

A
H
A

19

~~TOP SECRET~~

HISTORY OF CONVERTER M-134-C

VOLUME 2

Declassified and approved for release by NSA on
11-18-2013 pursuant to E.O. 13526

HISTORY OF CONVERTER M-134-C

VOLUME 2

Do Not Destroy. Return to the NSA Library when no longer needed.	
L-1547	Copy No. 1
TL	

RECORD COPY
DO NOT DESTROY OR MUTILATE

TABLE OF CONTENTS

CHAPTER	VOLUME 1	Pages
I	INTRODUCTION (Summary).....	1-12
II	THE BEGINNING OF THE ELECTRICAL MACHINE AGE IN ARMY CRYPTOGRAPHY.....	13-16
III	HEBBERN CONVERTER (and Related Patents).....	17-25
IV	CONVERTER M-134-T1.....	26-44
V	CONVERTER M-134-T2.....	45-56

VOLUME 2

VI	CONVERTER M-134.....	1-9
VII	CONVERTER M-134-A.....	10-27
VIII	DISTRIBUTION AND USE OF CONVERTER M-134-AND CONVERTER M-134-A.....	28-34
IX	KEYING UNIT M-229.....	35-49
X	CONVERTER M-134-B (and other Unadopted Modifications of Converter M-134-T2 and Converter M-134-T1).....	50-52
Appendix	CHANGES IN KEYING INSTRUCTIONS FOR CON- VERTER M-134, M-134-A	

VOLUME 3

XI	DEVELOPMENT OF CONVERTER M-134-C.....	1-9
XII	PROCUREMENT OF CONVERTER M-134-C.....	10-16
XIII	DISTRIBUTION AND USE.....	
XIV	CRYPTOGRAPHIC SECURITY OF CONVERTER M-134-C.....	
XV	PHYSICAL SAFEGUARDING OF CONVERTER M-134-C.....	
XVI	THE COMAR COMMISSION.....	
XVII	MAINTENANCE OF CONVERTER M-134-C.....	
XVIII	THE ZERO MACHINE.....	

DETAILED TABLE OF CONTENTS

FOR

VOLUME 2

CHAPTER		PAGE
VI	CONVERTER M-134.....	1
	A. General.....	1
	B. Adoption as Standard.....	3
	C. Procurement.....	4
VII	CONVERTER M-134-A.....	10
	A. General.....	10
	B. Procurement.....	11
	C. Description.....	15
	D. Keying Instructions.....	19
	E. Cryptographic Security.....	23
	F. Tape Numbering Machine 190.....	24
	G. Evaluation.....	25
VIII	DISTRIBUTION AND USE OF CONVERTER M-134 AND M-134-A.....	28
IX	KEYING UNIT M-229.....	35
	A. General.....	35
	B. Converter M-229-T1 and its Official Approval.....	37
	C. Keying Unit M-229-T2 and Procurement.....	40
	D. Cryptographic Functioning.....	40
	E. Keying Instructions.....	45
	F. Cryptographic Security.....	48
X	CONVERTER M-134-B (AND OTHER UNADOPTED MODIFICA- TIONS OF CONVERTER M-134-T2 AND M-134-T1).....	50
Appendix	CHANGES IN KEYING INSTRUCTIONS FOR CONVERTER M-134, M-134-A	

LIST OF TABS IN VOLUME 2

TAB

A	Photograph - Converter M-134, front view
B	Photograph - Converter M-134, plan view
C	Photograph - Converter M-134, rear view
D	Photograph - Cryptograph MC-164 of Converter M-134; plan view
E	Photograph - Cryptograph MC-164 of Converter M-134; showing two cipher discs removed
F	Photograph - Cryptograph MC-164 of Converter M-134; showing cipher disc stepping mechanism
G	Photograph - Converter M-134-A
H	Photograph - Converter M-134-A; rear view
I	Photograph - Cryptograph MC-164-A of Converter M-134-A; plan view, cover removed
J	Photograph - Cryptograph MC-164-A of Converter M-134-A; plan view, Tape Transmitter MC-185 and two rotors removed
K	Photograph - Cryptograph MC-164-A of Converter M-134-A; rotor stepping mechanism
L	Photograph - Typewriter MC-174-A of Converter M-134-A; showing space and carriage return contacts
M	Photograph - Rectifier RA-23
N	Photograph - Rectifier RA-23, cover open
O	Schematic diagram of Converter M-134-A
P	Encipher-decipher Reversing Switch of Converter M-134-A
Q	Tape Transmitter MC-185 of Converter M-134-A
R	Cryptograph MC-164-A of Converter M-134-A, Wiring Diagram
S	Wiring Diagram of Typewriter MC-174-A or Converter M-134-A
T	Photograph - Keying Unit M-229 (short title: SIGG00), shown in place on Cryptograph MC-164-A of Converter M-134-A
U	Photograph - Keying Unit M-229, plan view
V	Photograph - Keying Unit M-229, left stator view
W	Photograph - Keying Unit M-229, rear view
X	Photograph - Keying Unit M-229, cover in place
Y	Photograph - Keying Unit M-229, showing name plate
Z	Wiring Diagram of Keying Unit M-229
AA	Signal Corps Technical Committee Meeting No. 146; Supplemental Minutes

~~TOP SECRET~~

CHAPTER VI

CONVERTER M-134

For photographs of Converter M-134, see Tabs A, B, C, D, E, F. Since Converter M-134 and Converter M-134-A are almost identical, the detailed description of both converters is provided only with the photographs of Converter M-134-A. For detailed description applicable to both converters, see Tabs G, H, I, J, K, L, M, N, O, P, Q, R, S.

A. General

Converter M-134 is an electromechanical machine by means of which messages may be enciphered up to speeds of about 40 words per minute. Reference to the photographs appearing in Volume 1, Tab Q and Volume 2, Tab A, show that there are only two significant differences between the final production model, Converter M-134 (Vol. 2, Tab A) and the final experimental model, Converter M-134-T2 (Vol. 1, Tab Q). The main differences between the final production model and the final experimental model are (1) the way in which the typewriter and cryptograph are assembled and (2) the elimination on the final production model of the bank of 26 letter lamps. In the final production model, the two parts (cryptograph and typewriter) are assembled side by side and permanently attached to the base of the case designed to hold them; a copy holder, located between the two machines, is attached to the base of this case.

In accordance with the satisfactory results of the service test conducted in November 1936 (see Chapter V, Section D), Converter M-134-T2 was recommended for adoption as standard.¹ From this time on the

1. See Section B "Adoption as Standard", page .

~~TOP SECRET~~

~~TOP SECRET~~

experimental designation, T2, was dropped, and the converter became known as Converter M-134. During 1937, bids for the building of a limited number of Converters M-134 was received¹ and an order for twelve converters was placed with Wallace and Tiernan Products, Inc.¹ These twelve converters were delivered to the Office of the Chief Signal Officer in August 1938.¹ Minor changes, recommended as a result of experience with these twelve models, were incorporated into the 57 additional models procured. The 57 new models, with changes incorporated, became known as Converters M-134-A (see Chapter VII).

For an explanation of the cryptographic functioning of Converter M-134, see Chapter V, Section B. The section referred to describes the cryptographic functioning of Converter M-134-T2, which is cryptographically identical to Converter M-134.

For keying instructions, long and short titles, and classification of the machine, see Chapter VII, Section C. The section referred to is applicable both to Converter M-134 and M-134-A. The minor differences between the two types are explained.

1. See Section C "Procurement", pages thru .

~~TOP SECRET~~

~~TOP SECRET~~B. Adoption as Standard

On 11 January 1937, the Signal Corps Technical Committee took two ^(see Tab AA) important actions on Converter M-134 at its Meeting No. 146. The military characteristics¹ of the converter were approved and, acting upon the recommendation of the Chief Signal Officer, "the Committee recommended the adoption as to type and classification as standard of Converter type M-134". Disregarding this recommendation of the Signal Corps Technical Committee, on Converter M-134 was instead classified by The Adjutant General as a development type,² limited procurement type.²

1. In the Supplemental Minutes of Signal Corps Technical Committee Meeting No. 146, 11 Jan 1937, the military characteristics are listed as follows:
 - (a) This machine should be designed for the fundamental purpose of enciphering and deciphering messages with speed, accuracy, and the highest degree of cryptographic security. Secondary to these characteristics, there should be a minimum number of switches, keying elements, etc., which must be set before proper operation can begin.
 - (b) The cryptographic operations should be controlled by an external element which is variable and is not an intrinsic part of the mechanism itself, such as a perforated tape similar to that employed in printing telegraph apparatus. The underlying cryptographic principle should be that of a continuous, non-repeating, unintelligible or random-mixed key sequence of characters governing the encipherment of successive letters.
 - (c) The machine should consist of two units. (1) A cryptographic unit hereinafter called the "cryptograph", provided with a standard typewriter keyboard, and (2) a recording unit suitable for making a printed record of the work done by the machine, preferably an electrically operated typewriter, hereinafter called the "typewriter". The cryptograph is the part of the mechanism in which the enciphering and deciphering operations occur; the typewriter is electrically associated with the cryptograph and is to print the cipher text, in case of encipherment, in 5-letter groups, 10 groups per line; in the case of decipherment, the typewriter is to print the plain text, preferably in their original word lengths with proper spacing between words.
 - (d) The minimum speed of operation should be 30 words per minute.
 - (e) The cryptograph and the typewriter should be mounted upon the

For continuation of footnotes see following page.

~~TOP SECRET~~

~~TOP SECRET~~C. Procurement

On 1 March 1937, OCSigO notified Signal Corps Laboratories of the two actions of SCTC and directed them to procure, in accordance with Act of May 15, 1936 (Public No. 594, 74th Congress), as many machines as the limitation of funds permitted, "but not less than eight in any case".

Continuation of footnote 1 and footnote 2 from preceding page.

same base with fixed electrical connection between the two units. A side-by-side arrangement of these two units is preferable to a tandem arrangement, so that the keyboard of the cryptograph as well as the keyboard of the typewriter are both immediately in front of the operator.

(f) The apparatus should be designed to operate on 110-volt, D.C., power source.

(g) The weight of the cryptograph including its carrying case should not exceed 50 pounds; that of the typewriter including its carrying case 60 pounds. Both units should be rugged in construction and capable of withstanding jarring incident to transportation.

(h) The entire assembly should be so constructed that in case the typewriter is out of commission for any reason, cryptographic operations may be continued by means of electric light-bulb indicators on a lamp board on the cryptograph. (See note below.)

(i) There must be incorporated features to suppress interference with radio receivers operated in the vicinity of the machine.

Note: The military characteristics, as here quoted, were later amended to omit par. 1a(1)(h). (See par. (h) above).

2. Required types. - Required types comprise articles of equipment for which there are existing or expected needs and for which military characteristics have been approved. Development types are required types of equipment being developed to meet approved military characteristics as follows:

- (a) Experimental types...
- (b) Service test types...
- (c) Limited procurement types comprise articles of equipment which have passed service tests favorably but are not ready for classification as an adopted type and which before such classification should be subjected to an extended service test. The approval as to limited procurement type signifies that the item is probably suited for service use but requires refinement in design or further use of hands of troops to determine definitely its suitability. From AR 850-25, 30 June 1943, Page 8.

~~TOP SECRET~~

~~TOP SECRET~~

The original proposal for the budget of fiscal year 1937 included \$19,500 for the purchase of Converters M-134. However, this allotment was not included in the 1937 Expenditure Program of the Supply Division as finally approved.¹ Therefore, discussions, which began in December 1936 and continued intermittently during the first two months of 1937, concerned both how the \$19,500 of the original budget allotment could be redeemed for initial procurement and who should construct the converters. The first problem was solved by transferring \$19,500 from the Office Reserve.²

The second problem of who should construct the converters was solved only after a bit of disagreement. It seems that the letting of secret contracts to a commercial manufacturer was a new concept, allowable under the provisions of "Act of May 15 1936 (Public No. 594, 74th Congress", and not everyone concerned with the matter was satisfied that the new secret converter would be safe with a commercial concern. Much discussion ensued concerning the existence of spies in commercial plants. However, Research and Development Division of the Office of the Chief Signal Officer, recommended to the Executive Office that the converter could be best

1. Memorandum, Action 6, From: Fiscal; To: Ex. O., 2/25/37. Folder 3, "M-134, M-134-A, Procurement (thru 1940), CSGAS-80.
2. Memorandum, Action 9, From: Fiscal; To: Ex. O., 2/26/37. Folder 3, "M-134, M-134-A, Procurement (thru 1940), CSGAS-80.

~~TOP SECRET~~

~~TOP SECRET~~

manufactured by a commercial concern.¹ Therefore, the decision of the Chief Signal Officer, concurred in by a G-2 representative, was "to negotiate a secret contract with one party, the contract to include the wiring of the wheels".²

On 27 May 1937, Signal Corps Laboratories reported to OCSigO that a bid had been received from Wallace and Tiernan Products, Inc., Belleville, N. J. to manufacture Converters M-134 in lots of 8 @ \$2,310 each, total \$18,480; in lots of 10 @ \$2,200, total \$22,000; 12 @ \$2,135, total \$25,620. The answer from OCSigO directed that a contract with Wallace and Tiernan, Inc. be let for 8 converters and that it should provide for an increase in quantity in case further funds became available during F. Y. 1938.³

1. Memorandum, From: R&D Division, To: Ex. O.; 2/2/37. Folder 3, "M-134, M-134-A, Procurement (thru 1940), CSGAS-80.
2. ...3. This Division does not appreciate the objections raised to placing the entire machine with one manufacturer. SCL has recently placed one order for secret apparatus and is in process of placing another with reputable commercial concerns under the provisions of "Act of May 15, 1936 (Public No. 594, 74th Congress)". The provisions of this act apply equally to commercial manufacturers and to governmental agencies, and it is the opinion of this Division that the M-134 would be as well safeguarded by a reputable commercial concern as it would be by any of the agencies listed in basic letter. This Division, therefore, recommends that the entire procurement be made from one agency, preferably a reputable commercial concern.
2. Memorandum, Action 7, "Decision of the CSigO and concurred in by G-2 representative", 2/3/37. Filed in Folder 3, "M-134, M-134-A, Procurement (thru 1940), CSGAS-80.
3. 1st Ind., From: WD OCSigO, To: SC Labs, 28 May 1947. Folder 3, "M-134, M-134-A, Procurement (thru 1940), CSGAS-80.

~~TOP SECRET~~

~~TOP SECRET~~

The original order was actually made for 12 converters,¹ the additional four being decided upon at the last moment in order to effect a saving of 7.6%. The procurement of the additional four machines decreased the unit cost to \$2,135 (as opposed to a unit cost of \$2,310 when ordering 8) and made a grand total for the 12 of \$25,620.² The \$7,140 required for the additional four machines was forwarded to Signal Corps Laboratories under Procurement Authority SC 3412 P5-3059 A 0605-8.³ The contract number for these 12 converters was W 1077-SC-443, Order No. SCL 37-1082, date . The contract was fulfilled in August 1938 when the 12 converters were shipped to the Officer in Charge of Signal Intelligence Service, Office of the Chief Signal Officer.⁴ These 12 converters proved satisfactory but experience with them showed

1. Memorandum, Ex. O. to Fiscal, Action 8, "Approved purchase 12 machines". Folder 3, "M-134, M-134-A, Procurement (thru 1940)", CSGAS-80.
2. The memorandum which discusses increasing the order to 12 converters states in Action 3 (Supply to R&D, 8/12/37) that the "approved procurement program for P-5 includes \$5,000 for the procurement of 2 M-134's. This sum can be made available..." and states in Action 7 (Fiscal Div. to Ex. O., undated) that "the Fiscal Division can make available the additional \$2,140 required in addition to the amount set up in the Supply Division Program." Memorandum, op. cit.
3. Memorandum, Action 9, Fiscal Div. to R&D thru Supply & WP&T, 8/14/37. Folder 3, op. cit.
4. Shipping Ticket, Consignor: S.P.O., Signal Corps Laboratories; To: Officer in Charge, Signal Intelligence Service, Office of the Chief Signal Officer; Authority: Le OCSigO 413.52 (7-2-38). Evidently the 12 converters were retransported by SC Labs to Signal Intelligence Service from the manufacturer.

~~TOP SECRET~~

~~TOP SECRET~~

the desirability of minor changes¹ in any new models procured. The incorporation of these minor changes into the next and all additional models procured resulted in the new designation for them: Converter M-134-A. (For a discussion of the differences between Converters M-134 and M-134-A, see page . For a discussion of the reason for the differences, see page .

1. Letter, Subject: Converter M-134, To: Director, Signal Corps Laboratories; From: Louis B. Bender, Lt. Col., Signal Corps, By order of the Chief Signal Officer, 19 Sept 1938.

...2. The following changes, which have been found desirable as a result of experience with the twelve converters purchased last year, should be included in the new converters:

a. The sheels of the five plugs connecting to jack strip should be engraved with the numbers 1,2,3,4, and 5 respectively. It is also desired that sixty extra plug shells suitably engraved be furnished this office for installation in the old converters.

b. The connectors to the plugs should be approximately two inches longer and made of more flexible wire.

c. Dispense with the apertures in the lid which covers the rotor assembly of the cryptograph and cut a large rectangular opening in the lid so that the entire rotor assembly including the stators will be exposed to view.

d. The numbers engraved on rotors 6 and 9 should be differentiated to preclude the possibility of misreading. It is suggested that Roman numerals might be engraved on these two rotors above the Arabic numerals.

e. The copy holder should be removed entirely from the base of the machine and made a separate item. It should also be made tiltable in order that the operator may tilt the copy holder to suit his convenience.

f. The right and left margin stops on the typewriter should be provided with set screws with hexagonal heads and hexagonal locknuts to prevent stops from working loose.

g. The margin release should be rendered inoperative. It is suggested that this could be done by inserting a washer between the typewriter frame and the removable margin release button. It is desired that twelve washers be furnished this office for installation on the old machines.

h. The top cover plate of the tape transmitter, which is now black, should be made approximately the same color as the unfinished metal of the rest of the transmitter top.

For continuation of footnote see following page.

~~TOP SECRET~~

~~TOP SECRET~~

Continuation of footnote 1 from preceding page.

3. The following changes are also desirable and should be made if it can be done without necessitating any appreciable delay or involving any major changes in design. This matter is left to the discretion of your Laboratories.

a. The warning bell on the typewriter is not loud enough to insure that the operator will hear it at all times. If it cannot be made louder, it is suggested that it might be advisable to convert the present pilot lamp on the cryptograph into a warning signal for the operator. There seems to be no necessity for the neon glow lamp to indicate that the motor is running.

b. It is rather difficult to remove and replace the lid of Case CS-54 without exerting too much pressure. It would seem advisable to modify the case to make the removal of the lid less difficult.

c. The IBM typewriter is usually equipped with a stroke counter. This would be useful addition to the M-134, inasmuch as it would enable a check to be made of the number of keys struck on the cryptograph and the number of operations of the typewriter. It would be especially useful in deciphering.

1st Ind., WD, OCSigO, Wash. Nov. 17, 1938. To: Director of SC Labs.
The following instructions are given in reply to basic letter:

a. Your proposal for the purchase of 10 converters M-134 is approved except:

- (1) No stroke counters are desired.
- (2) As many of the modifications listed in attached letter dated Nov. 14, 1938 from Wallace and Tiernan as you consider practicable should be included.

b. The cost of the electrical registers mentioned in par. 2 and of the extra 60 engraved plug shells is considered excessive. They should not be purchased.

c. Twenty-two copy holders, Rite-Line with 10" eye guide are desired. They should, however, be purchased on a non-secret basis.

d. The removal of the copy holder from the machine will eliminate the trouble mentioned in paragraph 3b of our letter of Sept. 19, 1938. The trouble mentioned, therefore, should be disregarded.

By order of the Chief Signal Officer:

H. P. Browning,
Major, Signal Corps.

~~TOP SECRET~~

~~TOP SECRET~~

CHAPTER VII. CONVERTER M-134-A

For photographs and detailed description, see Tabs C, H, I, J, K, L, M, N, O, P, Q, R, S.

A. General

Converter M-134-A is a modification of Converter M-134. After the delivery by the manufacturer in August 1938 of the first twelve Converters M-134, experience with these converters suggested minor improvements¹ which were incorporated into all succeeding models. The more obvious of these improvements were (1) addition of the rotor-release lever,² (2) addition of a slow-operate relay,³ (3) the cutting of a well in the lid just above the rotors,⁴ and (4) the removal of the copy holder from the base of the case for issue as a separate item. All models after the first 12 contained these changes and were designated as Converters M-134-A. Between December 1938 and May 1942, 57 Converters M-134-A were procured according to the schedule outlined in Section B, "Procurement".

1. For list of the changes suggested in Letter, Subject: Converter M-134, To: Director, Signal Corps Laboratories, Signed: Louis B. Bender, Lt. Col., S.C., by Order of the Chief Signal Officer, 19 Sept. 1938, see footnote , page .
2. Rotor-release lever. (Compare photograph of Converter M-134, Tab A with photograph of Converter M-134-A, Tab G.) This lever, included only on Cryptograph 164-A is mounted on the left of the rotor assembly, in front of the plug and jack strip. By pulling forward on this lever the rotors are disengaged from all pawls and are free to be turned in either direction. Rotors of Converter M-134 can be turned only toward the front.
3. Slow-operate relay. - The function of this relay is to hold the rotor stepping solenoids energized for a sufficient length of time to insure complete pluger travel and subsequently to clear the circuit to the normal open state.
4. Well cut in lid just above rotors. Compare Tabs A and G. This well in conjunction with the rotor-release lever permits insertion and removal of rotors without removing the lid.

~~TOP SECRET~~

~~TOP SECRET~~B. Procurement

The second procurement of Converters M-134, with the changes which made them Converters M-134-A (see page for differences), was of 10 converters obtainable with \$25,000¹ allotted to Signal Corps Laboratories for the purpose. The actual cost of the 10 machines was \$23,850.00.² They were obtained on Contract W 1077-SC-317, Order SCL 39-771, 13 Dec. 1938,³ with Wallace and Tiernan Products, Inc. This order for 10 converters was completed 1 April 1940.

In 1939, 12 more Converters M-134-A were ordered from Wallace and Tiernan, Inc. @ \$2,385.00 each, total \$28,620. In procurement of Converters M-134 and M-134-A, the associated equipment or spare parts was almost as big an item as the converters themselves. The original allotment to SC Labs for the 1939 procurement of 12 converters was \$48,300.00, only \$28,620 of which was used for converters. The remainder was all

1. Letter, Subject: Converter M-134, To: Director, Signal Corps Laboratories; From: Louis B. Bender, Lt. Col., S.C., 19 Sept. 1938. "Funds in the amount of \$25,000 are being allotted to your Laboratories for the procurement of ten (10) Converters M-134 and spare parts."
2. Memorandum, Action 1, To: Supply Division, R&D Division, Signed: S.B.A., 13 Sept 1939. "...Contract W 1077-SC-317...calls for 10 machines at a total cost of \$23,850.00..." Folder 3, M-134, M-134-A, Procurement (thru 1940), CSGAS-80.
3. Memo, Subject: Shipment of Converters M-134; To: Director, SC Laboratories, From Louis B. Bender, Col. S.C., By order of the CSO, 13 Oct. 1939. "...Contract No. W 1077-SC-317, file SCL 39-771, dated Dec. 13, 1938.

~~TOP SECRET~~

~~TOP SECRET~~

CONTRACT DATA

Converter M-134; M-134-A

(over)

*The contract information given in the chart can be completed only by discovering the contracts. The total cost of the converters proper are not the same as the total cost of the contract because many contracts contain orders for rotors and other parts which cost as much as the converters themselves. (See footnote , page J) Therefore, to list the cost of the converters, which are the only numbers given in the M-134 folders, is to present a distorted picture.

~~TOP SECRET~~

CONVERTER M-134; M-134-A
Procurement* (See text also)

*See footnote on reverse
side of this page.

