TOP SECRET

HISTORY OF CONVERTER M-134-C

VOLUME 1

TOP SECRET

HISTORY OF CONVERTER M-134-C

TOP SECRET

TABLE OF CONTENTS

DETAILED TABLE OF CONTENTS
FOR
VOLUME 1

LIST OF TABS IN VOLUME 1

HISTORY OF CONVERTER M-134-C

CHAPTER I. INTRODUCTION

For photographs of Converter M-134-C, see Tabs A, B and C. For additional photographs, see Vol. ___, Tabs ___, ___.

A. General
(Summary)

Converter M-134-C is an electromechanical, transportable, cipher machine used in permanent and mobile message centers for the purpose of automatically enciphering and deciphering messages, both tactical and administrative, with speed, accuracy, and security. It was introduced into the military service shortly after the entrance of the United States in World War II. Because of its extremely high degree of cryptographic security coupled with its transportability and its adequate speed of 25 to 50 words per minute, it became the "backbone" of Army and Navy joint and individual cryptographic communications. Navy nomenclature designated the machine as ECM Mark II (short title: CSP 888/889) and Army nomenclature designated it as Converter M-134-C (short title: SIGABA). According to the new Army nomenclature plan, its designation has been changed to ASAM 1. Since it was known in the Army as Converter M-134-C during the most important phase of its existence, World War II, it is referred to in this history by its earlier Army nomenclature.

The history of Converter M-134-C necessitates following two important cryptographic principles through a rather intricate develop-

ment. The first of these principles is encipherment by means of an electric current passing through a series of cipher wheels or rotors.[1] The second of these principles is concerned with how these enciphering rotors step. In Converter M-134-C the two principles, which constitute the basic cryptographic phenomenon of Converter M-134-C, are given physical embodiment by means of 15 rotors contained in a removable cipher basket (short title: SIGIVI). These 15 rotors are arranged in three rotor banks (see photograph, Tab C): 5 of these rotors are the enciphering rotors (marked 19, Tab C), which convert a plain-text letter into a cipher-text letter by means of an electric current passing through this 5-rotor cipher maze. The remaining 10 rotors are composed of two groups: a group of five rotors, called control rotors (marked 18, Tab C), which step in metered fashion, and a group of five small stationary rotors, called index rotors (marked 17, Tab C). Electric currents pass through the control and cipher rotors (marked 18 and 17, Tab C), successively, in order to produce simulated random stepping of the five rotors (marked 19, Tab C) which accomplish the enciphering. Briefly, the two concepts to be traced are

(1) encipherment by means of electric current through a rotor maze, and

(2) random stepping of the enciphering rotors.

(These two cryptographic concepts are further explained in Section B of this chapter.)

1. For an explanation of the cryptographing functioning of a rotor; see page .

The two important cryptographic principles listed just above were not suddenly conceived, and once they were conceived, mechanical and electrical applications of them were made separately and inadequately on early models long before they finally evolved into the cryptographic, electrical, and mechanical perfection of Converter M-134-C. The experimental and adopted models in the direct line of cryptographic development which culminated in Converter M-134-C are as follows: Hebern Cryptograph (first Hebern device presented to Chief Signal Officer in 1923); Converter M-134-T1 (conceived about 1926 and built between 1930 and 1933), Converter M-134-T2 (conceived about 1933 and built in the same year); Converter M-134 (the adopted form of Converter M-134-T2); Converter M-134-A (first built in December 1939), and Keying Unit M-229 (proposed in 1941 as new means of stepping the rotors of Converter M-134, M-134-A). The exact manner in which each of these experimental and adopted models is in the direct line of cryptographic development which culminated in Converter M-134-C can be seen only by understanding the details of each. Such details are given in the separate chapters which concern each model. (To locate the chapter concerning any particular model, see index.)

B. Cryptographic Functioning of Converter M-134-C

In order that the reader may have a better understanding of the cryptographic concepts to be traced, it is necessary to present here a brief description of the manner in which Converter M-134-C converts a plain-text letter into a cipher-text letter. Physically, the electro-

mechanical Converter M-134-C consists of the following main component parts: a keyboard, a printer unit (8, Tab A; 9 and 10, Tab B), a controller (3, Tab A), and a cipher unit (2, Tab A; 17, 18, and 19, Tab C). The functions of the keyboard and printer unit are obvious: When a key of the keyboard is depressed, it causes the printer unit (10, Tab B) to print on the tape either the same plain-text letter or an encipherment of that letter according to the position of the controller (3, Tab A). The controller is a switch (3, Tab A), the main function of which is to switch the current through the cipher unit so that encipherment ("E" position) or decipherment ("D" position) will occur, or to switch the current directly to the printer unit so that plain-text letters will be printed exactly as typed ("P" position).[1] The cipher unit (short title: SIGIVI) consists of six rigidly mounted bakelite separators which form a support for the three rotor shafts (17, 18, 19, Tac C). The purpose of the unit is to support the index (17, Tab C), control (18, Tab C), and cipher rotors (19, Tab C) in much relative positions that electrical circuits are formed through each row of rotors. The five small rotors in the front row (17, Tab C) are called index rotors. The index rotors can be moved manually only. The five rotors in the middle row are known as control rotors (18, Tab C). The three middle control rotors step in metered fashion (see footnote 1, page 2) and

1. The only other position of the controller besides the Off ("O" position) is the Reset position ("R"). When the controller is in the "R" position and the Zeroize-operate key at "Zeroize," the effect is automatic advancement of the rotors until they all present the letter "O" at the bench mark.

the two end control rotors remain stationary during encipherment and decipherment. The five rotors in the rear row are known as the cipher or alphabet rotors. All five cipher rotors step in an irregular manner during encipherment and decipherment.

To properly encipher a message, the three sets of rotors must be arranged and aligned in such a way that the arrangements and alignments can be reproduced by the deciphering operator. The means by which these arrangements and alignments of rotors are selected by the enciphering operator and transmitted to the deciphering operator in disguised form constitute a rather complicated set of keying instructions. These instructions are discussed in Chapter . Here, we are concerned only with the fact that in order to decipher a message the arrangement and alignment of the rotors must be the same as those used to encipher the message.

In order that the reader may understand the two cryptographic principles mentioned above (page 2), it is necessary to understand the cryptographic function of the SIGABA rotor. The SIGABA rotors are merely switching commutators which carry an electric current across the rotor maze in a circuitous path determined by the wiring of the rotors and the alignment of the rotors relative to one another. The rotors of SIGABA consist of two types: 5 small rotors with ten contact points on each side face and 10 large rotors with 26 contact points on each side face. Each of the 10 contact points on the left side face of each index rotor are wired at random to one of the 10 contact

points on the right side face of each index rotor. Each of the 26 contact points on the left side face of each control and cipher rotor are wired at random to one of the 26 contact points on the right side face of each control and cipher rotor.[1] The five small rotors (index rotors) fit only into the front rotor bank. The 10 large rotors (control rotors or cipher rotors) fit into either the rear or center rotor bank.

The actual encipherment of a letter is performed by the five irregularly turning rotors of the rear rotor bank. The center rotor bank (control rotors) and the front rotor bank (index rotors) perform the function of controlling the stepping of the five rear rotors in such a way that simulated random stepping of the rear rotors is the effect.

The five irregularly stepping rear rotors perform their function of encipherment of a letter as follows; The path of the electric current is from the contact of the key depressed to the contact to which it is wired in the right end plate, to the touching contact on the right face of the first rotors, to the contact to which it is wired on the right side of the first rotor , and on through the cipher maze in this manner (see diagram below) to the touching contact on the left end plate, to the magnet which effects a certain letter of the type wheel (10, Tab B), thus causing that letter (the cipher letter) to be printed on the tape.

1. This wiring is accomplished according to a chart (composed by random selection) so that sets of the 15 rotors can be wired exactly alike for intercommunication between SIGABA holders.

Illustration of Path of Electric Current
through Alphabet Rotor Maze

With each encipherment of a plain-text letter one or more of the five cipher (alphabet) rotors advance one step. Which of the five cipher (alphabet) rotors step and how many is determined by the paths of four electrical circuits through the control rotor maze and the index rotor maze. The paths of these four circuits are varied by the change which occurs in the relative positions of the control

rotors[1] with each encipherment of a letter. The index rotors remain stationary.[2] The paths of the four electrical circuits, (which select the cipher (alphabet) rotors to step with each encipherment of a letter) are determined in the manner described in the paragraphs which immediately follow (pages 8 - 11). The diagram on the following page (page 9) illustrates the effect of the four circuits through the two (control and cipher) rotor mazes. The description in the paragraphs which immediately follow refer to this diagram.

On the right end stator or right contact face, four contact points are energized or become "alive" with each depression of a key. The four "live" contact points remain the same for each encipherment. In the diagram (page 9), the "live" contacts of the right end stator are shown at points designated by the letters E, J, O, and Q.[3] The four circuits which begin at these four "live" contact points are indicated by a red, blue, orange, and green arrow. The paths of the four circuits through both the alphabet and index maze can easily be traced by following the red, blue, orange, and green arrows. The paths across the control maze is of course determined by the wiring of the rotors and the relative positions of the rotors for this particular encipherment.

1. The control rotors advance in metered fashion: The control rotor in position no. 3 is the fast-stepping control rotor; it steps once for each depression of a key of the keyboard. The control rotor in position no. 4 is the medium-fast-stepping rotor; it steps once each time the fast-stepping rotor has made one complete revolution (or has stepped 26 times). The control rotor in position no. 2 is the slow-stepping rotor; it steps once each time the medium-stepping rotor no. 4 has made one complete revolution (or has stepped 26 times). Rotors 1 and 5 remain stationary.
2. The index rotors remain stationary throughout one day. They are realigned manually at the beginning of each new day.
3. The "live" contact points here designated are not the actual contact points of the right end stator which are "live." This is an illustration only.

FIGURE ____

DIAGRAM OF THE PATHS OF FOUR ELECTRICAL CIRCUITS

THROUGH

THE CONTROL AND INDEX ROTOR MAZES

(causing certain rotors of the cipher or alphabet maze to step)

The four circuits each leave the control rotor maze at one of the 26 contact points of the left end stator (left contact face). The 26 contact points of the left end stator are wired together in 9 groups or bands. These 9 bands lead to 9 of the 10 contact points on the left end stator of the index maze. The 9 bands or groups in the wiring of the left end stator of the control maze is made up as follows: Six of the contact points of the left end stator are wired together and lead to one contact of the left end stator of the index maze. The six-wire band of the left end stator of the control rotor maze is designated on the diagram by the orange lines which connect the contact points designated by the letters C, D, F, H, J, R.[1] In the diagram, this 6-point band[2] leads to the contact point of the left stator of the index maze designated by the number, 0.[3] The significance of this banding is that if one (or more) of the four circuits established leaves the control maze at any one of these 6 contact points, it will be directed by means of this banding to the same contact point of the left stator of the index maze, (in the illustration, contact 0). The other bands can easily be noted on the diagram. There is a 5-point band (indicated in the diagram by the green lines leading from the left end stator of the control maze to contact 7 of the left end stator of the index maze); there are two 3-point bands (indicated on the diagram by

1. The contact points here indicated are <u>not</u> the actual points banded together in the right end stator. This is an illustration only.
2. The <u>number</u> of contact points banded together are accurately given throughout this text. Which points they are is a matter of illustration only and are <u>not</u> the actual points concerned.
3. This right-end stator band does <u>not</u> actually lead to the contact point of the right end stator of the index maze indicated on the diagram or if it does it is merely a coincidence. This is an illustration only.

two groups of blue lines leading from the right end stator); there is one 4-point band (red lines); there is one 2-point band (purple lines); there are two singly wired contact points (black lines). These bands include all 26 contact points of the left-end stator of the control maze. There are 9 of these bands leading to 9 of the 10 contact points of the left-end stator of the index maze; this leaves one "dead" or inactive contact point on the left-end stator of the index maze. In the illustration on page 9, the "dead" or inactive contact point, on the left-end stator of the index maze, is contact point 2.

From the left end stator of the index maze, the four circuits follow the path established by the wiring and relative positions of the index rotors. The ten contact points of the right end stator of the index maze are banded together in pairs; each pair of wires is connected to a magnet, which when energized, will step one of the five cipher rotors. (On the diagram, page 9, these contact points of the right end stator of the index maze are banded in pairs as follows: 0 and 4 are banded together, indicated by blue lines; 2 and 8 (orange lines), etc.)

Following, by means of the diagram on page 9, the circuits designated by the red and green arrows from the original contact points all the way through the control and index mazes, it will be noted that these two circuits eventually lead through the same band of the paired contacts of the right end stator of the index maze; thus both circuits influence the same rotor. In the example, the red and green circuits designated by the arrows both move rotor no. 3. The circuit designated by the blue arrows moves cipher

rotor no. 4. The circuit designated by the orange arrows move cipher rotor no. 1. Therefore, the example shows that with this particular encipherment of a letter, three cipher rotors (~~1, 3, 4~~) advance one step. With the next encipherment of a letter, the change in the relative positions of the control rotors will direct the four circuits through different paths.

CHAPTER II. THE BEGINNING OF THE ELECTRICAL MACHINE AGE IN ARMY CRYPTOGRAPHY

Each of the successive models[1] mentioned in the preceding chapter, and which are discussed in detail in the succeeding chapters, were attempts to produce a rapid electrical cipher machine having an extremely high degree of cryptographic security. The necessity for both security and speed were made apparent by the lessons learned during World War I. Codes and a few manual cipher systems--but mostly codes--were the means of enciphering classified communications during the first great war. The military operations of World War I were conducted on such an extensive scale that the use of codes and manual cipher systems became "a serious menace to the prompt transaction of military business".[2] Because of the delay and irritations inevitable in manual and pencil and pad procedures, field commanders in the heat of battle disregarded cryptographic precautions or neglected the decipherment of pertinent messages.

These inadequacies became apparent before the end of World War I and a serious attempt was made to produce a rapid and secure machine. In the last phases of World War I, the Office of the Chief Signal Officer[3] placed the problem of evolving an indecipherable "printing-

1. Converters M-134-T1, M-134-T2, M-134, M-134-A, M-134-C, Keying Unit M-229.
2. Memorandum for the Chief of Staff, from the Chief Signal Officer, Subject: "The development of an indecipherable printing telegraph cipher for military purposes", Sept. 11, 1918. See Tab D.
3. The cryptographic activities of the U.S. Army during and immediately subsequent to World War I were the joint responsibility of the Chief Signal Officer and the Director of Military Intelligence. The responsibility of the Chief Signal Officer placed emphasis on the establishment and development of enciphering and deciphering methods and procedures.

telegraph cipher" before the engineering staff of the American Telegraph and Telephone Company. All pertinent cipher knowledge possessed by the Signal Corps was placed at its disposal and it was also given all the assistance it needed from the cipher experts of the Military Intelligence Branch[1] of the General Staff. The work was vigorously undertaken and two months before the end of World War I, the development of a "printing-telegraph cipher"[2] for use with the telegraphic apparatus was completed. (See Tab D)[3] Plans for extensive field use of the "cipher" were suspended with the cessation of hostilities.

---

1. See footnote 3, page 13.
2. The printing-telegraph cipher made use of the well-known features of the printing telegraph art, such as tape, the keyboard perforator, the transmitter, and Baudot code. A set of electrical impulses released by a tape perforated in the telegraph Baudot code as the plain text were combined with a set of impulses released by a tape, perforated with random Baudot characters, as the principle of selection, to set up a third set of impulses controlling the perforation of a third tape as the cipher text. This cipher text tape was then transmitted by telegraphic facilities. In reverse manner, impulses released by a duplicate of the random perforated tape used in the encipherment of a given message were combined with impulses released by the perforated cryptotext tape of the message to produce a perforated plain text in the telegraph code. This information is from "Cipher Printing Telegraph Systems, Address presented by G. S. VERNAN, AT & T Co., at the Midwinter Convention of the American Institute of Electrical Engineers, New York, 8-11 February 1926." Copy filed: Office of Director of Communications Research, ASA, File: AT & T Printing Telegraph Machine. This description of the printing telegraph cipher shows that this early device was similar to the secure one-time tape systems in current use. However, the keying tapes of the printing-telegraph cipher were not "one-time" but were re-used. For a detailed exposition of the development of the printing-telegraph cipher, see the "History of the Converter M-228".
3. Tab D is "MEMORANDUM for the Chief of Staff, from the Chief Signal Officer, Subject: "The development of an indecipherable printing-telegraph cipher", Sept. 11, 1918".

Considering the vigor of this beginning, it seems logical that the development of electrical cipher equipment would have continued at a rapid pace. But such was not the case. The cessation of hostilities, which curtailed the immediate need for such equipment, seems to have negated the interest of the top policy makers. Thus the development of electrical cipher machines fell into an almost complete lull for the next ten years. Since the new peaceful era created little need for secret communications, there was no impetus to produce cryptographic apparatus and even if there had been, no funds.

However, this situation did not prevent those most interested in cryptography from thinking about such devices. In 1921, Mr. William F. Friedman joined the staff of the Office of the Chief Signal Officer. He had had extensive cryptographic experience before joining the staff of the Office of the Chief Signal Officer and had for a long time been preoccupied with the idea that hand-operated systems were not consonant with the machine age. Therefore, he, from time to time, drew up sketches[1] of his own new cryptographic ideas or improvements of already existing systems. He worked out some of these ideas in

1. Some of the new ideas set down in sketches were improvements of the Printing-Telegraph cipher. These improvements will not be discussed in this history because they are more pertinent to the development of Converter M-228. Those improvements, which were designed for use in conjunction with telegraph or teletype equipment, are discussed in the "History of Converter M-228".

conjunction with certain engineers of the staff, namely, Mr. Louis M. Evans and Mr. George A. Graham.[1] Most of these early sketches are more directly related to the development of Converter M-228[2] than to the development of Converter M-134-C. However, one of them bears an important relationship to Converter M-134-C development. This sketch, conceived and drawn in about 1926, possibly 1925, by Mr. Friedman, was a sketch for what later became Converter M-134-T1. (See Chapter IV.)

1. Several of the ideas for new developments were covered by patents: Patent No. 1,552,775, Friedman, filed: April 14, 1922, issued: Jan. 13, 1925 (Secret Signaling Apparatus for Automatically Enciphering and Deciphering Messages, plugboard used to change Baudot keying characters); Patent No. 1,516,180, Friedman and Evans, filed: June 5, 1922, issued: Nov. 18, 1924 (third and irregular key-tape transmitter); Patent No. 1,857,374, Evans, Friedman, Graham, filed: March 28, 1929, issued: May 10, 1932; (Baudot system of Enciphering) Patent No. 2,028,772, Friedman and Graham, filed: Jan. 23, 1932, issued: Jan. 28, 1936. — (Converter M-134-T1)
2. See "History of Converter M-228".

CHAPTER III

HEBERN CONVERTER
(and related patents)

For photograph of original Hebern Converter, see Tab G.

A. General

As emphasized in the first chapter, the two concepts to be traced from their beginnings to their culmination in the rapid and secure Converter M-134-C are (1) encipherment by means of an electric current through a rotor maze and (2) random stepping of the enciphering rotors. Although the second all-important principle was developed by the cryptographic experts of the Signal Intelligence Service of the Office of the Chief Signal Officer, the first principle was not. Since, in the 1920's, the office of the Chief Signal Officer devoted very little money or energy to the development of cryptographic equipment, it is easily understandable that the first steps in this direction were taken by inventors associated with commercial houses which manufactured cryptographic equipment for sale on any available market. Just how many inventors were working in this direction during the early 1920's is, for our purpose, indeterminable. However, it is known that several inventions for varying the paths of energy established in an enciphering mechanism between a plain-text letter and the resulting cipher-text letter were patented during the early 1920's and before.

Four examples of patents which can easily be recognized as development work which points in the direction of the first principle are

(1) British Patent Specification 163,357 (May 10, 1920)[1] granted to Hugo Alexander Koch of The Hague, Holland, (2) U.S. Patent 1,472,775 (Oct. 30, 1923)[2] granted to Herman August Thorwald Wahnoe of Copen-

---

1. From Koch, British Patent 163,357 (1920): "...I declare that what I claim is:
   (1) A ciphering and deciphering machine of the type hereinbefore referred to having an intermediate separate path carrier or valve which is capable of being bodily and freely adjusted between a stationary transmitter and receiver element and which is formed with a number of paths in which at any moment for any desired transmission of energy the whole number of such paths in the intermediate path carrier or valve is available and the intermediate path carrier moves in the direction of an imaginary line joining the successive ends of the receiver paths, the arrangement being such that each intermediate path has only two orifices of contacts, one on each side of the intermediate path carrier so that the total number of contacts on the intermediate path carrier is equal to twice the number of paths in the intermediate path carrier.
   (2) A ciphering and deciphering machine as claimed in Claim 1 in which a plurality of intermediate path carriers or valves are disposed between the ends of the transmitter paths and the ends of the receiver paths.
   (3) A ciphering and deciphering machine as claimed in Claim 1 or 2, in which the movement of the intermediate path carrier or carriers is effected automatically on any key of the transmitter being depressed.
   (4) A ciphering and deciphering machine according to Claim 3 in which the movement of one or more of the intermediate path carriers is effected irregularly... etc., etc.
2. From Wahnoe, U.S. Patent 1,472,775 (1923):
"The present invention relates to an automatic cryptograph which in consequence of its nature may be used for a number of various purposes.
The distinguishing feature of the present cryptograph is one or more sets of double drums--in the following referred to as duplex alternators--being each in similar manner as the commutator of an ordinary electromotor fitted with a number of segments, the said segments being electrically interconnected from drum to drum and from one duplex alternator to the other one in any suitable manner, the said duplex alternators with their interconnections being inserted as electrical intermediate members between the keys on a letter keyboard and moving mechanisms for a system of type levers, the said keys when operated in ordinary manner actuating the type levers by electrical means and at the same time, causing the interposed duplex alternators to alter their mutual position, so as to effect a constantly varied mutual transposition of the letters of the alphabet, numerals and signs.

hagen, Denmark, (3) U.S. Patent 1,510,441 (Sept. 30, 1924) granted to Edward H. Hebern of Oakland, California, and (4) U.S. Patent 1,683,072 (Sept. 4, 1928) also granted to Hebern.

The two Hebern patents mentioned above (1,510,441 and 1,683,072) are particularly pertinent to this developmental history: the first, because it describes the rotor (see Tab E for copy of Hebern Patent 1,683,072, which includes description of Hebern rotor); the second (see Tab F for copy of Patent No. 1,683,072) because it describes a machine which was physically rebuilt to produce the Converter M-134-T2 (see Chapter V). This particular Hebern model (for photograph, see Tab G) was a 5-rotor non-printing machine. The improvements made so that it became Converter M-134-T2 eliminated the basic weakness of the original device by substituting a means of producing random instead of metered stepping of its enciphering rotors. This improvement was not developed and applied to the Hebern machine until ten years after the Hebern machine had been submitted to the Office of the Chief Signal Officer.

B. Cryptanalytic Tests of Hebern Converters

The "Hebern Electric Code Machine", (for photograph, see Tab G) as it was called, was submitted to the Chief Signal Officer in the latter part of 1923 for examination and consideration relative to its suitability for use in the military service. The usual claims for indecipherability were made for this machine. Since a cursory examination of the machine showed it to be worthy of the closest study, a detailed cryptanalytic

test was undertaken by Signal Intelligence Section, OCSigO. The cursory examination showed that the degree of secrecy which it afforded seemed to be considerably higher than that afforded by any other machine so far examined except the Printing Telegraph Machine (see Chapter II). The Printing Telegraph Machine was much bulkier and not at all suitable for use in a theater of war below Army Headquarters whereas the Hebern machine was small, compact, and rugged, making it the most suitable device for field use which had been developed and presented to OCSigO by 1923. The detailed cryptanalytic investigation of the machine proved that although the cryptograms which it produced were by no means "absolutely indecipherable" or even "practically indecipherable", the degree of security was fairly high, and the machine offered possibilities for modification with a view to augmenting the degree of security.[1] This prediction of its possibilities made by William F. Friedman in 1924 was realized in 1933 when its secrecy was tremendously augmented by the improvements which made it Converter M-134-T2.

A step-by-step description of results of the detailed cryptanalytic study of Hebern's machine was written by Mr. William F. Friedman of SIS, OCSigO in early 1924. However, this technical paper was not published until 1934 along with a second paper[2] on a cryptanalytic test of a

1. Friedman, William F., Analysis of a Mechanico-Electrical Cryptograph, Technical Paper, Part I, written in early 1924, published in 1934.
2. Friedman, op. cit., Part II, published in 1934 along with Part I.

second Hebern device.[1] This second test was made[2] by Signal Intelligence Section in 1932 at the request (in April, 1932) of the Code and Signal Section, Office of Naval Communications, Navy Department. Both of these papers have for years proved particularly valuable as training literature for students preparing to cryptanalyze the later and more secure Army machines. The importance of these two technical papers to the Navy is expressed in the Navy "History of Invention and Development of the Mark II ECM" in a chapter called "The Contribution of the Signal Corps" as follows:

> ...These solutions were very important, in three ways, namely: -
>
> a. They showed the weaknesses of the meter action of the 1923 HCM and of 6 of the 30 optional stepping actions of the 1930 HCM.
>
> b. The 1924 solution was the basis of further analysis by the Navy which disclosed stepping actions that would block analytical solutions or short-cut solutions based on possession of the code wheels. Friedman arrived at similar conclusions, independently. Othersise, we would have had to abandon the Electric Cipher Machine as being deficient in inherent security.
>
> c. In recent years, the principles and techniques of these solutions were instrumental in the solution of certain systems which are still using a modified meter action.

