

A Project History

1946

HISTORY OF CONVERTER M-325
(Short Title: SIGFOY)

NSA/CSS #SRH-010

SUMMARY

cryptographic machine FOR FIELD USE

An idea for a small, portable, field device, incorporating the basic features of the German commercial Enigma machine, was conceived and roughly sketched by William F. Friedman, Principal Cryptanalyst, U.S. Army, on 1 August 1935.¹ Seven years later, on 2 June 1942, Signal Intelligence Service requested assignment of nomenclature and type number to a device for low-echelon use similar to that visualized by Mr. Friedman in 1935. This device, according to its military characteristics, was to be designed for "enciphering messages in the combat or field code and for identifying stations engaging in radio communication." Storage and Issue Division, OCSigO, on 5 June 1942, assigned the nomenclature "Converter M-325" to the device.

Two development models of the Converter M-325 were produced by the development contractor, Teletype Corporation, Chicago, Illinois, and delivered to this agency on 5 May 1943. Quantity production of the device was turned over to Smith-Corona Typewriter Company, Incorporated.

1. Although the Enigma was not used in U. S. military or diplomatic communications, a study had been made to determine its degree of security. It was the conclusion of this study that the novel manner in which known cryptographic principles were used in the Enigma insured a relatively high degree of security.

Although the first model was the ^{CNE} model intended to be distributed and used,
only a few ~~models of this machine~~ were built and none ^{was} were put into actual
operation. On the basis of security studies made on this model, several
technical changes were made ⁽⁵⁾ in the device. The first improved ^{parts} models of
the M-325 were completed and delivered by Teletype Corporation to this
Agency in April 1944. The ^{MACHINE} ~~device~~ was standardized on 22 December 1944
by the Signal Corps Technical Committee as a Required Type, Adopted Type,
Standard Article.

[add statement of service test, distribution
to State Dept. revisions, T C S committee
action, obsolete, salvage]
[mention of Sig Case]

(5)

INTRODUCTION

On 21 April 1936, Mr. Friedman prepared a sketch (See Figure 1) of the small portable cryptographic device originally conceived by him in August 1935 and recorded a description of his invention as follows:

Invention of a Stylus-operated Keyboard for a Small Portable Cryptograph

1. The keyboard of this cryptograph consists of a plate having 26 small windows underneath which are small lamps. The windows are arranged in three rows and on them are painted the letters of the alphabet, distributed as on a standard typewriter keyboard. Alongside each window is an aperture through which a non-conducting stylus may be inserted to operate a contact lever below.
2. The circuits are reciprocal and one pair of such circuits is shown in operative association in the accompanying Figure (Figure 3 in this history), viz., the circuits for the $A = Q$, $Q = A$ relationship. This is accomplished by means of the usual "return" commutator (as per Enigma System).
3. The drawing shows a set of three cipher commutators, two of which are of the ordinary "through" type, one of the "return" type, but additional commutators of the "through" type may be employed. "Through" commutators are all interchangeable.
4. Means are provided for advancing the commutators for cryptographic variation, either a meterlike, or aperiodic movement being available according to schemes not forming a part of this invention. Probably a hand-operated power source for angularly displacing the commutators would be practicable in such a device, the particular selection being determined by cams, tapes, or the like.

(Signed) William F. Friedman

6

CRYPTOGRAPH

The inventor initiated action to obtain a patent for the device on 22 April 1936 by submission of his idea to the Signal Corps Patents Board. This Board on 26 May 1936 found the invention of value to the Government and recommended that the inventor submit specifications to the Patent Section, Office of the Chief Signal Officer, in order to obtain letters patent. It was also recommended that the invention not be considered important in the National Defense and that a non-exclusive license to the Government, in writing, be required. The inventor was informed on 16 June 1936 by the Chief Signal Officer that there was no objection to the sale of right under the patent application for "Stylus-operated Keyboard for a Small Portable Cryptograph" or to disclosure of the principles set forth in that patent application. (T)

Action was initiated by the inventor, personally, on 1 November 1937 to patent the keyboard because the Patent Section, OCSigO, had delayed filing application until certain high priority radio equipment had been patented.³ On 22 June 1942 the item was withdrawn for further coordination between General Development Division, OCSigO, and Signal Intelligence Service.

-
3. Patent application was never actually filed, although the Signal Corps Patent Section, OCSigO, instigated new action, 6 December 1941. Another application was also filed by Development Branch, SIS on 11 August 1944.