				Completed:	Ser. Nos.
1st Purchase M-134	12	Wallace & Tiernan Products, Inc.	Contract W 1077-SC-243 Order SCL 37-1082	2 Aug 1938	1 - 12
2nd Purchase M-134-A	10	Wallace & Tiernan Products, Inc.	Contract W 1077-SC-317 Order SCL 39-771 13 Dec 1938	1 Apr 1940	13 - 22
3rd Purchase M-134-A	12	Wallace & Tiernan Products, Inc.	Contract W-1077-SC-355 Order 706-SCL-40 1 Nov 39	15-23 Oct 1940	23 - 34
4th Purchase M-134-A	16	Wallace & Tiernan Products, Inc.	Contract W-1077-SC-443 Order 799-SCL-41 The last 12 converters built under this contract were modified according to change to Contract W 1077-SC-443, 3 Oct 1940. Of the 12 modified con- verters, the first 4 were differently wired: the connections to the left and right stators were changed and 4 sets of secret and confidential rotors were differently wired. The wiring in the 4 converters and 4 rotor sets were changed for special State Dept. use.		35 - 50
5th Purchase M-134-A	10	Wallace & Tiernan Products, Inc.	Contract W-1077-SC-1474 Order 13321-SCL-42 25 May 1942		51 - 60
6th Purchase M-134-A	8	Wallace & Tiernan Products, Inc.	Contract W 2261-SC-126 Order 1224-SCGDL-43 18 July 1942		61 - 68

~~TOP SECRET~~

spent for spare parts.¹ The SC Labs were directed on 16 Sept. 1939 by OCSigO to procure these 12 converters from Wallace and Tiernan Products, Inc.² The contract for these 12 converters was Contract No. W 1077-SC-355, Order 706-SCL-40, 1 Nov. 1939. They were delivered 12-23 October 1940.

1. 2nd Ind., WD, OCSigO; To: Director, SC Labs, 17 Oct. 1939:

1. It is desired that the following equipment be procured from Wallace & Tiernan Products, Inc., Belleville, N.J. by secret contract:

<u>Quantity</u>	<u>Item</u>		<u>Total Cost</u>
12	Converters M-134	@ \$2,385.00 ea.	\$28,620.00
14	Sets of Tools	@ 16.00 ea.	224.00
10	Slow pull-up relay with microadjustment	@ 7.50 ea.	75.00
14	Sets of 3 fuses	@ .45 ea.	6.30
14	Sets of keyboard contact springs	@ 2.70 ea.	37.80
24	Sets of 3 insulated movable key contacts	@ 1.65 ea.	39.60
24	Green top micro switch with spring plunger	@ 1.35 ea.	32.40
24	50-ohm suppressor resistor	@ .35 ea.	8.40
24	0.5 mfd. suppressor condenser	@ .80 ea.	19.20
24	1 mfd. oil-filled suppressor condenser	@ 1.10 ea.	26.40
10	Modified tape transmitter	@ 139.75 ea.	1,397.50
24	Type bar solenoid without plunger	@ 11.40 ea.	273.60
10	End stator complete without engraving(a)	@ 61.25 ea.	612.50
10	Intermediate stator, complete (a)	@ 51.10 ea.	511.00
10	Lot of 50 stator springs (b)	@ 3.00 ea.	30.00
10	Lot of 50 gold-plated bronze stator contact balls (b)	@ 5.00 ea.	50.00
6	Set of stator assembly clamps (c)	@ 24.70 ea.	148.20

For continuation of footnotes see following page.

~~TOP SECRET~~

~~TOP SECRET~~

Continuation of footnotes from preceding page.

<u>Quantity</u>	<u>Item</u>		<u>Total Cost</u>
24	Set of 8 spring contacts for tape transmitter connecting block	@ 2.00 ea.	48.00
1	Electromatic typewriter, complete as modified for Converter M-134	@ 1,000.00 ea.	1,000.00
1	Cryptograph frame, includ- ing keyboard contacts, reversing switch less tape transmitter and rotor stepping mechanism	@ 1,000.00 ea.	1,000.00
200	Rotors completely assembled but with wires soldered only to one side (as per Wallace and Tiernan quota- tion of Sept 22, 1939	@ 49.30 ea.	9,860.00

2. It is also desired that 12 Rectifiers RA-23 for 60 cycle operation, complete, and 60 spare Tubes EL-6C be purchased.

3. Funds in the amount of \$48,300.00 are being furnished your laboratories for this purpose. Since the cost of some of these items are only estimated, this amount may not be sufficient. If not, adjustment will be made upon notification of the additional amount required.

2. Letter, Subject: Purchase of Converter M-134; To: Director, SC Laboratories, 16 Sept 1939. Procurement Folder.

~~TOP SECRET~~

~~TOP SECRET~~

Two more contracts for Converters M-134-A were let to Wallace and Tiernan Products, Inc.: Contract No. W 1077-SG-1474 (Order No. 13321-SCL-42) dated 25 May 1942 for 10 converters and Contract No. W 2281-SG-126 (Order No. 1224-SCGDL-43) dated 18 July 1942 for 8 converters.

The contracts here discussed account for a total order of 12 Converters M-134 and 56 Converters M-134-A, making a grand total of 68.¹

C. Description

For detailed description, see Tabs G, H, I, J, K, L, M, N, O, P, Q, R, S.

When Converter M-134 was issued, official long and short titles were assigned to the various main parts of the machine for more efficient accounting purposes and to better distinguish between the SECRET and unclassified parts. The Converter M-134² comprises two main components, namely, Cryptograph MC-164³ (see Tab A) and Typewriter MC-174⁴ (see Tab A). When the second order for the machines was placed with the manufacturer and minor changes were incorporated (see page), the distinguishing title, Converter M-134-A⁵ was assigned to the whole assembly and the

1. Mr. Conder's distribution figures give the total as 57 Converters M-134-A and therefore a grand total of 69, instead of 68, converters.
2. Nomenclature, Converter M-134, assigned by Nomenclature Section, OCSigO, on 28 Nov 1932.
3. Nomenclature, Cryptograph MC-164, assigned by Nomenclature Section, OCSigO, on 17 April 1937.
4. Nomenclature, Typewriter MC-174, assigned by Nomenclature Section, OCSigO, on 17 April 1937.
5. Nomenclature, Converter M-134-A, assigned by Nomenclature Section, OCSigO, on 8 Nov 1939.

~~TOP SECRET~~

~~TOP SECRET~~

titles, Cryptograph MC-164-A¹ and MC-174-A² were assigned to the two chief components.

DIMENSIONS OF CONVERTER M-134; M-134-A

	<u>Width</u>	<u>Depth</u>	<u>Height</u>	<u>Cubic Displacement</u>
a. In operation, Cryptograph MC-164:	14 $\frac{1}{2}$ "	16"	11 $\frac{1}{4}$ "	Mounted on One Base 7.4'
b. In operation, Electric Typewriter MC-174:	17 $\frac{1}{2}$ "	16"	9 $\frac{3}{4}$ "	
c. Packed in carrying case:	37 $\frac{1}{4}$ "	22 $\frac{1}{2}$ "	15"	7.4'

Weight

- a. In operation, Cryptograph MC-164: 35 lbs.
- b. In operation, Electric Typewriter MC-174: 43 lbs.
- c. Packed in carrying case: 160 lbs.

Three other long titles were assigned to parts of the Converter M-134; M-134-A. These were Copyholder MC-184 (later MC-184-A), Tape Transmitter MC-185 (later MC-185-A) and Case CS 54³ (later CS 54-A).⁴

In addition to the above named long titles, the following short titles were assigned to the various items pertaining to Converter M-134:

1. Nomenclature, Cryptograph MC-164-A, assigned by Nomenclature Section, OCSigO, on 9 Nov 1939.
2. Nomenclature, Typewriter MC-174-A, assigned by Nomenclature Section, OCSigO, on 8 Nov. 1939.
3. Nomenclature, CS-54, assigned by Nomenclature Section, OCSigO, on 17 April 1937.
4. Nomenclature, CS-54-A, assigned by Nomenclature Section, OCSigO, on 9 Nov. 1939.

~~TOP SECRET~~

~~TOP SECRET~~

Converter M-134 (less Cryptograph MC-164 and Rotors SG-14).....SIGTUK
 Cryptograph MC-164 (exclusive of rotors).....SIGTIP
 Rotors SG-14 (individual rotors indicated by arabic numeral after short title).....SIGTER
 Rotors SG-15 (individual rotors indicated by arabic numeral after short title).....SIGLIC
 Set of key tapes (individual tapes to be indicated by arabic numerals after short title).....SIGREP

While the converter assembly less cryptograph and rotors (SIGTUK) is SECRET because the assembly as a whole gives an indication of the functioning of the converter, the individual units such as the Typewriter MC-174, Copyholder MC-184, Tape transmitter MC-185, and Case CS-54 are unclassified when removed from the converter assembly.

The functions of the two main components, Cryptograph MC-164 and Typewriter MC-174, are as follows: When the cryptograph has been properly prepared according to keying instructions and the encipher-decipher switch has been placed in the ENCIPHER position, striking the keys of the keyboard of Cryptograph MC-164 in accordance with the individual characters of the plain-text message results in the production by Typewriter MC-174 of a printed, unintelligible cryptogram spaced in 5-letter groups. Conversely, by setting the apparatus to the same key used in enciphering and placing the encipher-decipher switch in the DECIPHER position, this cryptogram may be deciphered by striking the keys on the keyboard of the Cryptograph MC-164 in accordance with the individual printed characters of the cryptogram, whereupon the typewriter prints the original plain-text message in normal word lengths.

~~TOP SECRET~~

~~TOP SECRET~~

Typewriter MC-174 may also be operated directly in typing the plain-text parts of messages, such as addresses and signatures, message reference numbers, dated, indicators, etc. For this operation the encipher-decipher switch is placed at DECIPHER. In order to transmit to its destination the cryptogram produced by Converter M-134, it is necessary to employ one of the conventional means of communication such as wire or radio.

The features of encipherment which provide cryptographic security are described in the chapter on Converter M-134-T2 (Chapter V, Section B).

According to the first operating instructions issued, Converter M-134 was provided with 10 rotors (SIGTER rotors). This number of rotors issued prevailed until April 1940 when the new instructions provided that the number of rotors issued would be 15. Five of the 15 rotors provided were red-colored and 10 gray-colored. The new red-colored rotors, consisting of the set of 5, bore the short title: SIGLIG. The two types, red (SIGLIG) and gray (SIGTER) were issued in order to provide different rotors for Secret and for Confidential messages. The five red SIGLIG rotors were used for Confidential messages only. The ten gray SIGTER rotors were used for Secret messages only. This method of using two sets of rotors prevailed for about a year. In March 1942, new keying instructions were published which provided that 15 rotors would be issued with each machine but that these 15 rotors would constitute one set. The old red and gray rotors were still used but the old distinction between them was eliminated.

~~TOP SECRET~~

~~TOP SECRET~~

The documents containing the operating instructions for Converter M-134; M-134-A are as follows:

"Operating Instructions for Converter M-134", (short title: (SIGQUG), September 1938.

"Operating Instructions for Converters M-134 and M-134-A", (short title: SIGKOC), July 1, 1940.

"Supplement to Operating Instructions for Converters M-134 and M-134-A", (Photographs and Drawings of Converter M-134-A), (short title: SIGVIJ), July 1, 1940.

Associated documents:

"Parts Tape Transmitter and Auto Control Relay Unit", Teletype Corporation Bulletin No. 1018, December 1930.

"Description and Adjustments of the Tape Transmitter", Teletype Corporation Bulletin No. 103 (Issue 2), October 1938.

D. Keying Instructions

The documents containing the keying instructions for Converters M-134 and M-134-A are as follows: (An outline of the changes occurring through the years in the keying instructions is given in Appendix I.)

"Keying Instructions for Converter M-134", (short title: SIGPUF), Sept. 1938.

"Keying Instructions for Converters M-134 and M-134-A", (short title: SIGJUX), April, 1940.

"Keying Instructions for Converters M-134 and M-134-A", (short title: SIGLOG), March 1942.

Keying instructions for the Converter M-134; M-134-A are as follows: Converter M-134; M-134-A employs five keying elements, two which are changed at the beginning of each day and two which are changed with

~~TOP SECRET~~

~~TOP SECRET~~

every message. The two daily keying elements are (1) the rotor assembly, by which is meant the selection and arrangement of rotors, and (2) the selection of the key tape to be used for the day. The three message keying elements are (1) the variation of the connections between the sensing pins of the tape transmitter and the rotor stepping magnets, which variation is accomplished by changing the order of the plugs in the jacks of the plug and jack strip; (2) the initial alignment of the rotors; (3) the initial position of the key tape.

The rotor assembly (or selection and arrangement of rotors) is accomplished at the beginning of each day by means of the current rotor assembly table of the system. For example, if the table shows that for January 1 the rotor assembly is 8-3-1-9-7, it means rotor 8 is inserted in position 1, rotor 3 in position 2, etc. The arrangement is made from left to right. The first instructions published in September 1938 provide that a set of 10 rotors be issued with each machine. The superseding instructions of April 1940 provide for 15 rotors: 5 red rotors to be used for Confidential messages and 10 gray rotors to be used for Secret messages. The superseding instructions of March 1942 still provide for 15 rotors but, contrary to the use prescribed in the April 1940 instructions, these 15 rotors constitute one set.¹

1. "Keying Instructions for Converter M-134 and M-134-A", (short title: SIGLOG), March 1942: "The red-colored rotors heretofore used for confidential systems are no longer to be used as such; all 15 rotors constitute one set. The 10 gray-colored rotors are identified by arabic numerals (except numbers 6 and 9 which are roman), the red-colored rotors are identified by roman numerals, preceded by the letter C. These differences will serve to differentiate all the 15 rotors of the set, for keying purposes."

~~TOP SECRET~~

~~TOP SECRET~~

The key tape to be used for the day is selected as follows: A set of numbered tapes is issued with each M-134 system. To select the tape to be used for the day, the tape numbers are used in conjunction with the current Key Tape Selection Table of the system. For example, the table may show that on January 1 the tape to be used is 17. According to the September 1938 and the April 1940 keying instructions, each set of key tapes issued with a Converter M-134 system consists of 48 numbered tapes issued in duplicate. The duplicate copies are explained as being merely reserve editions for use in case one copy of the tape became damaged. The superseding keying instructions of March 1942 provides for a change in the policy of issuing tape sets as follows: one set of 48 tapes, furnished in duplicate, for each Secret M-134 system and one set of 30 tapes, furnished in triplicate, for each Confidential M-134 system.

The variation, with every message, of the connections between the sensing pins of the tape transmitter and the rotor stepping magnets is accomplished by changing the order of the plugs in the jacks of the plug and jack strip. The order of the plugs in the jacks is determined before encipherment of every message as follows: An indicator consisting of five letters is chosen at random by the operator. Suppose the group selected by the operator is FHBGR. These letters are assigned numbers in accordance with their relative order in the normal alphabet thus:

F-H-B-G-R
2-4-1-3-5

~~TOP SECRET~~

~~TOP SECRET~~

These numbers determine the order of the plugs in the jacks. (For detail, see Chapter V, Section B, page). For the next message a new indicator is selected at random and the order is again derived in the same way.

The initial alignment of the 5 rotors is accomplished before the encipherment of every message as follows: The same five letters as was selected to determine the order of the plugs in the jacks are used. Using the same example (see above), the indicator selected at random by the operator was FHBGR. The operator aligns the rotors by hand individually to the randomly-chosen indicator group, in this case, aligning FHBGR on the bench mark from left to right.

The initial position of the key tape is derived as follows: Every tenth Baudot character of each key tape is numbered by a large number in white ink. To determine the initial position, the middle 3 letters of the same 5 letters previously chosen as indicator (see above), are used. The value of the middle 3 letters is found by referring to the current table of the system. This table is called "Table for Determining Initial Position of Key Tape". It is merely a table which assigns a numerical value to each letter of the alphabet. For example, using the letters FHBGR and a Position of Key Tape Table which gives the following values for the middle three letters: H = 8, B = 2, G = 7, the key tape would be set at the bench mark of the tape transmitter. The method here described was prescribed both in the September 1938 keying instructions and in the April 1940 keying instructions. The keying instructions

~~TOP SECRET~~

~~TOP SECRET~~

published in March 1942 modified this procedure as follows: For Secret messages, the 1st, 2nd, and 3rd letters of the indicator are used; for Confidential messages, the 2nd, 3rd, and 4th letters; for Restricted messages, the 3rd, 4th, and 5th letters.

All keying instructions provided for a maximum number of groups of cipher text which could be enciphered with the same message keying elements.¹ In the September 1938 instructions, the maximum length was 50 to 60 5-letter groups. In the September 1940 and March 1942 instructions, the maximum length was 100 5-letter groups.

E. Cryptographic Security

Converter M-134-A was an advanced cryptographic machine for its day and had great potentials for security. However, the indicator system and the makeup and use of the key tapes rendered the machine vulnerable to cryptanalytic attack. With a secure indicator system and careful tape makeup with one-time use, the machine would have had more security than Converter M-134-C. The security of the machine as it was used was dependent on the following:

-
1. The rule in the instructional documents was worded as follows:
"If the cryptographed text of a message will exceed 50 to 60 (later 100) 5-letter groups, the plain text will first be divided into two or more approximately equal parts and each part will be treated as a separate message.
 2. This cryptographic security evaluation is copied from "Historical and Cryptologic Summary of Cryptosystems", Volume I, (short title: ASAG-23).

~~TOP SECRET~~

~~TOP SECRET~~

At least 10 messages in depth or a large amount of perfectly matched plain and cipher text from several messages in one classification are necessary before the endplates, rotors, and key tape can all be reconstructed. In general, less material would be needed than for reconstruction of Converter M-134-C rotors. Since the tapes were made up so that the levels were all nearly random, each rotor stepped approximately 50% of the time and thereby produced many lobsters, delayed lobsters, and partial lobsters. These lobsters constituted an opening wedge for an attack.

With matched plain and cipher text, the number of exhaustive trials necessary to identify known rotors is large, but not so large as to be impractical. There are $10 \times 9 \times 8 \times 7 \times 6$ rotor arrangements for the SECRET classification and $5 \times 4 \times 3 \times 2 \times 1$ rotor arrangements for the CONFIDENTIAL classification. For each of these, 31 possible motions must be assumed between encipherments. With the identification of the rotors, the key tape is recovered as messages are read.

With known key tapes as well as known rotors, the number of exhaustive trials equals $10 \times 9 \times 8 \times 7 \times 6 \times 48$ for the SECRET classification and $5 \times 4 \times 3 \times 2 \times 1 \times 30$ for the CONFIDENTIAL classification.

F. Tape Numbering Machine M-190

So that the operators of Converter M-134; M-134-A could locate on the keying tape the exact five-unit code group with which the encipherment of a message began, it was necessary that the tape be

~~TOP SECRET~~

~~TOP SECRET~~

marked. To accomplish this end, a project for development of an automatic key-tape marking device was begun in August 1937.¹ The work was done at Signal Corps Laboratories, using as a basis for the development work, "an old model of the tape marking device made by the Laboratories several years before."¹ The model was completed by Signal Corps Laboratories about June 1938. In May 1938, the following nomenclature was assigned:² Tape Numbering Machine M-190.

A brief description of Tape Numbering Machine M-190 follows:³

The tape numbering machine operates from 110 volts a.c., 60 cycles, or 110 volts d.c. to number a five-unit-code tape from 0 to 999, every ten holes of the tape. A universal motor drives a transmission and cam system to automatically advance the tape every tenth-hole position, depress, ~~advance~~ elevate, and advance the number-printing wheels, and feed a typewriter ribbon between the printing wheels and the tape. The over-all size of the machine is approximately 8 in. by 13 in. by 5 in. and the weight about 96 pounds.

G. Evaluation

Converters M-134 and M-134-A have a high security value and a low operational value. The inventor, Mr. Friedman, realized very early that

1. Letter, Subject: Automatic Key Tape Marking Device; To: Director, S.C. Labs; From: Louis B. Bender, Lt. Col. S.C.; Aug. 27, 1937. Folder 11, Converter M-134; M-134-A; Associated Equipment.
2. 1st Ind., From WD, OCSigO; To: Director, S.C. Labs; 21 May 1938. Folder 11, Converter M-134; M-134-A; Associated Equipment.
3. Letter, Subject: Request for Nomenclature; To: CSO; From: Lt. Col. Van Duesen, Lt. Col., S.C., 19 May 1938. Folder 11, M-134; M-134-A; Associated Equipment.

~~TOP SECRET~~

~~TOP SECRET~~

tape control would require critical adjustments, possibly necessitating frequent servicing. Therefore, when Mr. Frank B. Rowlett conceived, about June 1935, a novel idea for controlling rotor stepping in simulated random fashion by sending an electrical impulse through the circuits of a rotor maze, it was soon recognized by Mr. Friedman and Mr. Rowlett as operationally superior to the key-tape control currently under consideration. Mr. Friedman helped Mr. Rowlett to develop his fortunate idea¹ and together they urged the Chief Signal Officer to convert the preproduction model of Converter M-134-T2, then being constructed, to the new type of rotor stepping control. However, the Chief Signal Officer was committed to the type being currently built into the preproduction model of Converter M-134-T2 (key tape control) and could not be persuaded to make any change. Therefore, 68 Converters M-134; M-134-A were built. It required actual operational experience with the new converters to confirm the original belief of the inventors in the practicability of abandoning tape control in favor of the Friedman-Rowlett concept of control¹ by means of an electrical current through the circuits of a rotor maze to generate a long, irregular sequence of characters.

The Friedman-Rowlett concept¹ found expression in an astonishing manner. The Chief Signal Officer, having refused to adapt Converters M-134, gave Mr. Friedman permission to disclose the new, unadopted

1. Patent Application 70,412, Friedman and Rowlett, filed March 23, 1936. This patent is still under a Patent Office Secrecy order. Conceived about June 15, 1935.

~~TOP SECRET~~

DCM 569

~~TOP SECRET~~

principle to the Navy. The Navy's development of the idea to produce the converter which is the main subject of this history (Navy ECM Mark II or Army Converter M-134-C) is explained in Chapter XI. Army orders for the new Converters M-134-C began in June 1940. Even though a few more Converters M-134-A were ordered after this date (to a total of 68) Converters M-134-C soon took precedence.

By May 1941 the operational inefficiency of tape control of the enciphering rotors of Converter M-134, M-134-A had been sufficiently demonstrated so that the Chief Signal Officer not only agreed to ordering Converters M-134-C in quantity but also agreed to an adaptation of the existing Converters M-134, M-134-A by means of a keying unit, called Keying Unit M-229. Keying Unit M-229 is one of the possible variations of the Friedman-Rowlett concept¹ of control by an electrical current through the circuits of a rotor maze. Its development and description are presented in Chapter IX.

For distribution and use of the 68 Converters M-134 and M-134-A, see Chapter VIII.

1. See footnote 1, previous page.

~~TOP SECRET~~

~~TOP SECRET~~CHAPTER VIII. DISTRIBUTION AND USE OF
CONVERTER M-134 AND CONVERTER M-134-A

Only 68 Converters M-134 and M-134-A were manufactured. Since the basis of issue was two converters per establishment, it is immediately apparent that these converters did not attain very wide usage. The distribution plan for Converter M-134 (drawn up in 1937) called for supplying the General Staff, the Air Force General Headquarters, each Corps Area and Department Headquarters, and the Signal Corps Training School. Even this limited distribution plan did not get off to a very fast start, for delivery of the machines by the manufacturer was slow in addition to the fact that the orders were placed in mere dribbles. The first order for 12 machines was delivered 2 August 1938, the second order for 10 machines was delivered 1 April 1940, the third order for 12 machines was delivered between 15-23 October 1940. Another 16 converters were ordered in the summer of 1940 (delivery date unknown) and the last 18 were ordered as late as the summer of 1942 (delivery date unknown).

The just-listed scheduled orders and deliveries shows that from August 1938 until 1 April 1940, only 12 converters were in existence. The first five of these 12 converters were escorted to their destination by their inventor, William F. Friedman, in order to insure proper installation and adequate instruction in their operation. The inventor, who left New York with the converters on 15 November 1938 (USAT Republic)

~~TOP SECRET~~

~~TOP SECRET~~

delivered two to the Panama Canal Department, Quarry Heights; one to the 9th Corps Area, Presidio of San Francisco; and two to the Hawaiian Department at Honolulu. The remainder of the first 12 were delivered within the next several months to the Porto Rican Department, The Phillipine Department and the 8th Corps Area. One was held by the War Department Message Center. Experience with these 12 converters provided the basis for the changes which made the next order, Converters M-134-A. The directive for incorporation of the changes is probably partially responsible for the considerable delay in delivery of the second order.

The second order of 10 converters arrived in Washington on 1 April 1940. Distribution of these 10 converters introduces an interesting aspect of general cryptographic history, namely, the beginning of the modern type code room or what later became known as the cryptocenter. On 5 April, letters were sent to the Signal Officers of the 1st, 2nd, 3rd, 4th, 5th, 6th, and 7th Corps Areas and to the Commanding Officer, General Headquarters, Langley Field, Virginia stating that within the next month one Converter M-134-A would be issued to them. These future recipients of the Converter were instructed to provide secure storage space of sufficient size that the Converter could be operated with the space. The delivery schedule of shipment within the month was not met because the Corps Areas immediately answered the statements

~~TOP SECRET~~

~~TOP SECRET~~

that suitable storage space¹ was not available for housing the converter. Never before had there been issued a large electrical machine which could be seen only by authorized operating personnel and, in addition, was such a large and delicate a mechanism that it could not be moved around. Therefore, these new factors caused the scheduled recipients of the converter to spend the next few months in making ready for the new code rooms. It was necessary that each room have only one entrance and that the doors, windows, and possibly ceiling and floor be covered by a grid system so that any attempt to enter the room by unauthorized persons should set off a burglar alarm. It was also considered highly desirable that the vault be of fireproof construction throughout. By the time satisfactory rooms were completed, the summer of 1940 had gone by; the converters were actually shipped in August and September.

