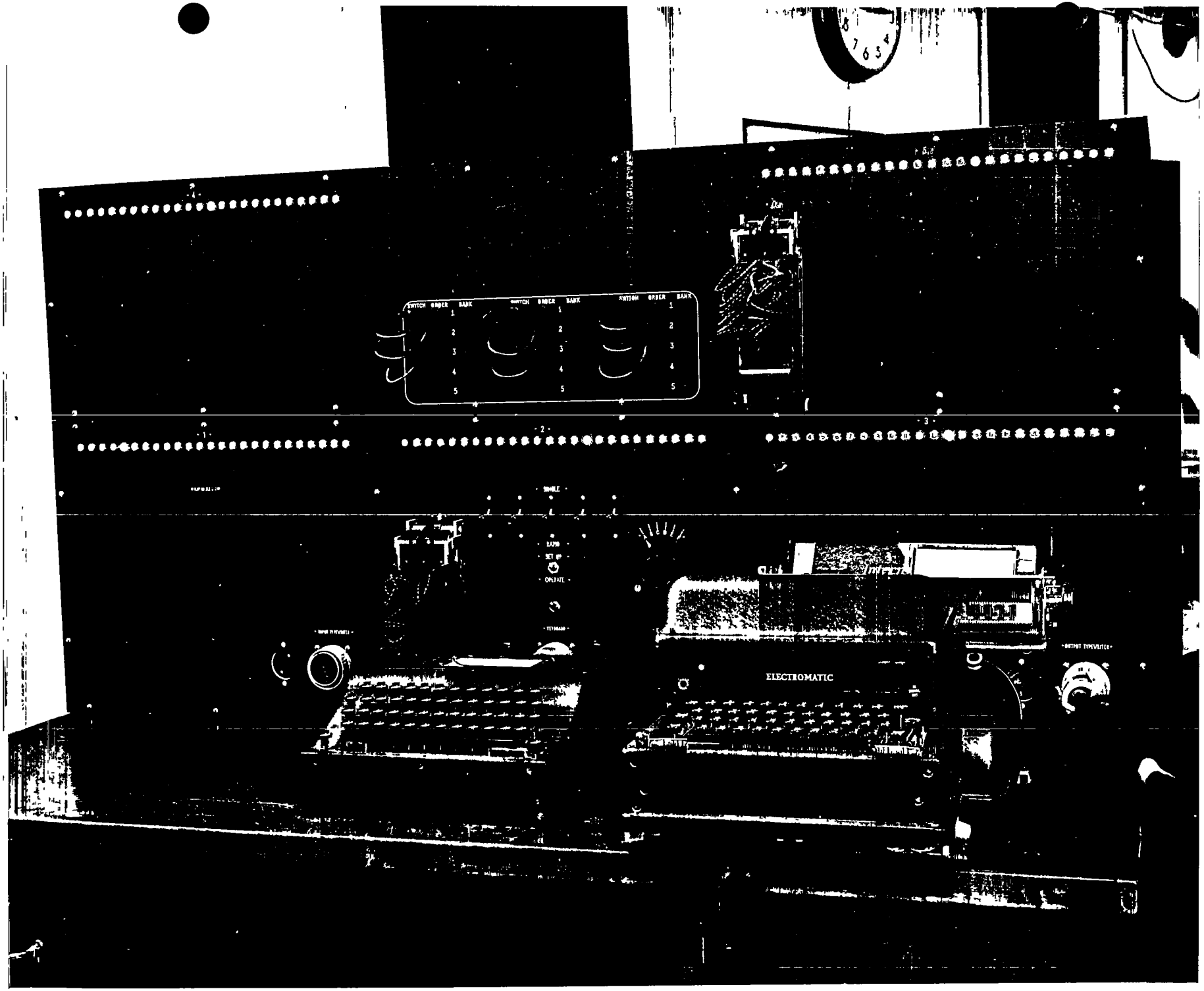
TAN KEY GENERATOR

TAN KEY GENERATOR




READER
AUTOMATIC LETTER WRITER
13851
A
A4
A5
A6
D1
D2
C4
C5
C6
PUNCH

HORIZONTAL DIFFERENCER



VIPER
CXMT, N-900