1. See next page for cryptographic differences between the first and second Hebern devices herein referred to.
2. The test was conducted by Mr. F. B. Rowlett, Dr. S. Kullback, and Dr. A. Sinkov under the supervision of Mr. W. F. Friedman, Chief, of Signal Intelligence Section.

The second Hebern device (referred to above, page 21) which was cryptanalyzed in 1932 for the Navy, differed from the earlier model in that the stepping arrangement was no longer meterlike.[1] Any two of the five rotors (depending upon the action selected) moves forward continuously, a third rotor moves forward one step per 26 depressions of the keyboard, and the two remaining rotors move one step after 650 depressions on the keyboard.

C. Cryptographic Functioning

The original Hebern device (see Tab G for photograph), presented to the Office of the Chief Signal Officer in 1923, consists of the following component parts necessary to understand the machine cryptographically: a keyboard, a bank of 26 letter lights, 6 bakelite separators, two aluminum wheels, and an encipher-decipher switch.

A plain-text letter is enciphered by depressing a key of the keyboard, which action opens an electric circuit through the rotor maze to a lamp of the lampbank. The lamp which is lighted by this action indicates the cipher letter. The rotor maze provides a circuitous path for the travel of the current. The path of the current is as follows: From the contact of the key depressed to the contact to which it is wired in the left[2] end plate,[3] to the touching contact on the left face

1. For a detailed explanation of the mechanical stepping of these rotors, see Friedman, William F., Analysis of a Mechanico-Electrical Cryptograph, Part II, published 1934, pages 2-8. File CSGAS-83, Analysis Section.
2. The keyboard is wired to the left-end plate and the lamps to the right-end plate when the encipher-decipher switch is at "Direct". The lamps are wired to the left-end plate and the keyboard to the right end-plate when the encipher-decipher switch is at "Reverse."
3. The left-end plate is wired to the letters of the keyboard according to a random-mixed but necessarily fixed sequence.

of the first rotor, to the contact to which it is wired on the right side of the first rotor, to the touching contact on the left face of the bakelite separator, directly through the separator to the opposite contact on the right face of the separator, to the touching contact on the left face of the second rotor...and on through the rotor maze in this manner to a lamp which lights. For a graphic explanation of this principle, see the diagram of the current going through a rotor maze, page 7.

Three of the five rotors step mechanically in metered fashion by means of a universal bar and rocker shaft, two aluminum wheels, and associated levers and rotor stepping dogs. The effect of this mechanical action[1] is as follows: The fifth or extreme right-hand rotor steps forward continuously once per depression of the keyboard; the first rotor steps forward once per 26 depressions; and the middle rotor steps forward once per 650 depressions. Rotors 2 and 4 are displaceable only by hand.

D. Evaluation

Mr. Hebern is currently bringing suit against the government for infringement of his patents. This fact makes an evaluation of his contribution difficult. However, if it were not for this suit, the legal aspects of Hebern's claim to distinction would never have come to the fore. All of the other cryptographic machines in this history

1. For a detailed explanation of the mechanical stepping of these rotors, see Friedman, William F., Analysis of a Mechanico-Electrical Cryptograph, Part I, published 1934, pages 6-8. File CSGAS-83, Analysis Section.

are evaluated without regard to the intricacies of legal claims. Therefore, the same criterion is applied in the evaluation presented in the following paragraphs.

Edward H. Hebern invented the type of rotor which is used in many rapid, electrical, rotor cryptographs of the Army and Navy. Use of such rotors in cascade (or encipherment by means of electric current going through a rotor maze) is, as has been pointed out previously, one of the two basic principles of Converter M-134-C. This principle was reduced to practical means by Edward H. Hebern. Whether anyone else independently conceived and patented the same practical means (namely, that which has become known as the Hebern-type rotor) for use of this principle is for the courts to decide. Regardless of their decision, however, it was Hebern's machine which first brought the physical embodiment of this principle to the attention of the Army and Navy in a form so practical that it has never been abandoned.

The following evaluation of Hebern's contribution is most interesting. It is presented by Captain L. F. Safford, U.S.N. in his History of Invention and Development of the Mark II ECM:

> Hebern has never received adequate recompense for his part in the development of the Electric Cipher Machine. He is the original inventor. He brought his machine to the attention of the Navy Department, built numerous models, and by his perseverance developed it to the point where it almost became a practical machine. Hebern organized three or four different companies, which went bankrupt in turn. He lived in poverty, and during much of this period was supported by his wife who ran a boarding house. Hebern was put in jail by irate stockholders and would have been much better off personally if he had not invented the ECM or had not had any dealings with the Navy

Department. However, Hebern has no legal claim on the Government because in the opinion rendered in J.A.G. Conf. Ltr C-867/68 (8-25-W9) of 30 Sept. 1932: -

'Hebern has contributed substantial improvements in the ciphering art and while his claims are limited and are believed not to be infringed, yet there are several points of fact and law that may be urged. Taking the decisions of the courts as a guide, however, it is believed that any decision on the patents involved herein (Hebern #1,510,441, #1,683,072 and #1,861,857) would be in favor of the Government.'

For additional evaluation, in the light of improvements made on the Hebern converter, see Chapter V, page 46.

CHAPTER IV. CONVERTER M-134-T1

For photographs of Converter M-134-T1, see Tabs H, I, J, K, L, M, N, O, P.

A. General

The actual construction of models of automatic cryptographic machines for the Army begins with Converter M-134-T1. Converter M-134-T1 is a highly portable unit (9" x 11" x 12", weight: 22 lbs. without batteries) which constitutes the following principle parts: a keyboard (marked 4, Tab K), a bank of 26 letter lamps (marked 5, Tab K), a single rotatable cipher wheel or rotor (marked 2, Tabs J and K), a key tape transmitter (marked 1, Tab J), certain associated solenoids and relays, and a small electric motor. Encipherment of a plain-text letter is accomplished by depressing the plain-text letter of a message on the keyboard, which action causes a lamp of the lamp bank to light, designating the cipher letter. The cipher letter must then be copied by hand. Converter M-134-T1's single rotor serves to vary the connections between the contacts of the keyboard letters and the lamps. The manner in which this single rotor accomplishes its function is explained in Section E of this chapter.

B. Invention

Converter M-134-T1 was conceived in 1926 or possibly 1925, by William F. Friedman. Mr. Friedman revealed his original conception for this machine to George A. Graham (then Chief Engineer of the Wire Section at Signal Corps Development Laboratories), who contributed

sufficient detail to the original idea to be considered co-inventor. In the 1920's however ~~ideas~~ new conceptions for cryptographic devices remained in the form of ideas or sketches. Only a few individuals were vitally interested and these were not, at the time, in a position to bring pressure to bear in favor of either actual construction or allotment of sufficient funds for adequate research.

C. Building and Preliminary Testing of the First Model

Finally, on 1 July 1930, after Converter M-134-T1 had remained in the form of a sketch for four years, the comparatively insignificant sum of $1,500 was made available to Research and Engineering Division, OCSigO, for building a cryptographic machine.[1] As a matter of routine, this project was given to Signal Corps Laboratories, specifically the Wire Section, for the working out of details. Since Mr. George Graham, Chief Engineer of said Wire Section, was co-inventor of the machine, it was convenient that he was at the Laboratories to personally supervise the building of the model. However, even with Mr. Friedman's constant urging, through channels, to get the construction started and the understandable interest of Mr. Graham, in addition to the fact that the small sum of $1,500 had finally been allotted for the construction, it was still very difficult to get it started. The reason was that

1. Memorandum for Major Crawford, from William F. Friedman, Signal Intelligence Section, 5 Aug. 1930. "...on 1 July 1930 there became available to the Research and Engineering Division the sum of $1,500 for the development of cipher machinery...." Source of funds is not indicated in available correspondence.

"priorities" were established for the various projects in the laboratories and "cryptographic development work was at the bottom of the list, or nearly so. The emphasis was on the development of radio equipment and the absurdity of spending millions of dollars on producing radio communications apparatus without spending at least a few thousands on producing apparatus to protect these communications should have certainly been as clear as it was completely disregarded by those in charge of policy in such matters."[1] This almost universal attitude that development of cryptographic apparatus was comparatively unimportant resulted in undue delays. First of all, unnecessary time was spent in an attempt to decide whether the developmental work should be done by a commercial manufacturer. (Ironically, a commercial manufacturer was considered not in order to produce a better machine but so that the development work would not interfere with other projects at the laboratories.) However, all time spent on such a consideration was wasted, for "no commercial firm would have dreamt of undertaking any such development for the very small amount of money available."[2]

Finally, on 28 November 1930, the Laboratories received from the Chief Signal Officer the directive to proceed. Almost a year later (July 1931), the Laboratory reports showed such slow progress that the following important memorandum, which registered a definite change in

1. Friedman, William F., "Draft of Brief History of the Development of Cryptographic Apparatus in the Army", filed Headquarters Building, Historical Unit.
2. Friedman, op. cit.

attitude toward development of cryptographic apparatus, was written by the Officer in Charge of Training Division.[1]

MEMORANDUM TO: Executive Officer (THRU Research and Development Division)

1. According to the last progress report of the laboratories at Ft. Monmouth, the development of the cipher machine, funds for which became available on July 1, 1930, was but 20 per cent completed by April 30, 1931.

2. This Division regards the development of this cipher apparatus as of prime importance not only to the Signal Corps but to the whole Army, as well as to the various larger administrative offices of the military establishment. It believes that this development should be prosecuted much more vigorously than has thus far been the case.

3. The recent visit of the Assistant Chief of Staff, G-2, to this office, during which over an hour's conference was devoted to a discussion of cipher machines and their development, leads this Division to believe that the General Staff is vitally interested in such a project as is now being carried on in this connection, and that the Staff deems the completion, as soon as possible, of the development of a cipher machine as highly advisable.

4. During the recent conference between Mr. Graham and Mr. Friedman, on the occasion of Mr. Graham's visit to this office last week, it was reiterated by the former that this development can be persued only as vigorously as the low priority accorded this project permits, it now being near the tail end of all wire projects assigned to the laboratories.

5. For the foregoing reasons it is urgently recommended that the priority now accorded this project be changed, and that the project be granted as high a priority as is consistent with the development of other projects of similar importance.

D. M. Crawford,
Major, Signal Corps

1. Memorandum to: Executive Officer (THRU Research and Development Division), from D. M. Crawford, Major, Signal Corps, July 24, 1931. Filed in Folder "Converter M-134-T1, SISDE-5", Office of Director of Communications Research.

In response to this memorandum, the priority assigned the cryptographic development project was finally, on 12 September 1931, "tentatively raised from Number 19 to 6 in the Wire Section of the Laboratories"[1] and the Laboratories were "instructed to expedite the development."[2]

Seven months later, in March 1932, when the first model was at last ready for inspection[3] at the Signal Corps Laboratories, Mr. Friedman made a trip from Washington to Ft. Monmouth, N. J. in order to see and use the model and to discuss this and other matters with Mr. Graham. Mr. Friedman spent the better part of four days at the Laboratories--from Monday afternoon, March 21, through Thursday afternoon, March 24. Monday afternoon and Tuesday were devoted to another matter.[4] On Wednesday, March 23, the final touches were put on the new Converter M-134-T1 by Mr. Graham's assistants, thereby placing it in complete readiness for its preliminary test on Thursday

1. Notation of informal routing sheet to: War Plans and Training Division, from Research and Development Division of OCSigO, 12 Sept. 1931. Folder "Converter M-134-T1", op. cit.
2. Friedman, op. cit.
3. All information in this and the following paragraph concerning this March 1932 inspection trip was taken from the cited memorandum unless otherwise indicated: MEMORANDUM TO: Executive Officer (THRU O.I.C. War Plans and Training Division and O.I.C. Research and Development Division), March 29, 1932. Filed in Folder "Converter M-134-T2, SISDE-5", Office of Director of Communications Research.
4. MEMORANDUM TO: Executive Officer (THRU O.I.C. War Plans and Training Division and O.I.C. Research and Development Division), from William F. Friedman, March 29, 1932. "Immediately after arrival, Monday afternoon, and after reporting at headquarters, Fort Monmouth, I had a conference with Mr. Graham in regard to the cipher facsimile system of the German inventor, Dr. Wrede, for the purpose of discussing the outlines of the conference to be held with the inventor the next day, Tuesday...."

morning. Mr. Friedman performed the test himself by personally enciphering a plain-text message of 500 letters. This process required 20 minutes. Even though the machine performed satisfactorily, its slow rate of speed was a disappointment. It took 20 minutes to encipher these 500 letters, or in other words the rate of speed was only 25 letters per minute. This low rate of speed was caused by two factors:

(1) the manual processes involved -- first selecting the proper letter on the keyboard, noting the cipher letter on the light bank, and writing down the cipher letter.

(2) the slowness of one of the control relays.

It was thought by those present at the scene of the test that practice on the part of the operator would considerably improve the slow speed caused by the manual processes involved. However, improving the speed of the manual processes was contingent upon effecting a greatly increased mechanical speed. Therefore, the possibility of providing the converter with an adapter for this purpose[1] was discussed. In its ultimate form this adapter was to make it possible "without any intermediate steps, to encipher, transmit, receive, decipher, and print cryptograms at a high rate of speed... (sic) No doubt 30-35 five-letter words per minute, possibly more."[2] It was estimated that $5,000 would be required in order to build such an adapter since much developmental

1. Actually the adapter discussed could not have produced the desired increase in speed since its function was solely for production of instantaneous printing. The explanation of this statement is given in the text on pages 33 and 34.

work remained to be done. Of course, "it was absurd to expect the money would be forthcoming and it was not."[1]

However, minor modifications were made in the existent model in an attempt to improve it and increase its speed of operation. These changes took 9 months and in January 1933 the revamped model was delivered to Washington for test.

D. Service Test

During January 1933 this revamped model of Converter M-134-T1 was service tested.[2] The most important fact proved by this service test was that the mechanical speed of the machine, determined by

---

1. Friedman, op. cit.
2. By what agency the Converter M-134-T1 was service tested is unknown. The final report of the service test, dated 28 March 1933, presents the following information concerning speed and reliability of the converter:
"....A test of the cipher machine disclosed the following:
a. Speed.
(1) The maximum mechanical speed of the machine, determined by depressing the same key repeatedly and as rapidly as possible, is 33 depressions per minute.
(2) The maximum speed of encipherment or decipherment by an operator working as rapidly as possible for a short length of time, approximately five minutes, is 30 letters per minute.
(3) The average speed of encipherment or decipherment by an operator working in a methodical manner for a fairly long period, approximately 30 minutes, is 25 letters per minute. This average is based upon the actual encipherment and decipherment of 1066 five-letter groups, equivalent to approximately 6000 letters.
(4) Comparative speed tests of Cipher Device M-94 and with the Division Field Code, using portions of the same test as above, showed that the cipher machine is approximately twice as fast as the M-94, but no faster than the Division Field Code.
b. Reliability. - In general it may be said that the machine is quite reliable in operation, but the following mechanical failures were noted during the test:
For continuation, see footnote on following page.

the same key repeatedly and as rapidly as possible, was 33 depressions per minute. Since the necessary minimum was 60 characters per minute and the desirable optimum was 200 to 250 characters per minute, the speed of the model was pitiably slow by comparison. The limitation on its speed was imposed by the fact that the cipher wheel had to be displaced through angular distances and brought to rest at a precise spot. Even the addition of a printing mechanism, which was again considered after this second test, would not have added to the speed of the converter to any great extent because most of the time lost in operation was due to the necessity for waiting (a variable length of time in each case) until the cipher wheel had stepped to the proper position. This delay would have intervened even if the entire operation from depression

---

Continuation of footnote 2 from preceding page:

(1) When the keyboard keys are allowed to come up slowly after depressing, the cipher wheel occasionally fails to rotate and orient itself to its next correct position. This failure seems to be caused by faulty action of the tape-stepping mechanism, and renders all subsequent text incorrect. In normal operation of the keyboard, however, this failure does not appear.

(2) Occasionally, the cipher wheel is brought to a stop in a position slightly off that required to bring the contacts on the wheel in juxtaposition with those on the fixed discs between which it revolves. When this happens the lamps will fail to light and the cipher wheel must be given a slight push by hand in order to establish contact for lamp indication.

(3) Unless the perforations in the keytape are accurately placed with respect to the pins of the keytape transmitter, there will be occasions when the transmitter pins will be set up for a permutation either not represented on the cipher wheel, or not correct with respect to the tape. When this happens the cipher wheel, in the first case, will not stop revolving, and in the second case, will stop at an incorrect position. While the first case happened many times during the test, the second either did not happen or if it did, remained unnoticed, as it involves only a single-letter error.

of a key to printing of the character had been automatic because it was an inherent feature of the converter.[1] This inherent difficulty recognized, in writing, in both the preliminary (1 February 1933) and final (28 March 1933) reports of the service test, led to the logical conclusion that Converter M-134-T1 be at least temporarily set aside in favor of a new type design which would accomplish the necessary increase in speed. Stimulated by the disadvantages of the Converter M-134-T1, its co-inventor William F. Friedman, conceived a new type converter, the idea for which he presented in detail on 28 March 1933 as an attachment to the final service-test report on Converter M-134-T1. The description contained in this attachment was entitled "The Proposed New Cryptograph".

The result was that Converter M-134-T1 was abandoned and work on the "Proposed New Cryptograph", which eventually became Converter M-134-T2, was begun. (See Chapter V.) In the development of the new converter, one feature of the old was retained, namely, use of the random key tape, although, in the new machine, it was used to step several rotors individually rather than, as in Converter M-134-T1, to stop a single rotor.

1. This sentence and the one preceding are a paraphrase of paragraph 2a, "Preliminary Report on Signal Corps Converter, Type M-134", dated 1 Feb. 1933.

E. Cryptographic Functioning

For photographs and diagrams, see Tabs H, I, J, K, L, M, N, O, P.

Converter M-134-T1 (Tabs H and I) (9" x 11" x 12"; Weight: 22 lbs) consists of the following principle parts: a keyboard (marked 4, Tab K), a bank of 26 small letter lamps (marked 5, Tab K), a rotatable cipher wheel (marked 2, Tabs J and K), a key tape transmitter (marked 1, Tab J), certain associated solenoids and relays, and a small electric motor. This cryptographic machine has only one rotor (marked 2, Tabs J and K) which revolves between two fixed end plates. The 26 keyboard contacts are wired, individually, to the 26 contacts of the left end plate. The 26 lamps of the lamp bank are wired individually to the 26 contacts of the right end plate. The large rotor between the two fixed end plates has 52 brush type contacts, 26 on one side face and 26 on the other side face (these contacts, unmarked, can be seen in picture of rotor, marked 3, Tab L). The contacts are equidistant from one another. The rotor is wired crisscross, from the 26 contacts on one side of the rotor to the 26 contacts on the opposite side, as shown in the wiring diagram on the opposite page. The contacts are wired in pairs, meaning that if contact 1 on the left side face (key side) is wired to contact 18 on the right side face (lamp side) then contact 18 on the left side face is wired to contact 1 on the right side face. (See diagram opposite.) Since the current goes through the rotor only from left to right, it is necessary that the rotor be wired in this manner in order to produce

reciprocity; in other words, so that if plain-text Q equals cipher-text W in enciphering, then cipher-text W will equal plain-text Q in deciphering.

The path of the electric current in encipherment of a letter is as follows: From the contact of the key depressed to the contact to which it is wired in the left end plate, to the touching contact on the left face of the rotor, to the contact to which it is wired on the right side of the rotor, to the touching contact on the right end plate, to the lamp to which it is wired.

The manner in which the contact on the left face of the rotor is selected during the enciphering process is as follows: When any particular letter of the keyboard is depressed, the same contact of the left end plate is always selected by that action. For example, if Q of the keyboard is wired to contact 3 of the left end plate, then contact 3 of the left end plate will be activated every time the key Q is depressed. The variation in the cipher letter substituted for the plain-text letter Q is produced by the rotation of the rotor. Rotation of the rotor causes different contacts of the 26 left face contacts of the rotor to be presented to contact 3 on the left end plate.

Converter M-134's only rotor revolves step-by-step but continually until it is stopped by certain unusual factors. A key of the keyboard can be depressed only when the rotor is stationary which is the same as saying that a letter can be enciphered only when the rotor is stationary. A small electric motor turns the rotor, step-by-step, until a certain

coincidence occurs which is described in the paragraph following.

On the wide periphery of the rotor are 130 pins arranged in 26 rows of 5 pins each (see rotor pin, marked 3, Tabs J and K). These pins can be elevated into operative positions or left remaining in inoperative positions. The reason for these pins is to allow simulation of the Baudot code. For example, according to the Baudot code, the permutation of elements for the letter A is represented thus 12345. +++-- The sign + indicates that a pin is to be elevated into its operative position; the - sign, that it is to be left in its inoperative position. All the pins can be arranged in operative or inoperative positions to correspond with any sequence of signals of the Baudot code. This sequence may be varied at will. The function of the pins on the periphery of the rotor is to control the set of 5 contact-levers (marked 1, Tab K) just behind the rotor in such a way that when a pin is in its operative position and therefore presents itself to the contact lever, it presses against the latter and causes it to make contact. Pins in the inoperative position do not act upon these contact levers. The function of the rotor pins and contact levers are further explained in the paragraph following.

The key tape transmitter functions jointly with the rotor pins (see pin, marked 3, Tabs J and K) and contact levers (marked 1, Tab K). A random Baudot code tape, containing permutations for the 26 letters of the alphabet, is started through the tape transmitter (marked 1, Tab J) at the right rear of the converter. When the first character of the

key tape is over the sensing pins, the motor driven rotor will continue to revolve, step-by-step, until a Baudot code rotor-pin set up (on the periphery of the rotor) exactly equivalent to the Baudot character over the sensing pins in the tape transmitter is contacting the contact levers. This coincidence opens two relays which stop the rotor. At the moment when the rotor is thus stationary, the key may be depressed and the current will go from the key contact to the contact to which it is wired in the left end plate, through the rotor by means of the contacts selected by this simulated random stopping of the rotor, to the appropriate contact of the right end plate, to a lamp which lights and thus designates the cipher letter. This process is repeated for each cipher letter, the most important feature of each encipherment being this simulated random stopping of the rotor which effects a random selection of the left-face rotor contact used for encipherment of each letter.

F. Cryptographic Security

The following security evaluation of Converter M-134-T1 was made by Analysis Section, Methods Branch, Security Division.[1] The basic weaknesses were presented as follows:

Since Converter M-134-T1, in effect, produces a total of 26 enciphering alphabets from which one is selected by means of a random key tape

1. The evaluation given here was made especially for this history by Josephine Waggoner, Analysis Section, Methods Branch, Security Division.

for any one encipherment, the system resembles a one-time pad system. Consequently, if the disc and end plates are known, two messages in depth can be read. If the disc and end plates are unknown, multiple depths can be read fairly easily since columns representing encipherments with the same monoalphabet can be combined. However, since the square of the one-time pad is replaced by a one rotor device, this machine has some additional weaknesses not inherent in the one-time pad system. These are as follows:

1. If the fixed endplates are wired identically, the plain-cipher text will be reciprocal. This reciprocal nature of the text aids in crib-setting since a letter cannot encipher itself. It also aids in depth reading, since there are only 13 reciprocal plain-cipher pairs possible at any one setting of the disc.

2. If the fixed endplates are wired differently, crib setting is possible even though the text is not reciprocal. Any twenty-six point rotor must have at least one parallel wire. If it is randomly wired, it will probably have several parallel wires. (As many as 18 have been found on a randomly wired rotor.) Any one plain-text letter can therefore have only 25 or less cipher equivalents. This fact can be used in crib setting, since the missing cipher letters for high-frequency plain letters such as E, T, O, etc. can be readily determined.

The following two specific problems were evaluated by the cryptanalyst[1] as follows:

1. See footnote 1, preceding page.

First problem:

1. Given: a. Knowledge of the operation of the machine.
   b. Wiring of disc and end plates.
   c. Two messages in depth.

2. Conclusions: a. The two messages can be read.
   b. Relative stepping key can be recovered.

3. Solution: A deciphering table of the 26 possible alphabets is made up. Messages can then be read in same manner as two in depth on a one-time tape system. Key recovered would be a relative stepping key.

Second problem:

1. Given: a. Knowledge of the operation of the machine.
   b. Stepping tape.
   c. 500 or more letters of matched plain and cipher.

2. Conclusions: a. Stepping tape can be matched.
   b. Wiring of the end plates and disc can be recovered.

3. Solution: Stepping tape is matched to plain-cipher text by using repeats, that is, occurrences of encipherment of same plain letter at same setting of disc. Once stepping key is set, twenty-six partial alphabets are available for study. These alphabets are used to recover Friedman table for the disc, from which a relative wiring of both end plates and disc can be obtained. If end plates are known, recovery of disc is straight-forward.