The third order for 12 machines (delivered 15-23 October 1940) were distributed in two ways: (1) to increase by one the number of machines held by the Porto Rican Department, the Hawaiian Department, the Panama Canal Department, and the 4th Corps Area and (2) to establish a special London-Washington circuit between the U.S.M.A., London and the War Department Message Center.

-
1. This problem of secure storage space within which the converter could be operated did not come up until the second shipment simply because no one seemed to realize that it would take so long to provide it. The recipients of the first order were notified of the necessity for this type of storage space but the shipments occurred so soon afterward that it is probable that the first converters were housed under improper conditions for the first few months of their installation.

~~TOP SECRET~~

~~TOP SECRET~~

In order to establish this special Washington-London circuit, four converters (Reg. Nos. 23, 24, 25, 26) were specially wired¹ by SC Labs. The connections to the left and right stators were changed and four sets of secret rotors and four sets of confidential rotors were differently wired. Two of these specially wired machines were held by MA, London and two by the WDMC. On Aug. 6, 1941 the MA London requested² a third converter. He gave two reasons for his request. First, the traffic handled by the two machines was heavy. Secondly, since the code rooms of the State Department, Army, and Navy were all located within fifty feet of each other in the Embassy at 1 Grovesnor Square and therefore all three were in constant danger of being destroyed by a single bomb, it was advanced that a third unit should be placed in the new bomb-proof shelter being built at 20 Grovesnor Square, one room of which was to be a code room. This request was approved but delivery was delayed until . The delay was due to slowness of delivery by the manufacturer who was having difficulty obtaining some of the needed materials.³ This request was eventually answered with Converters M-134-A, register nos. 49 and 50.

It is unnecessary to describe the distribution of the remainder of the Converters M-134-A in detail for the following list of original and final holders completes an adequate outline of the distribution of Converters M-134, M-134-A.

1. The rewiring was being accomplished about October 1940.
2. This letter from MA, London was written to AC of S, G-2.
3. Letter, for AC of S, G-2 from O. K. Sadtler, Col., S.C., 27 Aug. 1941. Folder 13, London Circuit.

~~TOP SECRET~~

~~TOP SECRET~~

Converter M-134

<u>Reg. No.</u>	<u>Original Holder</u>	<u>Final Disposal</u>
1	Puerto Rican Department	Destroyed
2	W D M C	Destroyed
3	Panama Canal Department	Destroyed
4	Panama Canal Department	Museum
5	9th Corps Area	Destroyed
6	8th Corps Area	Destroyed
7	Puerto Rican Department	Destroyed
8		Destroyed
9	Hawaiian Department	Destroyed
10	Hawaiian Department	Destroyed
11	Philippine Department	Destroyed
12	Philippine Department	Destroyed
13	2nd Corps Area	Destroyed
14	6th Corps Area	Destroyed
15	GHQ Air Force	Destroyed
16	2nd Corps Area	Destroyed
17	W D M C	Destroyed
18	3rd Corps Area	Destroyed
19	5th Corps Area	Destroyed
20	7th Corps Area	Destroyed
21	1st Corps Area	Museum
22	4th Corps Area	Destroyed
23	U S M A London	Destroyed
24	U S M A London	Destroyed
25	W D M C	Destroyed
26	W D M C	Destroyed
27	Panama Canal	Destroyed
28	Hawaiian Department	Destroyed
29	Philippine Department	Destroyed
30	4th Corps Area	Destroyed
31	W D M C	Destroyed
32	2nd Air Force	Destroyed
33	Hawaiian Department	Destroyed
34	Philippine Department	Destroyed
35	3rd Corps Area	Destroyed
36	W D M C	Destroyed
37	Wright Field	Destroyed
38	7th Corps Area	Destroyed

~~TOP SECRET~~

~~TOP SECRET~~

<u>Reg. No.</u>	<u>Original Holder</u>	<u>Final Disposal</u>
39	State Department (Bought)	Destroyed ¹
40	State Department (Bought)	Destroyed
41	State Department (Bought)	Destroyed
42	State Department (Bought)	Destroyed
43	W D M C	Destroyed
44	Puerto Rican Department	Destroyed
45	G H Q Air Force	Destroyed
46	Major Doud	Destroyed
47	Hawaiian Department	Destroyed
48	Hawaiian Department	Destroyed
49	U S M A London	Destroyed
50	U S M A London	Destroyed
51	State Department (Bought)	Destroyed
52	State Department (Bought)	Destroyed
53	State Department (Bought)	Destroyed
54	State Department (Bought)	Destroyed
55	S S U, Secy of War	Destroyed
56	MIDPAC	Destroyed
57	S S U, Secy of War	Destroyed
58	S S U, Secy of War	Destroyed
59	U S HQ Calcutta	Destroyed
60	U S HQ Calcutta	Destroyed
61	Warehouse	Destroyed
62	Warehouse	Destroyed
63	Warehouse	Destroyed
64	Warehouse	Destroyed
65	310th Bomb Wing	Destroyed
66	310th Bomb Wing	Destroyed
67	310th Bomb Wing	Destroyed
68	310th Bomb Wing	Destroyed
71	Air Force	Destroyed

(Numbers 69 and 70 were apparently never noticed as being skipped. There were only 69 SIGMYC's manufacturer and No. 71 above should have been assigned the number 69.)

1. Memorandum for the Chief, ASA, from L.W. Parke, USN, Chief, Division of Cryptography, 8 March 1948. Filed: Folder 1, Converters M-134, M-134-A (General), CSGAS-80. "Reference is made to your letter... requesting information relative to the disposition of eight SIGMYC... devices... The SIGMYC devices have been cryptographically destroyed; the ciphering units have been dismantled and the typewriters are being used for other purposes."

33
~~TOP SECRET~~

~~TOP SECRET~~

KEYING DEVICE M-229 (SIGG00)

75 units manufactured. These were assigned Register Numbers 2 - 76, omitting No. 1.

Of these 75 units,

No. 18 is in the Museum

35 was destroyed

7 sold to State Department; subsequently destroyed ¹

13 sold to State Department; subsequently destroyed

14 sold to State Department; subsequently destroyed

15 sold to State Department; subsequently destroyed

42 sold to State Department; subsequently destroyed

54 sold to State Department; subsequently destroyed

58 sold to State Department; subsequently destroyed

67 sold to State Department; subsequently destroyed

The remainder are now all in the Warehouse.

-
1. Memorandum for the Chief, ASA, from L. W. Parke, USN, Chief, Division of Cryptography, 8 March 1948. Filed: Folder 1, Converters M-134, M-134-A (General), CSGAS-80. "Reference is made to your letter...requesting information relative to the disposition of...eight SIGG00 devices... The SIGG00 devices have been cryptographically destroyed by complete disassembly".

~~TOP SECRET~~

~~TOP SECRET~~

CHAPTER IX. KEYING UNIT M-229

For photographs of Keying Unit M-229, see Tabs T, U, V, W, X, Y, Z.

A. General

Keying Unit M-229 consists of a single unit of three rotors in cascade through which electrical circuits are passed to produce a lengthy disarranged sequence of keying characters for controlling the permutations of the rotors of Converters M-134 and M-134-A. It is of such a nature that it can be slipped into the same position as that occupied by the tape transmitter. (See Tab T for photograph of Keying Unit M-229 in place. Compare with Tab G which shows tape transmitter in place.) The way in which Keying Unit M-229 controls the enciphering rotors of Converter M-134 or Converter M-134-A is explained in Section D.

The principle involved in Keying Unit M-229 was conceived by Mr. Frank B. Rowlett in June 1935 during the interval when preproduction models of Converter M-134-T2 were being built. Mr. William F. Friedman and Mr. Rowlett developed the idea together and urged its adoption. However, the Chief Signal Officer was committed to the type (tape control) embodied in the model of Converter M-134-T2 currently being built and he could not be persuaded that a change was advisable. Therefore, development of Converter M-134 continued, using tape control. Sixty-eight models of this type were constructed.

It was not until experience in operation of the converters confirmed the original belief of the inventors in the high security value and low

~~TOP SECRET~~

~~TOP SECRET~~

operational value of Converters M-134, M-134-A that the new method of controlling its rotors was given consideration. When it was finally decided, in June 1941, to adapt the 68 converters M-134, M-134-A to the new type control by means of Keying Unit M-229, the Navy had already shown to the Army their own mechanical and electrical embodiment of the ^{Friedman-Rowlett} principle in a converter which they called ECM Mark II (later Army Converter M-134-C). When, in 1935, Mr. Friedman and Mr. Rowlett were unable to persuade the Army to change to the new-type control of enciphering rotors,¹ Mr. Friedman obtained permission (see Chapter XI) to disclose the idea to the Navy. The first time that anyone in the Army knew that the "Friedman-Rowlett stepping maze", disclosed by Mr. Friedman in 1935, had been used by the Navy was on February 3, 1940 when Admiral Noyes of the Navy invited Friedman, Rowlett, and other signal corps personnel to see their new model. (See Chapter XI.)

The reason that the use of the concept of the "Friedman-Rowlett stepping maze" to produce the ECM Mark II (or Converter M-134-C) is important in a discussion of Keying Unit M-229 is because both Keying Unit M-229 and the stepping maze of Converter M-134-C are variations of the same concept, conceived by Rowlett in 1935, and developed by Rowlett and Friedman.² The "Friedman-Rowlett stepping maze" was conceived in

1. The change desired was from control of the stepping of the enciphering rotors by means of a Baudot-code tape to control of the stepping of enciphering rotors by means of electrical circuits passed through a series of rotors in cascade to produce a lengthy disarranged sequence of keying characters.
2. Patent Application No. 70,412, Friedman and Rowlett, filed March 23, 1936. This patent is under a Patent Office Secrecy Order. See also Chapter XI.

~~TOP SECRET~~

~~TOP SECRET~~

several variations in June 1935 and, as mentioned in the preceding paragraph, revealed to the Navy. Nothing was done about it in the Army until five years later when the Navy surprised Signal Corps personnel with a model which used the basic principles disclosed to them by Friedman. It was only after all this had occurred that Signal Intelligence Service was able to convince the Chief Signal Officer of the efficacy of the new type control over tape control. Upon presentation of the ECM Mark II by the Navy, the Army immediately switched its orders to Converters M-134-C. It was after Converters M-134-C had begun to be ordered in quantity that Keying Units M-229 were ordered for the purpose of converting Converters M-134, M-134-A to a variation of the same type control of its enciphering ^{rotors as that} ~~as that~~ used in Converter M-134-C.

B. Converter M-229-T1 and Its Official Approval

On 9 May 1941, Signal Intelligence Service wrote to War Plans and Training Division that the tape transmitter of Converters M-134 and M-134-A "appears to require a very critical adjustment for satisfactory operation, necessitates frequent servicing and causes numerous errors and delays in moving enciphered traffic. It has also been found that the production, distribution, and handling of key tapes presents difficulties..." Inspired by these considerations, Signal Intelligence Service, using the limited shop facilities and personnel available, constructed an experimental keying mechanism (later to be called Keying Unit M-229-T1) which consisted of a single unit of three rotors through which electrical circuits were

~~TOP SECRET~~

~~TOP SECRET~~

passed to produce a lengthy disarranged sequence of keying characters for controlling the permutations of the rotors of Converter M-134 and M-134-A. The new experimental keying unit was built from existing elements and spare parts of Converters M-134 and M-134-A. It required no modification of the existing converters except very minor ones which could be accomplished by the personnel at the using stations.

The existence, purpose, and advantages of the new Keying Unit M-229-T1 were made known to War Plans and Training Division by its originator, Signal Intelligence Service, on 9 May 1941 by means of a Routing and Work Sheet. This R & W recommended the immediate procurement of the keying unit and made the following specific requests:

- (1) That the keying unit be considered as a required type.
- (2) That a type number be assigned.
- (3) That the military characteristics accompanying the R & W be approved.
- (4) That a project be set up for the development of a keying unit having the required military characteristics.
- (5) That consideration be given to the adoption of this keying unit as a standard article of use by the Signal Corps as a new type of equipment to be used interchangeably with the present tape transmitter for converters type M-134 and M-134-A.
- (6) That the subject equipment and all matters pertaining to its development, standardization, and contemplated use be placed in the secret classification.

War Plans and Training Division gave quick approval (10 May 1941) to the submitting of the military characteristics to the Signal Corps Technical Committee. But it did not concur in the request that the new keying

~~TOP SECRET~~

~~TOP SECRET~~

unit be adopted as a required type. It recommended instead that "a sufficient number of service test models be manufactured and turned over to the various arms and services for service tests.

In spite of the fact that all the original recommendations of Signal Intelligence Service were not followed to the letter, the processing of the new keying unit (according to the regulations outlined in AR 850-25 for new equipment) occurred in record time. In 26 May 1941, at its meeting No. 193, the Signal Corps Technical Committee recommended that the military characteristics,¹ as drawn up by the Signal Intelligence Service, be adopted. It further recommended that a project be set up for the development and procurement of one pilot model, the project to be classified as SECRET. On June 14, 1941, the Nomenclature Section of Supply Division, OCSigO, assigned to the new equipment the nomenclature, Keying Unit, type M-229.

1. Military Characteristics:

1. This apparatus to be designed for the fundamental purpose of controlling the stepping of the cryptographic rotors of the Converters M-134-() in an irregular manner, so as to perform the same functions as the present tape transmitter when used on the Converters M-134-(), but without employing key tapes.

2. The apparatus to consist of a single unit, comprising a set of three control rotors in cascade, through which electrical circuits are passed to produce a lengthy disarranged sequence of keying characters for controlling the stepping of the cryptographic rotors. The three control rotors are to be driven by solenoid stepping mechanisms identical in type with those now used in Converters M-134-(). The order of stepping of the three control rotors of the keying unit to be variable by means of a 6-point gang switch or similar device.

3. The apparatus to be capable of being used interchangeably with the present tape transmitter used with Converter M-134-() and to fit in the position now occupied by the present tape transmitter, preferably without necessitating re-design of the present cover case for Converter M-134-().

4. The keying unit itself to be enclosed within a suitable housing, with apertures for the insertion and setting of the three control rotors.

~~TOP SECRET~~

~~TOP SECRET~~C. Converter M-229-T2 and Procurement

Accordingly, the Signal Corps Laboratories were instructed¹ to initiate action for the procurement of one pilot model from Wallace and Tiernan Products, Inc. Wallace and Tiernan, Inc. did their work of developing a pilot model directly on the model built by Signal Intelligence Service. The Corporation notified the Chief Signal Officer on 25 March 1942 that their modification of the model was complete. This modified preproduction model was known as Keying Unit M-229-T2. It was produced by Wallace and Tiernan, Inc. on Contract No. 1077-sc-776. The model was inspected and accepted by the Office of the Chief Signal Officer on 27 March 1942. Immediately thereafter an order was placed with Wallace and Tiernan, Inc. for 75 Keying Units M-229 (Cost: Approximately \$450.00 each). The contract number for this order of 75 units were delivered by Wallace and Tiernan during August and November, 1942.²

D. Cryptographic Functioning

Keyer M-229 (short title: SIGG00) consists of a single unit (Tab T), comprising a set of three control rotors in cascade, through which electrical circuits are passed to produce a lengthy disarranged series of keying characters for controlling the stepping of the five cryptographic rotors

-
1. Letter, Subject: Keyer for Converter M-134, To: Director, Signal Corps Laboratories; From: Hugh Mitchell, Lt. Col., S.C. (By order of the Chief Signal Officer), 26 May 1941.
 2. Delivery: 15 units: Aug. 24, 1942; 20 units: Sept. 24, 1942; 20 units: Oct. 24, 1942; 20 units: Nov. 24, 1942.

~~TOP SECRET~~

~~TOP SECRET~~

of M-134; M-134-A. Keyer M-229 consists of two distinct main parts: These two parts are (1) the small rotor bank, comprising the set of three control rotors in cascade (see Tab U)¹ and (2) the control multi-switch (see Tab U, W)² and its associated stepping solenoids. The functions of these two parts of the keyer differ as follows: The function of the small rotor bank is to control the stepping of the five cipher rotors of the M-134; M-134-A. The function of the control multi-switch is to provide a variation in the stepping of the control rotors of the small rotor bank. The manner in which the control rotors of the small rotor bank of Keying Unit M-229 carry out their function of stepping the cipher rotors of Converter M-134; M-134-A is explained in the paragraphs immediately following. The manner in which the control rotor themselves step is explained directly thereafter.

The small rotor bank of Keying Unit M-229 consists of three randomly wired rotors which act as switching commutators between two end plates or stators. Each time a letter of the keyboard of Converter M-134; M-134-A is depressed, five circuits are established through the control rotor maze (the three rotors of Keying Unit M-229). The direction of the current is from the right end plate, through the rotor maze, to the left end plate, to the stepping magnets of the five rotors of the Converter M-134; M-134-A. The entire purpose of these five circuits through the control rotor maze is to step the rotors of the Converter M-134; M-134-A in random fashion.

1. The rotors themselves are shown only in Tab T. All other pictures show the rotor bank without the rotors.
2. Control multi-switch can be located by means of noting small plate containing the numbers 1, 2, 3, 4, 5, 6 and a switch with pointer.

~~TOP SECRET~~

~~TOP SECRET~~

The exact manner in which the control rotor maze of Keying Unit M-229 effects stepping of the five rotors of the Converter M-134 (M-134-A) can be best understood by examining the wiring in detail. On the right stator of Keying Unit M-229, there are five entrance spots for the current which become "alive" each time a key of the converter keyboard is depressed. Since there are 26 contact points on the sides of each rotor, there are 26 numbered entrance points on the right stator (see Tab U) but all of these entrance points are "dead" except five. The five "live" entrance points (as the Keying Unit is presently wired) are contact points 16, 20, 26, 3, 10. (These numbers, 16, 20, 26, 3, 10, appear on the Wiring Diagram, Tab Z, designating the five "live" entrance points on the right stator. In Tab U, some of the wires can be seen attached to these five designated entrance points on the right stator. The current enters the right stator at these five "live" spots and thereby establishes five paths through the control rotor maze.) From here on, each of the five paths of current established is through the alphabet maze in normal fashion,¹ that is, directly through the stator to the touching contact on the left face of the first rotor, to the contact to which it is wired on the right face of the first rotor, and on through the control rotor maze in this manner (see diagram on Page) to the touching contact on the right end plate or stator.

The left end plate or stator (Tab V) of Keying Unit M-229 contains 26 contact points. The contact points are banded or wired together in

1. For description of the path of a current through an alphabet maze, see diagram, page .

⁴²
~~TOP SECRET~~

~~TOP SECRET~~

groups as follows: Contact points 7, 8, 9, 10 and 11 are wired together in such a way that if one of the circuits through the control rotor maze ends in any one of these contact points, it will cause rotor no. 1¹ of the Converter M-134; M-134-A to step. (These five contact points, 7, 8, 9, 10, 11, are designated on the Wiring Diagram, Tab Z, by the letter A. The wire can be followed on the Wiring Diagram, Tab Z, from the banded contact points designated by A directly to the stepping solenoid of rotor No. 1¹ of Converter M-134.) In the same way, contact points 13, 14, 15, and 16 are wired together (designated on Wiring Diagram, Tab Z, by the letter B) and affect the stepping of rotor no. 2.¹ Contact points 2, 3, 4, 5 are wired together and control rotor no. 3.¹ Contact points 18, 19, 20, 21, 22 are wired together and control rotor no. 4.¹ Contact points 23, 24, 25, 26 are wired together and control rotor no. 5.¹ Contact point no. 1 of the right stator is a dead end; it is wired to nothing.

To better show the effect of the five circuits through the control rotor maze on the stepping of the cipher rotors, an example is given. Suppose that the current enters at the five "live" spots, 16, 20, 26, 3, 10 on the left stator (which is an invariable circumstance of every encipherment) and leaves the control maze at the exit points, 18, 7, 20, 1, 22 (which points are varied by the variable path through the control

1. This banding of contacts can be switched as a unit by the operator to control instead any of the other four rotors. This switching is accomplished by means of the plug and jack strip of Converter M-134; M-134-A.

~~TOP SECRET~~

~~TOP SECRET~~

rotor maze caused by the stepping of the control rotors.¹ According to the Wiring Diagram, Tab Z:

Exit point 18 (Group D) causes rotor 4 to step.
 Exit point 7 (Group A) causes rotor 1 to step.
 Exit point 20 (Group D) causes rotor 4 to step.
 Exit point 1 (Dead end).....
 Exit point 22 (Group D) causes rotor 4 to step.

Therefore, the effect of the five circuits of the example is that two rotors, rotor 1 and rotor 4, of Converter M-134; M-134-A step with this particular encipherment of a letter.

The control rotors of Keying Unit M-229 step as follows: One of the three rotors is a fast-stepping rotor which steps each time a letter is enciphered. A second rotor steps once each time the fast stepping rotor has stepped 26 times. A third rotor steps once each time the medium stepping rotor has stepped 26 times. This stepping is accomplished by means of stepping solenoids beneath the rotors, the energizing contacts for which are controlled by the control multi-switch (Tab W, Tabs U and V)² located at the right of the keying unit.

The function of the control multi-switch is to vary the positions of the fast-stepping, medium-stepping, and slow-stepping rotors. The control multi-switch has 6 positions which control the stepping of the three rotors of the keying unit as follows:

1. For explanation of stepping of the control rotors, see paragraphs immediately below.
2. The control multi-switch can be located by means of noting the numbers 1, 2, 3, 4, 5, 6, on small square plate which contains switch with pointer.

~~TOP SECRET~~

~~TOP SECRET~~

Position of Control Switch	Fast Rotor	Medium Rotor	Slow Rotor
1	1	3	2
2	1	2	3
3	2	1	3
4	2	3	1
5	3	2	1
6	3	1	2

E. Keying Instructions

The keying instructions for using Keying Unit M-229 with Converter M-134; M-134-A are as follows:

Converter M-134; M-134-A used in conjunction with Keying Unit M-229 employs 8 keying elements. Six of these keying elements are changed daily; two are changed with every message. The six daily keying elements are as follows:

1. The cipher rotor assembly of Converter M-134; M-134-A. - The rotors are selected and arranged daily according to the current cipher-rotor assembly of the system.
2. The control rotor assembly of Keying Unit M-229. - The rotors are selected and arranged daily according to the current control-rotor assembly table of the system.
3. The plug and jack arrangement on the terminal strip of Converter M-134; M-134-A. - The plugs and jacks are arranged daily according to the current Plug and Jack table of the system. (The effect of changing the plugs and jacks is to switch the bands of the left stator of the keying unit so that they are connected to different cipher-rotor solenoids. See footnote 2, page and associated explanation in text.)
4. Setting of the control multi-switch. - This switch, which is located to the left of the Keying Unit, is set daily to one of its six positions as indicated in the current control switch table of the system.

~~TOP SECRET~~

REF ID: A523186
~~TOP SECRET~~

5. Initial alignment of cipher rotors of Converter M-134; M-134-A. - The daily initial alignment of the cipher rotors is found in the current table of the system marked "INITIAL ALIGNMENT". This initial alignment is used during an entire day but cannot be set at the beginning of the day and then forgotten as can the first four daily keying elements. The cipher rotors must be aligned to the INITIAL ALIGNMENT each time a message is enciphered during the day. This initial alignment is that of the cipher rotors used for encipherment of the internal message indicator. It is never transmitted. For detail, see explanation of message keying elements below.
6. Initial alignment of the control rotors of Keying Unit M-229. - The same table and group of letters is used for the daily alignment of the control rotors as is used for the daily alignment of the cipher rotors. It is found in the current table of the system marked "INITIAL ALIGNMENT". The control rotors must be aligned to the first three letters of this INITIAL ALIGNMENT each time a message is enciphered. This initial alignment is that of the control rotors used for encipherment of the internal message indicator. It is never transmitted. For detail, see explanation of message keying elements below.

The two message keying elements are as follows:

1. Alignment of cipher rotors to the internal message indicator. - The internal message indicator is the initial alignment of the rotors when encipherment of the message text is begun. It is determined, enciphered, and used as explained below.
2. Alignment of the control rotors to the first three letters of the internal message indicator. - The internal message indicator is determined, enciphered, and used as explained below.

A group of any five letters except X and Z are selected at random to be used as the internal message indicator. For purposes of example, suppose that the internal message indicator selected is TLBMH. Since the internal message indicator is the group used as the initial alignment of the rotors when encipherment of the message text is begun, it must never be transmitted in the clear but must be disguised for transmission to the deciphering operator by enciphering it. The internal message

~~TOP SECRET~~

~~TOP SECRET~~

indicator is enciphered as follows: After the other daily keying elements have been set, align the cipher rotors to the five letters of the daily initial alignment given in the table marked "INITIAL ALIGNMENT"; align the control rotors to the first three letters of the same daily initial alignment. With the rotors so aligned, encipher the 5-randomly selected letters (in the example, TLBMH) by typing them on the keyboard of the typewriter of the converter. The 5-letter cipher resultant of this encipherment is the external message indicator. After thus determining the external message indicator (which is later to be transmitted with the message), align the cipher rotors to the five letters of the internal message indicator. (Using the 5 letters of the internal indicator of the example, align the cipher rotors to TLBMH). Then align the control rotors to the first three letters of the internal message indicator (example: TLB). The daily keying elements having been set at the beginning of the day, the converter and keying unit are now in complete readiness for typing the plain text of the message to produce cipher text.

To decipher the message, all of the keying elements are set exactly the same way as in enciphering. The only differences are that the encipher-decipher switch is set to decipher and the external message indicator is typed to produce the internal message indicator. When the internal message indicator is thus derived, the rotors are aligned to it and the cipher text deciphered.

~~TOP SECRET~~

REF ID: A62886
~~TOP SECRET~~

F. Cryptographic Security¹

The security of Converter M-134-A with Keying Unit M-229 is dependent on the following: At least 10 messages in depth or flagrant misuse of the indicator system are necessary before elements of the machine can be reconstructed. The number of exhaustive trials necessary to identify known rotors is very large, though not as great as in the case of Converter M-134-C. The number of trials equals 60 rotor arrangements for the control maze times 10 x 9 x 8 x 7 x 6 rotor arrangements for the cipher maze time 26^5 rotor alignments times 120 jack and plug settings time 6 settings for the control switch.

Although no security studies have been conducted on either Converter M-134-A or Keying Unit M-229, comparisons have been made with Converter M-134-C. Even though the present Converter M-134-C has greater security than Converter M-134-A had, as it was used, the latter was the best machine of its day and its chief weaknesses were the indicator system, the tape makeup, and the operating procedures. Since the machine with Keying Unit M-229 incorporated many of the features of Converter M-134-C, its security approaches that of the later machine. However, more variations of the cryptographic elements are possible in Converter M-134-C, as indicated below:

More variation in rotor speeds is possible in Converter M-134-C.

There were only 120 plug and jack settings in Converter M-134-A as compared to 10^5 settings of the index maze in Converter M-134-C.

1. This cryptographic security evaluation is copied from "Historical and Cryptological Summary of Cryptosystems", Volume I, (short title: ASAG-23).

~~TOP SECRET~~

~~TOP SECRET~~

Although the minimum guaranteed cycle for both machines is 26^3 , the addition of the two "dead" rotors in the first and fifth positions of the Converter M-134-C control maze provides 676 different cycles of 26^3 .

The use of reversible rotors in Converter M-134-C greatly increases the number of rotor arrangements.

~~TOP SECRET~~

~~TOP SECRET~~CHAPTER X. CONVERTER M-134-B (AND OTHER UNADOPTED
MODIFICATIONS OF CONVERTERS M-134-T2 and M-134-T1)

Converter M-134-B is an adaptation of Converter M-134-T2 which proposes cam-wheel control of the enciphering rotors instead of Baudot code tape control. Cam-wheel controlling of the enciphering rotors is covered by Patent Application 107,244, filed by William F. Friedman on October 23, 1936. No model was built because the introduction of Converter M-134-C (see Chapter XI) made it unnecessary.¹ The basic consideration² of the unadopted mechanism for controlling the stepping of the rotors of Converter M-134-T2, proposed by Mr. Friedman in April 1935 and filed for patent in October 1936 was a series of notched wheels driven stepwise by meshing gears. The notches were arranged on the wheel collars in random fashion. The notches on each wheel controlled a contact for opening and closing a circuit to the stepping solenoids of each cipher rotor. The number of "steps" around each notched wheel was different in order that the length of the cycle would be much longer than the distance around any one wheel. The key provided by the randomly placed notches on the stepping wheels could be lengthened in several ways: (1) the number of notched wheels could be double the number of cipher rotors (instead of equal) so that it would take 2 notched wheels to control one contact; (2) the notches on the wheels were to be contained

1. Letter, To War Plans and Training Division, From Research and Development Division, Signed: W.S. Rumbough, Major, S.C., 9 July 1935. Filed in Folder 2, Specifications, CSGAS-80. "It is recommended that no steps other than those already determined upon be taken at present in connection with the current development of Converter M-134-T2."
2. See description and sketch, signed William F. Friedman, dated 8 April 1935. Folder 2, Converters M-134, M-134-A, Specifications, CSGAS-80.

~~TOP SECRET~~

~~TOP SECRET~~

on removable collars which could be replaced by collars with a different random arrangement of notches; (3) the notched wheels were to be interchangeable. In June 1935, Mr. Graham made several suggestions for changing the mechanico-electrical set up of the above invention. In other words, the basic principle of the second arrangement was still the use of notched wheels for closing contacts to complete the circuits to the rotor-stepping solenoids, but the exact mechanico-electrical arrangement was different.¹

Although the Converter M-134-T1 was not any longer being considered by the Army, an arrangement of the above type² for controlling the one rotor of the earlier converter was also proposed by Mr. Friedman.³

In April 1936, Mr. Friedman conceived another modification of Converter M-134-T1, the basic principle of which is as follows: Instead of employing the comparing circuit to control the starting and stopping of the commutator wheel, the wheel was to be kept in constant, regular

1. See Sketch, signed William F. Friedman and George A. Graham, 17 June 1935. Filed: Folder 2, Converters M-134, M-134-A, Specifications, CSCAS-80.
2. That of using cam wheels instead of Baudot-code tape.
3. Part of Mr. Friedman's own description of the arrangement is as follows: "The cryptograph consists of a single, constantly rotating, 26-setment, 26-character commutator wheel of the Hebern type, controlled by a control system including a set of rotatable, differential cam wheels. This control system consists of five or a multiple of five cam wheels which operate make or break contact levers and their action (by causing suitable interaction between sets of five cam wheels in case 10, 15.... can wheels are used in sets of fives) results in setting up five-unit code, Baudot resultants. The cam wheels are of different diameters, individually rotatable in stepwise manner under control of the keyboard, the numbers of positions of the various cam wheels being preferably prime to one another so as to yield a very long resultant enciphering key of Baudot permutations, there being a total of 32 such permutations."

~~TOP SECRET~~

~~TOP SECRET~~

rotation, and the comparing circuit was merely to determine when electric potential was applied at the keyboard. Thus, when a key of the keyboard was depressed no current reached the indicating bank through the cipher commutator until the comparing circuit was completed. Since the latter event was controlled by the cipher-key transmitter, it was obvious that a result was indicated on the indicating bank once per revolution of the commutator, but the exact instant when it was indicated was a function of the character on the cipher-key wheel.

~~TOP SECRET~~

~~TOP SECRET~~

TAB A

Converter M-134

Front View

~~TOP SECRET~~

Copy Holder MC-184. - The copy holder for Converter M-134 is mounted on the base of the case between the cryptograph and the typewriter. Its height above the base is adjustable by upward or downward movement on its mounting standard. A clamping pin locks the holder securely in place. Messages for encipherment or decipherment are inserted under the spring-tensioned hinge at the top of the holder. A line guide moves vertically along a rod at the right of the copy holder.

~~TOP SECRET~~

APPENDIX I

Changes in Keying Instructions for Converter M-134, M-134-A

as they appear in

"Keying Instructions for Converter M-134"
(short title: SIGPUF), Sept 1938

"Keying Instructions for Converters M-134 and
M-134-A" (short title: SIGJUX), April 1940

"Keying Instructions for Converters M-134,
M-134-A" (short title: SIGLOG), March 1942

~~TOP SECRET~~

~~TOP SECRET~~

CHANGES IN KEYING INSTRUCTIONS FOR CONVERTER M-134

	SIGPUF, Sept 1938	SIGJUX, April 1940	SIGLOG, March 1942
Keying elements	<p>5 Keying elements: 2 Daily keying elements: (1) Rotor assembly - determined by table. (2) Key tape - determined by table. 3 Message keying elements: (1) Corrections between keytape transmitter and rotor stepping magnets. (2) Initial alignment of rotors. (3) Initial position of key tape.</p>	Same	Same
Rotor assembly	<p>Each machine is provided with 10 rotors. 5 used at a time. Rotor assembly changes daily in accordance with current rotor assembly table of system. For example, if the table shows that for Jan 1 the rotor assembly is 8-3-1-9-7, it means rotor 8 is inserted in rotor pos. 1, rotor 3 in position 2, etc.</p>	<p>Each machine is provided with 15 rotors: 5 red-colored rotors (short title: SIGLIG) for Confidential messages and 10 rotors (short title: SIGTER). The 5 reddish Confidential rotors (SIGLIG) are marked C-1 to C-V; the 10 Secret rotors are marked 1 to 10. NEVER INTERMIX SECRET AND CONFIDENTIAL ROTORS. The rotor assembly changes daily and is determined by table in the same manner as in SIGPUF (see rotor assembly under SIGPUF).</p>	<p>Each machine is provided with 15 rotors: 5 red colored rotors and 10 gray-colored rotors heretofore used for Confidential systems are no longer to be used as such; all 15 rotors constitute one set. Rotor assembly changes daily in accordance with rotor assembly table of system. For example, the table may show that for a particular day the rotor assembly is 8-C3-1-9-7 which means that (gray-colored) rotor no. 8 is inserted in rotor position 1, (red-colored) number 3 is inserted in position 2, etc.</p>

~~TOP SECRET~~

~~TOP SECRET~~

	SIGPUF, Sept 1938	SIGJUX, April 1940	SIGLOG, March 1942
Key tape selection	Each M-134 system used a different set of 48 key tapes in duplicate. Each tape bears the short title of the set, followed by an identifying number which appears at the head of the tape. It is these numbers which are used to determine the specific tape to be employed on a given day in accordance with the current key tape selection table of the system. For example, the table may show that for Jan 1 the tape to be used is number 17.	Same	Selection is the same. Difference: The secret system has 48 tapes furnished in duplicate; the confidential system has 30 tapes furnished in triplicate.
Plug and Jack Strip	The corrections between the key tape transmitter and the rotor stepping solenoids are established and varied by means of the plug and jack strip. These connections are changed with every message as follows: An indicator consisting of 5 letters is chosen <u>at random</u> by the operator. Suppose he selects FHBGR. These letters are assigned numbers in accordance with their relative order in the normal alphabet thus: F-H-B-G-R 2-4-1-3-5	Same	Same

~~TOP SECRET~~

~~TOP SECRET~~

	SIGPUF, Sept 1938	SIGJUX, April 1940	SIGLOG, March 1942
Plug and Jack Strip (cont'd)	This then determines the set-up of the plug and jack connections but these connections are in effect only for one message. For the next message a new indicator is selected at random and the order again derived in the same way.		
Initial alignment of rotors	A different initial alignment of rotors is used with every message. To determine the alignment, the same five letters as was selected to derive the order of the plugs in the jacks are used. In the example (see Plug and Jack Strip above), the indicator selected at random was FHBGR. The operator therefore aligns the rotors by hand individually so as to align FHBGR on the bench mark from left to right.	Same	Same
Initial position of key tape	The minimum length of each key tape is 1500 characters. Every 10th character of each key tape is numbered by a large number in white ink. (The 1st number printed by the numbering machine is 010, the second is 020, and so on until the 1000th character, which is numbered 000, the 1 being understood). The 1010th character is again numbered 010, etc.) To determine the initial position, the middle 3 letters of the same 5 letters	Same	The same method of determining the initial position of the key tape is used EXCEPT that different letters of the indicator are used for different classifications of messages. For Secret messages - Use the 1st, 2nd and 3rd letters. For Confidential messages - Use the 2nd, 3rd, and 4th letters. For Restricted messages - Use the 3rd, 4th, and 5th letters.

~~TOP SECRET~~

~~TOP SECRET~~

	SIGPUP, Sept 1938	SIGJUX, April 1940	SIGLOG, March 1942
Initial position of key tape (cont'd)	chosen as indicator are used. The value of the middle 3 letters is found by referring to the current table in the system. This table is called "Table For Determining Initial Position of Key Tape". It is merely a table which assigns a numerical value to each letter of the alphabet. For example, using the letters, FHBCR, and a table which gives the following values for the middle 3 letters: H = 8, B = 2, G = 7, the key tape would be set to position 827, that is, the 827th character of the key tape would be placed at the bench mark of the tape transmitter.		
Length of message	If the cryptographed text of a message will exceed <u>50 to 60 5-letter groups</u> , the plain text will first be divided into two or more approximately equal parts and each part will be treated as a separate message.	If the cryptographed text of a message will exceed <u>100 5-letter groups</u> , the plain text will first be divided into two or more approximately equal parts and each part will be treated as a separate message.	Same as SIGJUX.