Third problem:

1. Given: a. Knowledge of operation of the machine.
   b. 4 messages and plain-text of one if text is reciprocal;
   5 messages and plain text of one if not reciprocal or
   8 or more messages in depth if text is reciprocal;
   10 or more if not reciprocal.

2. Conclusions: a. Messages can be read.
   b. Wiring of disc and end plates and relative stepping key can be recovered.

3. Solution: Partial alphabets obtained from depth reading are used to recover Friedman Square of disc as in Problem 2.

G. Patent[1]

Converter M-134-T1 is covered by a single patent, number 2,028,772 (see Tab II) issued 28 January 1936 to William F. Friedman and George A. Graham. The application was filed 23 January 1932 when Mr. Friedman was a member of the Signal Intelligence Section of the Office of the Chief Signal Officer and Mr. Graham was an electrical engineer with the Signal Corps Laboratories at Fort Monmouth, New Jersey. As filed, the application contains fifty claims, forty of these being directed to the apparatus and ten to the method by which encipherment was accomplished. The result of prosecution was the allowance of nearly all of the apparatus claims and the final rejection of all method claims. The allowed claims represent excellent patent coverage of the invention. Title to the patent (2,028,772) now rests jointly with the inventors, the Government having retained the customary royalty-free, nonexclusive license to practice the invention.

H. Conclusions

In evaluating the importance of Converter M-134-T1, it should be "regarded as representing the initial, experimental phases of a project to produce a safe, automatic, rapid cryptograph".[2] It was

1. This information was furnished by Henry B. Stauffer, Chief, Patents Section.
2. Friedman, op. cit.

REF ID:A522328

VY DEPARTMENT

M OF CALL

10 Aug, 1951

0920 { a. m. / ~~p. m.~~

2 Griffiss (AFSA-12)

ed Phone 463 (Extension)

{ a. m. / p. m. } (Date)

McKee

produced during a period when many unsuccessful attempts to produce a rapid cipher machine had been made by commercial manufacturers. So far as is known, no automatic cipher machines were, at that time, in actual service either in commercial or governmental offices anywhere. Converter M-134-T1 was the result of preliminary experiments which pointed in the direction of limitless possibilities at the same time that they demonstrated the limitations of one particular design.

The most important new idea of Converter M-134-T1 is the concept of the random Baudot code keying tape stopping a rotor. The idea of a random keying tape had been used before, but the concept to be watched is that of random characters (or random selection by electrical impulses) used for the particular purpose of producing a random stepping of rotors. In Converter M-134-T1, this concept of random characters (or random selection by electrical impulses) influencing the movement of, in this case, one rotor became so important in the inventor's mind that consideration of needed secondary alphabets was neglected. However, the concept itself (underscored above) is tremendously important. In Converter M-134-T1, the random keying tape was used to stop a rotor. Only a short step of imagination is needed to see how this concept became that of using a random keying tape to step the rotors of Converter M-134-T2. Looking many years ahead to the Converter M-134-C itself, it is found that the keying tape is dropped as the specific means of producing the random characters (or random selection by electrical impulses) which serve to step rotors in a random fashion.

But the principle of random characters (or random selection of electrical impulses) stepping rotors in random fashion is never dropped, but instead is kept to be the most significant single factor in the security of Converter M-134-C.

CHAPTER V. CONVERTER M-134-T2

For detailed description and photographs of Converter M-134-T2, see Tabs R, S, T, U, V, W, X, Y, Z, AA, BB, CC, DD, EE, FF, GG, HH, II.

A. General

The development of Converter M-134-T2 began in March 1933 immediately after the service test of Converter M-134-T1. The T1 model was not only too slow but it was believed that the desired optimum of 200 to 250 characters per minute could never be attained by a machine operating upon its basic principle, that of an irregularly displaced cipher wheel. Therefore, the report on the service test of the T1 model recommended a change in the basic design of the machine and, attached to the report, was a practical proposal for building a new model which would operate on a different principle. The new proposal offered a particularly great advantage from a practical point of view in that a commercial cipher machine, already in possession of the Office of the Chief Signal Officer, could be modified to produce the cryptographic technique which it outlined.[1] The machine to be modified was the 5-rotor Hebern Device, covered by Patent No. 1,683,072 (see Chapter III), which had been cryptanalyzed by OCSigO in 1924. (See Chapter III, Section B.)

The new proposal, the specific embodiment of which was to become Converter M-134-T2, eliminated the basic weakness of the Hebern machine,

1. "This office (WP&T of OCSigO) can furnish a machine which will, it is believed, readily lend itself to modification for the purposes in mind." Service Test Report on Converter M-134-T1, 28 March 1933.

which was "the fixed character of the successive rotatory movements of the cipher wheels".[1] This invariability of motion in the Hebern device produced predictable relationships between the plain-text characters and cipher characters for any given initial arrangement of the cipher wheels. The proposed new system eliminated this basic weakness by substitution of a variable mechanism for displacing the cipher wheels for the fixed mechanism of the Hebern machine. This variable mechanism was a random Baudot-code tape (Tab U) running through a tape transmitter (Tab U). It caused to progress in variable relationship the five rotors (Tab U) which acted as switching commutators to establish a resultant for each and every keyboard operation. The manner in which the Baudot-code tape effected random stepping of the rotors is explained in greater detail below.

B. Cryptographic Functioning

The following parts (arranged in two groups, (a) and (b), according to their function) of Converter M-134-T2 must be explained in order to understand the converter cryptographically: (a) a keyboard (Tab V), five rotors (Tabs V and W) which act as switching commutators between two end plates, and a lamp strip consisting of 26 small letter lamps (Tab V); (b) tape transmitter (Tab V), plug and jack strip (Tab V), and associated magnets and relays. The elements just mentioned are arranged in two groups because they belong to different functions of

1. Service Test Report on Converter M-134-T1, 28 March 1933.

the converter. The elements in group (a) provide for encipherment of the plain-text letters. The elements in group (b) provide the means of stepping the rotors.

The encipherment of a letter by means of the elements in group (a) is accomplished cryptographically in the same fashion in which it is accomplished cryptographically with the Hebern converter: The path of the electric current in encipherment of a letter is as follows: From the contact of the key depressed to the contact to which it is wired in the left end plate, to the touching contact on the left face of the first rotor, to the contact to which it is wired on the right side of the first rotor, and on through the cipher maze in this manner (see diagram, page 7)... to the touching contact on the right end plate to the lamp[1] to which it is wired.

The above-described process of encipherment (as regards the path of the current through the cipher maze) is that used in the Hebern converter as well as in Converter M-134-T2. The difference—the all-important difference between the Hebern converter and Converter M-134-T2— lies in the introduction of the second group of elements, group (b), above: the tape transmitter (Tab V), plug and jack strip (Tab V), and associated relays and magnets. These elements of Converter M-134-T2 control the stepping of the rotors (Tabs V and W) in random, and therefore unpredictable, fashion (see paragraphs immediately

1. This process causes the lamp to be illuminated if only the cryptograph is in use; if the cryptograph is connected to the electric typewriter, designed for use with it, the designated letter is printed on the page copy.

below for detailed explanation) whereas the mechanical, metered stepping of the rotors of the Hebern converter (see page 25) is its cryptographic weakness.

The function of the tape transmitter (Tab V) in Converter M-134-T2 is to step forward the cipher discs (Tabs V and W) in accordance with the Baudot-code key tape (Tab V). The tape operates the rotors as follows: The five sensing pins of the tape transmitter are individually wired to five magnets which, when energized, cause the associated rotors to step. (For a detailed description of the "Cipher Disc Step Forward Mechanism", see Tab Z.) The first sensing pin[1] of the tape transmitter influences the first rotor;[1] the second pin influences the second rotor;[1] etc. When a tape is put through the tape transmitter, the first rotor will step if a perforation is directly over the first sensing pin; the first rotor will not step if a "non-hole" position is over the first sensing pin. The same is true of the second sensing pin and second rotor, etc. For example, if the character of a Baudot-code tape placed over the sensing pins is + - - - +, then rotors 1 and 5 will move forward one step while rotors 2, 3, and 4 will remain stationary.

A plug and jack strip (Tab U), consisting of 5 plugs and 5 jacks, is provided for the purpose of changing the connections between the sensing pins of the tape transmitter and the rotor-stepping magnets.

1. This relationship is accurate only if plug 1 of the plug and jack strip is in jack 1, plug 2 in jack 2, etc. For explanation of the variable factor which the plug and jack strip offers, see paragraph beginning "A plug and jack strip..." on this page and page 49.

(See also description of plug and jack strip, Tab R.) It is explained above that sensing pin no. 1 controls the stepping of rotor no. 1; sensing pin no. 2 controls the stepping of rotor no. 2, etc. In order to vary this relationship, the plug and jack strip is installed in the 5 connections between the tape transmitter contacts and the rotor magnets. By means of it, sensing pin no. 1 can be made to control rotor no. 5 simply by placing plug no. 1 in jack no. 5 or it can be made to control any of the other rotors by placing plug no. 1 in the jack which is connected to the corresponding rotor magnet. By changing the order in which the plugs are inserted in the jacks, the tape transmitter can be made to control the rotor-stepping magnets in different order to a total of 120 different arrangements.

The diagram below shows the plugs and jacks arranged so that sensing pin 1 controls rotor no. 2; sensing pin 2 controls rotor no. 4; sensing pin 3 controls rotor no. 1; sensing pin 4 controls rotor 3; and sensing pin 5 controls rotor 5.

At the time that the proposal for Converter M-134-T2 was offered in March 1933, specific keying instructions were not provided. (The keying instructions were first published in September 1938. For keying instructions by which Converter M-134 was operated by using personnel, see page .) However, all the elements which provided its inherent security were offered in the first proposal attached to the service test report. It was not a gradual development as far as its inherent cryptographic security was concerned. Comparatively, only a very little developmental engineering work[1] was needed in order to provide the specific embodiment of these ideas in the machine called Converter M-134-T2.

---

1. An example of the type of developmental work to be done on Converter M-134-T2 is evidenced by the following correspondence:

   The service test report on Converter M-134-T1, which document contained the proposal for Converter M-134-T2, contains the following quote:

   > This office can furnish a machine which will, it is believed, readily lend itself to modification for the purposes in mind. All that would be necessary would be to add to it the present key-tape transmitter, five magnets, and associated wheel-stepping mechanisms consisting of simple levers acting directly upon the present cipher wheels. The modification suggested might be accomplished in this manner within a short time and without difficulty.

   Later, while SC Labs was in the process of building the model proposed, there came a second suggestion, Sept. 2, 1933:

   > The following alternative to the use of magnets for stepping the cipher wheels is suggested for consideration. Suppose a motor is provided for continuously driving a shaft upon which five cams are mounted in a line above the respective cipher wheels; the function of the tape transmitter is then merely to actuate five small magnets which, by interposing or withholding small bars between the cams and their followers, control the stepping of the cipher wheels by direct action of the shaft drive. By such an arrangement it may be possible to provide

For continuation, see footnote on following page.

C. Building of First Models and Two Preliminary Tests

On 12 April 1933, the Office of the Chief Signal Officer directed Signal Corps Laboratories to proceed with the development of Converter M-134-T2 by converting the Hebern machine as proposed in the attachment to the service test report on Converter M-134-T1.[1] (At the same

---

Continuation of footnote 1 from preceding page:

> speed, accuracy, and certainty of cipher wheel displacements and at the same time eliminate certain of the disadvantages of direct magnetic action of the cipher wheels, which action might be too severe for smooth, long-continued functioning of the assembly. Your comments on this suggestion are invited.

The answer received by OCSigO from SC Labs, 18 Nov 1933, was as follows:

> ...3. In your 1st Ind. of Sept 2, 1933... the suggestion is made that a motor perform the actual work of stepping the discs forward by cam action under the selection of the magnets. This suggestion is well within the realms of practical application and is certainly not new in any respect, being the basic consideration of most printing telegraph machines and electrical typewriters. However, the application of the motor, the magnets, the selecting bars, the cam shaft, and the clearing features (restoring of the selected bars to normal) requires a combination of electrical and mechanical details which would necessitate considerably more time to construct than the relatively simple direct magnet action, assuming that the direct magnet action can be made entirely practical and positive in performance. Obviously, then the logical procedure is to first thoroughly expl it the simpler consideration, and to hold in reserve other considerations, in which case the motor drive is one possibility.

1. Letter, Subject: "Converter M-134-T1", To: Officer in Charge, S.C. Laboratories; From: Hugh Mitchell, Maj. S.C., Signed "By order of the Chief Signal Officer", 12 April 1933.

> 1. There is attached a copy of the report of service test of Converter, type M-134-T1 which indicates that this model is not satisfactory due to its inability to operate at the speed desired. The service-testing agency has recommended that a new model of a Converter, type M-134 be constructed by converting a commercial cipher machine as recommended in the attached proposed cryptographic machine.

For continuation, see footnote on following page.

time "military characteristics" of a cipher machine for use in message centers of divisions and higher headquarters, describing the basic features of the Converter M-134 development were drawn up.)[1]

In accordance with the directive, an instrument maker at Signal Corps Laboratories devoted his full attention to conversion of the Hebern device into Converter M-134-T2. In March 1934, the revamped Converter was pronounced by the Laboratories as ready for service test and between then and 14 July 1934, it was given a preliminary test in the Office of the Chief Signal Officer. The report (14 July 1934) on this preliminary test stated that the machine had proved to be "very satisfactory as regards its cryptographic functioning". It was

---

Continuation of footnote 1 from preceding page.

> 2. It is desired that your Laboratories proceed with this development by converting the cryptographic machine which was delivered to your Laboratories by Lieut. Elder on March 30th, in accordance with the attached proposal.
> 3. This office should be kept advised of the status of this project, and any comments or recommendations relative to the attached report or proposed new cryptographic machine should be submitted to this office with the least practical delay.

1. "These characteristics have not been submitted to the Signal Corps Technical Committee, inasmuch as it is for sole use by the Signal Corps, and in vew of the fact that the project is considered as confidential. However, these characteristics have been approved by this office and should govern you in this development." CONFIDENTIAL Ltr, WD OCSigO-311.5-(M-134), Subject: Converter M-134, 12 April 1933. [redacted].

returned to the Laboratories with a list of suggested changes.[1]

In March 1935, the process report of the Laboratories stated that the Converter M-134-T2 was again ready for test. Due to the fact that the Laboratories were then in the process of moving from one location to another, the test was postponed until early May. On 15 May 1935, the War Plans and Training Division of OCSigO completed its study of the converted Hebern model and concluded that the device was then "in satisfactory shape to warrant the purchase of at least six additional models for service test".[2] Also, additional suggestions

---

1. Letter, To: R&D Division, From: Henry L. P. King, Capt. S.C., 14 July 1934. Folder No. 2, M-134, M-134-A, Specifications. This letter directed that the following list of changes be submitted to Signal Corps Laboratories:
   a. Remove "Start-stop" switch lever on the key tape transmitter. This is unnecessary and its removal will lessen the possibilities for improper functioning of the machine.
   b. Remove "On-off" switch lever on the key-tape transmitter, for the same reason as under a.
   c. Remove one set of connection-changing plugs and jacks at the rear of the cryptograph. Only one set is necessary to accomplish the purpose for which these are intended. The plugs should be numbered from 1-5.
   d. Provide means for rotating the cipher wheels backward or forward by hand, for ease in setting up a keyword.
   e. Add a letter counting device, which can be reset to zero at will by a simple hand operation, so that the number of letters cryptographed can easily be checked.
   f. Insulate key bars of keyboard from the frame.
2. Memorandum, For: Maj. Cotton, R&D Division, From: S. B. Akin, Major, S.C., 15 May 1935. Folder M-134, Specifications.

in the line of engineering development were made.[1]

---

1. The following suggestions were made by WP&T, OCSigO. (Memo, For: Maj. Cotton, R&D Division, From: S. B. Akin, Maj. S.C., 15 May 1935. Folder M-134, M-134-A, Specifications):

a. The keyboard of the cryptograph should be made standard and the space between the keys should be made approximately equal to that on a standard typewriter keyboard.

b. For greater surety of electrical continuity across the five cipher wheels, the latter should be modified in whatever respect necessary to accomplish the purpose.

c. Means should be incorporated in the apparatus, so as to prevent the typewriter from operating more than once per depression of a key of the keyboard of the cryptograph. This means that some sort of a locking circuit or a locking mechanism will have to be provided.

d. Means should be incorporated to prevent the typewriter from printing a character unless the tape transmitter is also actuated. This may be accomplished in any manner which will insure that no printing will occur until the key that is being depressed on the cryptograph keyboard has reached the limit of its travel. At present the printing impulse occurs at the time when the depressed key has progressed only about 1/3 of the full distance of its travel. On hearing the striking of the type bar, if the operator releases the key and proceeds to the next depression, the tape has not stepped forward nor have the cipher wheels been moved as they should have been moved. As a consequence the enciphering operator, by incomplete depression of the keys, may cause the printing of cipher characters without accompanying stepping forward of the key tape and cipher wheels; the deciphering operator, however, not having any way of knowing when encipherment occurred without any tape and cipher wheel step-forward operation at the enciphering station, will not be able to decipher the message. Of course, instructions for operating the apparatus may emphasize the necessity for completely depressing all keys to the full limit of their travel; but it is through best to provide an automatic means of obviating this difficulty if possible.

...After these service test models have been procured the next steps in the development of this project should consist of studies regarding:

a. Methods for the production of the key tapes.

b. Improvement of the tape transmitter. The transmitter now in use was designed for use in a start-stop printing telegraph system and presents the art as it existed twenty years ago. No doubt a better transmitter, more suitable for the purpose for which it is intended in Converter Type M-134-T2, is now available on the market or can be more or less easily designed, the latter to use the brush-sensing principle employed in modern tabulating machinery.

For continuation, see footnote on following page.

Although the first report recommended the purchase of "at least 6 additional machines",[1] this number was later modified to two models, to be built by Signal Corps Laboratories. The two new models were completed and available for service test by June 15, 1936.

D. Service Test

When the two new models were completed in June 1936 (see Section C above), plans were made during the next few months for testing of Converter M-134-T2 by using the two machines for exchange of messages between two distant points. To accomplish this type of test, Mr. William F. Friedman took one of the machines to Panama by ship, leaving New York City on October 30, 1936. The other model was placed in the message center of the Office of the Chief Signal Officer. All preliminary arrangements for this test were completed by early November and from 7 until 23 November, inclusive, many cryptograms were exchanged between Panama and Washington. This service test demonstrated that the new cipher machine was operable at the rate of 30-35 words per minute and that it afforded "the highest degree of cryptographic security".[2]

Continuation of footnote 1 from preceding page.

In particular, it is desirable that the tape transmitter mechanism be such as to cause as little wear and tear on the tape as possible. If this can be accomplished, the life of the tapes will be very much extended and will by that much make the system more successful. Possibly a tape stepping mechanism similar to that used in motion picture projectors offers good opportunities for application.

1. Ibid.
2. Notes on Preliminary Service Test on Converter M-134-T2, filed in Folder 3, Converter M-134, M-134-A, Procurement (thru 1940), CSGAS-80.

Only minor difficulties manifested themselves during the Panama-Washington test conducted between 7 and 23 November 1936 (see Section D above). As a result of this test, the Converter M-134 was recommended for adoption as standard[1] with a number of modifications and additions. One of the two models used for the test was returned to Signal Corps Laboratories where the suggested modifications and additions were incorporated. Based upon this model, specifications for quantity production were drawn up. At about this time the designation of the test model, M-134-T2, was dropped and the machine was henceforth called Converter M-134.

E. Patent[2]

Application for Patent Serial Number 682,096 (see Tab JJ), of William F. Friedman covers Converter M-134-T-2, Converter M-134, and Converter M-134-A.

The application was filed relatively early, 25 July 1933, and contains probably the first disclosure of a rotor machine controlled by an externally generated key. Specifically, the application discloses a five-wheel machine in which the wheels are stepped depending upon the presence or absence of perforations in a tape, the tape being provided with a succession of Baudot code groups. More broadly, the invention contemplates means assuring substantially aperiodic stepwise displacements of the several rotors.

Although numerous claims have been allowed, the application is considered classified and is under a Patent Office secrecy order. There is no likelihood of the early issue of the patent.

HENRY B. STAUFFER
Chief, Patents Section
CSGAS-71

1. For details concerning adoption as standard, see Chapter VI, Section B, pages 3 Volume R
2. This paragraph was written by Henry B. Stauffer, Chief, Patents Section, CSGAS-71.

TAB A

Converter M-134-C

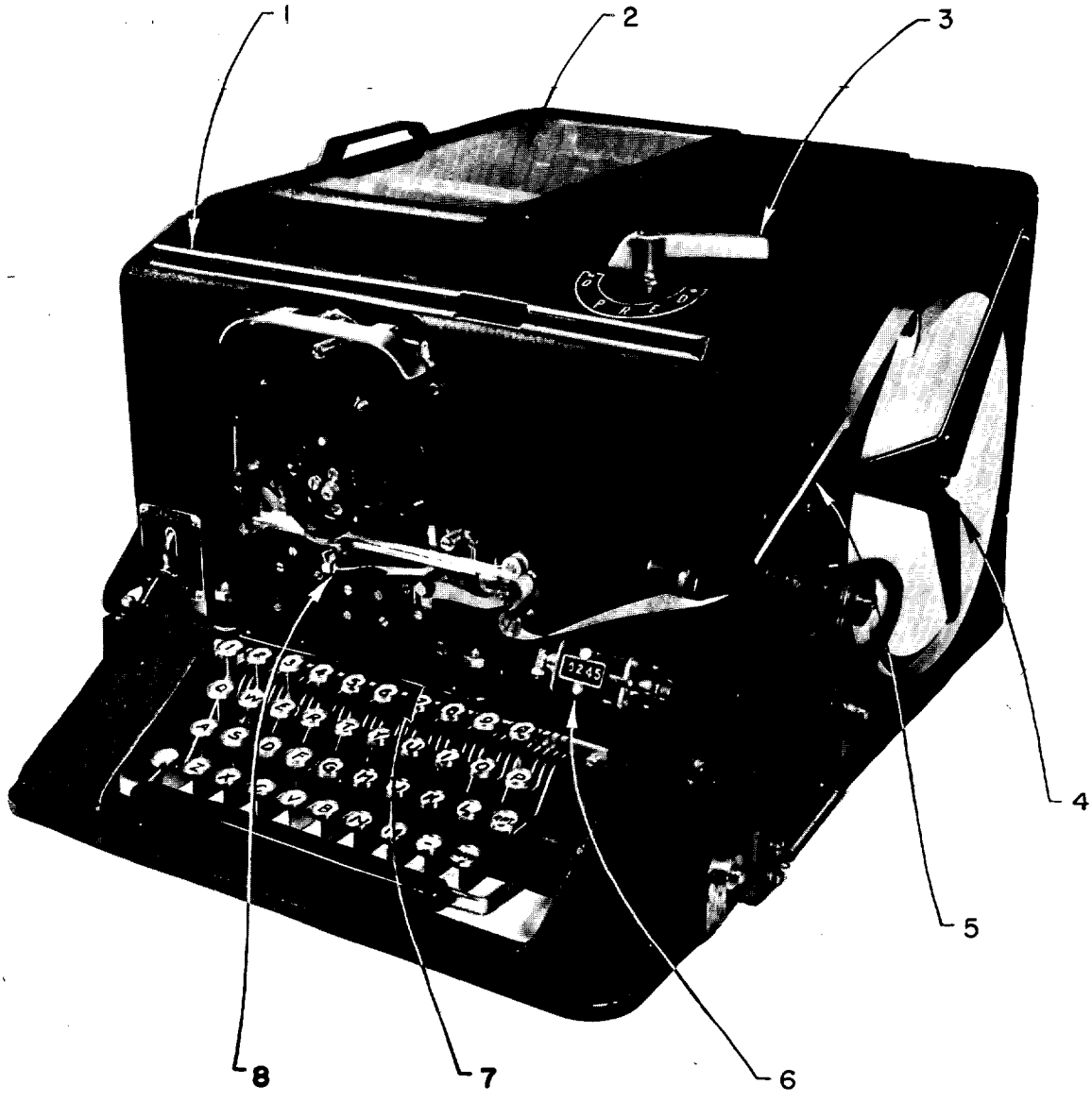


FIG. 1

1. Tape chute
2. Cover lid
3. Controller
4. Tape retaining arm
5. Side tape chute
6. Stroke counter
7. Name plate with register number
8. Print hammer