~~TOP SECRET~~

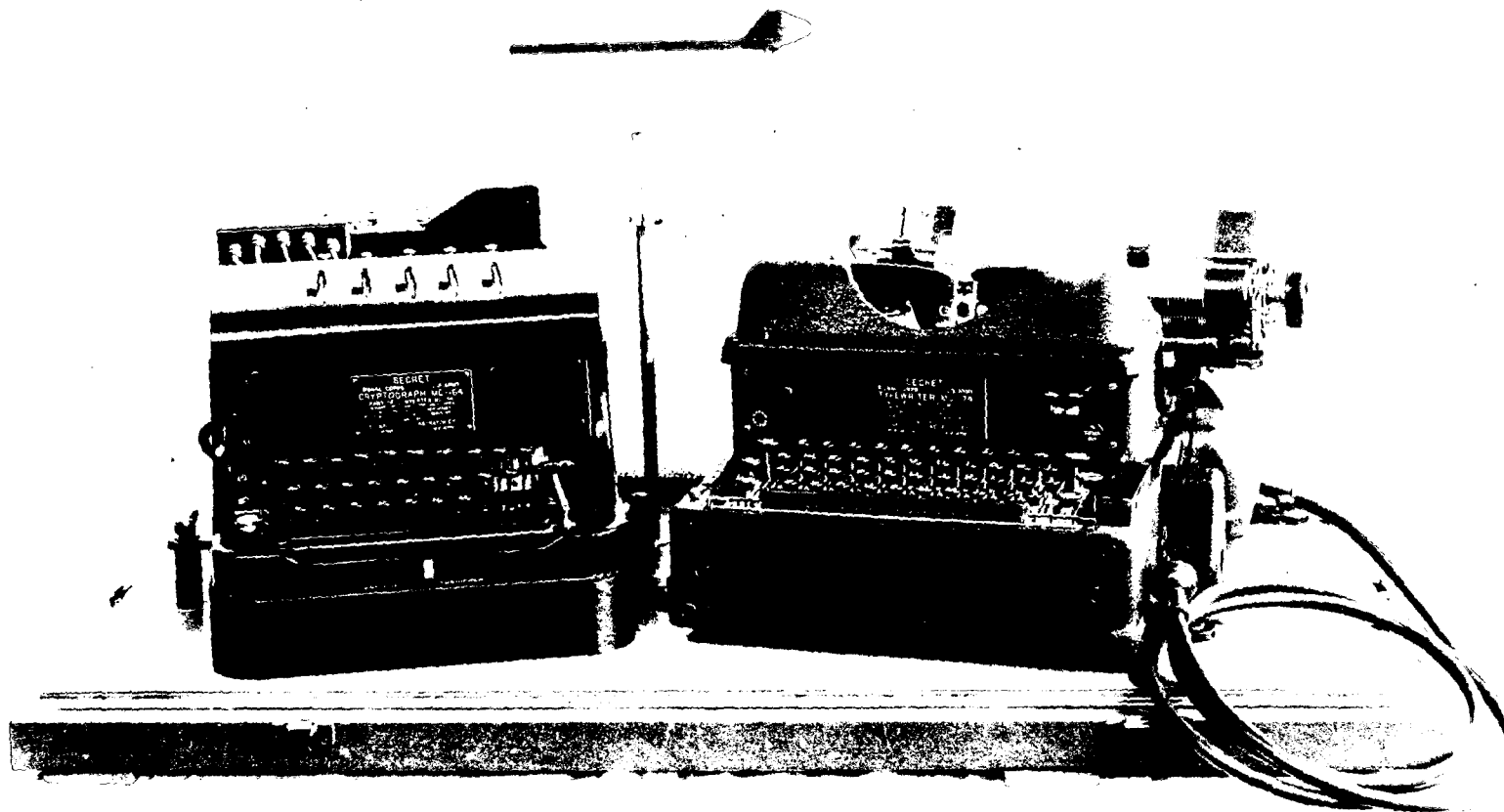


Fig. 1 - Converter M-134, Front View

~~SECRET~~

~~TOP SECRET~~

TAB E

Converter M-134

Plan View

~~TOP SECRET~~

~~SECRET~~

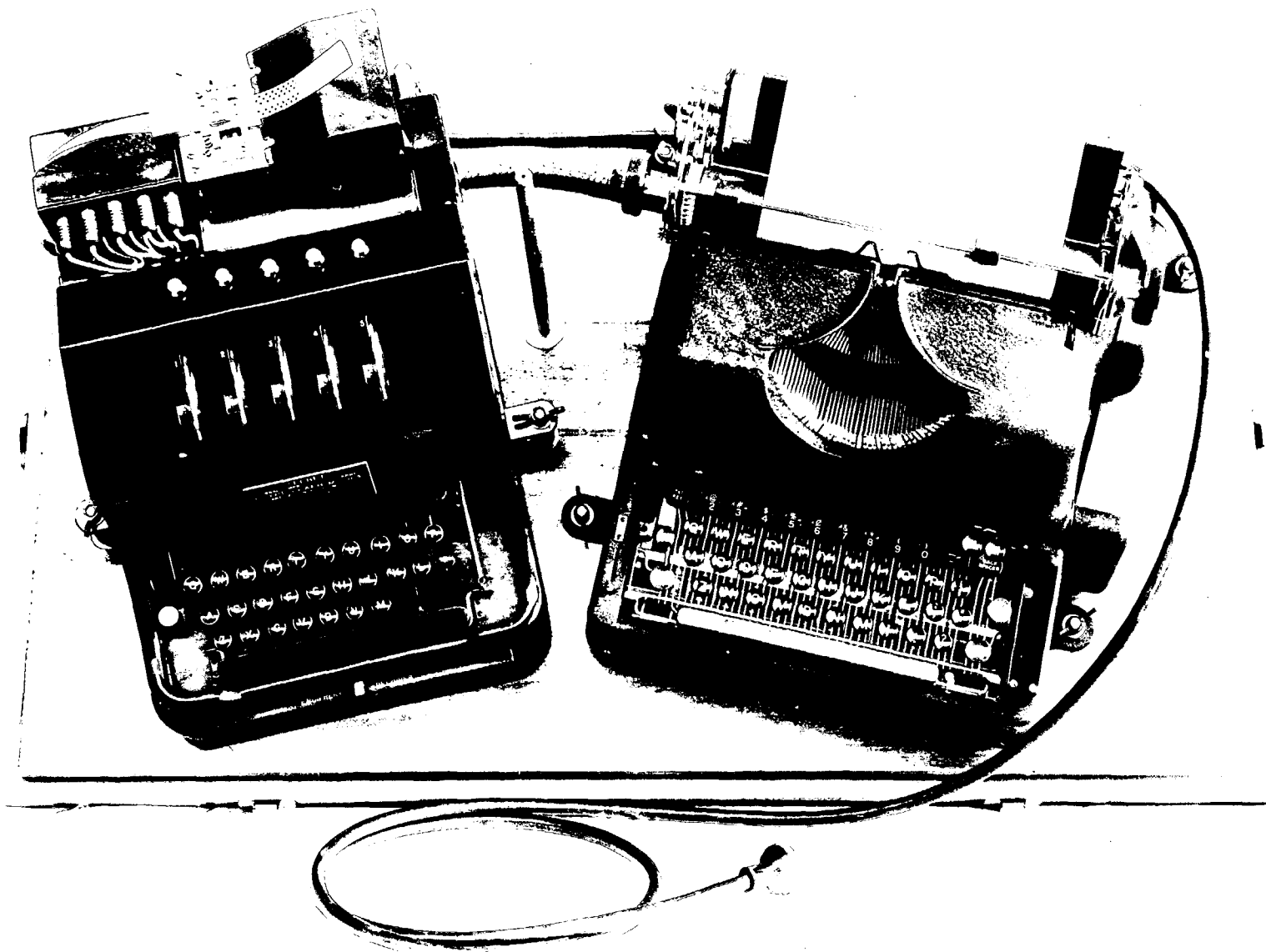


Fig. 2 - Converter M-134, Plan View

~~TOP SECRET~~

TAB C

Converter M-134

Rear View

~~TOP SECRET~~

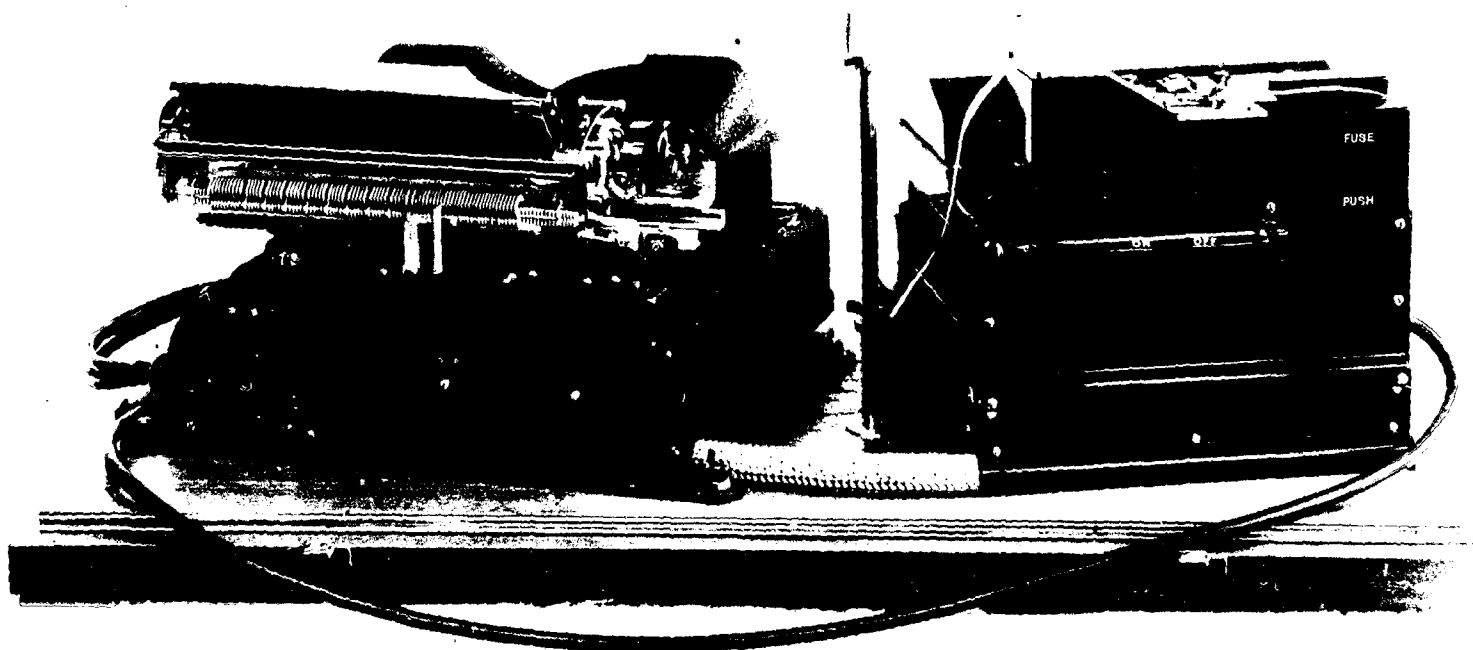
~~SECRET~~

Fig. 3 - Converter M-134, Rear View

~~SECRET~~

~~TOP SECRET~~

TAB D

Converter M-134

Cryptograph MC-164

Plan View

~~TOP SECRET~~

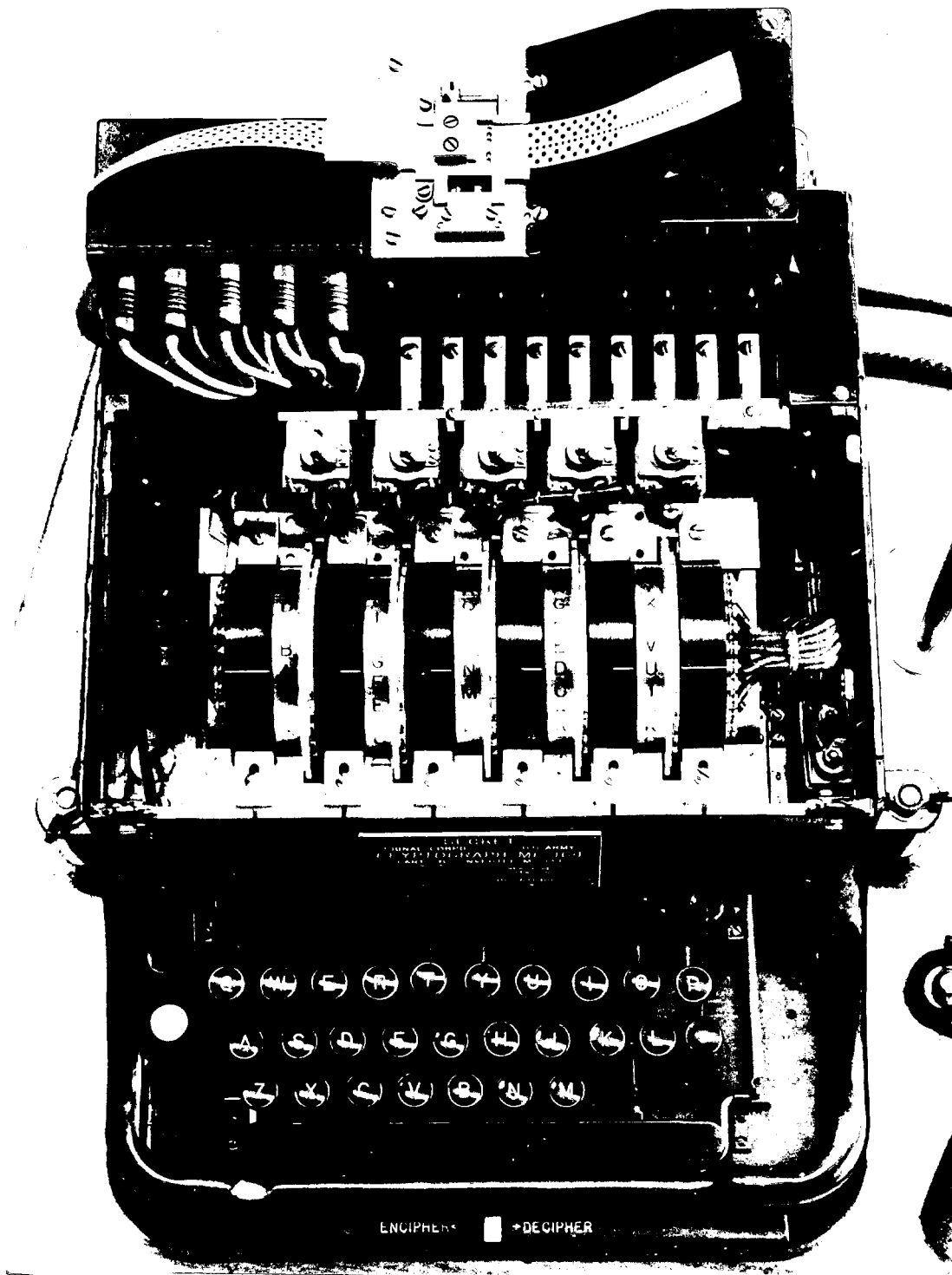
~~SECRET~~

Fig. 4 - Converter M-134, Cryptograph MC-164, Plan View
with Cover Removed

~~SECRET~~

~~TOP SECRET~~

TAB E

Converter M-134

Cryptograph MC-164

Plan View

~~TOP SECRET~~

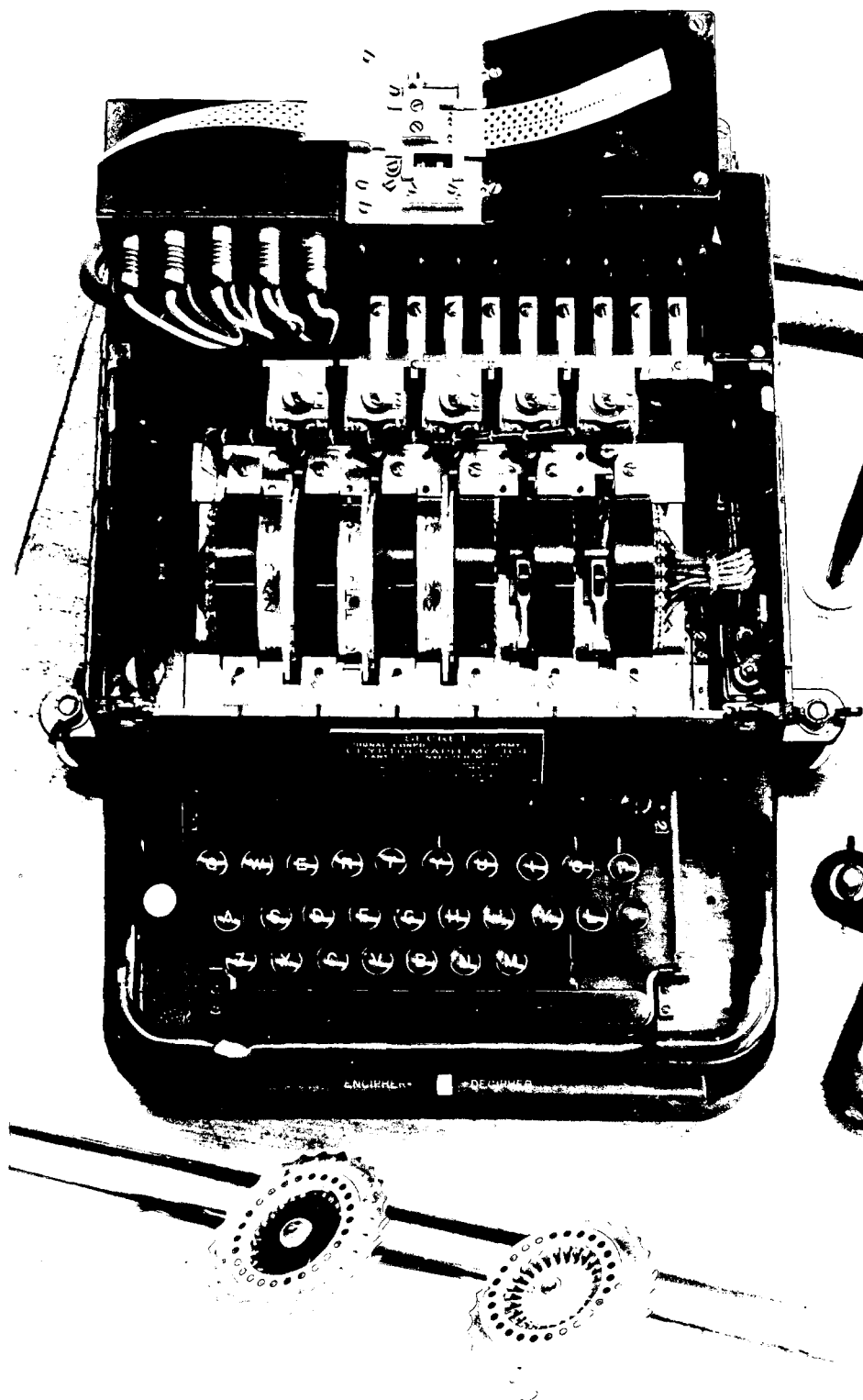


Fig. 5 - Converter M-134, Cryptograph MC-164, Plan View

Showing Cipher Disks Removed

~~SECRET~~

~~TOP SECRET~~

Tab F

Converter M-134

Cryptograph MC-164

(Showing Cipher Disk Stepping Mechanism)

~~TOP SECRET~~

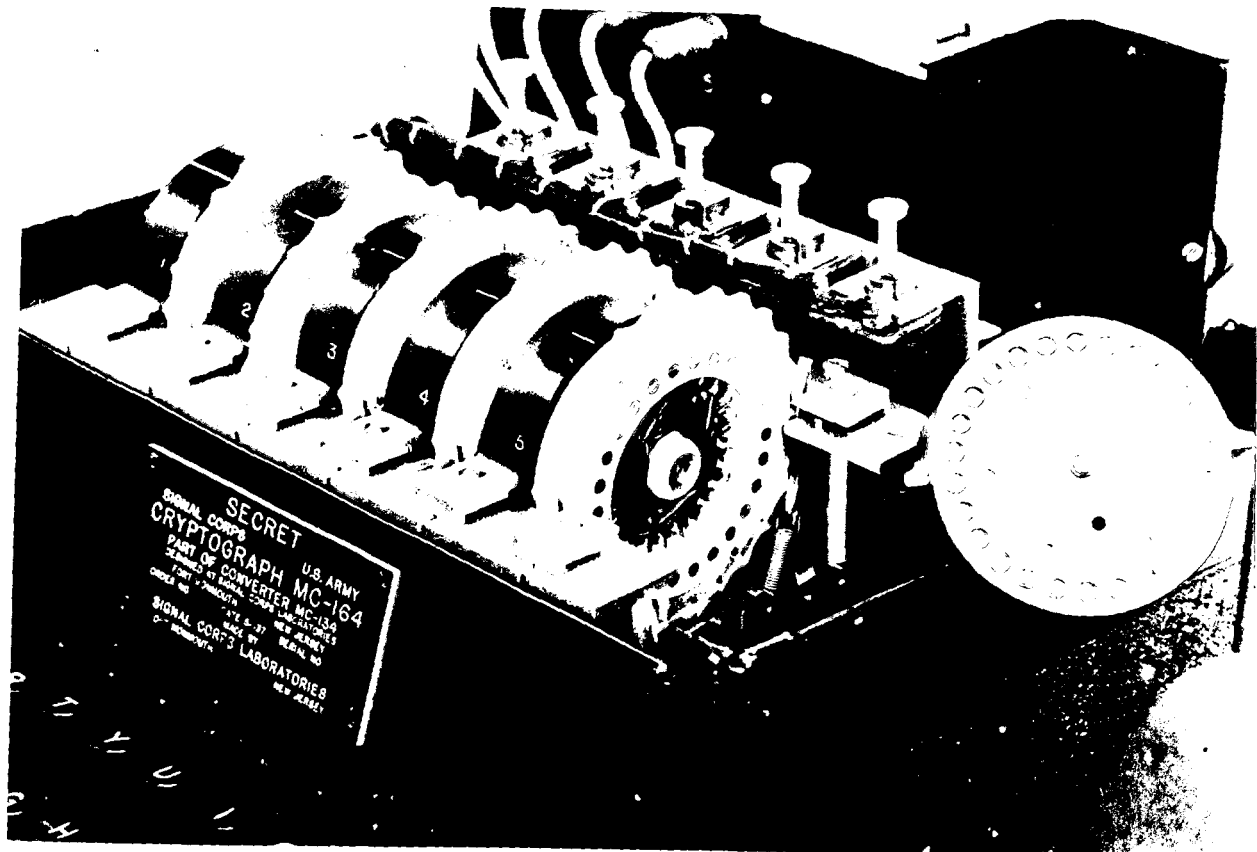
~~SECRET~~

Fig. 6 - Converter M-134, Cryptograph MC-164, Showing
Cipher Disk Stepping Mechanism

~~SECRET~~

~~TOP SECRET~~

TAB G

Converter M-134-A

~~TOP SECRET~~

DETAILED DESCRIPTION AND FUNCTIONING OF CONVERTER M-134; M-134-A¹

Cryptograph MC-164. (Reference Tabs I, J, K, and photograph opposite.) - The cryptograph consists of a base frame, keyboard, keyboard universal bar and contact combination, five rotors operating between stator elements, five rotor stepping mechanisms, rotor-stop release lever (only on MC-164-A), encipher-decipher reversing switch, tape transmitter, plug and jack strip, slow-release relay, slow-operate relay cord, and incidental wiring. Interference suppressors were installed in order to avoid interference with adjacent radio sets. A drawer for storing message blanks, pencils, etc., is provided in the front of the base.

Typewriter MC-174. (Reference photograph opposite and Tabs H and S). - This typewriter is a modification of the electromechanical typewriter manufactured by the International Business Machines Corporation. The modification consists of the incorporation of: 26 solenoid magnets with drag links arranged to operate the 26-letter key bars; a universal bar operating a contact combination upon the depression of any key bar; an automatic five-character space contact with 2 solenoid magnets operating upon the space bar; an automatic carriage-return contact with solenoid magnet operating upon the carriage-return key bar and including a warning bell signal; a terminal strip for interconnection with the cryptograph; and capacitors for the suppression of radio interference. 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 interference-suppressing capacitors are connected across the universal-bar contacts and across the terminals of the driving motor as shown in Tab S. The typewriter is permanently interwired with the cryptograph in such a manner that the two normally function as a single unit. The typewriter may be operated independently by striking the keyboard in the conventional manner for plain-text recording. The reversing switch of the cryptograph should be thrown to its DECIPHER position to cut out the automatic spacing feature.

Copy Holder MC-184-A. (Not shown) - For a description and picture of the copy holder for Converter M-134, see Tab A (this volume). The Copy Holder MC-184-A, for Converter M-134-A is a standard commercial copy holder manufactured by the Rite-Line Corporation, Washington, D.C. To use, it is merely necessary to remove from the case and set in any convenient position.

Detailed description continued in Tab H.

1. Throughout this description, all designations of the machine as Converter M-134-A apply equally to Converter M-134 except where the differences are described.

SECRET



SECRET

SECRET

Fig. 1-A

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A

~~TOP SECRET~~

TAB H

Converter M-134

Rear View

~~TOP SECRET~~

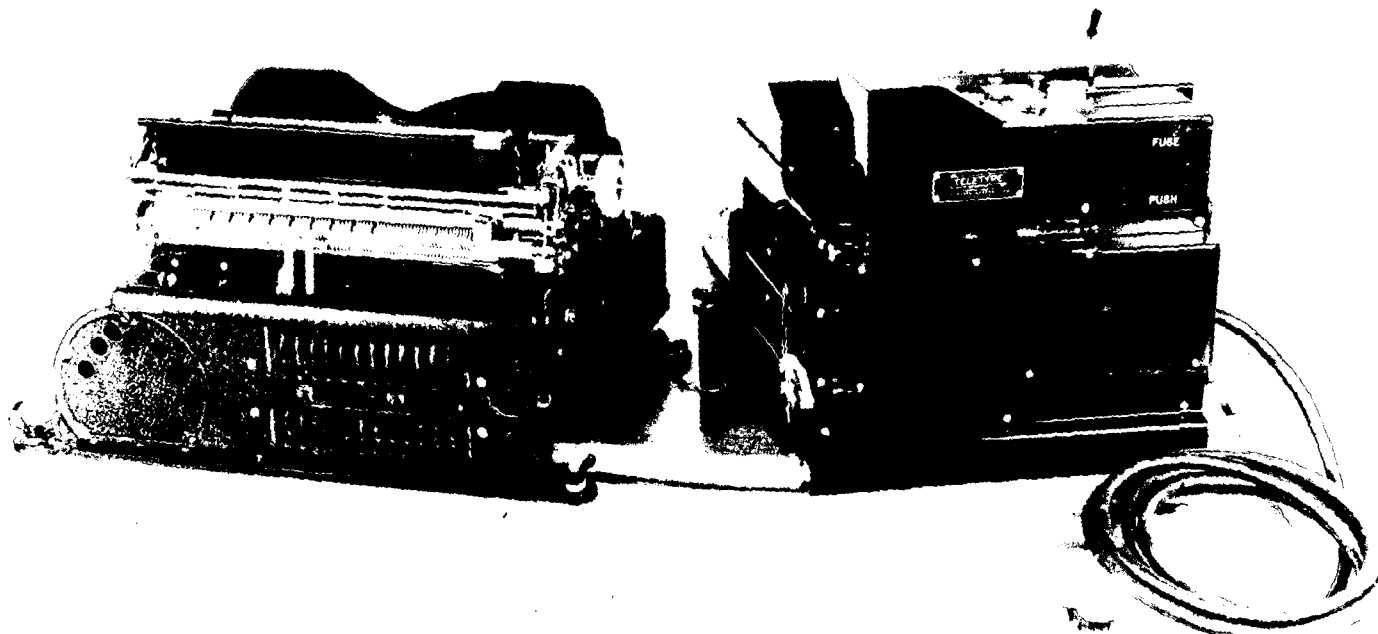
Continued from Tab G.

Rotor Release Lever. Reference photograph opposite, also Tabs G and I. - This lever, included only on Cryptographs 164-A, is mounted on the left of the rotor assembly, in front of the plug and jack strip. By pulling forward on this lever the rotors are disengaged from all pawls and are free to be turned in either direction.

Base Frame. See also Tab G. - The base frame is a modification of the base of the Remington noiseless typewriter Model 10, manufactured by the Remington Noiseless Typewriter Works, Middletown, Connecticut. All elements of the cryptograph are mounted on this frame.

Continued in Tab I.

~~SECRET~~



~~SECRET~~

OL 300

Fig. 2-A

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A
REAR VIEW

~~TOP SECRET~~

TAB I

Converter M-134-A

Cryptograph MC-164-A

Plan View, Cover Removed

~~TOP SECRET~~

Continued from Tab H.

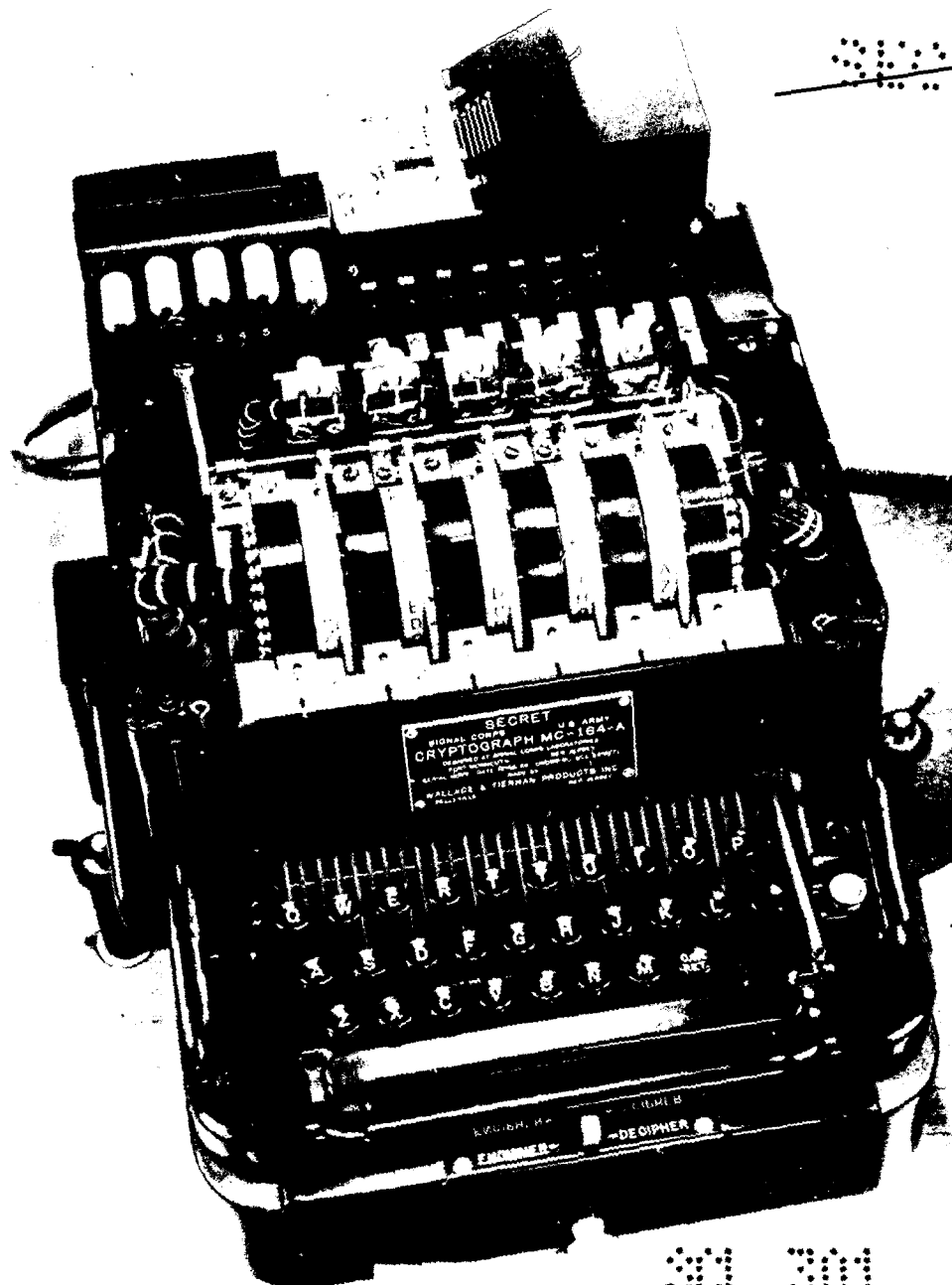
Keyboard. - The standard typewriter keyboard is used, but all keys other than the 26 letters of the alphabet, the space bar and one blank key have been eliminated. The blank key is blocked up inoperative and is used to provide a guide key for the normal position of the operator's hands. A keyboard locking mechanism has been provided to make it impossible to depress two keys at the same time or to depress a second key until the first has been released. This mechanism consists of a series of steel balls within a slotted comb, between the teeth of which one and only one key bar may be pushed at a time. Each key bar is provided with a vertical contact extension which operates between two contact jaws below the bar and, when the key is depressed, serves to close a circuit from that key contact to a solenoid under a key bar of the typewriter. Electrically each key contact has one jaw connected in common to one side of the circuit mentioned and the other jaw connected to one of the studs of the stationary plate of the encipher-decipher reversing switch. The individual circuits pertaining to the various keys of the cryptograph are connected through this switch and then through the whole set of stators and rotors to the solenoids of the typewriter. The key contact jaws of the cryptograph are of the wiping type and should give a minimum of trouble. If a key tends to "stick;" that is, when a key has been depressed and then released and fails to spring back to inoperative position, this is probably caused by some of the bakelite of the contact extension wearing off and forming abrasive foreign matter to make the contact extension stick between the contact jaws. To remedy this situation, all that is necessary is to place a very small amount of a good grade of petroleum jelly (vaseline) on the contact jaws, using either a toothpick or thin slip of paper and then work the key a few times to spread the lubricant in a thin film on the contact extension.

Keyboard Universal Bar. - The keyboard is equipped with a universal bar mounted transversely and directly beneath the key bars so that the depression of any key rotates this universal bar on its axis to close, by means of a lever extension, the universal-bar contact combination.

Keyboard Universal Bar Contact Combination. - The contacts of this combination are in "make" relationship with the universal bar in such a manner that the depression of any key causes those contacts to close before the individual key contact closes. It is important that this relationship be preserved for proper operation of the cryptograph. Upon permitting the key to rise (return to normal), the universal contacts open after the individual key contact opens. The position of the universal bar contacts in the circuit is shown in Tab O and their function is explained in detail in Tab .

Rotors. - a. **Rotors SG-14.** Each converter is provided with a set of 10 rotors which are to be used only for SECRET messages. Each of these rotors is identified by a number engraved on its inner face. The short title SIGTER should be written in India ink on the inner face of each rotor, near the identifying number. The rotors are differently wired as explained below, but they are all mechanically interchangeable though, of course, electrically and cryptographically they are not identical in their effects. Only 5 of them are used at one time, selection being made

Description of rotors continued in Tab J.



SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A,
CRYPTOGRAPH MC-164-A,
PLAN VIEW, COVER REMOVED

Fig. 3-A

~~TOP SECRET~~

TAB J

Converter M-134-A, Cryptograph M-164-A

Plan View

Tape Transmitter MC-185 and Two Rotors Removed

~~TOP SECRET~~

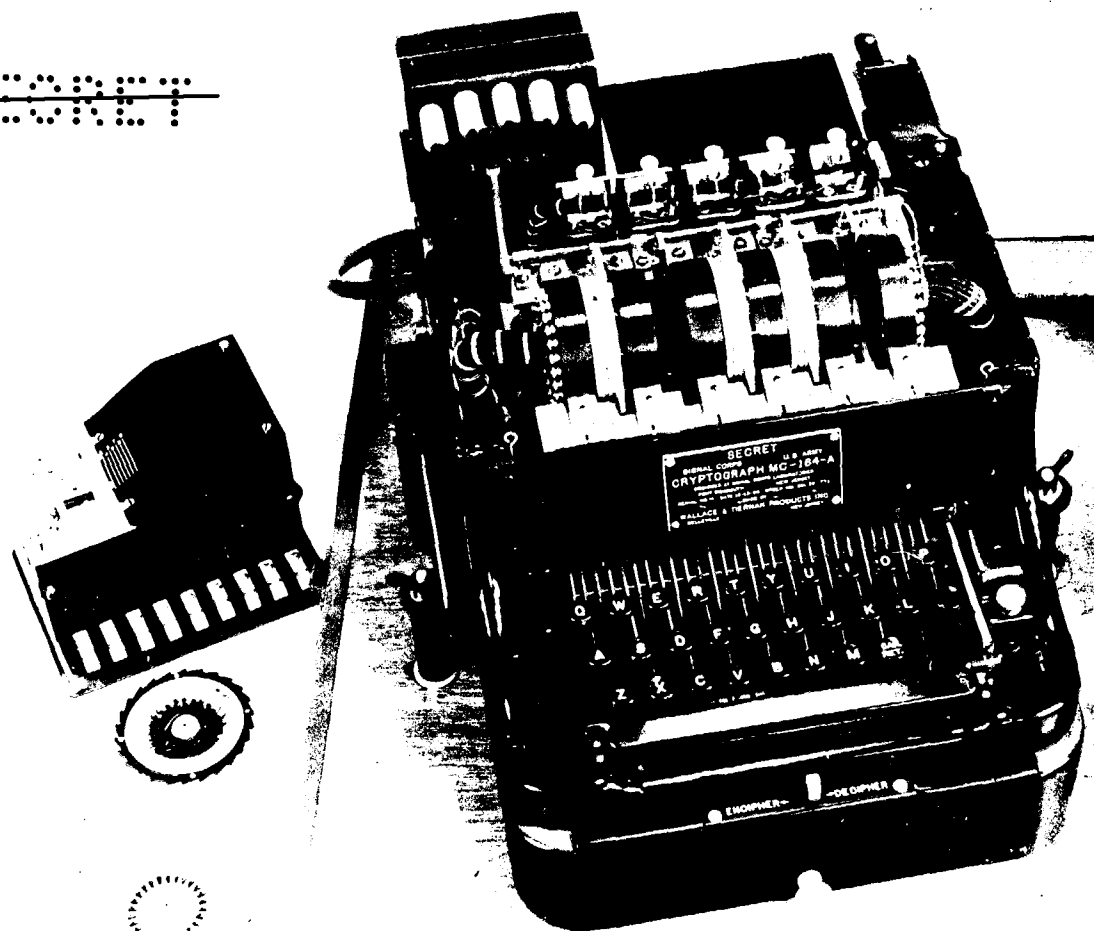
Description of Rotors continued from Tab I.

according to keying instructions. The 5 selected rotors are inserted into 5 rotor positions according to a key and positioned to rotate between six stators. The four intermediate stators separate the rotors and are provided with distributor faces against each rotor. The right and left stators are provided with distributor faces internally contacting the end rotors, and are externally connected by means of stud terminals to the key contacts and the typewriter solenoids through the encipher-decipher reversing switch. In making any change in the wiring to either the right or left stator, follow the instructions in Par. 31 of "Operating Instructions for Converters M-134 and M-134-A" (short title: SIGKOC). Each rotor presents on each face 26 segments, which are in contact with 26 spring and ball contacts on each stator. The connections through the intermediate stators are direct. The segments on one face of each individual rotor are wired in random fashion to the segments on the opposite face of the rotor. The exposed periphery of each rotor is divided into 26 positions designated alphabetically from A to Z. No through shaft is used, each rotor being rotatable upon a spring-tensioned ball in the center of the stators. In order to remove the rotors it is first necessary to remove the metal lid which covers the rotors when in position. This should be done quite gently by grasping the lid at the sides and rocking it with an upward motion, being careful to get the vertical extensions and protruding buttons of the plungers of the rotor stepping mechanisms (see Tab K) centered within the holes in the lid so that the lid can be lifted clear without striking the buttons or the vertical extensions of the plungers.¹ After this has been done any particular rotor is simply withdrawn from between the stators. Each rotor presents a scalloped edge to facilitate setting of the rotors by hand and to act as positioning centers in conjunction with the step-forward mechanism. In setting the rotors to an initial position they may be turned in one direction only — toward the front of the cryptograph, in Cryptograph MC-164. In Cryptograph MC-164-A rotors may be turned in either direction by pulling forward the rotor-release lever. If a rotor is to be advanced only a few steps it is best to do so by depressing the button extension of the step-forward solenoid plunger located directly behind each rotor position. But if a rotor is to be advanced more than a few steps it is best to depress the button by a finger of one hand, move the rotor forward by the fingers of the other hand until within two or three steps of the position desired, then release the rotor and complete its positioning by depressing the button. As regards electrical continuity through the combination of rotors and stators, there are 26 wires connected to each end stator and 26 circuits through the rotors no matter in what position the rotors happen to stop. Therefore 26 through circuits are provided at all times even though the relationship of all circuits is altered by any rotor movement.

Description of Rotors continued on Tab K.

-
1. This does not apply to Cryptograph MC-164-A; as a well has been cut in the cover to permit insertion and removal of rotors without removing cover.

~~SECRET~~



~~SECRET~~

~~SECRET~~

Fig. 4-A

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A,
CRYPTOGRAPH MC-164-A, PLAN VIEW
TAPE TRANSMITTER MC-185 AND
2 ROTORS SG-14 REMOVED

~~TOP SECRET~~

TAB K

Converter M-134-A, Cryptograph MC-164-A

Rotor Stepping Mechanism

~~TOP SECRET~~

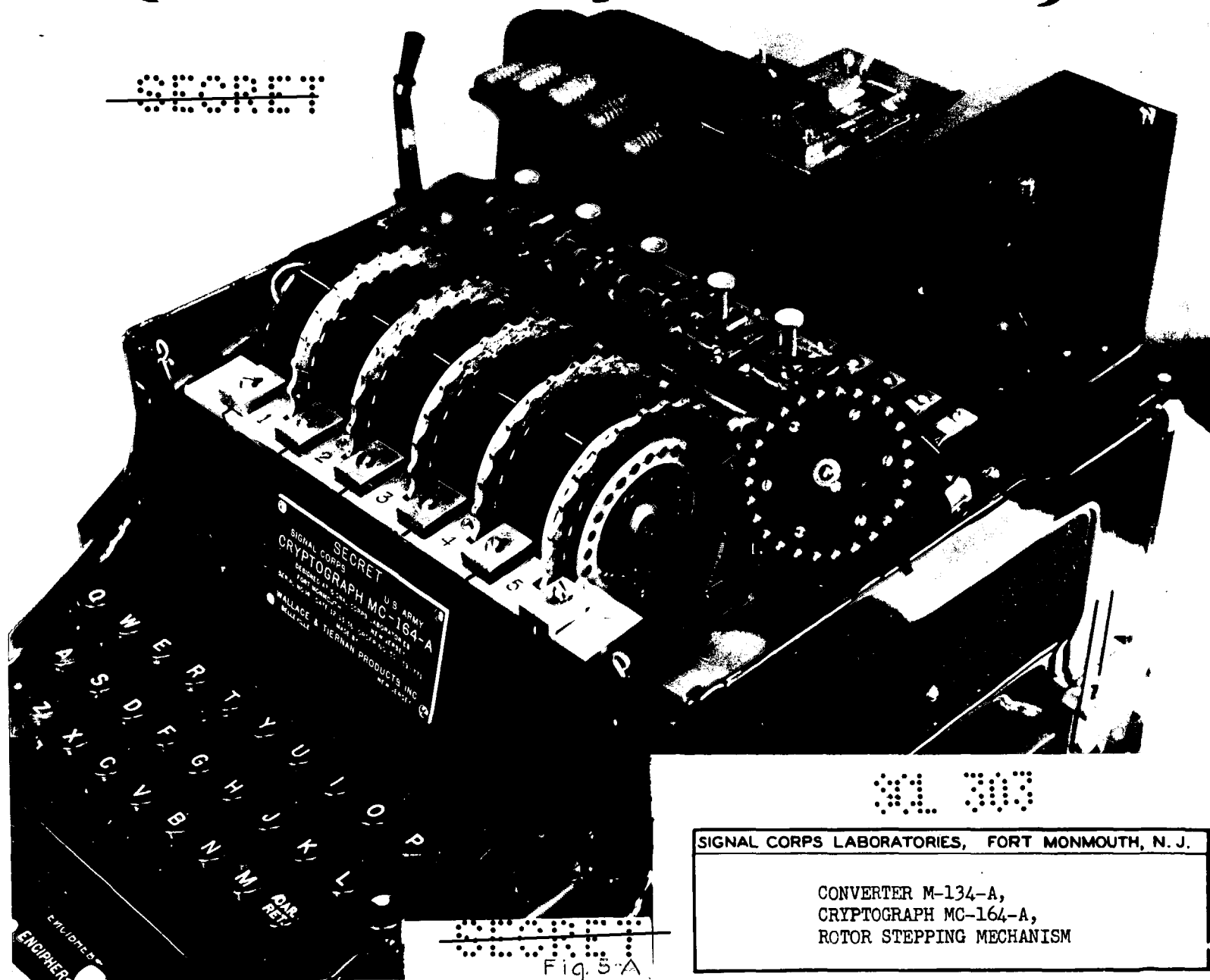
Description of Rotors continued from Tab J.

Rotors SG-15. - Each converter is also provided with a second set of 5 rotors which are to be used only for CONFIDENTIAL messages. These rotors are wired differently from Rotors SG-14, and their metallic rims are different in color from Rotors SG-14, to make them easily distinguishable. The short title SIGLIG should be written in India ink on the inner face of each rotor, near the identifying number. The nature and functions of Rotors SG-15 are the same as those of Rotors SG-14, and no further description is necessary.

Plug and Jack Strip. (Reference photograph opposite and Tab Q) - Five plugs, cords and jacks are connected in the five circuits between the tape transmitter contacts and the rotor stepping solenoids. The plugs are connected to the tape transmitter contacts and are numbered accordingly from 1 to 5 inclusive. The jacks are connected to the rotor solenoids and are also numbered respectively from 1 to 5 inclusive. When the connections at this strip are direct; i.e., cords 1, 2, 3, 4, 5 connected to jacks 1, 2, 3, 4, 5, respectively, then the 1st rotor stepping solenoid at the left as one stands facing the cryptograph is controlled by the transmitter pin nearest the observer. The plug and jack connections must be established and changed according to special keying instructions, since they serve to extend the cryptographic security of the machine.

Rotor Stepping Mechanism. (Reference photograph opposite.) Each of the five rotors is equipped with an individual stepping mechanism comprising a solenoid, tension spring, step-forward pawl and location roller. The individual solenoids are controlled by the contacts of the tape transmitter. When a contact closes the circuit through a given solenoid, that solenoid draws down its plunger, building up tension in a spring. Near the end of the stroke and step-forward pawl is drawn into engagement with a ratchet tooth on the associated rotor. Upon de-energization of the magnet the energy stored in the spring is delivered to advance the rotor one position through the step-forward pawl, which is disengaged following this action. A location roller and arm are combined with the step-forward action in such a manner that a definite step position for the rotor is established. The roller is positioned beneath the rotor and falls into the scalloped edge on its periphery. The step-forward solenoid plungers are extended through the cover of the cryptograph into buttons which can be used to step the rotors forward manually one step at a time, or to permit the manual disengagement of the pawls from the rotors in order to facilitate their rotation many steps at a time, as noted above.

Continued in Tab L.



SECRET

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A,
CRYPTOGRAPH MC-164-A,
ROTOR STEPPING MECHANISM

Fig. 5-A

~~TOP SECRET~~

TAB L

Converter M-134-A, Typewriter MC-174-A

Showing Space and Carriage Return Contacts

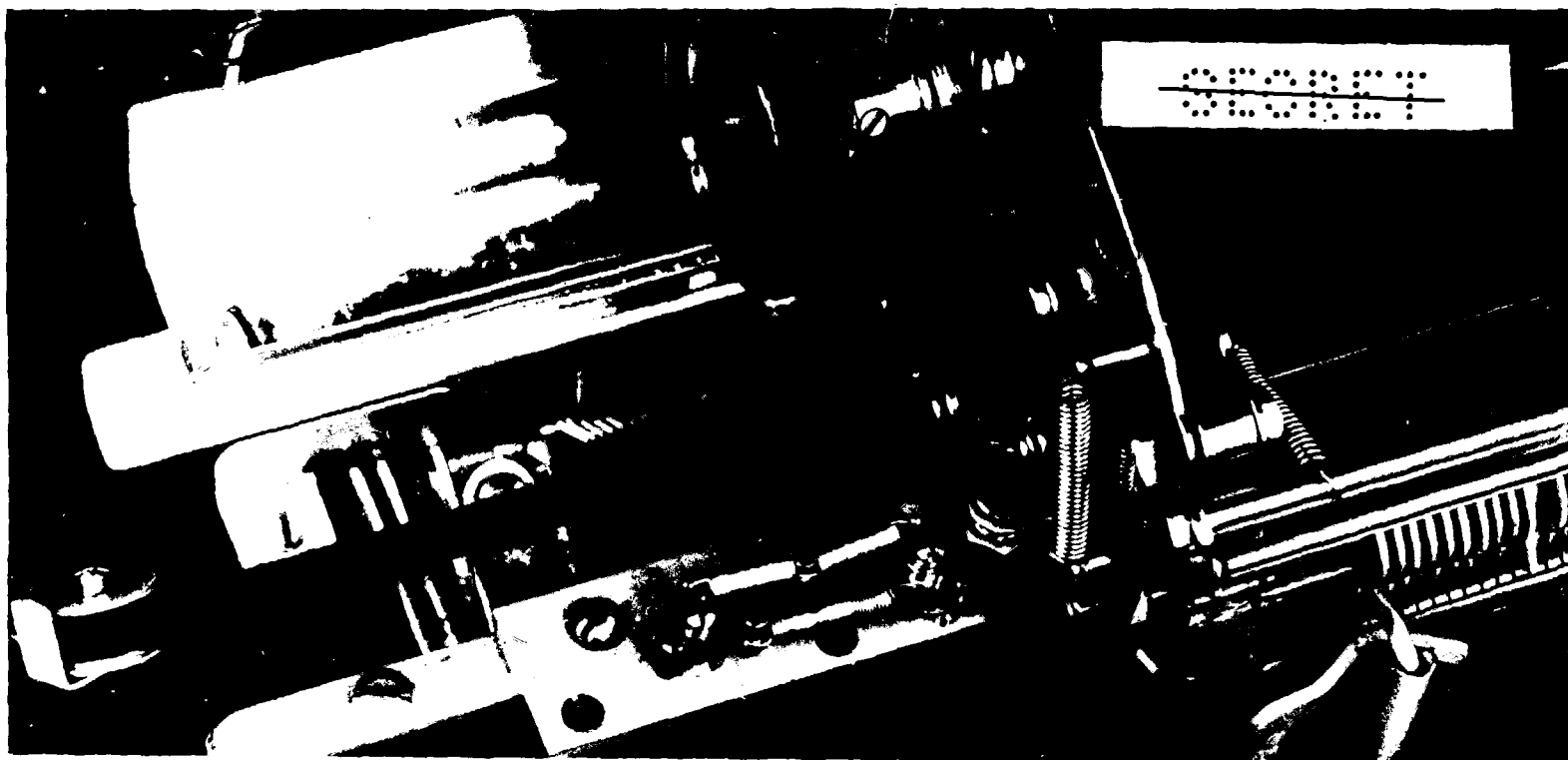
~~TOP SECRET~~

Continued from Tab K.

Automatic Carriage Return and Line Feed Action. - The typewriter carriage in progression from right to left operates a warning bell signal three characters prior to automatic carriage return in Typewriter MC-174, and five characters prior in Typewriter MC-174-A. At the end of the line a stud at the end of the tabulating rack closes the carriage-return contact which completes a circuit to energize the carriage-return solenoid. This solenoid operates to perform the carriage-return and line-feed functions simultaneously. This function is, of course, automatically performed regardless of the position of the encipher-decipher switch.

Automatic Spacing Action. - Every sixth detent of the typewriter tabulating rack closes the spacing contact which is mounted on the rear of the typewriter. With the reversing switch in ENCIPHER position, a circuit is then completed through the typewriter space-pole, single-throw switch which forms one element of the gang reversing switch, to the tabulating-rack spacing contact and back to power. The space bar of the typewriter is thus operated at every sixth detent of the tabulating rack, and the characters in the cryptogram are printed in groups of five. With the reversing switch in DECIPHER position the circuit is opened by the single-pole, single-throw switch, so that closing of the spacing contact on the cryptograph does not energize the space-bar solenoid.

Continued in Tab M.



~~SECRET~~

SECRET

Fig 6-A

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

CONVERTER M-134-A,
TYPEWRITER MC-174-A,
SHOWING SPACE AND CARRIAGE
RETURN CONTACTS

~~TOP SECRET~~

TAB M

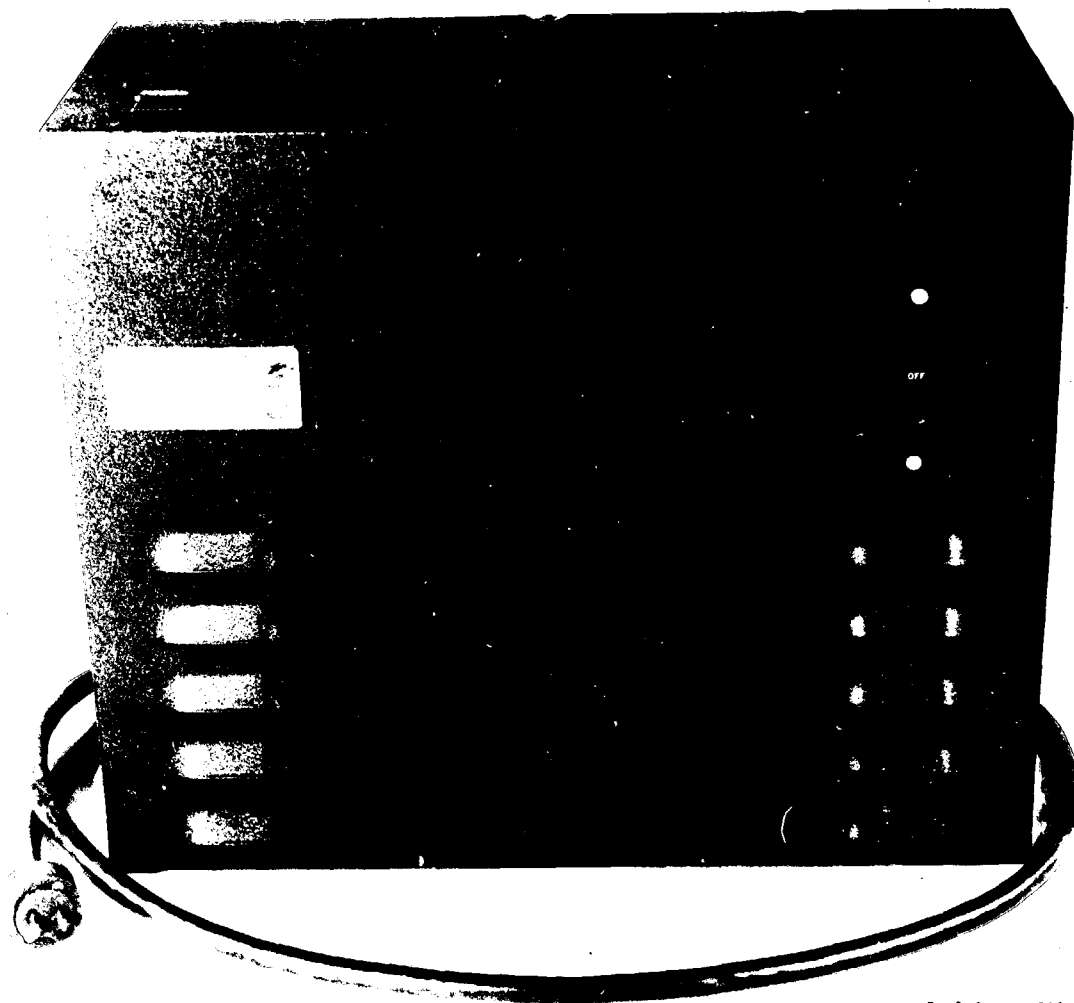
Rectifier RA-23

~~TOP SECRET~~

Continued from Tab L.

Rectifier RA-23. - (Reference photograph opposite and Tab N.) For installations where commercial a.c. is the only power available, Rectifier RA-23 is used as a source of d.c. for operating the converter. This rectifier has a rating of 500 watts at 115 volts d.c. and operates on 60-cycle a.c. The input transformer is provided with taps for operation on 110, 115 or 120 volts a-c supply. The rectifying element consists of a type EL6C vacuum tube, manufactured by Electronics, Inc., 127 Sussex Avenue, Newark, N.J. To put the rectifier in service remove the screws on the right-hand edge of the cover and open the hinged section. Measure the voltage of the a-c supply, then determine that the input transformer is connected at the proper tap. Insert the vacuum tube in the socket and replace the cover. Make certain that the rectifier switch is in the "OFF" position before plugging the cord into an a-c outlet. Operate the switch to position "1" and allow it to remain in that position for at least thirty seconds before advancing it to position "2." This will allow the filament of the vacuum tube to heat before voltage is applied to the plate. Some of the rectifiers are equipped with a two-position switch and a time-delay relay. After the switch has been advanced to position "2" the converter power cord may be plugged into the rectifier outlet receptacle and the converter operated in the manner described in Section II, "Operating Instructions for Converters M-134 and M-134-A" (short title: SIGKOC). The rectifier should normally require no further attention no adjustment. In the event that the rectifier output fails, examine the 10-ampere fuses which are provided in each side of both the input and output circuit for protection against overloads or short-circuits. If a fuse has not blown, check the vacuum tube to make certain that it is making good contact in its socket. If the tube appears to be defective it should be replaced with one which is known to be operative. The rectifier switch should always be thrown to the "OFF" position when power output is no longer desired. A wiring diagram of the rectifier is attached to the inside of the cover.

Continued in Tab N.



~~SECRET~~

Fig. 7-A

31 305

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

RECTIFIER RA-23

~~TOP SECRET~~

TAB N

Rectifier RA-23

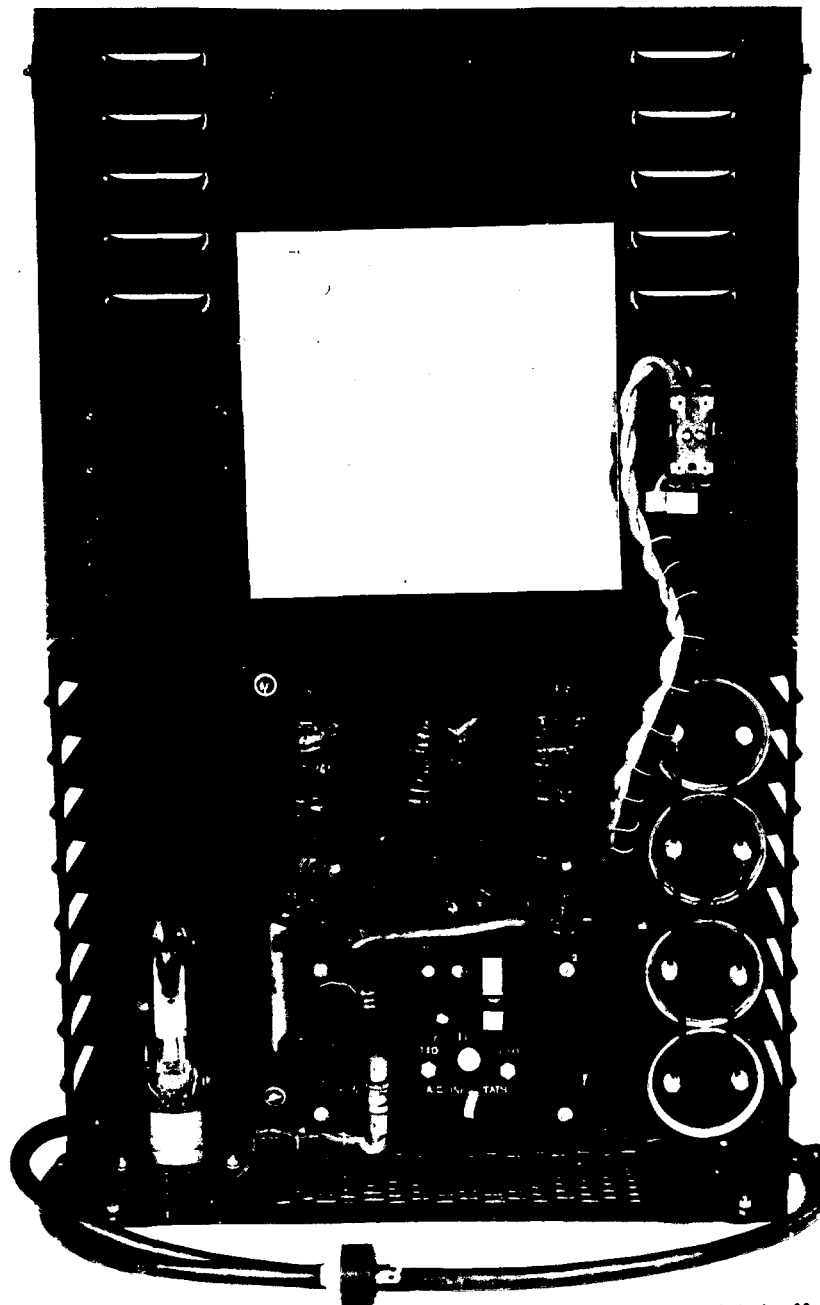
Cover Opened

~~TOP SECRET~~

Continued from Tab M.