TAB B

Converter M-134-C

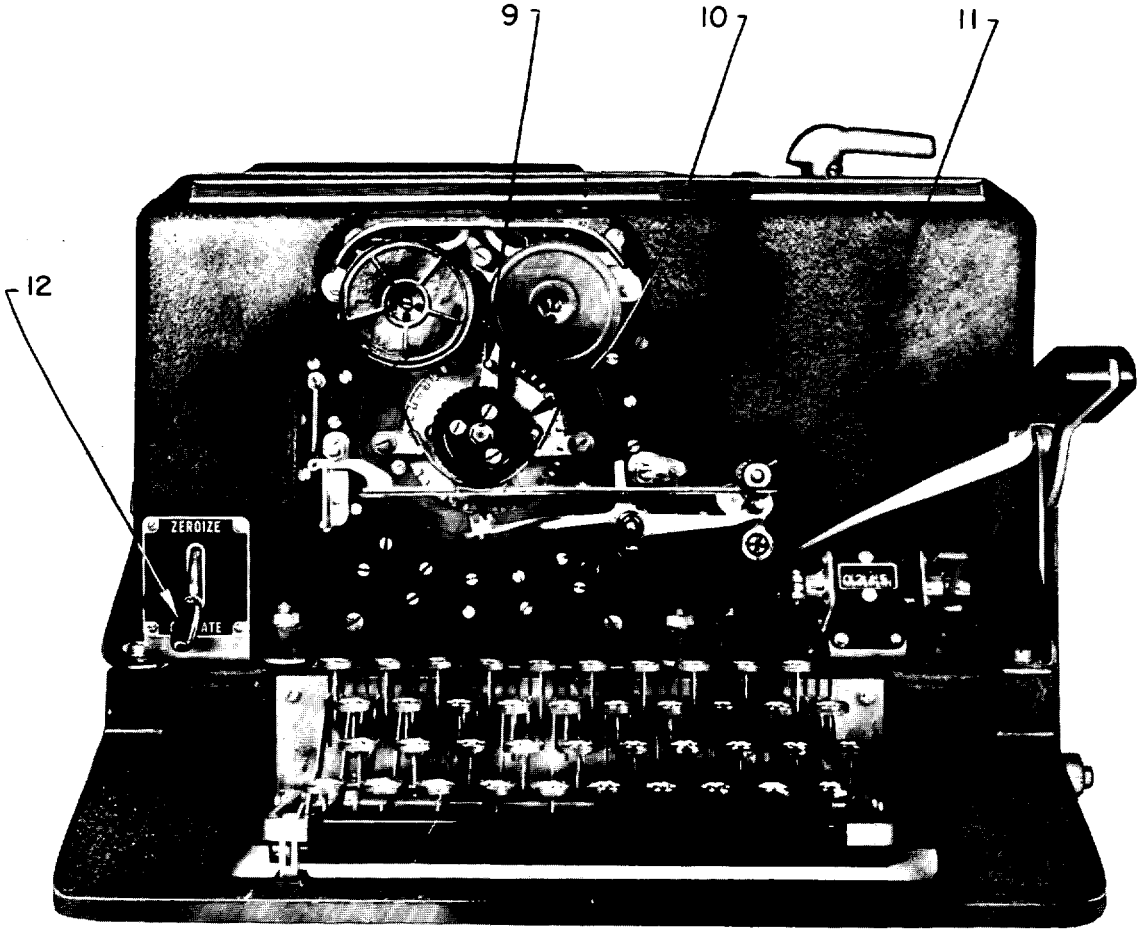


FIG. 2

9. Ribbon shift lever
10. Type wheel
11. Tape feed roller
12. Zeroize-operate key

TAB C

Photograph of Converter M-134-C

(showing especially the index, control, and cipher rotors)

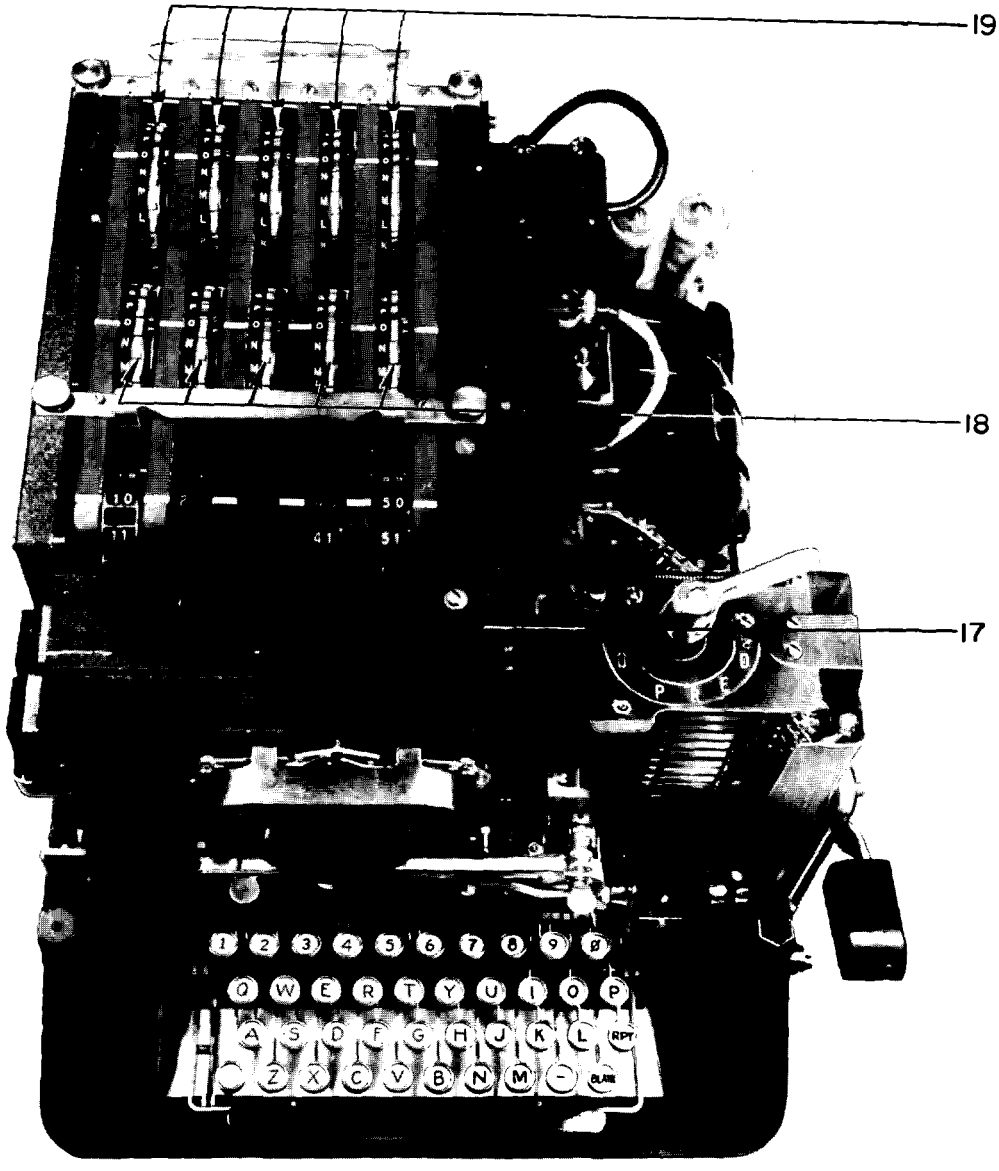


FIG. 4

17. Index rotors
18. Control rotors
19. Cipher rotors

TOP SECRET

TAB D

Memorandum to Chief of Staff

Subject: The development of an indecipherable printing telegraph cipher for military purposes.

From: The Chief Signal Officer

September 11, 1918

TOP SECRET

~~SECRET~~

September 11, 1918

MEMORANDUM for The Chief of Staff:

Subject: The development of an indecipherable printing-telegraph cipher for military purposes.

1. For many years experts in different countries have been at work more or less continuously, on the development of some form of secret telegraph cipher which could not be deciphered by outside agencies and which would, therefore, make possible the transmission by telegraph of the most secret messages involved in military operations, without any chance of these messages being interpreted.

2. A satisfactory solution of the problem presupposes a system involving the transmission of electrical impulses over the line which cannot be deciphered even when intercepted.

3. Modern military operations have reached such a scale and extend to such an enormous terrain that, in the absence of a suitable cipher, a very large volume of telegraphic business must be conducted in some form of code. The use of this necessary code has reached such a stage at present, in the different departments of war, as to involve a tremendous amount of expert labor in coding and decoding these messages. The delay in this necessary operation is a serious menace to the prompt transaction of military business. So far as is known, all previous efforts to obtain an absolutely indecipherable cipher have failed even in the hands of the most expert cryptographers. In the conduct of a conflict like the present war, the large volume of daily business has to be coded and decoded daily between two continents, involving great expense and the services of a large personnel. Not only is this a serious burden to the strictly military departments, but exactly similar conditions obtain in diplomacy, propaganda work, Department of Justice investigations, market reports, and many other activities of a confidential nature required in the conduct of the war.

4. Some months ago the Chief Signal Officer placed this particular problem of evolving an indecipherable printing-telegraph cipher before some of the best telegraph engineers of this country and the Engineering Department of the Chief Signal Officer's office under the charge of Lieutenant Colonel J. O. Mauborgne, was given direct charge of the development with instructions to cooperate, criticize, and to place at the disposal of these telegraph engineers all the cipher knowledge at the disposal of these telegraph engineers all the cipher knowledge the Signal Corps possessed. This work was undertaken vigorously by the engineering staff of the Signal Corps and the engineering staff of the American Telegraph and Telephone Company, with the added

assistance of the cipher experts of the Military Intelligence Branch of the General Staff, who have cooperated throughout this development.

5. The result of these efforts has been the development of such a system of cipher printing-telegraphy, and this system has now been installed for official tests between the Signal Corps laboratory 1710 Pennsylvania Avenue, Washington, D. C., and 463 West Street, New York City, where trained personnel, consisting of Signal Corps enlisted men, are now operating this apparatus with entire success.

6. The printing-telegraph, without cipher attachment, is now already installed in France extensively and is used in the conduct of official business between Headquarters A. E. F. and Headquarters S. O. S. in France, and also between London and Headquarters S. O. S. direct over a cable laid across the English Channel by the Signal Corps. General Pershing has recently asked for additional equipment for thirty more stations to be installed in the military telegraph system of our oversea forces.

7. The cipher apparatus already referred to has been designed, therefore, as an addition to the existing printing-telegraph system now in operation, and if adopted and approved by the Chief of Staff, cipher printing-telegraph units can be shipped and installed at any station where the printing-telegraph is now used.

8. This cipher apparatus, having been developed in the United States, is not known to our forces overseas, and the first line has been installed for the purpose of determining whether or not this cipher is thoroughly practical and adequate for military service, to supersede the present laborious and slow methods using code.

9. It is recommended that this model installation now in operation be immediately examined by a committee of the General Staff, with a view to determining, at the earliest practicable moment, whether or not this apparatus should be purchased and installed where necessary, both in this country and overseas.

Major General,
Chief Signal Officer of the Army.

1 Incl.

COPY

TAB E

Patent No. 1,510,441

Hebern, filed: March 31, 1921

issued: September 30, 1924

Includes description of Hebern Rotor

TOP SECRET

TOP SECRET

TAB F

Patent No. 1,683,072

Hebern, filed: November 20, 1923

issued: September 4, 1928

TOP SECRET

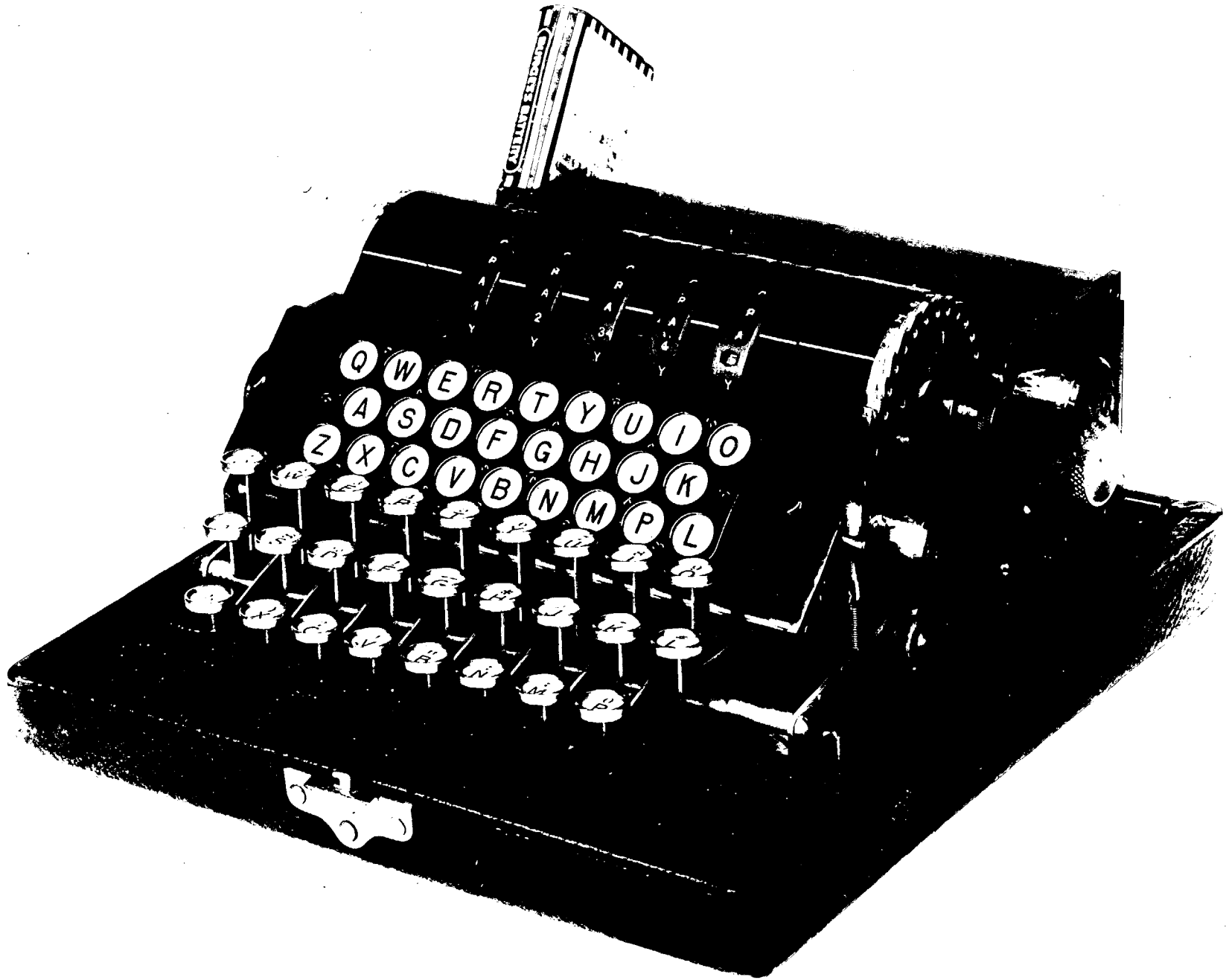
TOP SECRET

TAB G

Hebern Electric Code Machine

(presented to Army in 1923)

TOP SECRET

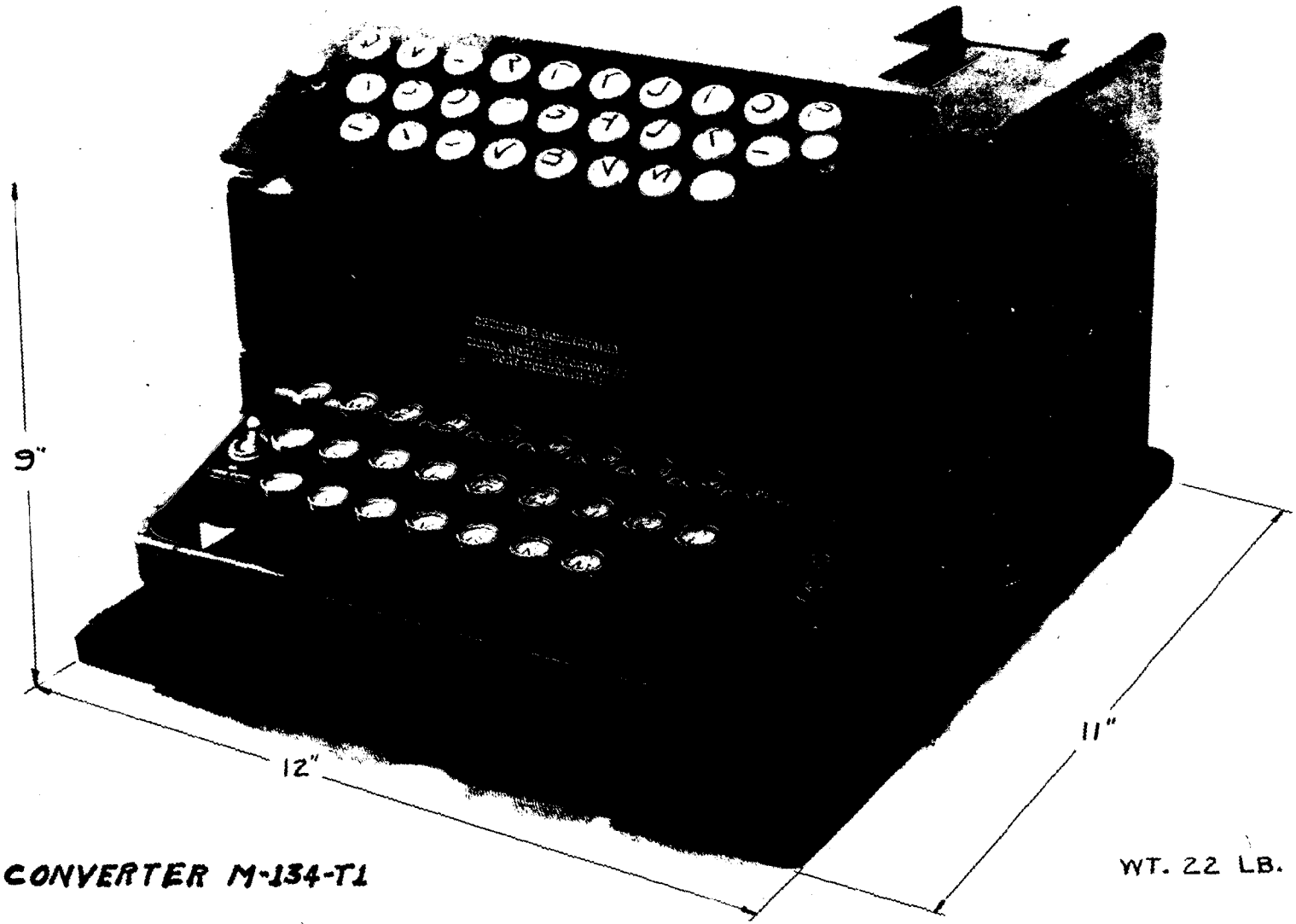


TOP SECRET

TAB H

Photograph of Converter M-134-T1

TOP SECRET



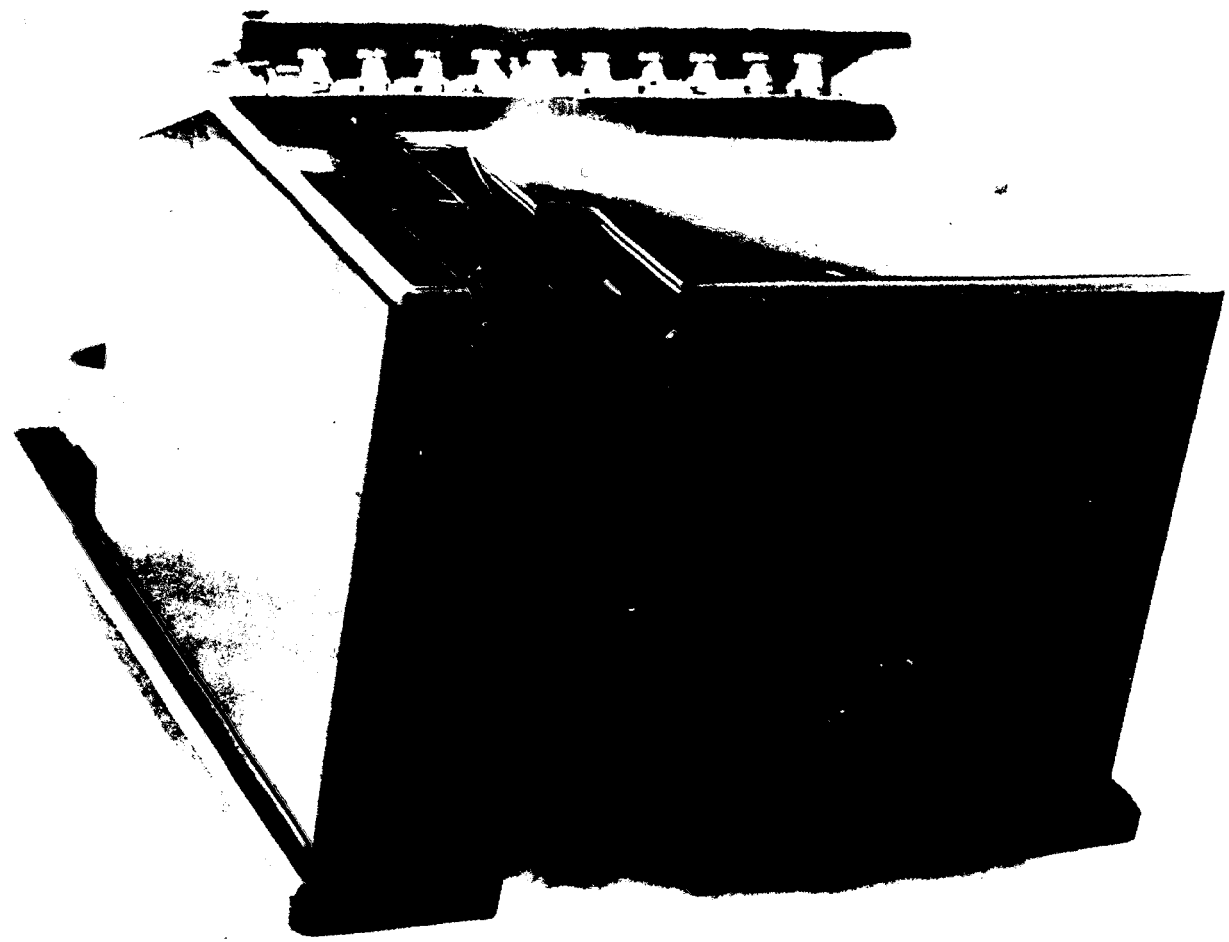
CONVERTER M-134-T1

WT. 22 LB.

TAB I

Photograph of Converter M-134-T1

Rear View



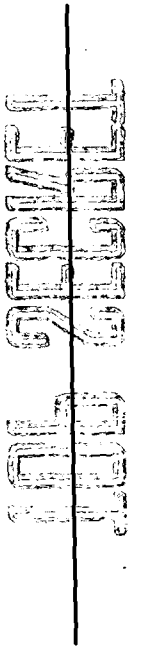
CONVERTER M-134-T1
REAR VIEW

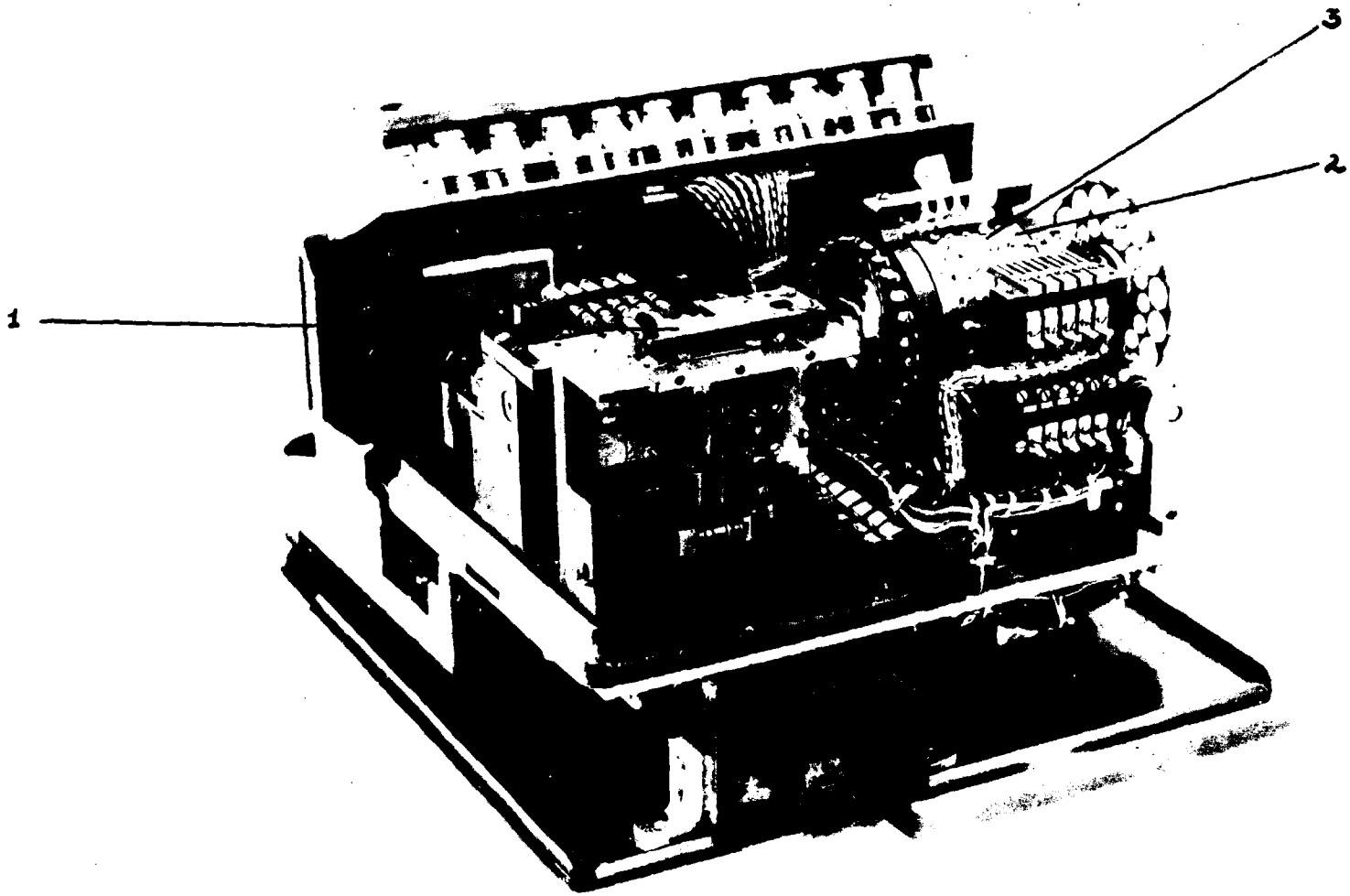
TAB J

Photograph of Converter M-134-T1

Rear view, cover removed.

1. Tape transmitter
2. Rotor
3. Rotor pin



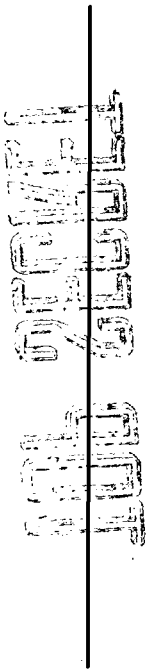


CONVERTER M-134-T1
REAR VIEW
COVER REMOVED

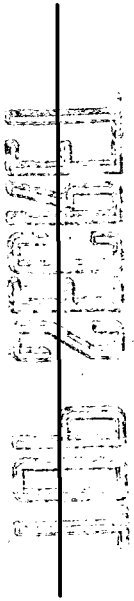
TAB K

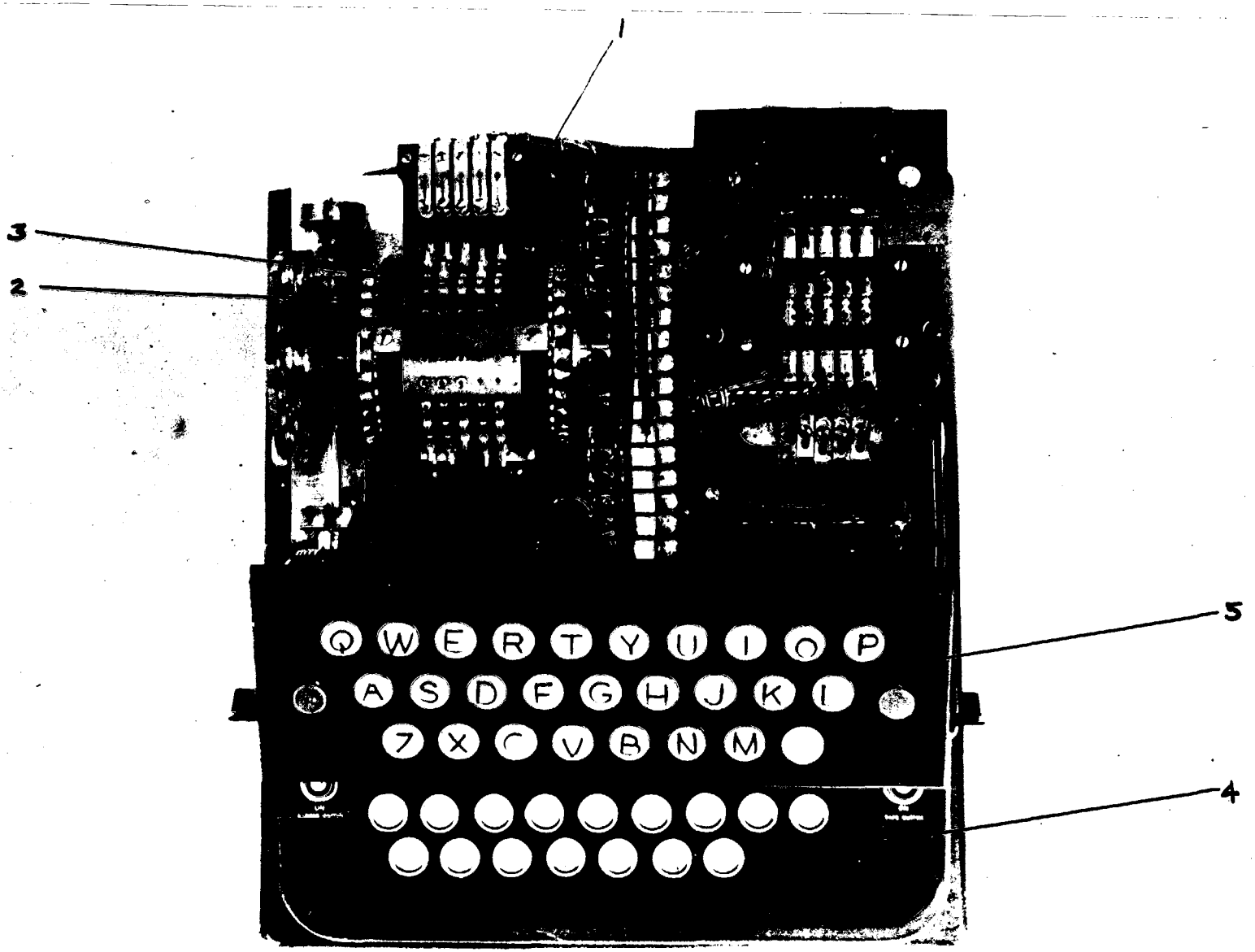
Photograph of Converter M-134-T1

Top view, cover removed.



1. Contact levers
2. Rotor
3. Rotor pin
4. Keyboard
5. Lamp bank



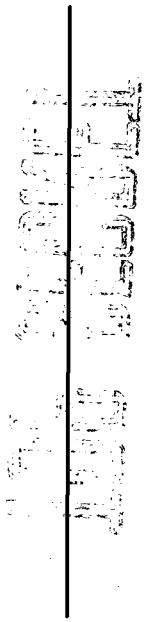


CONVERTER M-134-T1
TOP VIEW
COVER REMOVED

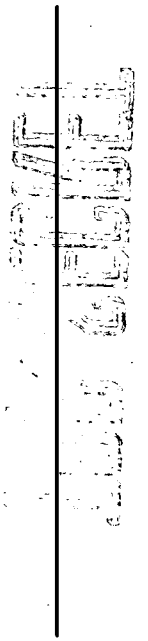
TAB L

Photograph of Converter M-134-T1

Partly dismantled; top view



1. U Clip
2. U Clip
3. Rotor removed from converter

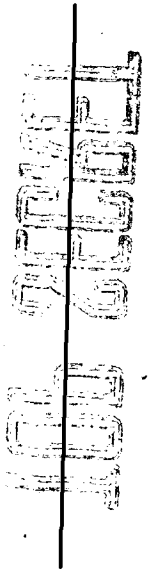


CONVERTER M-134-T1
PARTLY DISMANTLED
TOP VIEW

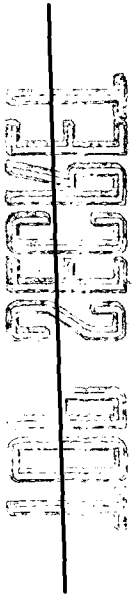
TAB M

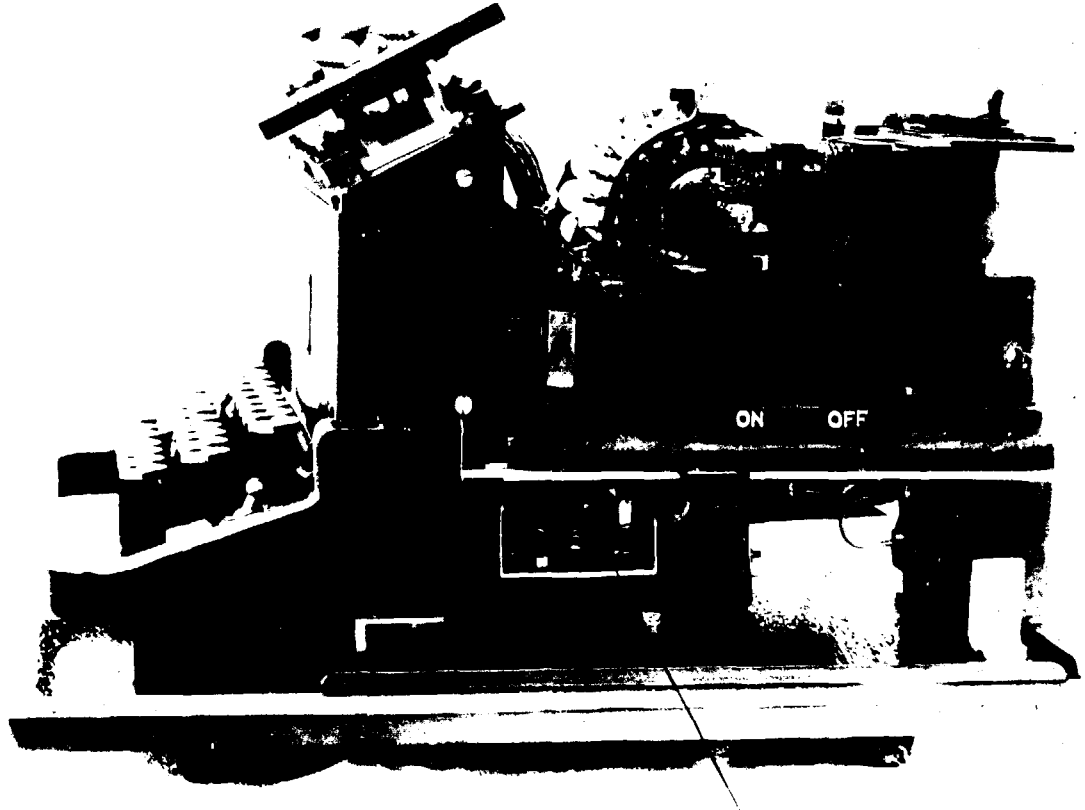
Photograph of Converter M-134-T1

Right side view, cover removed



1. Tape stepping contacts





CONVERTER M-154-T1
RIGHT SIDE VIEW
COVER REMOVED

TOP SECRET

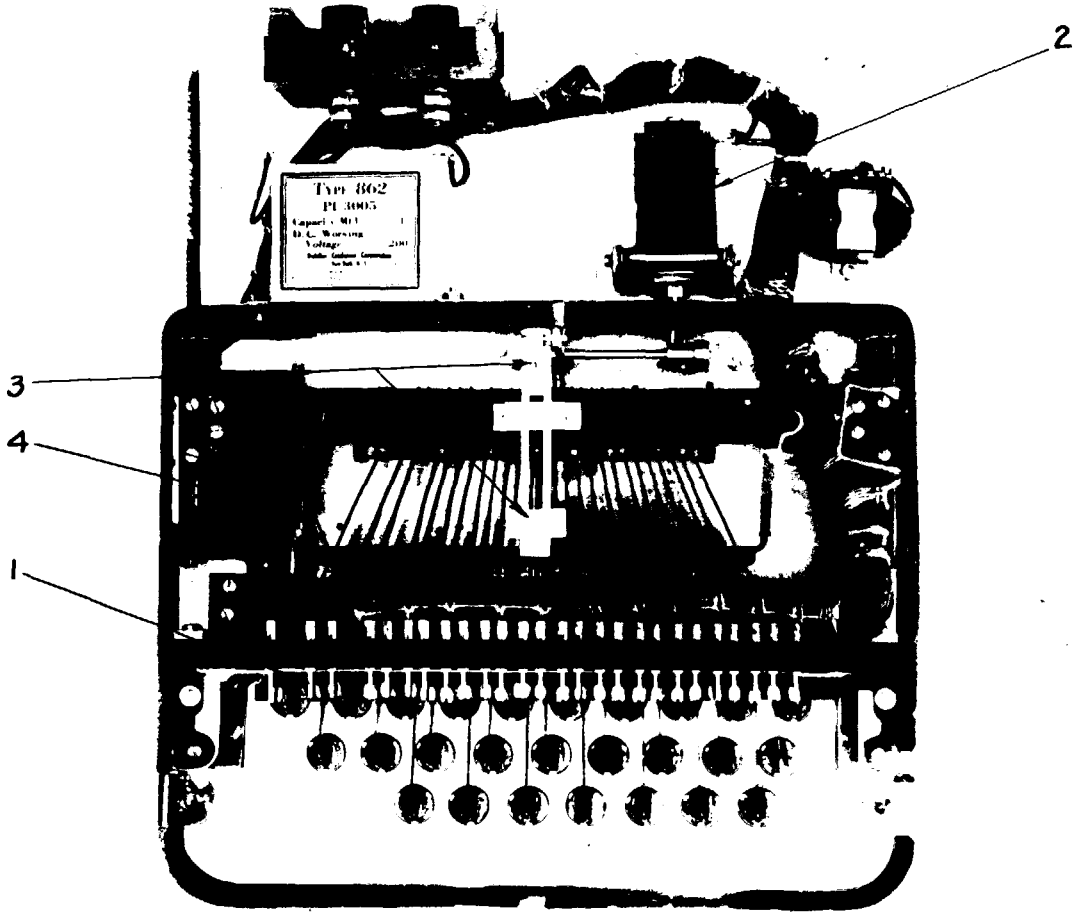
TAB N

Photograph of Converter M-134-T1

Under side

TOP SECRET

1. Individual keyboard key contact
2. Keyboard locking magnet
3. Lock-out bar
4. Universal bar



CONVERTER M-134-T1

UNDER SIDE

TOP SECRET

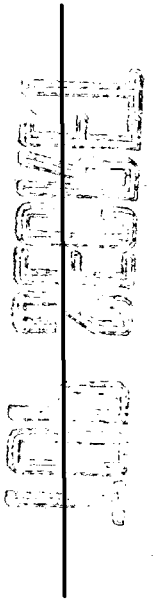
TAB O

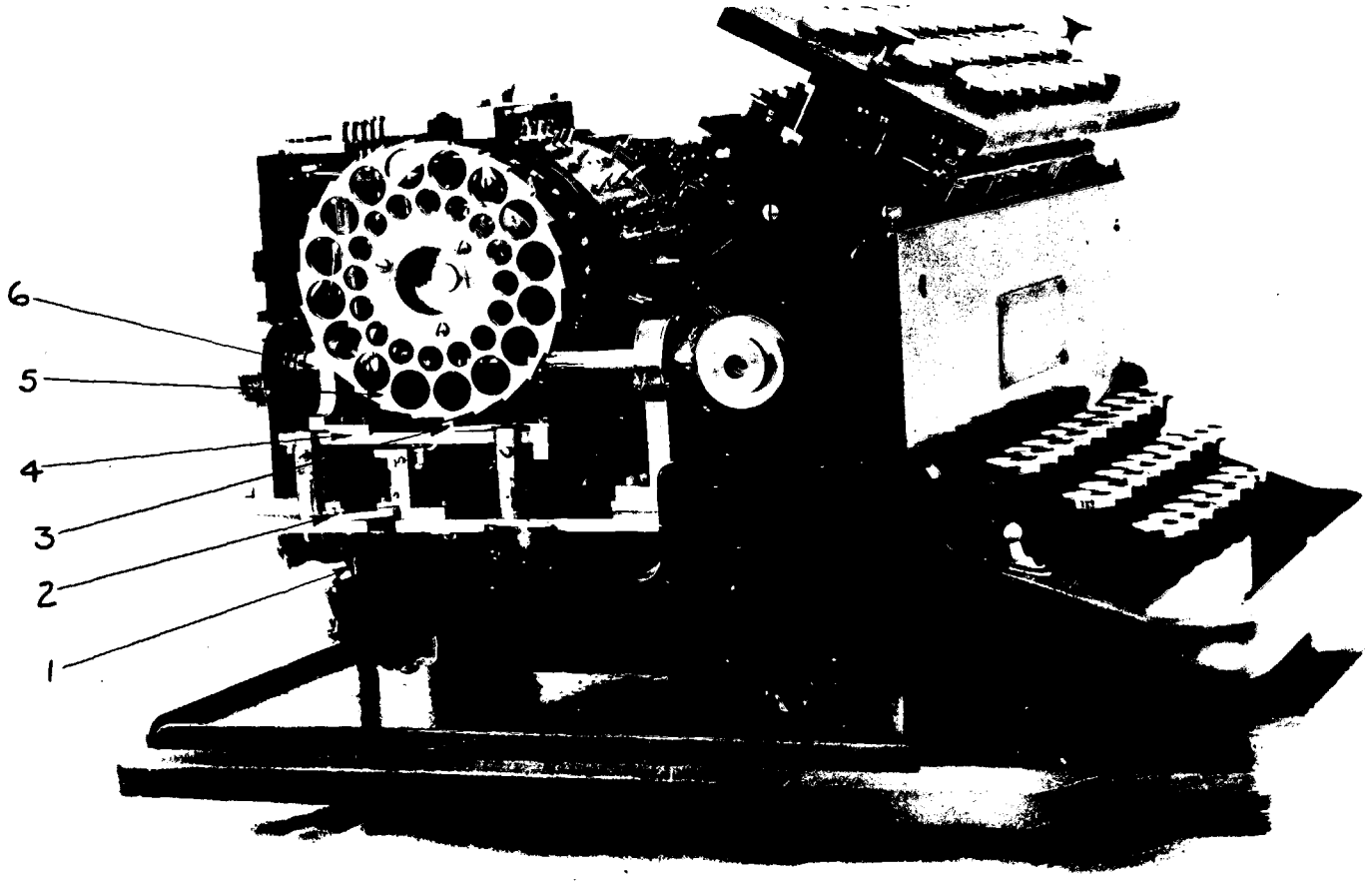
Photograph of Converter M-134-T1

Left side view, cover removed

TOP SECRET

1. Clutch disengaging magnet (stop magnet)
2. Armature of stop magnet
3. Pawl in normal position
4. Slide bar
5. Ratchet wheel attached to rotor shaft
6. Driving side of positive clutch





CONVERTER M-134-T1

LEFT SIDE VIEW

COVER REMOVED

TAB P

Three Drawings of Converter M-134-T1

Figure 1 - Wiring Diagram

Figure 2 - Plan of Wheel Stepping Pawl

Figure 3 - Side Elev. of Cipher Wheel (Rotor)

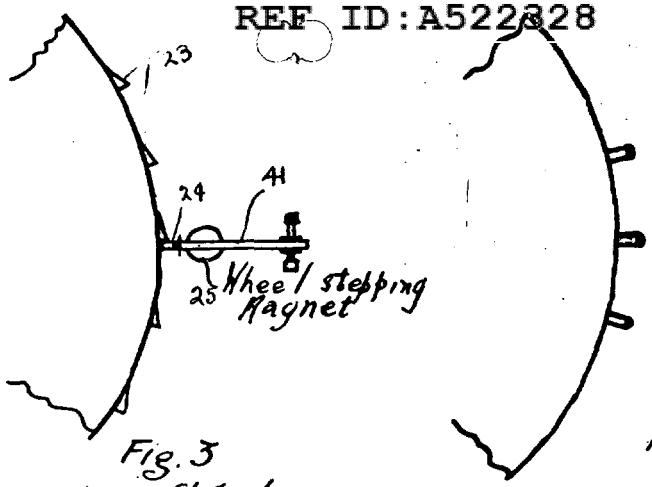


Fig. 3
Plan of Wheel stepping Pawl

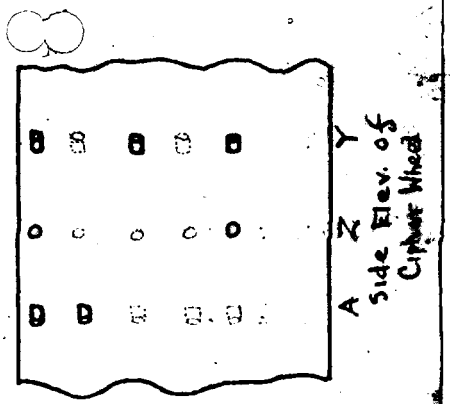
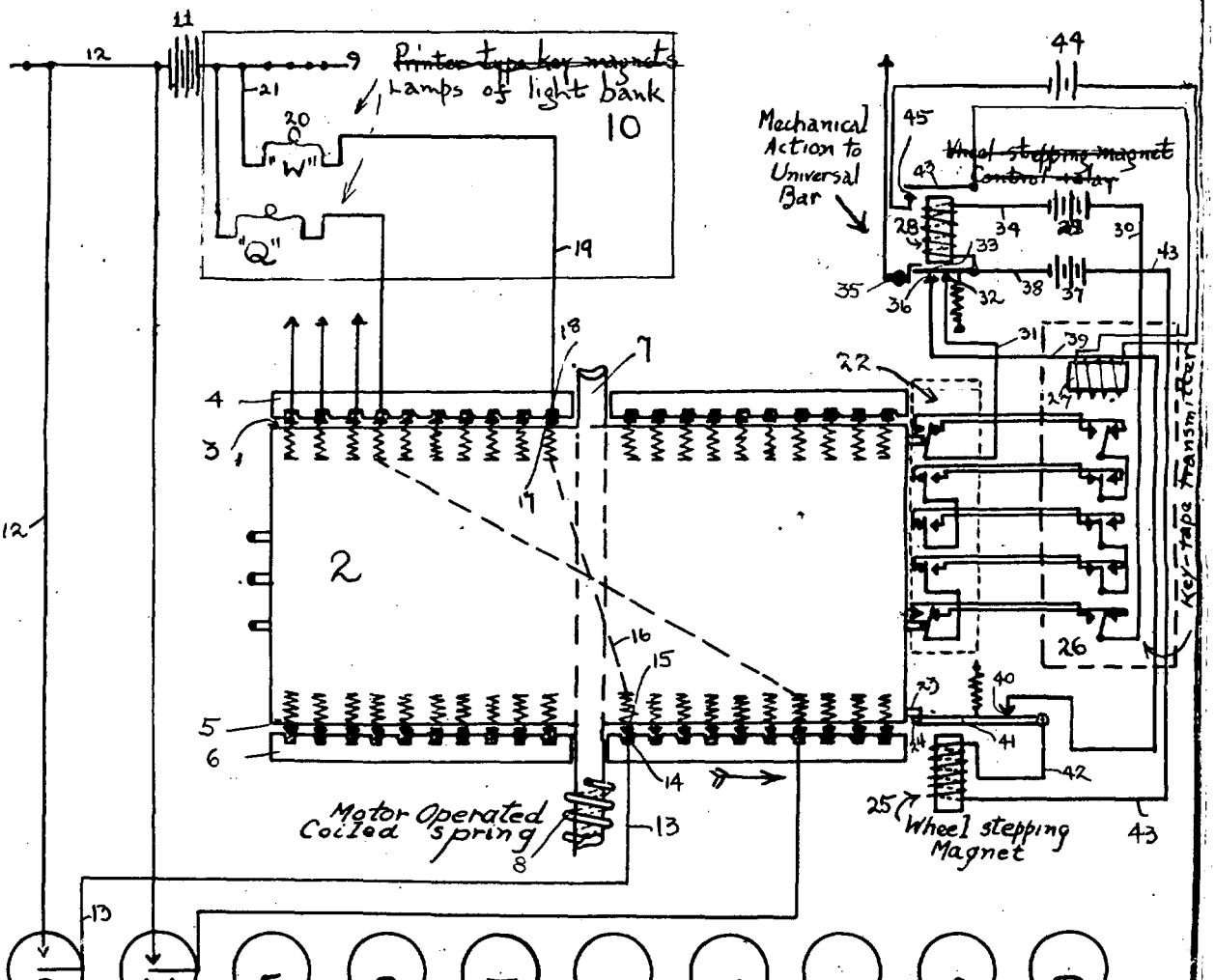


Fig. 2.



1

Fig. 1

TAB Q

Patent No. 2,028,772

(covers Converter M-134-T1)

Issued Jan. 28, 1936

to

William F. Friedman
and
George A. Graham

TOP SECRET

TOP SECRET

TAB R

Converter M-134-T2

and

Electrical Typewriter

TOP SECRET

Detailed Description of Converter M-134-T2 and Associated Electrical Typewriter. - Converter M-134-T2 (11" wide, 16" long, 9" high; weight 35 lbs.) in conjunction with the properly modified electrical typewriter (15" wide, 17" long, 11" high; weight 43 lbs.) constitutes an electromechanical machine by means of which messages may be enciphered or deciphered automatically up to speeds of about 40 words per minute. Converter M-134-T2 may be used to encipher or decipher messages without the electrical typewriter. In this case instead of the cryptographic resultant of the converter keyboard operation being printed by the electrical typewriter, each resultant character is indicated by lamp illumination on an alphabetically designated lamp strip.