For description of Rectifier RA-23 (pictured opposite
with cover opened) see Tab M.

Continued in Tab O.



~~SECRET~~

01 305

Fig. 8-A

SIGNAL CORPS LABORATORIES, FORT MONMOUTH, N. J.

RECTIFIER RA-23,
COVER OPENED

~~TOP SECRET~~

TAB O

Converter M-134-A

Schematic Diagram

~~TOP SECRET~~

730012
13/12/16

Continued from Tab N.

Plug and Jack Strip. (Reference Tab J for description.)

Slow Release Relay. (Reference photograph opposite and Tab R.)
The function of this relay is to hold the rotor stepping solenoids energized for a sufficient length of time to insure complete plunger travel and subsequently to clear the circuit to the normal or open state. This relay has a resistance of 1300 ohms and is equipped with a copper slug for slow-release action. The contacts are an application of the Burgess inclosed-type micro-switch. This switch has proved very dependable in service and should require no attention.

Slow Operate Relay. (Reference photograph opposite and Tab R.)
This relay is found only on Cryptograph MC-164-A. Its chief function is to insure that the magnet of the tape transmitter is energized for a sufficient length of time to advance the key tape to the next position. If the operating time of this relay is too short, faulty operation of the cryptograph will result; if too long, the speed at which the cryptograph may be operated will be reduced. The relay is equipped with a micro-adjustment to permit close regulation of the time delay.

Continued in Tab P.

730012
13/12/16

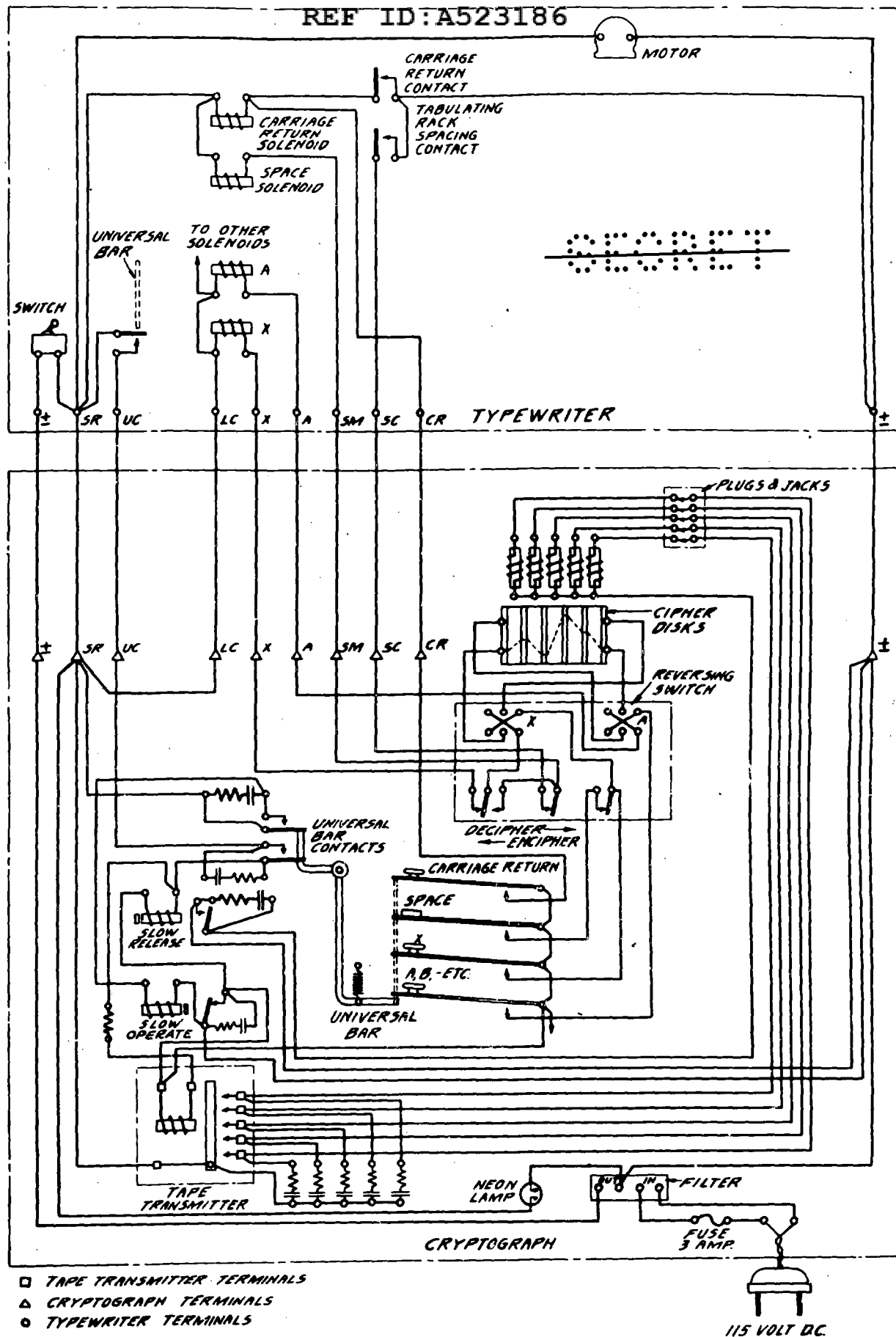


Fig. 9-A

Converter M-134-A, Schematic Diagram

~~TOP SECRET~~

TAB P

Converter M-134-A

Encipher-Decipher Reversing Switch

~~TOP SECRET~~

Continued from Tab O.

Encipher-Decipher Reversing Switch. (Reference photograph opposite.)

a. This switch is mounted beneath the keyboard of the cryptograph and is operated by a lever at the front. This switch acts primarily as a combination of 26 double-pole, double-throw switches in the 26 circuits from the key contact jaws through the rotor and stator assembly to the typewriter solenoids. Its function is two-fold: (1) to disconnect the automatic spacing feature of the typewriter; (2) to reverse the connections from the left and right stators with respect to the keyboard contacts of the cryptograph and solenoids of the typewriter so as to produce the enciphering-deciphering reciprocal relationship for which the converter is designed. The first feature has already been discussed in Tab .

b. As an example of the second feature, and as shown in the photograph opposite, with the switch in the ENCIPHER position, operation of the "A" key results in the printing of a "G." With the rotors in the same position and the switch in the DECIPHER position, striking the "G" key results in the printing of an "A." In addition, the reversing switch contains extra contacts which function in encipherment to print the cipher text in regular groups of five characters, and in decipherment to print the plain text in the original word lengths. These extra contacts function as two single-pole, single-throw switches and one single-pole, double-throw switch. One single-pole, single-throw switch connects the space-bar contact of the cryptograph in parallel with the "X" key contact when the switch is in ENCIPHER position and breaks this connection when in DECIPHER position. The other single-pole, single-throw switch connects the typewriter space-bar solenoids to the tabulating-rack spacing contact when in ENCIPHER position and opens this circuit when in DECIPHER position. The single-pole, double-throw switch connects the "X" stud of the reversing switch to the typewriter "X" solenoid when in ENCIPHER position and to the typewriter space-bar solenoids when in DECIPHER position. Thus, in enciphering a message, the space bar of the cryptograph is operated whenever a space occurs in the plain text, as in conventional typewriter operation, producing the same resultant in the cryptogram as would have been produced if the "X" key had been operated. In deciphering the message a space will occur wherever a space or an "X" occurred in the original plain text.¹ The letters in the deciphered message will therefore be automatically grouped in the original word lengths. However, since in some cases what would appear to be a word space should really be the letter "X," in order to avoid possibility of confusion or ambiguity, the double letter "QQ" is used to replace the letter "X" whenever "X" appears in the plain text of a message to be enciphered. Similarly, on decipherment, whenever the combination "QQ" appears in the deciphered text it is understood that the plain-text letter "X" is intended, and in retyping the message the "QQ" will be replaced by "X." Thus, SIQQEEN will be the word SIXTEEN.

Continued in Tab Q.

1. When the switch is in DECIPHER position the space bar on the cryptograph is dead. Depressing the space bar will consequently have no effect at all.

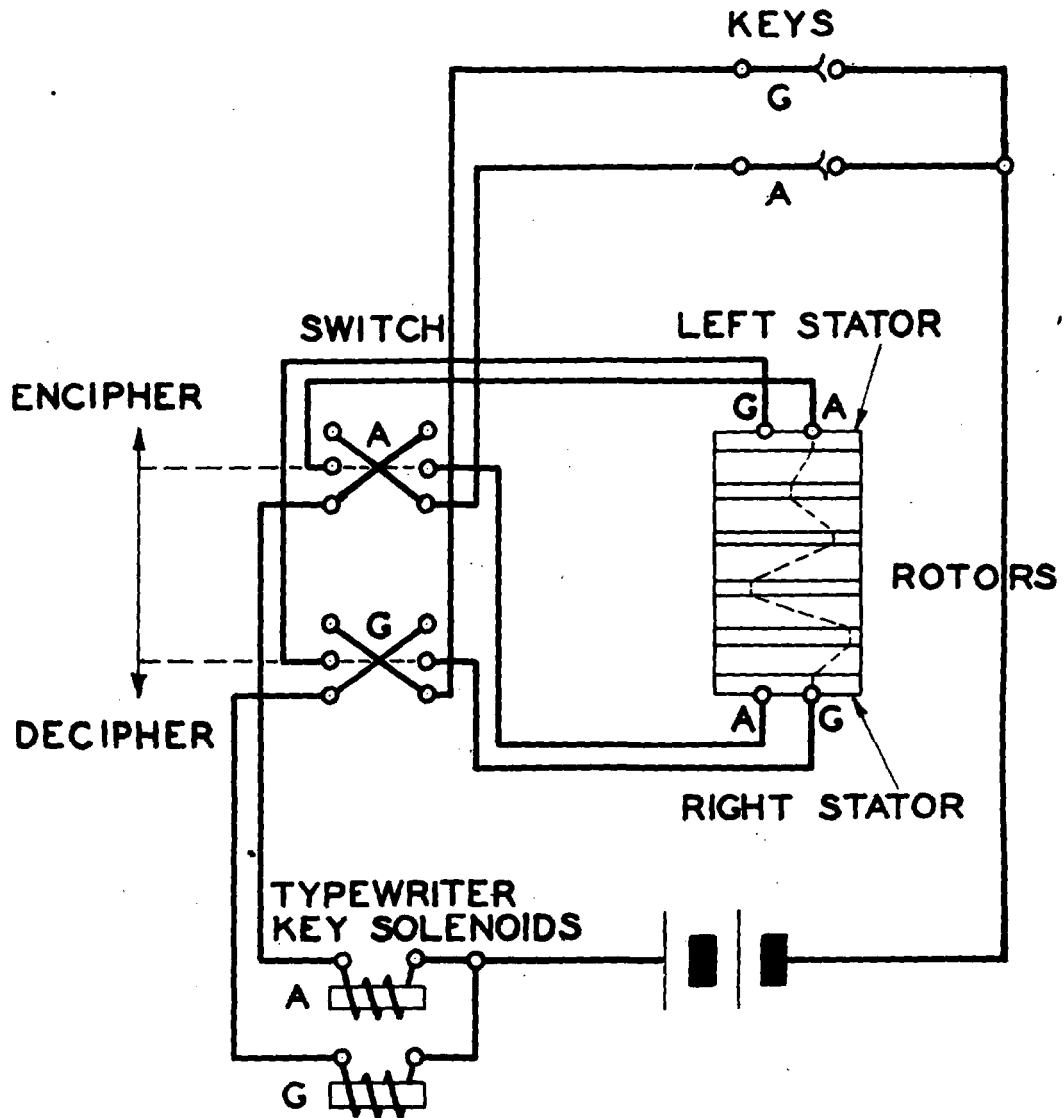
~~SECRET~~

Fig. 10-A

Converter M-134-A, Reversing Switch,
Schematic Diagram

~~SECRET~~

~~TOP SECRET~~

TAB Q

Converter M-134-A

Tape Transmitter MC-185

~~TOP SECRET~~

Continued from Tab P.

c. When the switch is set exactly midway between the encipher and decipher positions the entire cryptograph keyboard is "dead" but the typewriter keyboard is "live." This may be useful at times when it is desired to operate the keyboard of the typewriter without danger of actuating the the cryptograph keyboard inadvertently.

Tape Transmitter MG-185. (Reference photograph opposita)

a. This unit is a modification of the Teletype Model X4 tape transmitter, manufactured by the Teletype Corporation, Chicago, Illinois, and used commercially in printing telegraphy. This transmitter operates on the basis of the Baudot or five-unit code perforated in a paper tape and is constructed to establish five contact combinations in marking or spacing positions dependent upon the arrangement of code perforations in groups transversely disposed on the tape. There are 32 different permutations in the five-unit code, as shown in Tab T (which is provided merely to facilitate the preparation of special testing tapes when necessary). The tape is provided also with a continuous series of perforations in line longitudinally, their spacing being identical with the spacing between code permutations, to permit progressing the tape consecutively from one code permutation to the next. The tape transmitter is equipped with a tape groove and guide; a hinged retaining plate or latched die, often referred to merely as the "latch," to permit inserting the tape at any desired permutation; a feed wheel which engages the feed holes of the tape; five tape pins conjunctive with the code perforations in the tape and operative upon five contact levers in marking-spacing positions, and a magnet acting to depress all five tape pins from engagement with the tape and to step the tape forward to the next code permutation by ratchet movement of the feed wheel, after which the tape pins are released to assume their tape-controlled positions. When a tape pin is held down by the tape; that is, when there is no hole through which the tape pin can rise, the associated contact lever is held against the spacing bus. When a tape pin is permitted to rise through a hole in the tape, the contact lever is moved over to the marking bus.

b. The function of the tape transmitter in the cryptograph is to step forward the rotors in accordance with the code permutations in the key tape. Each code permutation in the key tape establishes, through the tape pins and contact levers of the tape transmitter, circuits which energize the solenoids of the selected rotors, causing the latter to be advanced one step and leaving the nonselected rotors in position. Each transmitter contact is connected in series with one of the stepping solenoids through a plug and jack and the contacts of the slow-release relay. The selected rotor solenoids are therefore energized only during the interval between the deenergization of the transmitter magnet and the opening of the slow-release relay contacts; i.e., between the release of a key of the cryptograph and the release of the slow-release relay. Hence, it is important that the time-delay setting of the slow-release relay be sufficient for the purpose.

Continued in Tab R.

~~TOP SECRET~~

TAB R

Converter M-134-A

Cryptograph MG-164-A

Wiring Diagram

~~TOP SECRET~~

Tape Transmitter MC-185 continued from Tab Q.

c. Key tapes for use with the cryptograph are issued by higher headquarters in a coordinated system of distribution described in special instructions. The key tapes must be handled carefully so as to prevent their damage, loss, or compromise. Tapes will be replaced by the issuing authority from time to time as conditions of usage warrant. Detailed directions for their use in encipherment or decipherment are issued in the special instructions referred to above.

d. The key tape is to be inserted in the tape transmitter with the feed wheel of the transmitter engaging the feed holes of the tape, and with the numbered side of the tape up. Make certain that the initial setting of the tape at the bench mark on the tape guide is correct.

e. On the left side of the tape transmitter; i.e., the side adjacent to the box containing the fuse, and set flush in the side of the transmitter, will be found a button. This can be pushed inside the transmitter to cause the tape to step forward by mechanical action on the stepping mechanism. This button will be found useful in setting the tape to a specific position.

General Description of Cryptographic Circuit.

a. Encipherment. - When, for example, the "A" key of the cryptograph is depressed, a circuit is established from power through the "A" key contacts, thence through the "A" reversing switch to the "A" stud on the left stator, thence through the rotors and intermediate stators and out at a certain stud on the right stator. Assume this to be the "G" stud in the present instance. The circuit is then continued to the "G" reversing switch and through that switch to the "G" solenoid of the typewriter and returned to power, with the result that "G" is printed by the typewriter.

b. Decipherment. - When the "G" key of the cryptograph is depressed, a circuit is established from power through the "G" key contacts, through the rotors (which are, of course, in the same alignment as they were when the letter "A" was enciphered) and intermediate stators and out at the "A" stud on the left stator. The circuit is then continued to the "A" reversing switch and through that switch to the "A" solenoid of the typewriter and returned to power, with the result that "A" is printed by the typewriter.

Detailed Description of the Complete Circuit.

a. Encipherment. When, for example, the "A" key of the cryptograph is depressed, a circuit is established from power through the "A" key contacts, thence through the "A" reversing switch to the "A" stud on the left stator. In the Cryptograph MC-164-A this circuit includes the contacts of the slow-operate relay. Assume that the path through the rotor assembly finally ends on the right stator at the "X" stud, connecting to the "X" reversing switch. The circuit is then continued through the special switch pertaining to the "X" key (which switch is described in detail later and is not a feature pertinent to the other keys) to the

Continued in Tab S.

~~TOP SECRET~~Detailed Description of the Complete Circuit continued from Tab B.

"X" solenoid of the electrical typewriter and thence returned to power through the upper contact of the cryptograph universal-bar contact combination. This combination is operated upon the depression of any key of the cryptograph. In the case of the Cryptograph MC-164-A this circuit does not include the universal contact combination. When the typewriter prints "X" the typewriter universal bar operates to close its contacts, completing a circuit through the lower contact of the cryptograph universal-bar combination to energize simultaneously the slow-release relay and the tape transmitter magnet. In the Cryptograph MC-164-A this circuit includes the contacts of the slow-operate relay. The tape transmitter now withdraws its five pins below the surface of the tape guide and advances the tape to the next permutation. Upon release of the "A" key of the Cryptograph MC-164 (or when in Cryptograph MC-164-A, the slow-operate relay contacts open) the typewriter "X" solenoid is de-energized, its universal-bar contact opens, the universal-bar contact combination of the cryptograph opens, and the tape transmitter magnet is de-energized. The slow-release relay, however, is designed to hold its contact closed for a brief interval after its coil is de-energized. When the tape transmitter magnet releases, it operates the transmitter contact tongues to marking or spacing position, according to the code permutations in the key tape. Circuits are established from power at SR through those contacts which have been operated to the marking position to energize the associated rotor-stepping solenoids. Each energized solenoid pulls down its plunger to tension a spring, and engages its stepping pawl in a tooth of the rotor ratchet. When the slow-release relay contact opens, the solenoids are de-energized and the associated rotors are advanced to the next position by spring action.

The cryptograph is now ready for the next operation of the keyboard.

b. Decipherment. - In the preceding paragraph it was assumed that striking the "A" key of the cryptograph resulted in the printing of an "X" by the typewriter. Assume now that the key tape setting and all rotor settings are unchanged, that the reversing switch has been moved to DECIPHER position and that the "X" key of the cryptograph is depressed. A circuit is then established from power through the "X" key contacts, thence through the "X" reversing switch to the "X" stud on the right stator and through the rotors and intermediate stators to the "A" stud on the left stator. In the Cryptograph MC-164-A, this circuit includes the contacts of the slow-operate relay. The circuit is then continued through the "A" reversing switch to the "A" solenoid of the typewriter, and back to power at SR through the upper contact of the cryptograph universal-bar contact combination. In the case of Cryptograph MC-164-A, this circuit does not include the universal contact combination. The typewriter prints "A" and its universal-bar contact closes to complete a circuit through the lower contact of the cryptograph universal-bar contact combination to energize the slow-release relay and the tape transmitter magnet simultaneously. In Cryptograph MC-164-A,

Continued on following page.

~~TOP SECRET~~

RECEIVED
JAN 12 1944

Detailed Description of the Complete Circuit continued from Tab R.

this circuit includes the contacts of the slow-operate relay. The tape transmitter then withdraws its five pins and advances the key tape. Upon release of the "X" key of the cryptograph (or in Cryptograph MC-164-A when the slow-operate relay contacts open), the "A" solenoid of the typewriter is de-energized, the typewriter universal-bar contact opens and the cryptograph universal-bar contact combination opens. The tape transmitter magnet then releases and completes circuits to the same rotor-stepping solenoids which were energized in the process of encipherment. When the contacts of the slow-release relay open, the selected rotors are advanced one step. The manner in which the circuits are completed and the sequence of operation are the same as in encipherment.

RECEIVED
JAN 12 1944

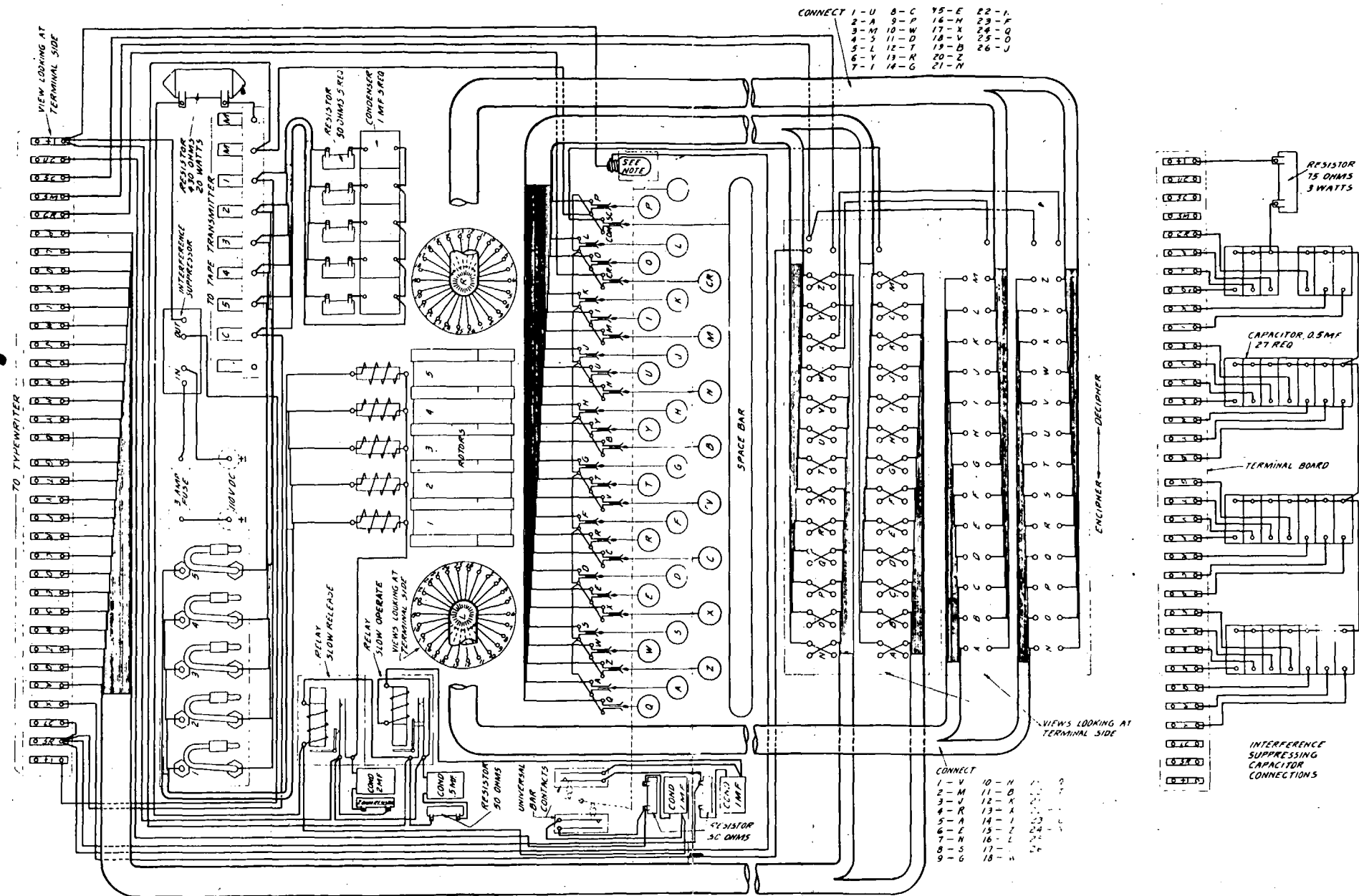


Fig. 12-A

Converter M-134-A
Cryptograph MC-164-A,
Wiring Diagram

SECRET

See description of Typewriter MC-174-A, Tab G.