Briefly, the cryptographic security of the converter is effected by the following features:

a. A celluloid tape, with pin holes punched in the five-unit code controlling a tape transmitter to progress in variable relationship five cipher discs (or rotors) as switching commutators to establish a resultant for each and every keyboard operation. Each resultant therefore depends upon the initial position of the key tape in the tape transmitter, upon the initial setting of the cipher discs and upon the subsequent positions of each.

b. A plug and jack strip which comprises a switching means for establishing various connections between the tape transmitter and the cipher discs.

The power facilities required for operation of the Converter M-134-T2 and the electrical typewriter are 110 volts d.c. with a capacity of at least 250 watts.

Converter M-134-T2. - Reference Tabs Q to Y inclusive. The converter comprises a base frame, keyboard, keyboard operation counter, keyboard universal bar contact combination, five rotatable cipher discs operating between stator elements, encipher and decipher reversing switch, five cipher disc step-forward magnets, tape transmitter, plug and jack strip, lamp strip, lamp resistance unit, one slow-release relay, multicontact terminal strip for connection to the electrical typewriter, power switch and lamp switch, power plug and cord, power fuse and incidental wiring.

Base Frame. - The base frame comprises a modification of the Remington noiseless typewriter as manufactured by the Remington Noiseless Typewriter Works, Middletown, Conn. All elements of the converter are mounted on this frame in order to employ a commercially available structure insofar as practicable.

Plug and Jack Strip. - Reference Tabs R and DD. Five plugs, cords and jacks are provided which are installed in the five connections between the tape-transmitter contacts and the cipher-disc magnets. The plugs are connected to the tape-transmitter contacts and are numbered accordingly from 1 to 5 inclusive. The jacks are connected to the cipher-disc magnets and are also numbered respectively from 1 to 5 inclusive. Accordingly, these connections may be patched across as desired and changed at will as a variable feature tending to further extend the cryptographic security of the machine. All stations must agree in this respect.

For continuation, see Tab S.

~~SECRET~~

~~SECRET~~

Fig. 1 - Converter M-134-T2 and Electrical Typewriter

TAB S

Converter M-134-T2

Front View

Continued from Tab R.

Lamp Strip. - Reference Tab R. The lamp strip may be used for the indication of resultants when the electrical typewriter is not used. The lamps are mounted beneath a bakelite strip which is provided with lettered opalescent inserts. One spare insert is also mounted on the strip to preserve the symmetry of the combination. The lamps are rated as 2.2 volts, .25 ampere Tung-Sol flashlight bulbs, non-focusing, as manufactured by the Tung-Sol Lamp Works, Inc., Neward, New Jersey, or equal. A 400-ohm resistance unit is connected in the lamp common.

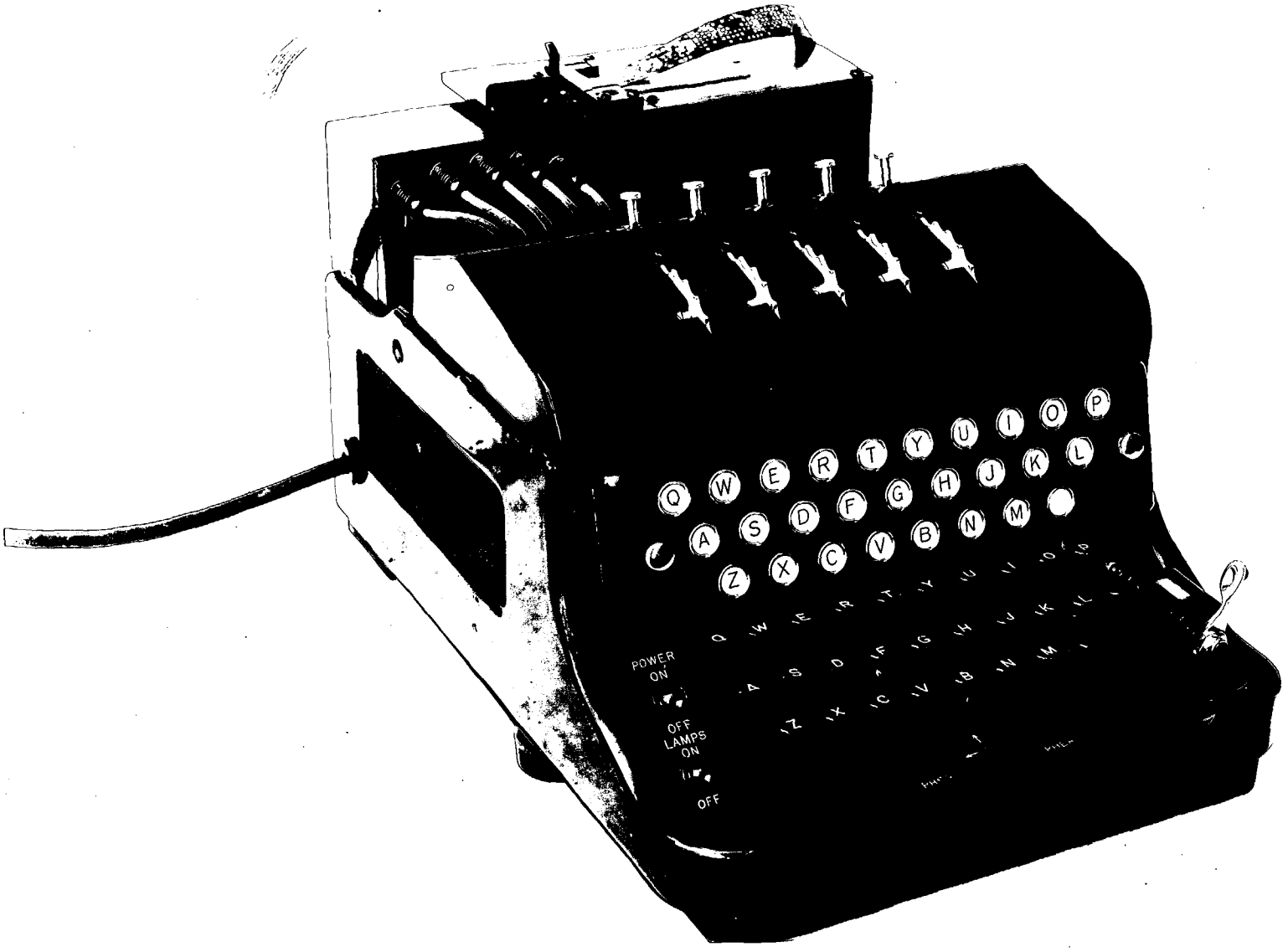
Keyboard. - The standard typewriter keyboard is used, so that the operator will not be required to learn a special keyboard. All keys other than the 26 letters of the alphabet and two blanks are omitted. The two blank keys are blocked up inoperative and are provided in order to make the plan view of the keyboard symmetrical as well as providing guide keys for the normal position of the operator's hands. In other words the keyboard is restricted to the 26 letters of the alphabet. Each key bar is provided with a contact extension which operates into contact jaws. Electrically all key bars are connected in common to one side of the circuit and the individual contact jaws are connected to the studs of the stationary plate of the enciphering-deciphering reversing switch. The individual circuits are connected through this switch and then through the cipher disc combination to the electrical typewriter solenoids or the lamps as the case may be. The key contact jaws are of the wiping type and should give a minimum of trouble.

Keyboard Universal Bar. - The keyboard is equipped with a universal bar mounted transversely and directly beneath the key bars and it is actuated by the depression of any of the keys. The depression of a key serves to rotate this universal bar on its axis, the movement being used for two purposes; i.e., to operate through a yoke coupling the operation counter; and also by means of a lever extension it closes two contact combinations.

Keyboard Operation Counter. - This counter is provided to record the number of keyboard operations as a check against the number of characters printed; the number of step-forward positions of the key tape: and the number of characters in the message or the cryptogram as the case may be. The counter may be restored to zero at any time by manual operation of the reset lever.

Keyboard Universal Bar Contact Combination. - These contacts are in "make" relationship with the universal bar in such a manner that the depression of a key causes these contacts to close before the individual key contacts are closed. It is important that this relationship be preserved for proper operation of the machine. Upon permitting the key to rise (return to normal) the universal contacts open after the individual key contacts open. The function of the universal contacts in the circuit is shown in Tab DD.

For additional description of parts, see Tabs R, U, W, Y, Z, AA, BB.



~~SECRET~~

Fig. 2 - Converter M-134-T2, Front View

TAB T

Converter M-134-T2

Rear view, tape transmitter removed

For detailed description of Converter M-134-T2

see Tabs R, S. U, W, Y, Z, AA, BB

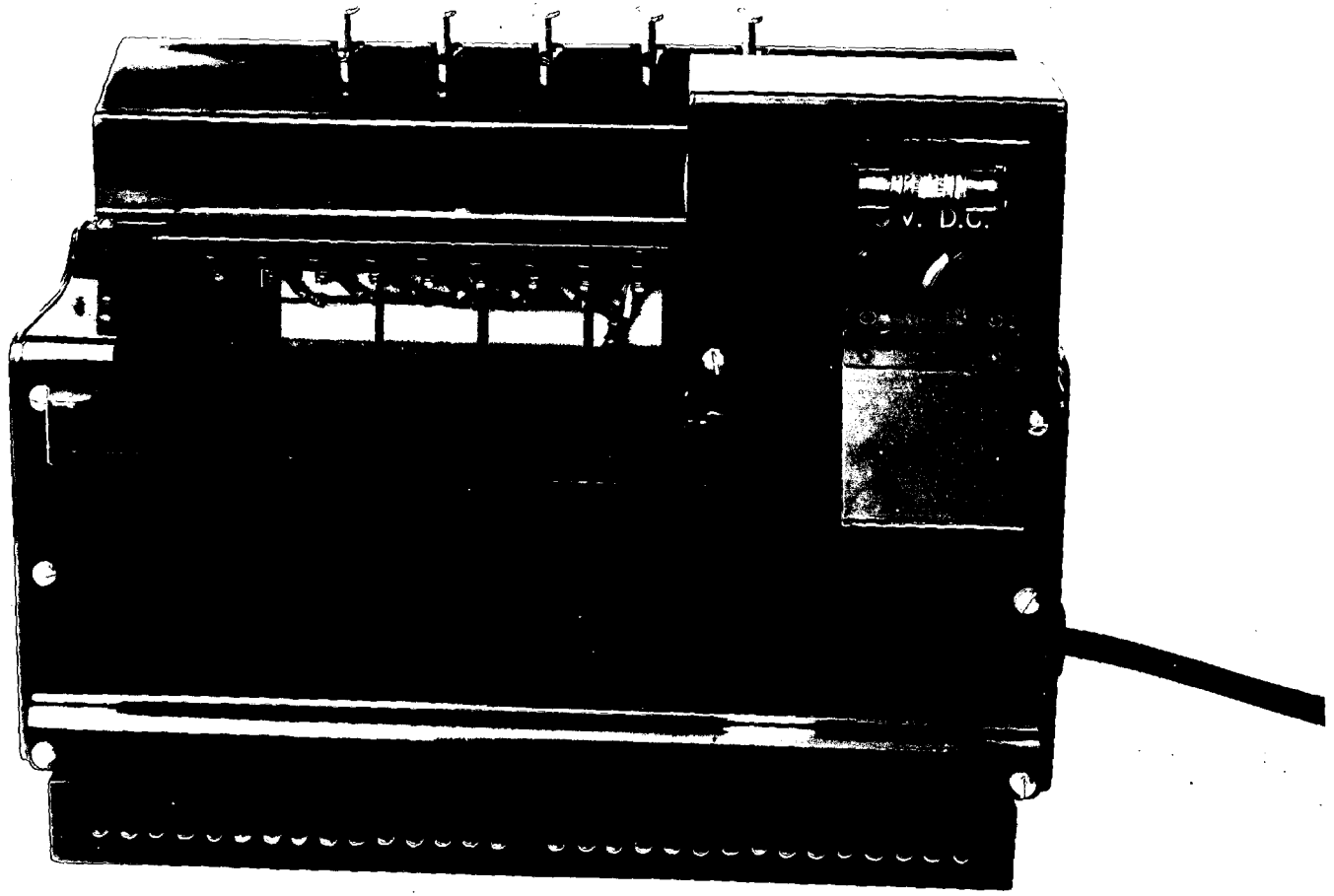


Fig. 3 - Converter M-134-T2, Rear View, Tape Transmitter Removed

TAB U

Converter M-134-T2

Rear View

Covers Removed

Slow Release Relay. - Reference Tabs T, X, and DD. The function of this relay is to energize the cipher-disc stepping magnets for sufficient time to insure a complete core travel and to subsequently clear the circuit to the normal or open state. This relay is of 1300 ohms resistence and is equipped with a copper slug for slow release. The contacts are an application of the Burgess inclosed type microswitch. These contacts have proved very dependable in service and should require no attention.

For additional detailed description of Converter M-134-T2, see Tabs R, S, W, Y, Z, AA, BB.

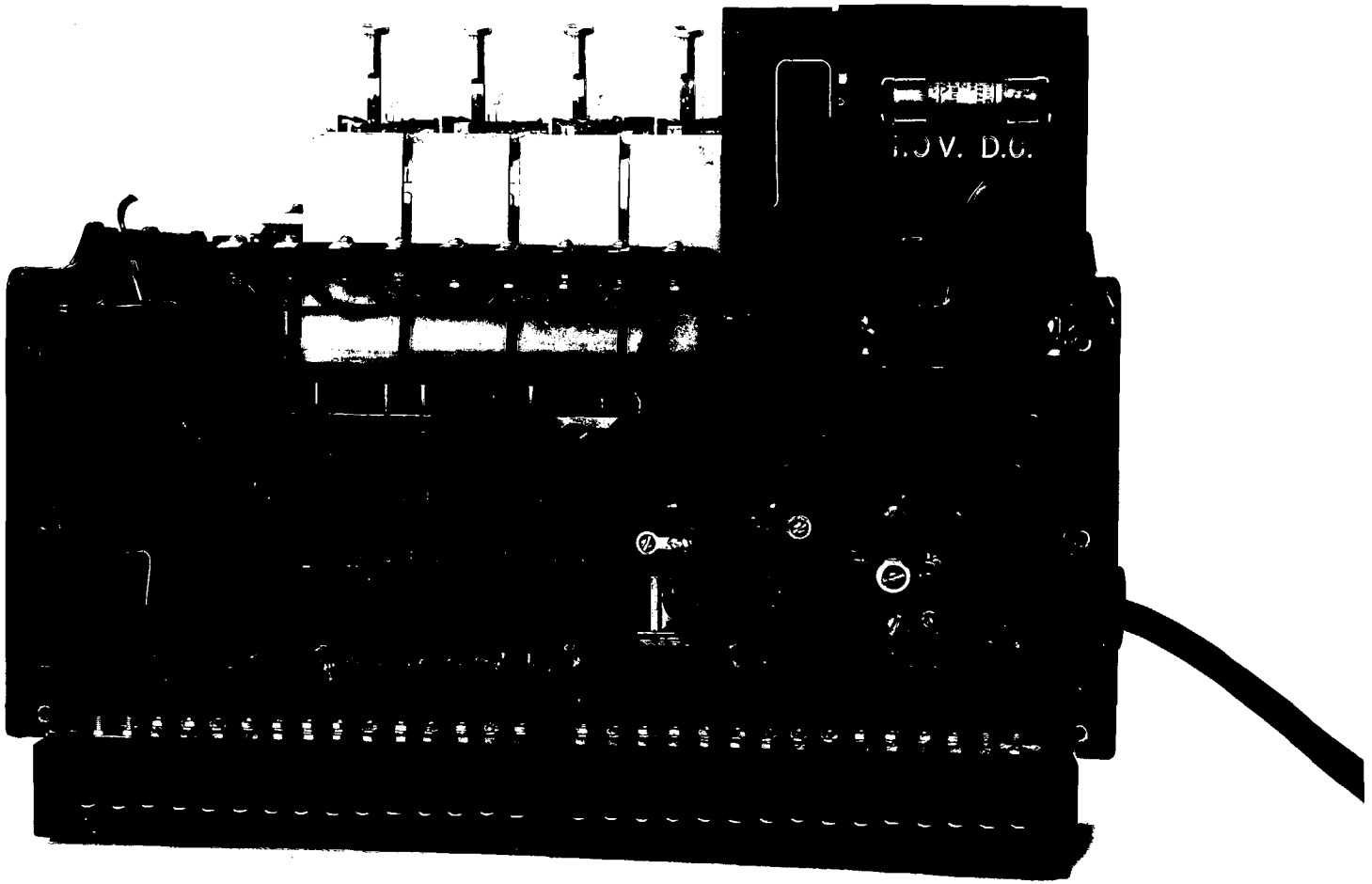


Fig. 4 - Converter M-134-T2, Rear View, Covers Removed

TAB V

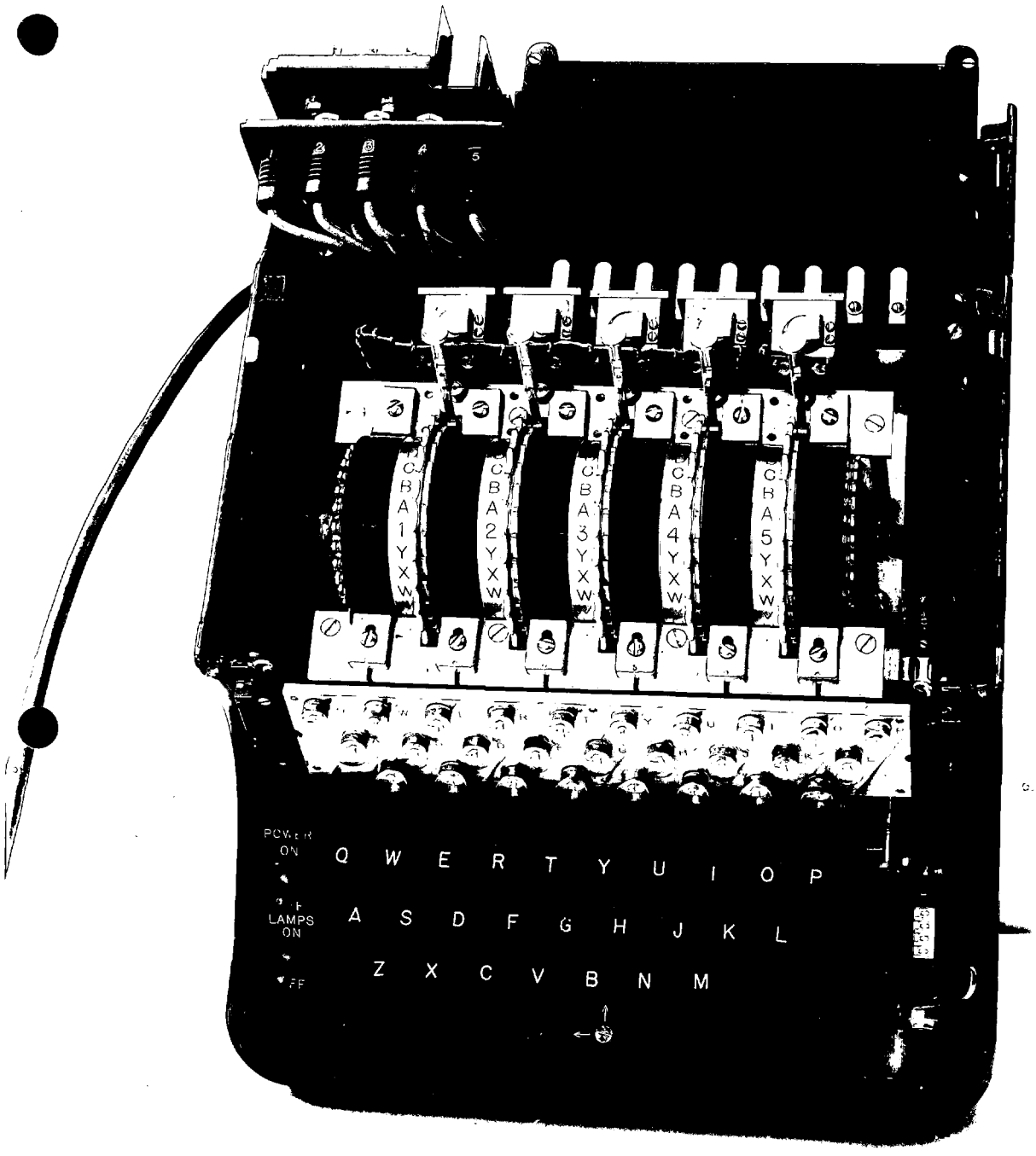
Converter M-134-T2

Plan View

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB

~~SECRET~~



~~SECRET~~

Fig. 6 - Converter M-134-T2, Plan View, Covers Removed

TAB W

Converter M-134-T2

Plan View

Covers Removed

Cipher Discs. - Reference Tabs V, W and GG. The converter is equipped with five cipher discs positioned to rotate between six stator heads as distributors or commutators. Four of these stator heads separate the cipher discs and are provided with distributor faces against each cipher disc. Two end stator heads are provided with distributor faces internally contacting the end cipher discs and externally by means of stud terminals are connected to the key contacts and the electrical typewriter solenoids or the lamps through the encipher-decipher reversing switch. Each cipher disc presents 26 segments on each face which are in contact with 26 spring and ball contacts on each stator head. The connections through the stator head are direct. The segments on one face of each individual cipher disc are wired in random fashion to the segments on the opposite face of the disc. The particular wiring for each disc and for the combination is shown in Tab GG. The exposed periphery or band of each disc is designated in 25 positions alphabetically from A to Y, the 26th or Z position being designated by a numeral. The numerals serve to identify the disc in addition to indicating the 26th position. Each disc is readily removable and interchangeable with any other disc. No through shaft is used, each disc being rotatable upon a spring tensioned ball in the center of the stator heads, and in removal any particular disc is simply withdrawn from between the stator heads. In addition to the designation band each disc presents a scalloped edge for two purposes; i.e., to facilitate setting of the discs by hand, and also acting as positioning centers in conjunction with the step-forward mechanism. In setting the discs to an initial position they may be turned in either direction by depressing and holding back the button extensions of the step-forward pawls located directly behind each disc position. As regards electrical continuity through the combination of disc and stator heads there are 26 wires connected to each end stator head and 26 circuits through the discs no matter in which position the discs happen to stop. It will be seen that 26 through circuits are provided at all times even though the relationship of all circuits is altered by any disc movement. One particular circuit is traced through the combination in Tab GG.

For additional detailed description of Converter M-134-T2
see Tabs R, S, U, W, Y, Z, AA, BB.

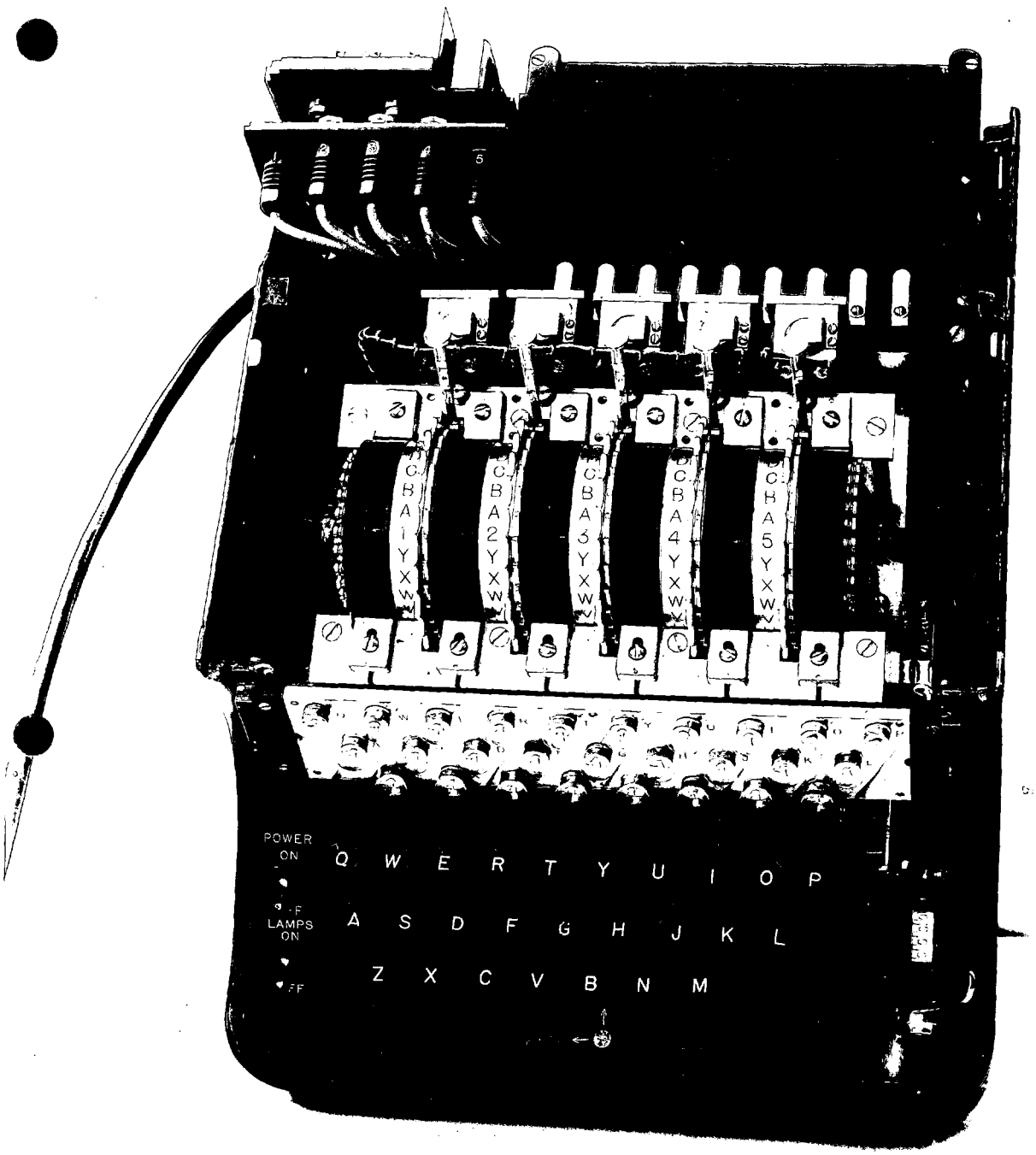


Fig. 6 - Converter M-134-T2, Plan View, Covers Removed

TAB X

Converter M-134-T2

Plan View, 2 cipher discs removed.