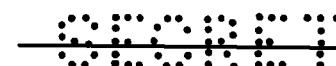
~~TOP SECRET~~

TAB S

Converter M-134-A, Typewriter MC-174-A

Wiring Diagram

~~TOP SECRET~~



Converter M-134-A, Typewriter MC-174-A,
Wiring Diagram

~~TOP SECRET~~

TAB T

M-229 (SIGG00)

shown in place on

Cryptograph MC-164-A of Converter M-134-A

~~TOP SECRET~~



~~TOP SECRET~~

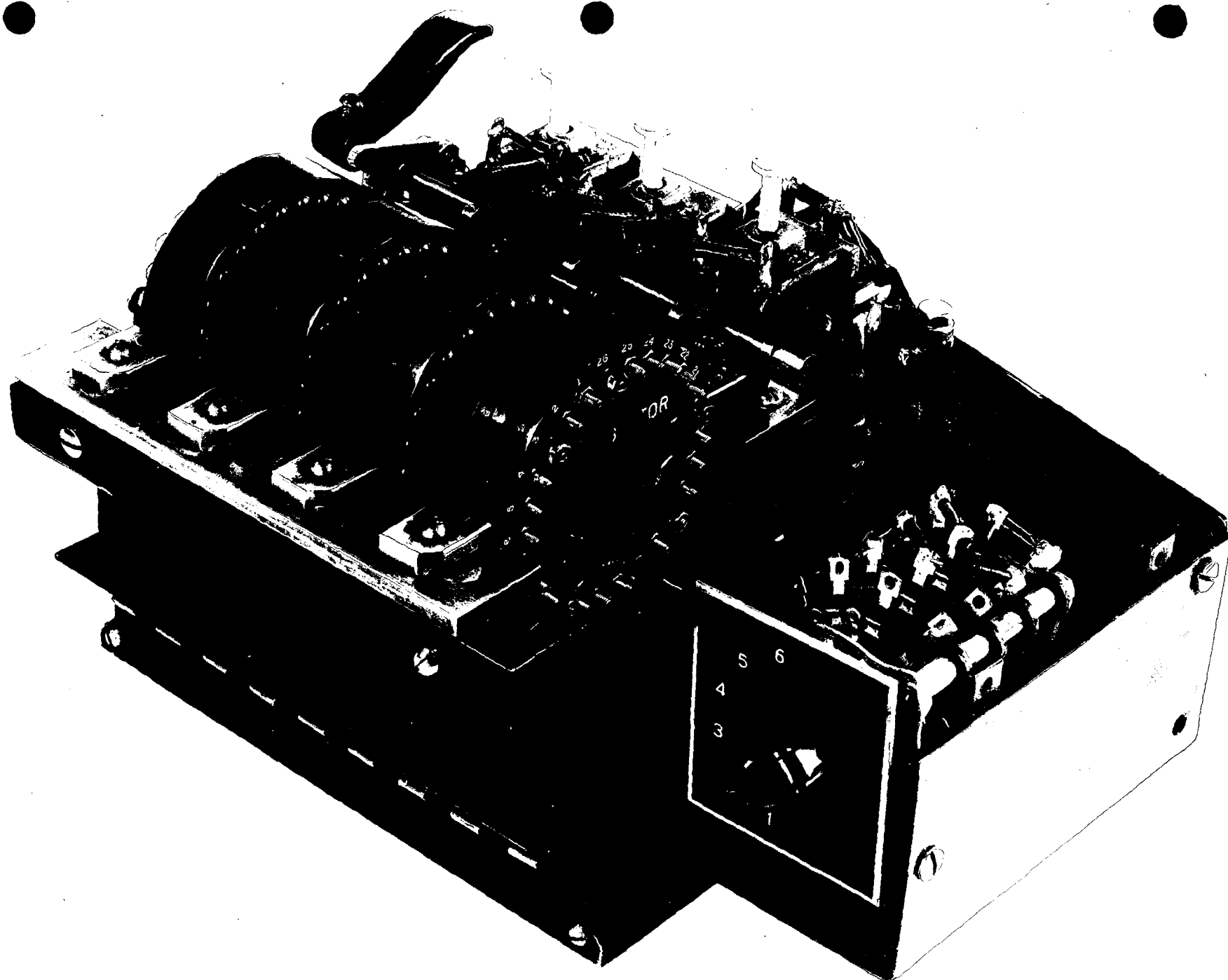
TAB U

Keying Unit M-229

(Short title: SIGG00)

(Plan View)

~~TOP SECRET~~

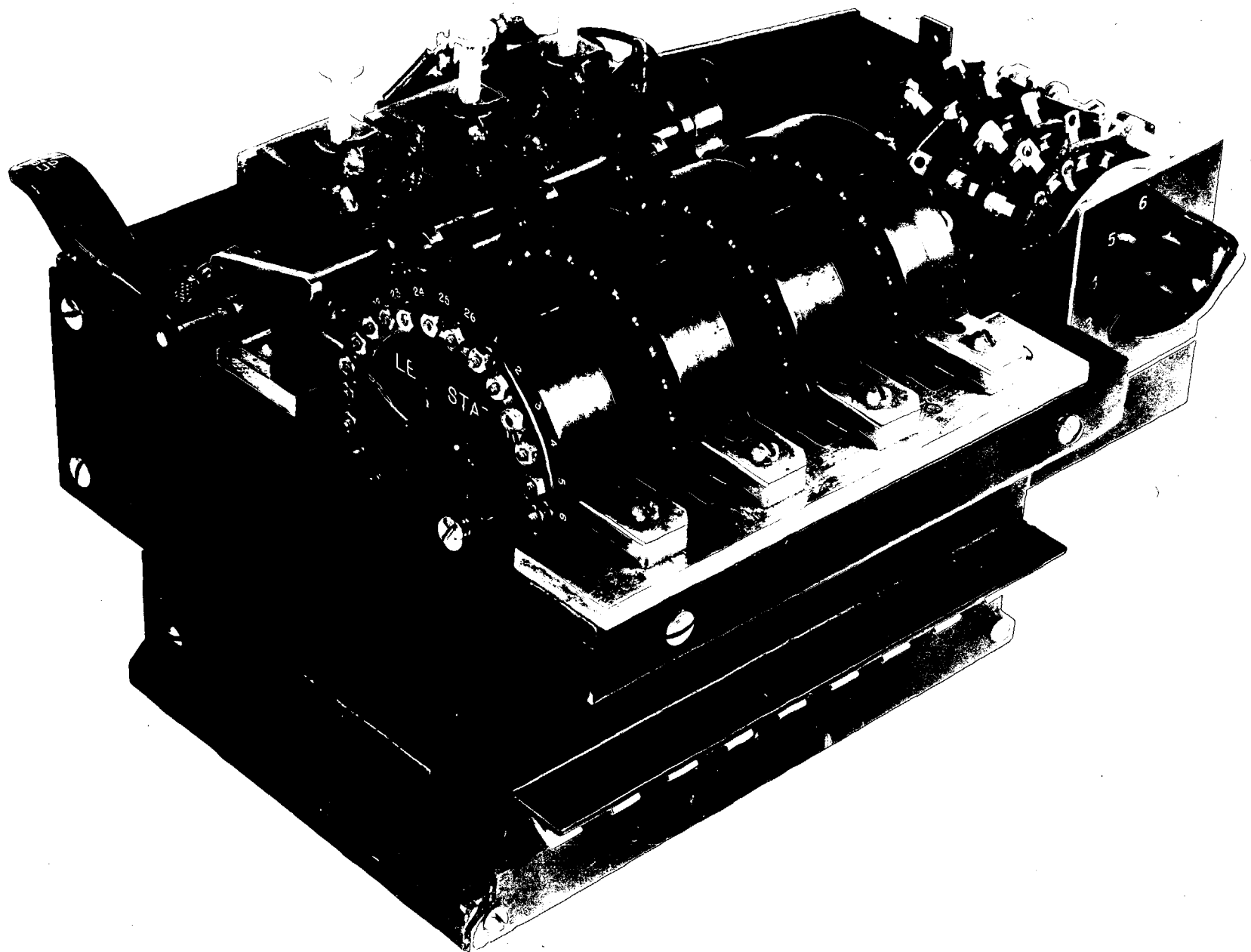


~~TOP SECRET~~

TAB V

Keying Unit M-229
(Left Stator View)

~~TOP SECRET~~



~~TOP SECRET~~

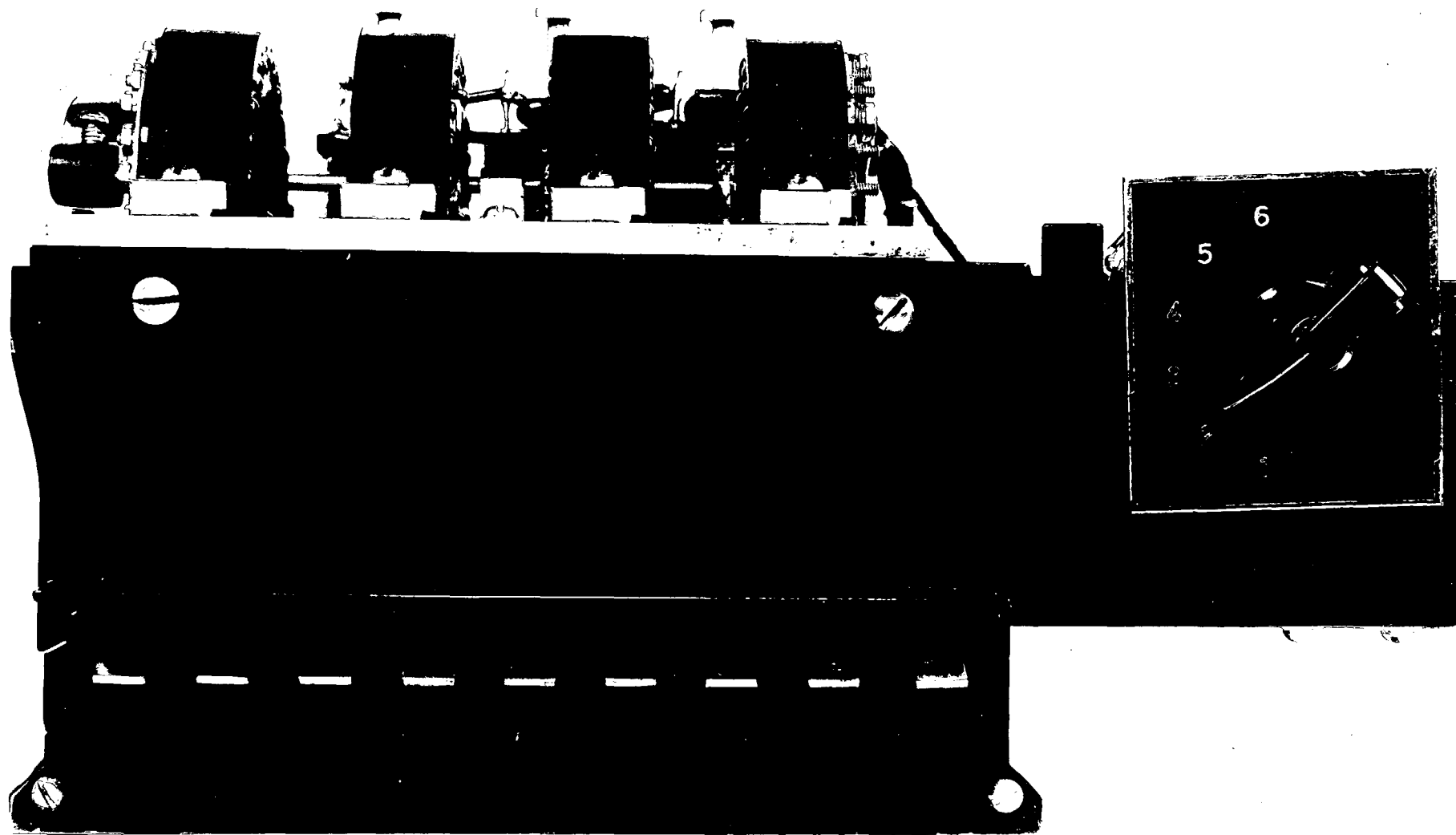
TAB W

Keying Unit M-229

(Short title: SIGG00)

(Rear View)

~~TOP SECRET~~



~~TOP SECRET~~

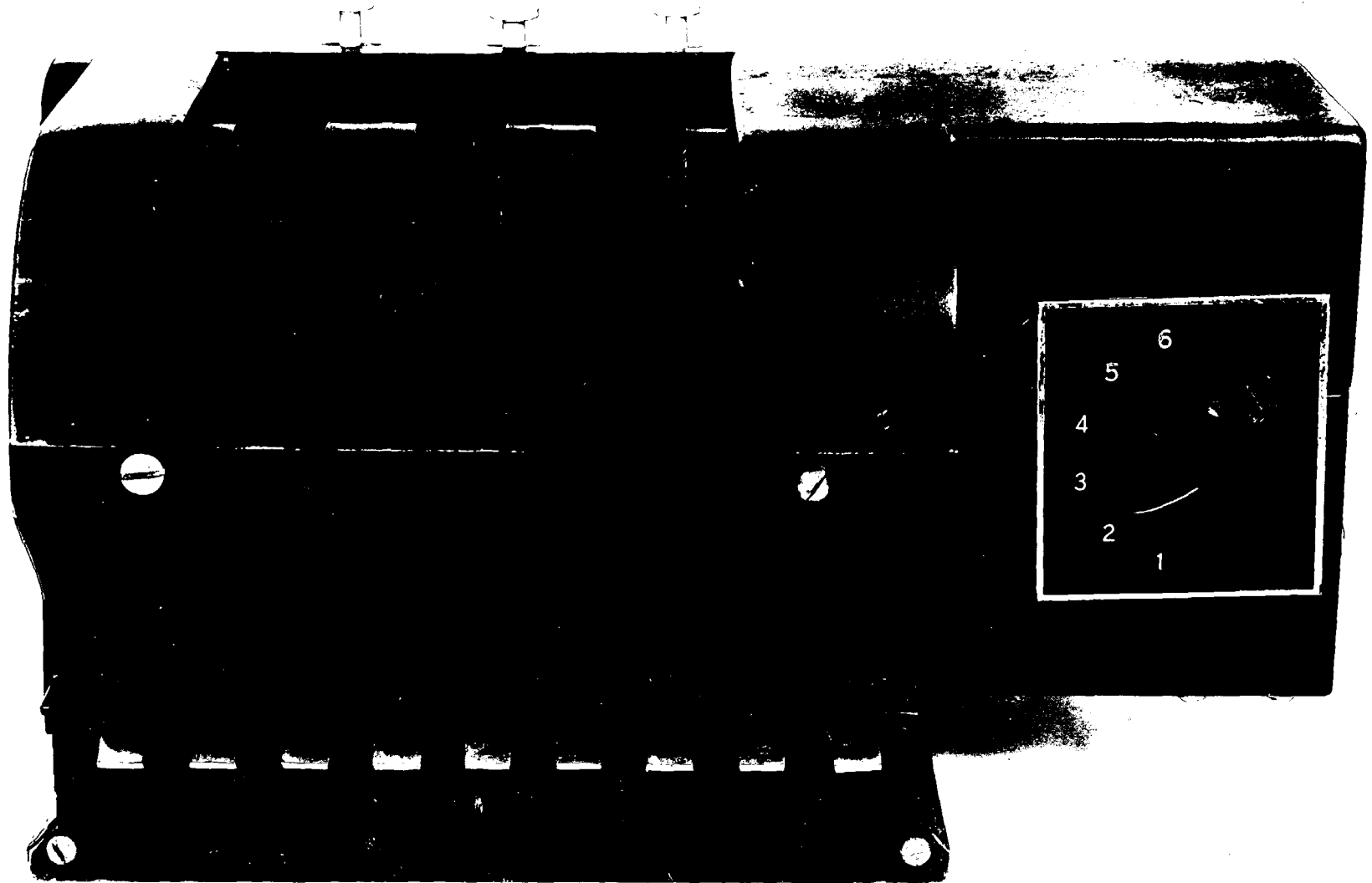
TAB X

Keying Unit M-229

(Short title: SIGG00)

(Cover in Place)

~~TOP SECRET~~



~~TOP SECRET~~

TAB Y

Keying Unit M-229-T2

~~TOP SECRET~~



SECRET

SIGNAL CORPS

U.S. ARMY

KEYING UNIT M-229-T2

SERIAL NO. 18

ORDER NO. 8658-SGL-42

MADE BY

WALLACE & TIERNAN PRODUCTS INC.

BELLEVILLE

NEW JERSEY

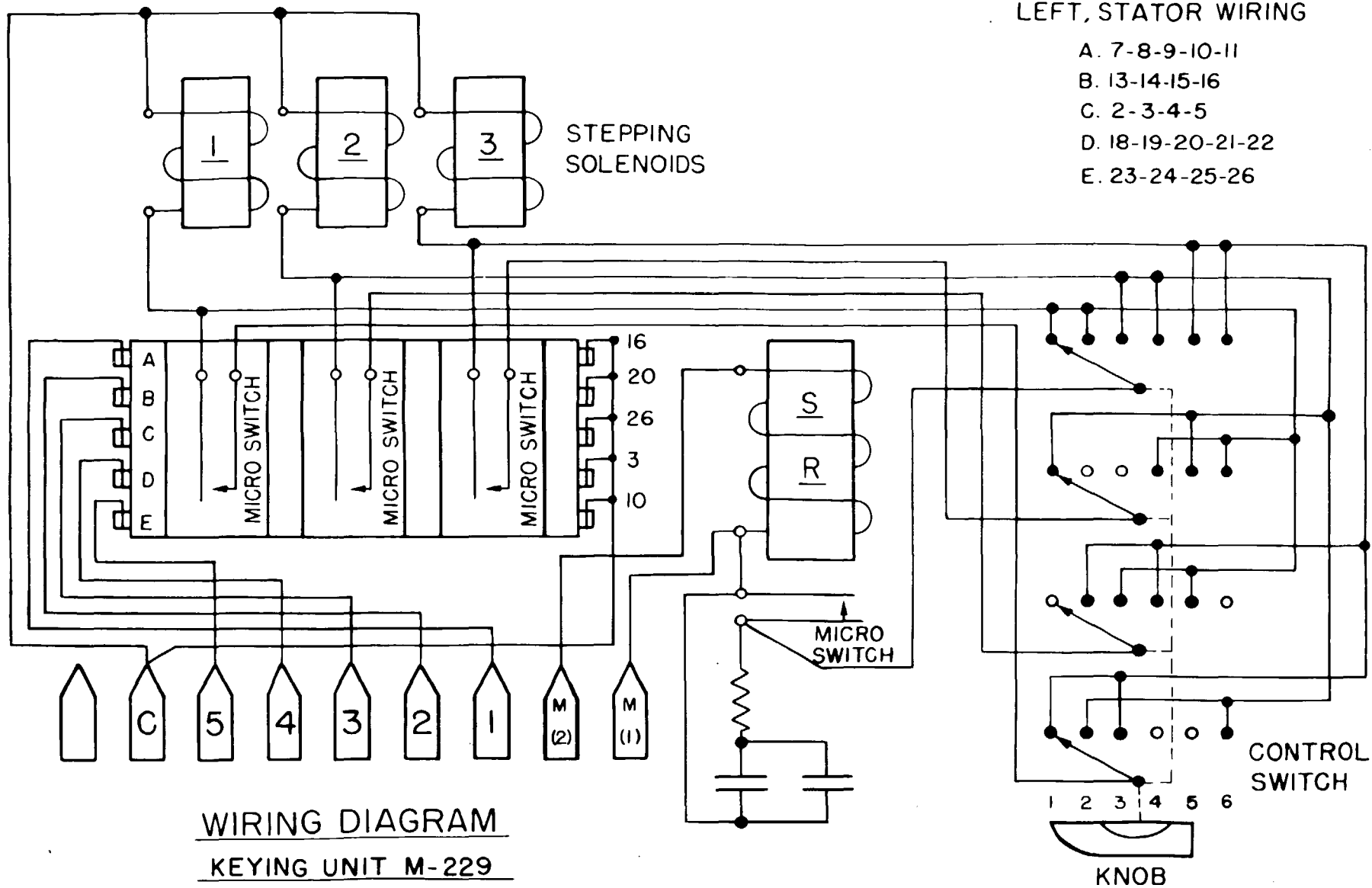
~~TOP SECRET~~

TAB 2

Wiring Diagram

Keying Unit M-229

~~TOP SECRET~~

~~SECRET~~~~SECRET~~

~~TOP SECRET~~

TAB AA

Signal Corps Technical Committee

Meeting No. 146

Supplemental Minutes

~~TOP SECRET~~

SIGNAL CORPS TECHNICAL COMMITTEE

MEETING NO. 146

SUPPLEMENTAL MINUTES

1. In addition to the matters acted on and reported in Minutes of Signal Corps Technical Committee Meeting No. 146, January 11, 1937, the Committee took the following actions with respect to Converter type M-134:

a. Military Characteristics:

(1) The Committee recommended that the following military characteristics be adopted for Converter type M-134:

- (a) This machine should be designed for the fundamental purpose of enciphering and deciphering messages with speed, accuracy, and the highest degree of cryptographic security. Secondary to these characteristics, there should be a minimum number of switches, keying elements, etc., which must be set before proper operation can begin.
- (b) The cryptographic operations should be controlled by an external element which is variable and is not an intrinsic part of the mechanism itself, such as a perforated tape similar to that employed in printing telegraph apparatus. The underlying cryptographic principle should be that of a continuous, non-repeating, unintelligible or random-mixed key sequence of characters governing the encipherment of successive letters.
- (c) The machine should consist of two units, (1) a cryptographic unit hereinafter called the "cryptograph", provided with a standard typewriter keyboard, and (2) a recording unit suitable for making a printed record of the work done by the machine, preferably an electrically operated typewriter, hereinafter called the "typewriter". The cryptograph is the part of the mechanism in which the enciphering and deciphering operations occur; the typewriter is electrically associated with the cryptograph and is to print the cipher text, in case of encipherment, in 5-letter groups, 10 groups per line; in the case of decipherment, the typewriter is to print the plain text, preferably in their original word lengths with proper spacing between words.
- (d) The minimum speed of operation should be 30 words per minute.
- (e) The cryptograph and the typewriter should be mounted upon the same base with fixed electrical connection between the two units. A side-by-side arrangement of these two units is preferable to a tandem arrangement, so that the keyboard of the

cryptograph as well as the keyboard of the typewriter are both immediately in front of the operator.

- (f) The apparatus should be designed to operate on 110-volt, D.C., power source.
- (g) The weight of the cryptograph including its carrying case should not exceed 50 pounds; that of the typewriter including its carrying case 60 pounds. Both units should be rugged in construction and capable of withstanding jarring incident to transportation.
- (h) The entire assembly should be so constructed that in case the typewriter is out of commission for any reason, cryptographic operations may be continued by means of electric light-bulb indicators on a lamp board on the cryptograph.
- (i) There must be incorporated features to suppress interference with radio receivers operated in the vicinity of the machine.

b. Standardization of Equipment:

(1) Acting upon the recommendation of the Chief Signal Officer, the Committee recommended the adoption as to type and classification as Standard of Converter type M-134.

P
PRESENT:

C. L. Marriott
C. L. Marriott,
Major, Chemical Warfare Service.

C. R. Huebner
C. R. Huebner,
Major, Infantry.

R. W. Grow
R. W. Grow,
Major, Cavalry.

H. B. Holmes, Jr.,
Major, Coast Artillery.

A. W. Marriner
A. W. Marriner,
Major, Air Corps.

Haskell Allison
Haskell Allison,
Major, Signal Corps.
for

W. S. Rumbough,
Major, Signal Corps.

Nathaniel White
Mr. Nathaniel White,
for
D. M. Crawford,
Lieut. Colonel, Signal Corps.

H. P. Browning
H. P. Browning,
Major, Signal Corps.
Acting Chairman and Recorder.

CONCURRING:

Louis E. Hibbs
Louis E. Hibbs,
Major, Field Artillery.

Earle Standlee
Earle Standlee,
Captain, Medical Corps.

G. P. Bush
G. P. Bush,
Major, Signal Corps.

A. D. Hopping
A. D. Hopping,
Capt., Quartermaster Corps.

APPROVED JANUARY 19, 1937:

J. B. Allison
J. B. Allison,
Major General,
Chief Signal Officer of the Army.