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB

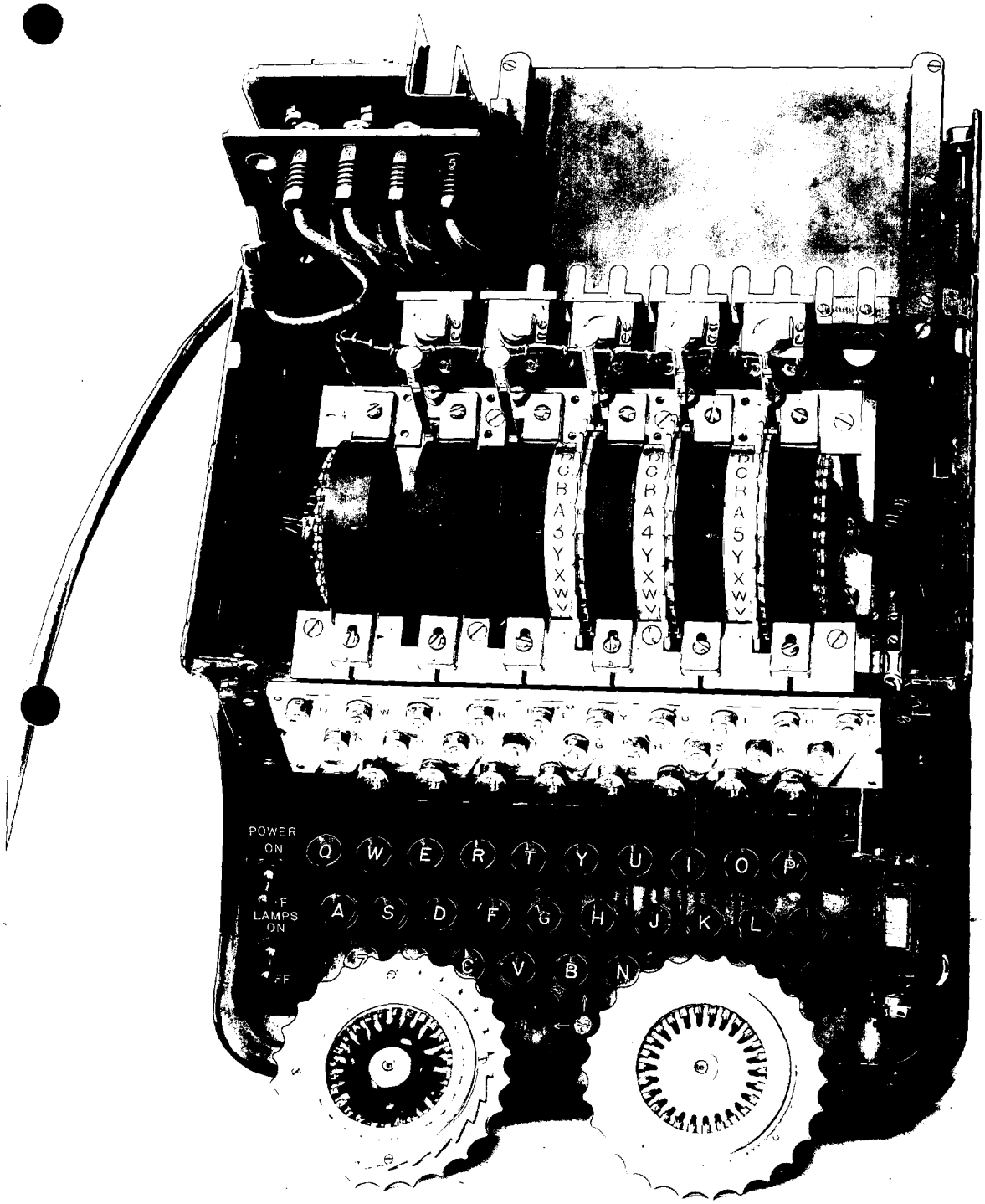


Fig. 7 - Converter M-134-T2, Plan View, 2 Cipher Disks Removed

TAB Y

Converter M-134-T2

Bottom View, Covers Removed

Encipher-Decipher Reversing Switch. - Reference Tabs X and EE. This switch is mounted beneath the keyboard and is operated through a rack and pinion drive, the pinion being extended to a knob in front of the keys. The switch acts as a combination of 26 double-pole, double-throw switches in the 26 circuits from the key contact jaws through the cipher-disc combination to the typewriter solenoids or lamps as the case may be, and it functions to reverse the cipher-disc combination in these circuits. This feature is necessary in order to maintain the reciprocal relationship between the resultant obtained in encipherment with respect to the resultant required in decipherment. As an example and as shown in Tab EE, with the switch in encipher position and striking the A key results in the printing of a G. Then with discs in the same position and switch thrown to decipher position, the striking of the G key results in the printing of an A.

For additional detailed description see Tabs R, S, U, W, Y, Z, AA, BB.

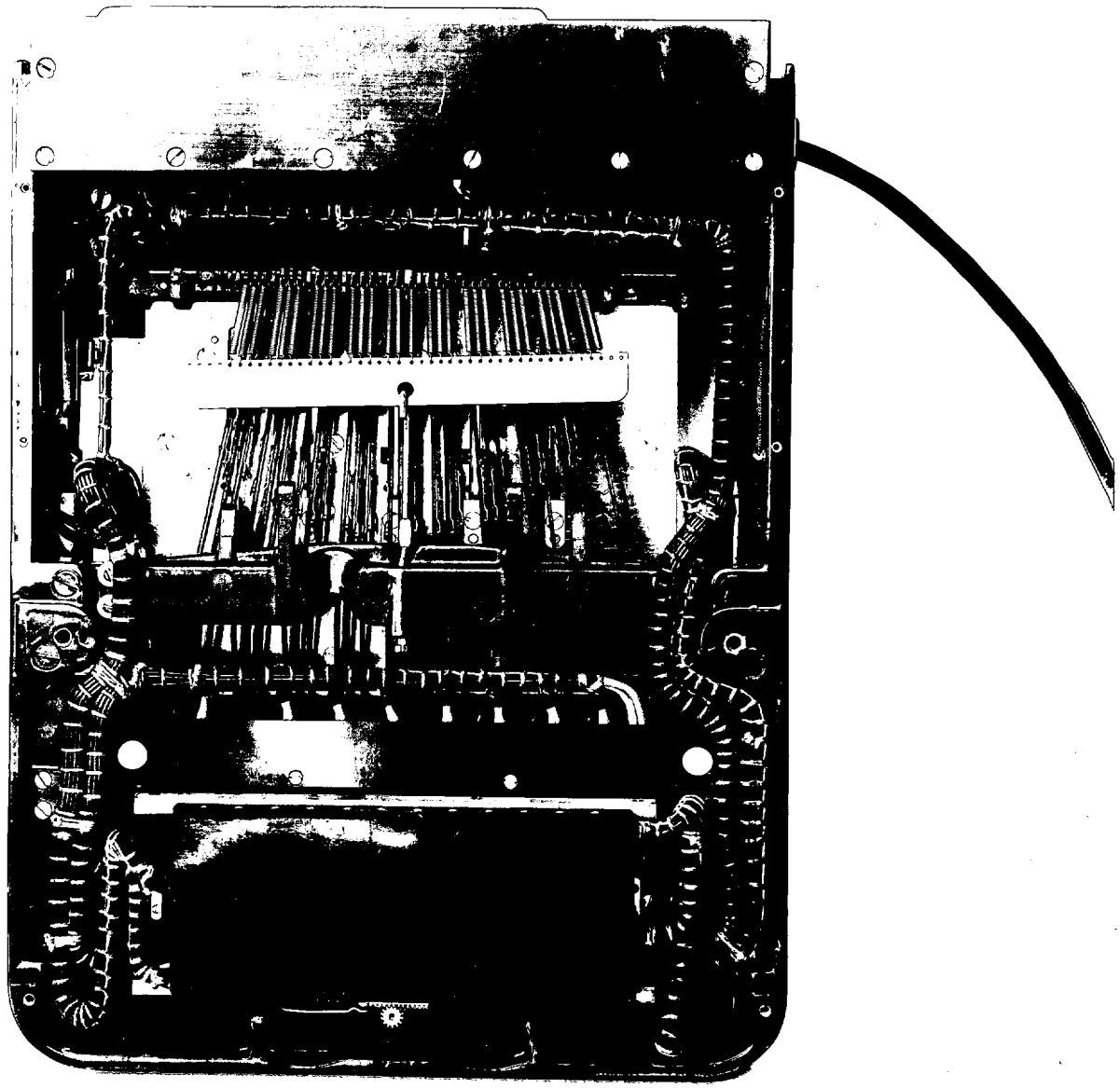


Fig. 8 - Converter M-134-T2, Bottom View, Covers Removed

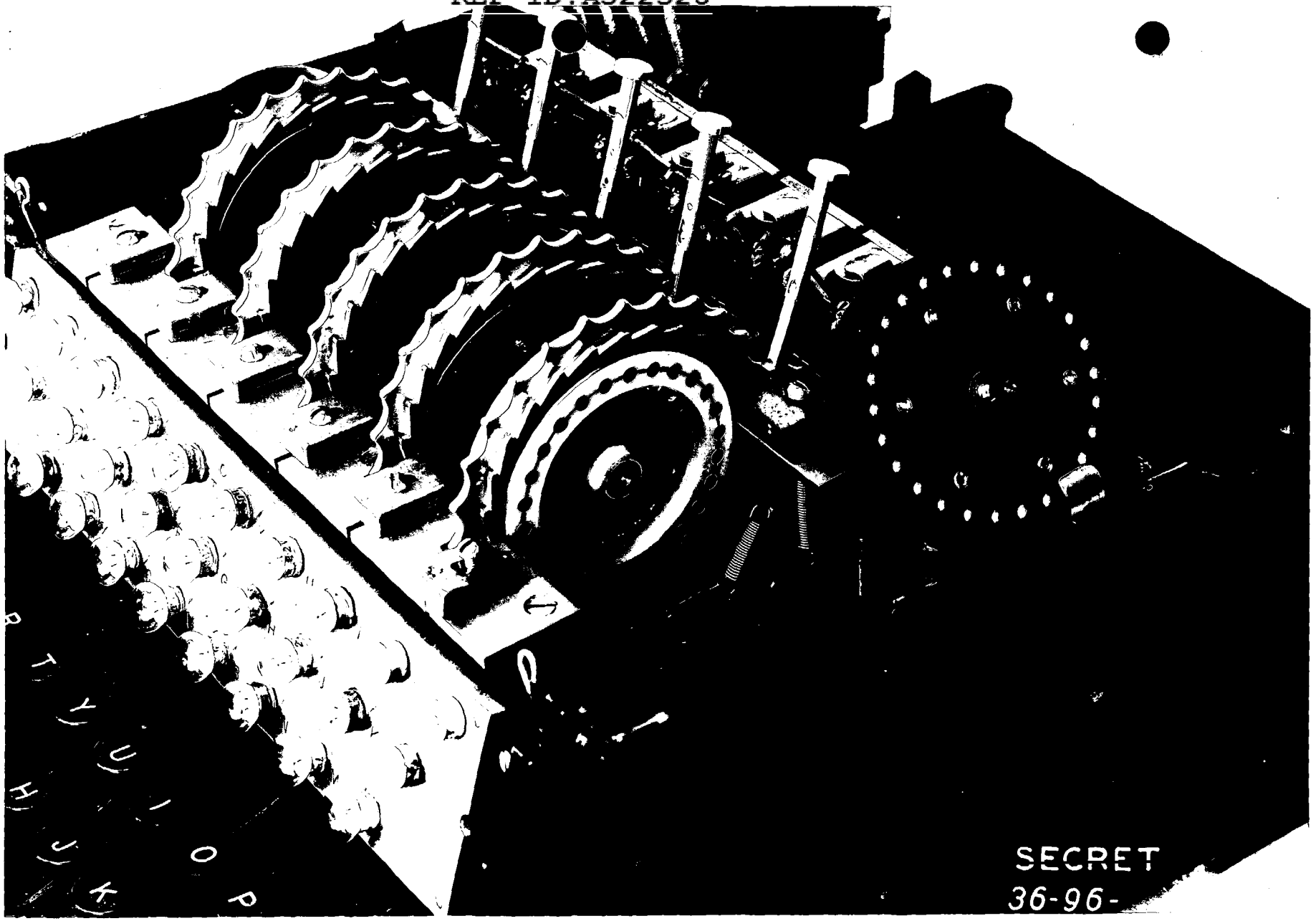
TAB Z

Converter M-134-T2

Disk Stepping Mechanism

Cipher Disc Step Forward Mechanism. - Each of the five cipher discs are equipped with individual stepping mechanisms comprising a magnet solenoid, tension spring, step-forward pawl, and location roller. The individual magnets are operated by the tape transmitter. Upon the circuit being closed through a given magnet, this magnet draws down the core building up tension in a spring and near the end of the stroke a step-forward pawl is drawn into engagement with a ratchet tooth on the pertinent cipher disc. Upon deenergization of the magnet the power stored in the spring is delivered to step forward the cipher disc through the step-forward pawl after which the step-forward pawl is disengaged. A location roller and arm is properly conjunctioned with this action to definitely establish the stop position of the cipher disc. This roller is beneath the cipher disc and falls into the scalloped edge on the periphery of the disc. The step-forward pawl arms are extended through the cover of the converter into buttons to permit the manual disengagement of the pawls from the cipher discs in order to facilitate the rotation of the discs by hand. The buttons should be depressed and moved to the rear when disengagement is desired.

For additional detailed description, see Tabs R, S, U, W, Y, Z, AA, BB.



~~SECRET~~

Fig. 9 - Converter M-134-T2, Disk Stepping Mechanism

TOP SECRET

TAB AA

Converter M-134-T2

Tape Transmitter

Featuring Contact Combination

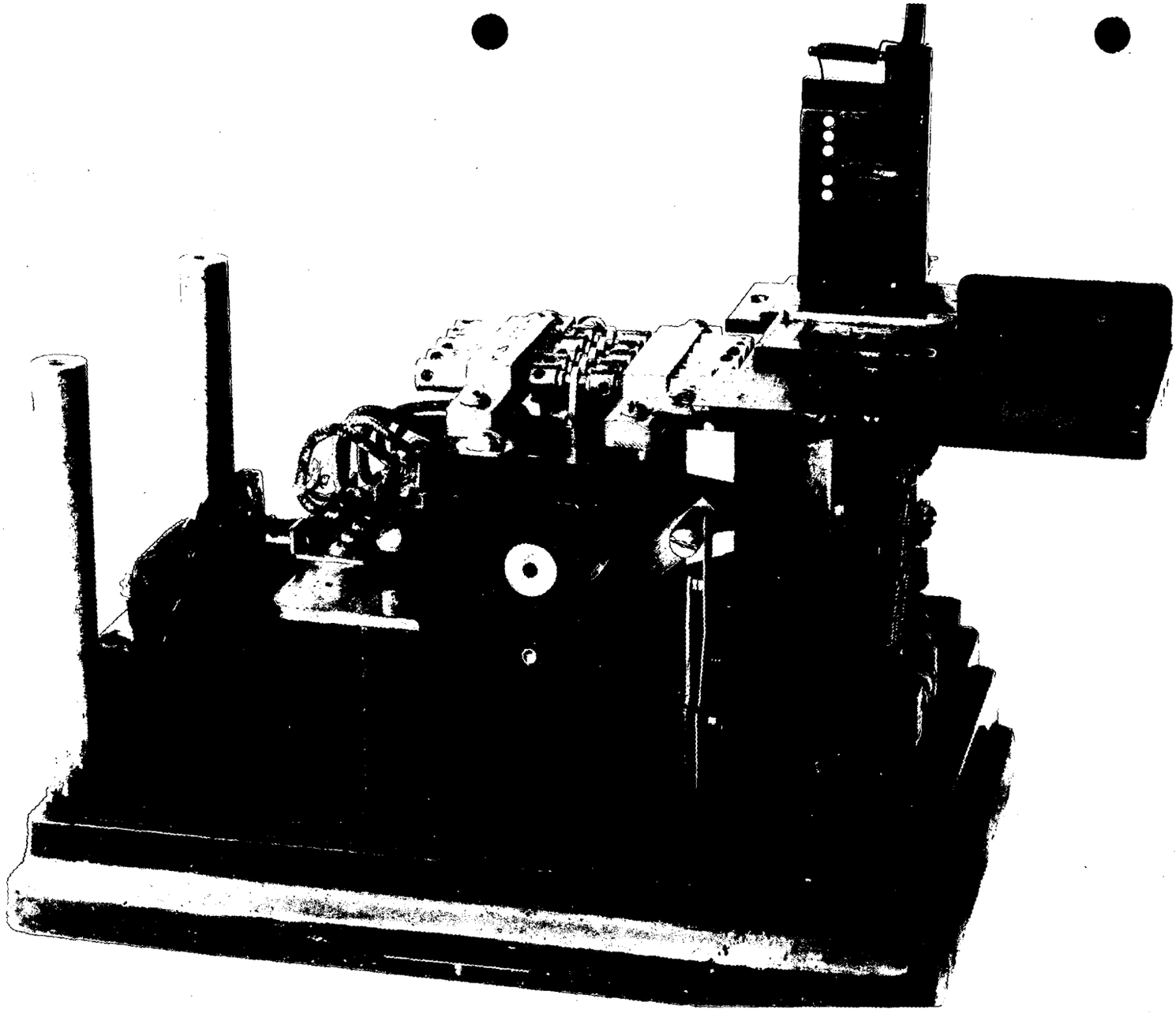
TOP SECRET

Tape Transmitter. - Ref. Tabs Z and FF.

(1) This unit is a modified Western Electric Co. multiplex transmitter 1-B as used commercially in multiplex printing telegraphy. This transmitter operates on the five-unit code from a perforated tape to establish five contact combinations in marking or spacing positions dependent upon the arrangement of the code perforations in groups transversely disposed on the tape. There are 32 different permutative possibilities in the five-unit code. The tape is provided also with a continuous series of perforations in line longitudinally, the spacing being identical with the spacing between code groups, to permit progressing the tape consecutively from one code group to the next. The tape transmitter is equipped with a tape groove and guide; a latched die to permit inserting the tape at any desired code group; a step-forward star wheel engaging the step-forward holes of the tape; five code pins conjunctive with the code-group hole positions of the tape and operative upon five contact levers in marking-spacing positions; and a magnet acting to depress all five code pins from tape engagement and to step forward the tape by ratchet movement on the star wheel to the next code group, after which the code pins are released to assume their tape dictated positions. When a code pin is held down by the circumstance of no hole in the tape, at that time the associated contact lever is held against the spacing-contact bus. On the other hand, when a code pin is permitted to rise through a hole in the tape, the contact lever is moved over to the marking-contact bus.

(2) The modification of the tape transmitter comprises the addition of a contact combination operated by the magnet armature and a wiring rearrangement to adapt the unit for its proper function in the converter.

(3) The function of the tape transmitter in the converter is to step forward the cipher discs in accordance with the key tape. The key tape is made of celluloid rather than paper in order to permit longer repetitive use. Each code group of the key tape establishes, through the code pins and contact levers of the tape transmitter, circuits energizing the pertinent cipher-disc magnets selected which act to step forward the pertinent discs one position, leaving the non-selected magnets in normal position. The circuits from the disc magnets to the tape-transmitter contacts are connected in series-parallel with respect to the contact combination of the tape-transmitter magnet, in order that the disc magnets be not energized until after the tape has been stepped forward and all pins and contact levers are in position. The necessity for this tape-transmitter, magnet-contact combination depends upon whether or not the common connection from power is connected to the marking of spacing bus of the transmitter. If the



SECRET

Fig.10 - Tape Transmitter, Featuring Contact Combination

common is connected to the marking bus, the magnet contacts can be eliminated, but if the common is connected to the spacing bus the inclusion of the magnet contacts is imperative. The common is normally connected to the marking bus but may very readily be changed to the spacing bus. Access to these busses may be had by removing the cover plate of the tape transmitter. The advantage of the use of the marking bus in that a tape hole means step forward of the pertinent cipher disc and is consistent with the telegraphic viewpoint of marking signals. On the other hand, the advantages of the use of the spacing bus are twofold; first, the transmitter contacts are somewhat more positive than in marking position due to spring tensions, and second, being inconsistent with the telegraphic viewpoint, offer possibilities in cryptographic security because the tape no-hole positions normally known as spacing then actually become marking insofar as the cipher-disc magnets are concerned. In either event it will be noted by reference to Tab DD that the cipher-disc, tape-transmitter circuit is closed through the contacts of a slow-release relay which in subsequently opening clears the circuits for spring step forward of the cipher discs leaving the circuit normally open. Note: All intercommunicating stations must be in agreement with regard to the use of the marking or the spacing bus for disc step forward.

For additional detailed description, see Tabs R, S, U, W, Y, Z, AA, BB.

TOP SECRET

TAB BB

Associated Electrical Typewriter

of

Converter M-134-T2

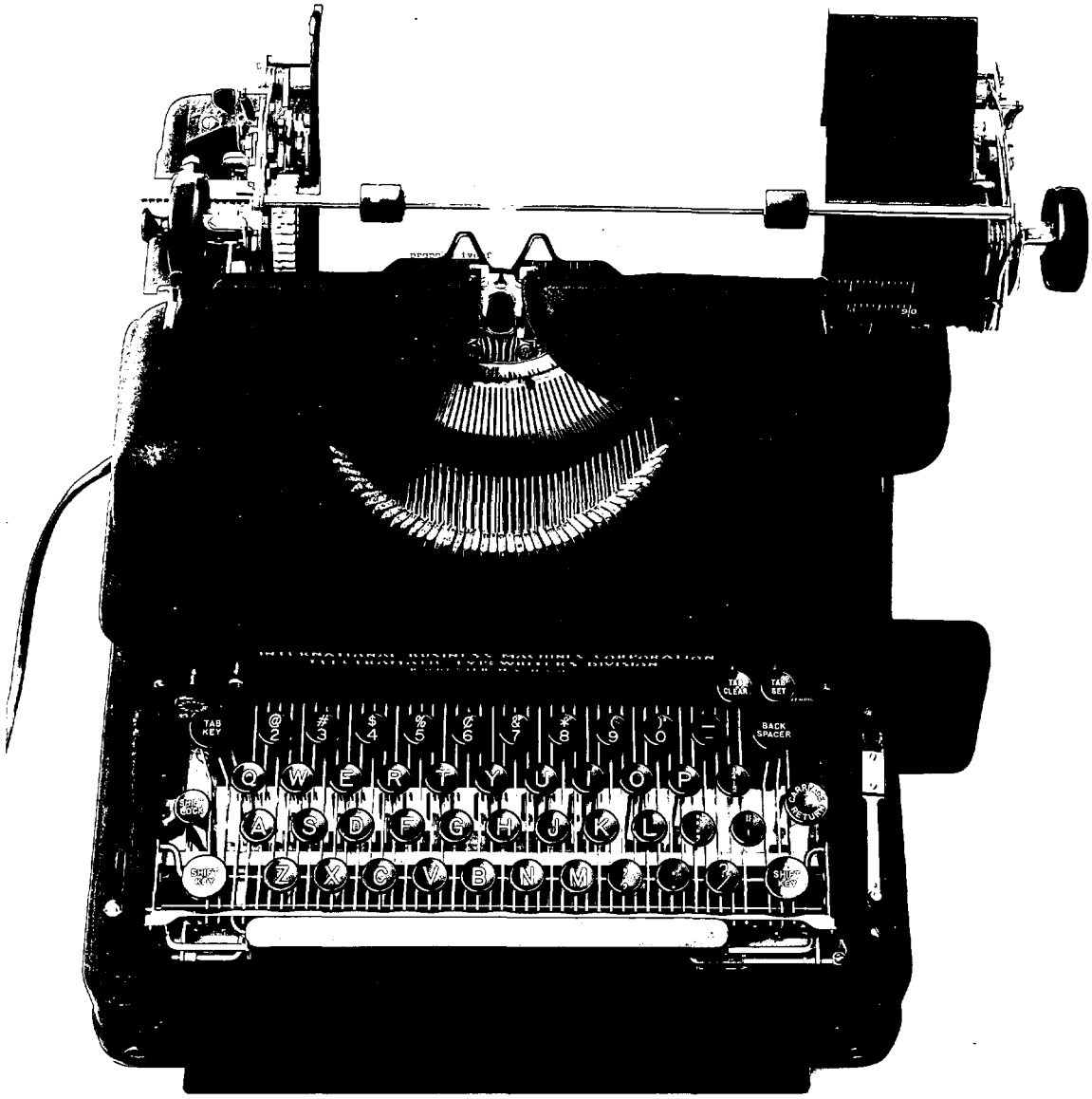
Plan view

TOP SECRET

Electrical Typewriter. - Ref. Tabs AA, BB, CC and DD. This typewriter comprises a modification of the International Business Machines Corporation electromatic typewriter. The modification consists of: the incorporation of 26 solenoid magnets with drag links arranged to operate the 26 letter key bars; the addition of a universal bar operating a contact combination upon the depression of any key bar; and the incorporation of an automatic five-character space contact and solenoid magnet operating upon the space bar; and an automatic carriage-return contact with solenoid magnet operating upon the carriage-return key bar and including a warning bell signal. The spacing contact is operated by every sixth detent of the tabulating rack. The carriage-return contact is operated by a stud at the end of the tabulating rack. The wiring is terminated in a plug strip on the base front of the typewriter proper for engagement with a jack strip at the rear of the converter. A plug and cord are provided for connection to power for the operation of the driving motor.

For additional detailed description, see Tabs R, S, U, W, Y, Z, AA, BB.

~~SECRET~~



~~SECRET~~

Fig.11 - Electrical Typewriter, Plan View

TAB CC

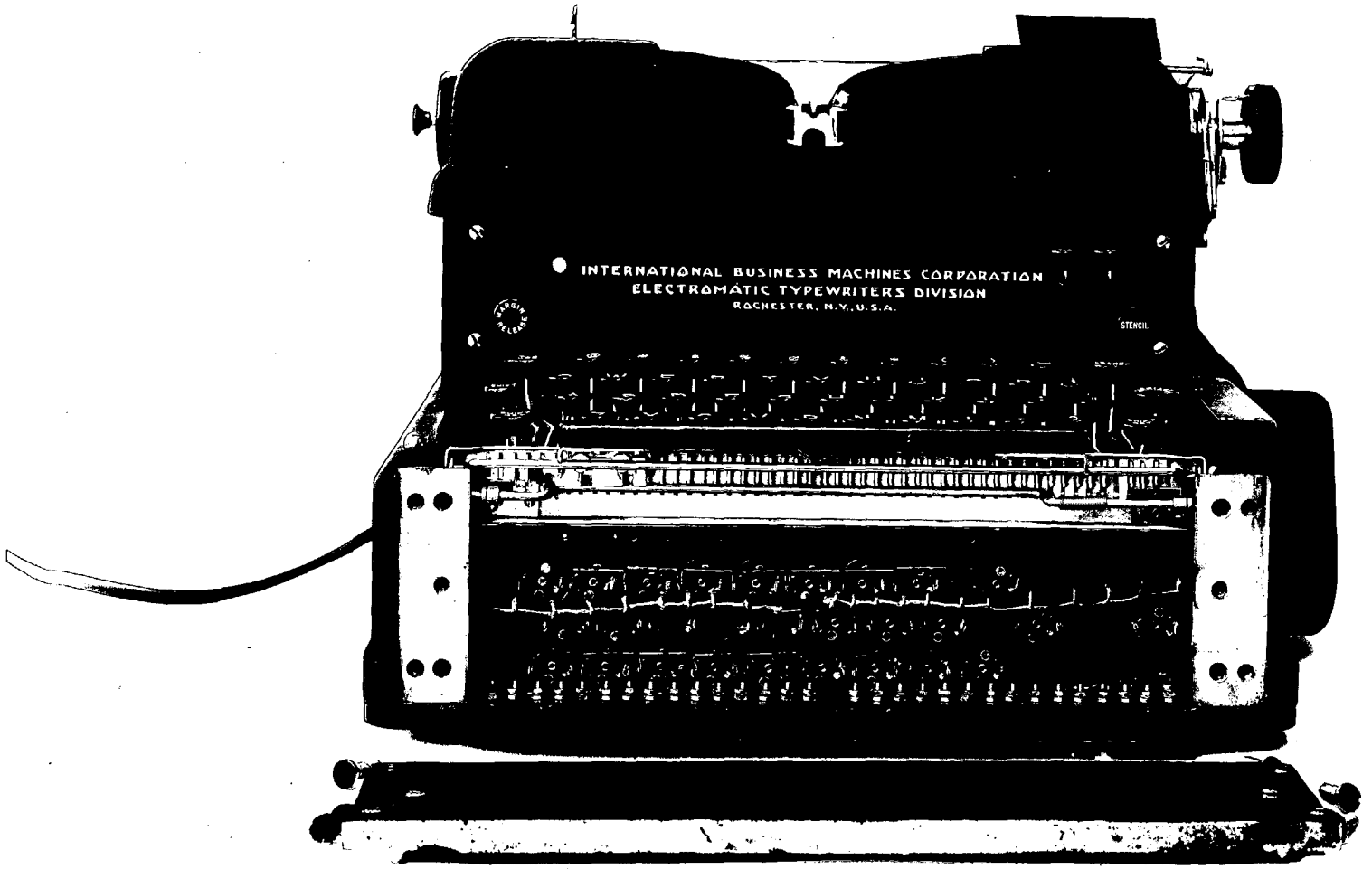
Converter M-134-T2

Associated Electrical Typewriter

(showing solenoids)

For detailed description of Electrical Typewriter, see Tab BB.

For other detailed description, see Tabs R, S, U, W, Y, Z, AA, BB.



~~SECRET~~

Fig.12 - **Electrical** Typewriter, Showing Solenoids

TOP SECRET

TAB DD

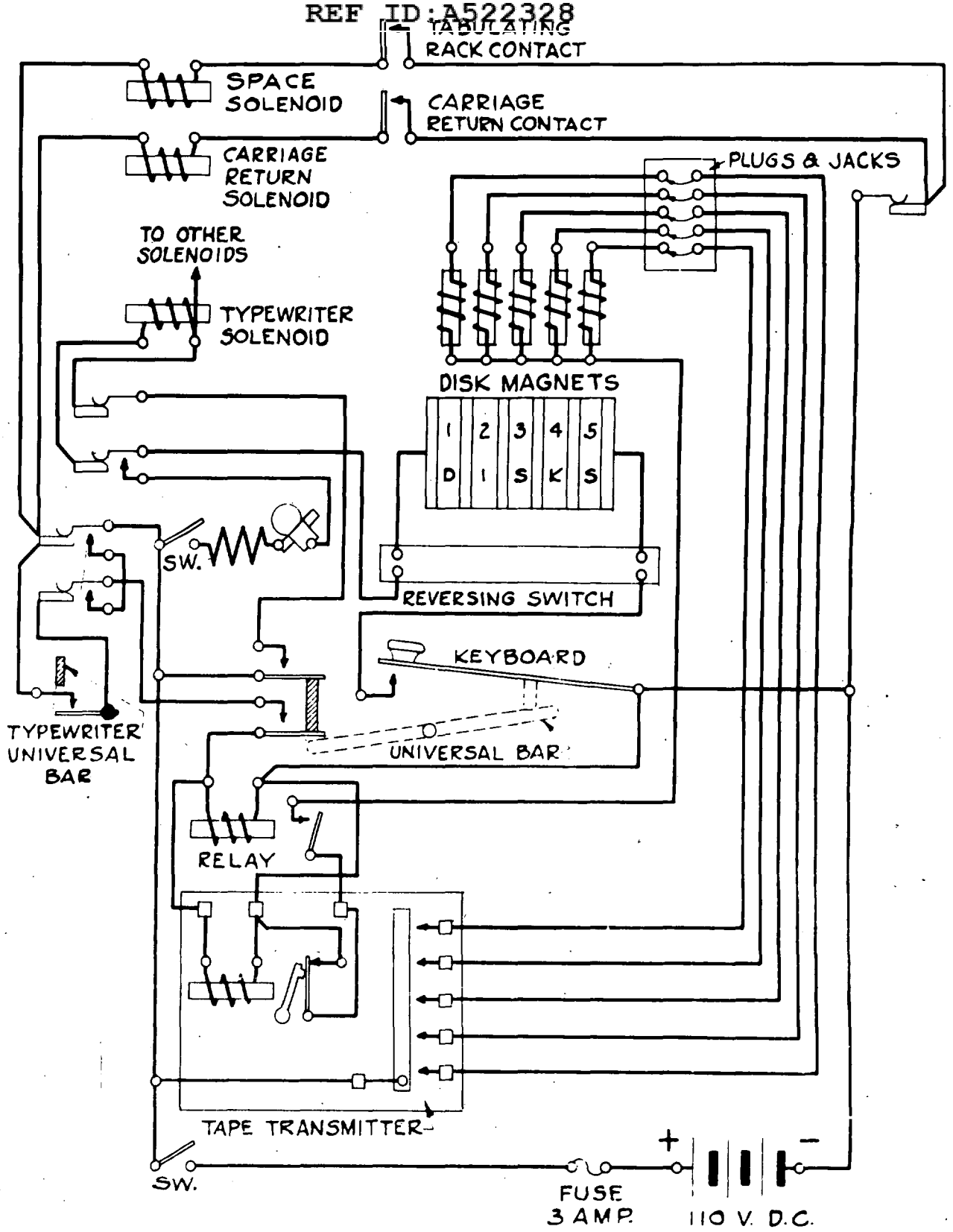
Converter M-134-T2

Schematic Diagram

TOP SECRET

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB



~~SECRET~~

FIG. 14
SCHEMATIC DIAGRAM

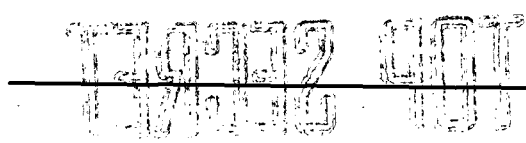
TAB EE

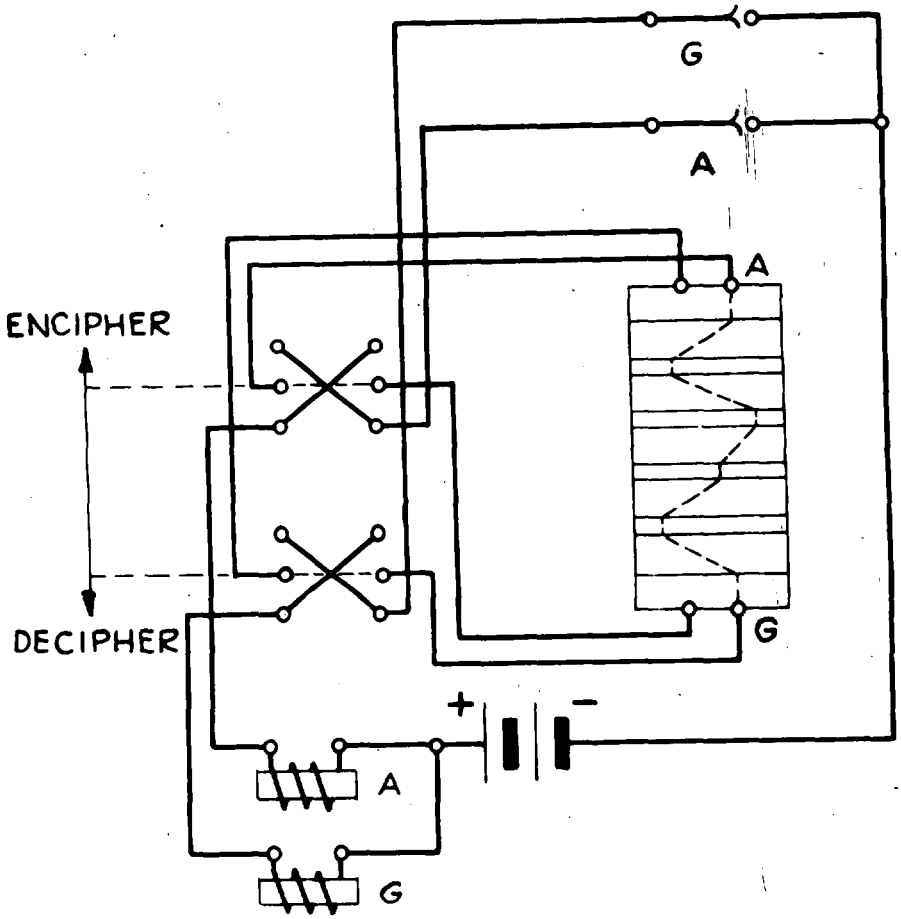
Converter M-134-T2

Theory of reversing switch

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB





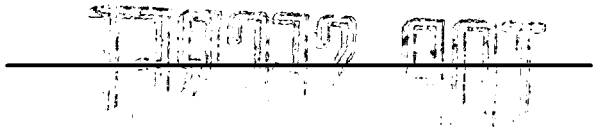
~~SECRET~~

FIG. 15
THEORY OF REVERSING SWITCH

TAB FF

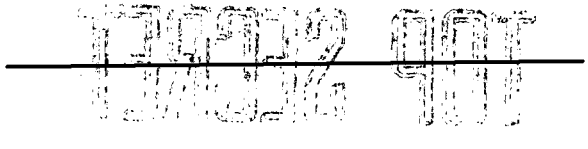
Converter M-134-T2

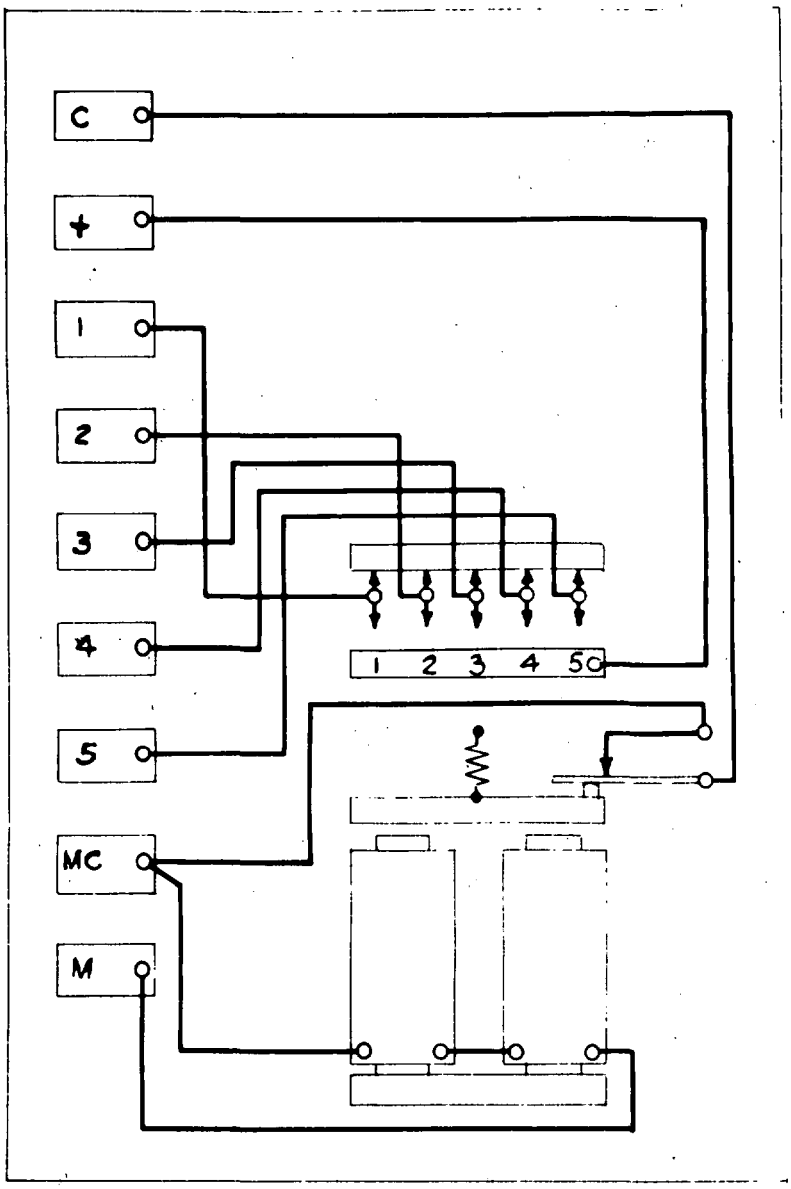
Wiring of tape transmitter



For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB





~~SECRET~~

FIG. 16
WIRING OF TAPE TRANSMITTER

TAB GG

Converter M-134-T2

Cross wiring of individual discs

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB

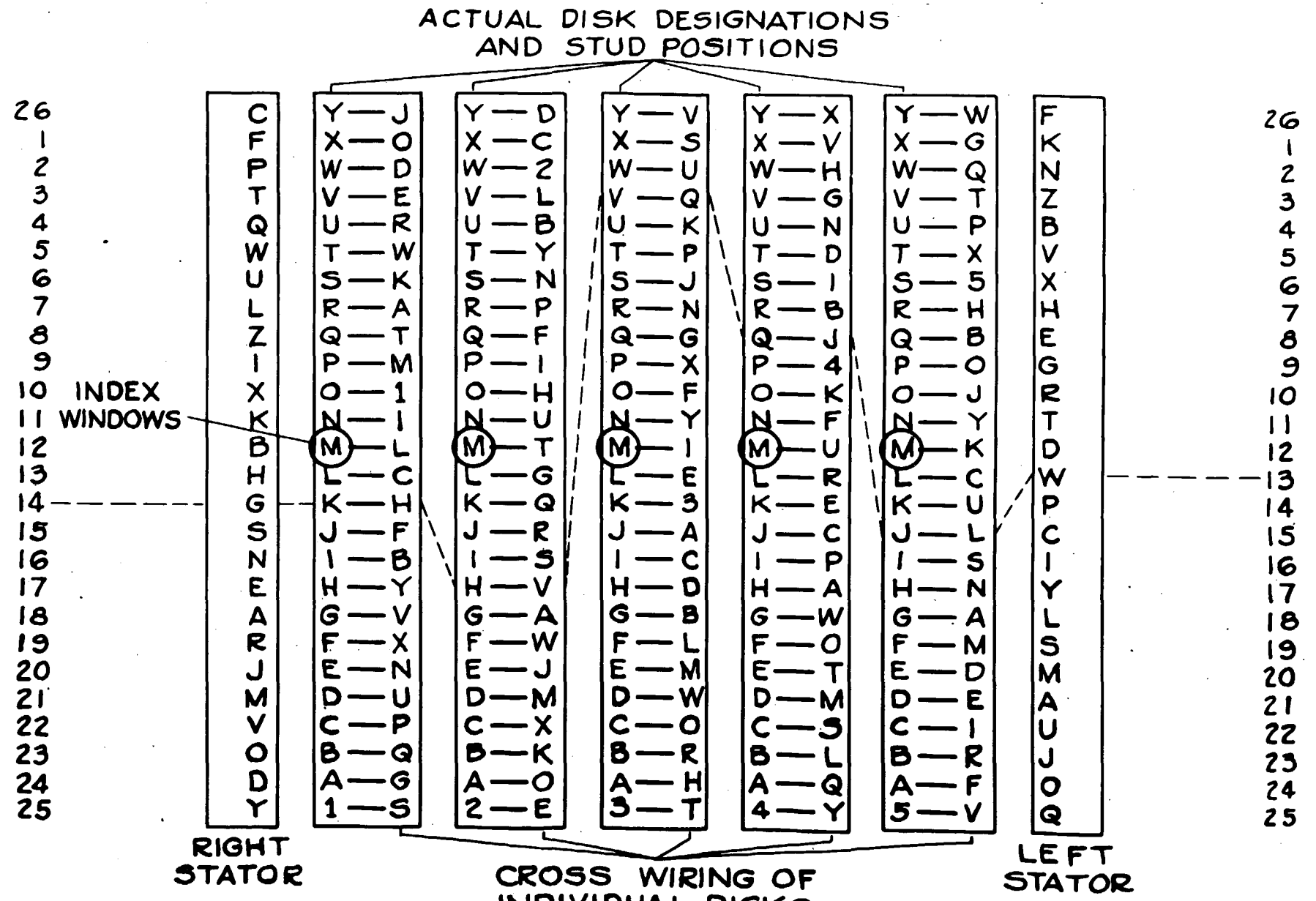


FIG. 17 CIPHER DISK CONNECTION

SECRET

TAB HH

Wiring Diagram of Converter M-134-T2

For detailed description of Converter M-134-T2

see Tabs R, S, U, W, Y, Z, AA, BB

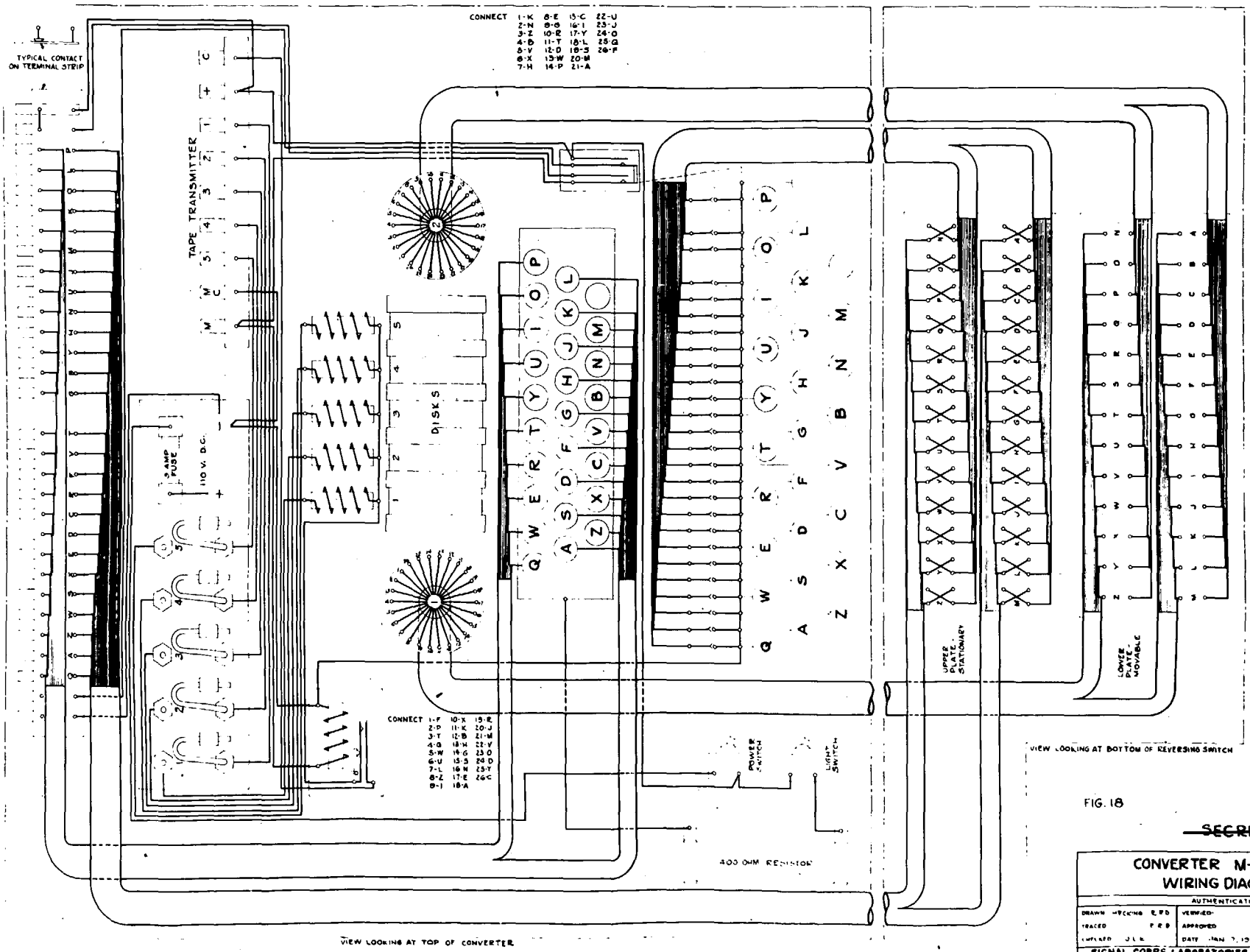


FIG. 18

~~SECRET~~

CONVERTER M-134-T2 WIRING DIAGRAM

AUTHENTICATION		
DRAWN HECKING E.P.D.	VERIFIED	ENGINEER A.G.F.
TRACED P.R.D.	APPROVED	CH. OF SECTION
CHECKED J.L.R.	DATE JAN 7, 1938	APPROVED

SIGNAL CORPS LABORATORIES
U. S. ARMY
FORT MONMOUTH NEW JERSEY

ES-D-2751-B

TOP SECRET

TAB II

Patent Application No. 682,096

(covers Converters M-134-T2, M-134, M-134-A)

Filed by William F. Friedman

July 25, 1933

Not issued: Under Patent Office Secrecy Order

TOP SECRET