(7)

From October 1944 through February 1945 several operational tests
 OF CONVERTER
 were made on the second model M-325 in order to determine the efficiency
 of the converter as a cipher ^{MACHINE} device. Outstanding among these tests was
 the initial operation of the M-325 in the Caribbean Defense Command where
 CONVERTER
 the ^{IT} device was used for three months as the normal cryptographic system
 to replace a system based on the strip cipher device. It was contem-
 plated that the M-325 would be used as replacement for all ^{ALPHABET} strip systems
 if its initial operation proved successful. However, the M-325 was not
 well received by operating personnel who objected principally to the slow-
 ness of the ^{OPERATION} device and numerous instances of faulty stepping of the rotors. (T)

Based on reports made following the operations tests of the second
 OF CONVERTER
 model M-325, the machine was modified in an attempt to eliminate the
 flaws uncovered. The machine was put in an operable condition, but more
 than this could not be accomplished without a basic redesign which the
 slowness of the ^{MACHINE} device did not warrant.

By this time, the idea of using the ^{MACHINE} device as an authenticator had
 been abandoned (a new ^{MACHINE} device to be used for this purpose, MX-573()/U,
 was under development), and the proposed use for encipherment of the
combat and field codes no longer existed because the subject codes were
 no longer in use. Also, the end of the war had materially reduced the
 requirements for cryptographic ^{MATERIAL} devices. In view of the above consider-
 ations and of the objections made to the use of the M-325 as a cipher
 machine by troops in the field, the AGF, AAF, ASF, G-4 and MIS approved

? check

(8)

the reclassification of the M-325 to obsolete; this action was carried out by this Agency in December 1945.

The Converter M-325 is a small, portable, manually operated, electro-mechanical cryptographic ^{MACHINE} device self-contained in a compact metal case. Rotors are used in the cryptographic mechanism. Self-contained BA-30 batteries furnish power; in the final modified model an external transformer is provided so that an outside source of power may be used when available.

9

INITIATION OF PROJECT

On 2 June 1942 Signal Intelligence Service requested assignment of nomenclature and type number to a converter, employing a keyboard similar to that conceived by the Principal Cryptanalyst in 1935, to be used for station identification and for encipherment of code. The following day action was initiated for adoption of military characteristics for such a converter and for funds in the amount of \$15,000 to be made available to Signal Intelligence Service to provide for development of the device^{MACHINE} by a commercial concern. Six months was the estimated time required for the development of this equipment. (T)

Storage and Issue Division, OCSigO, on 5 June 1942 assigned the nomenclature "Converter M-325" to the ~~device~~^{MACHINE} which had the following military characteristics: (T)

1. The converter is a machine with dual capacity primarily designed for enciphering messages in the combat or field code and for identifying stations engaging in radio communication.
2. ^{Don't place} The cryptographic principle of the converter, when used for enciphering code messages, shall be based on the use of a set of three 26-point rotors and a plugboard for modifying the action of these three rotors. The principle

- of encipherment shall be the same as that of the Converter M-161^{3a} except that no means shall be provided for rotating the rotors during encipherment. Results of encipherment or decipherment shall be the lighting of one of 26 indicating lamps identified by the letters of the alphabet. P
3. The cryptographic principle of the converter when used for station identification purposes shall be similar to that when used for enciphering combat or field code messages except that the rotors shall be caused to move in a regular odometer fashion with each identification step. Thus the converter will be caused to generate a long apparently random sequence of letters by successive operations; these letters shall be illuminated successively on the light bank.
 4. The converter shall be so designed as to be applicable for both types of service. The change from one type to the other shall be accomplished by the operator in the field by plugging in or otherwise connecting required parts. This change shall not require the use of tools.
 5. The speed of operation as an enciphering device shall be at least equal to that of Converter M-209. The speed of operation as a station-identification device shall be such that the identifying letter may be obtained from the converter in approximately one-half second.
 6. The skill required to operate the converter shall not be more than that required for the present Converter M-209.
 7. The converter shall be provided with a carrying case so as to protect it while in transit.
 8. The converter shall be operable under a wide range of light conditions i.e., from bright daylight to blackout lighting.
 9. The weight of the converter including the carrying case, batteries, etc., shall not exceed 20 lbs. The maximum dimensions including the carrying case shall be 9" wide, 9" deep and 5" high.
 10. The converter shall be operable from self-contained dry storage batteries of standard type.

⁴
~~3a.~~ ~~*****~~ The Converter M-161 is a cryptographic device developed by this Agency in 1935 for low-echelon use. However, the machine proved unsuccessful and was abandoned.

- 11. The converter shall be simple but rugged in construction, capable of withstanding heavy usage in the field.
- 12. The converter shall be classified as a confidential item of equipment.

The above military characteristics for the Converter M-325 were approved by the Signal Corps Technical Committee on 20 July 1942.

Teletype Corporation, Chicago, Illinois, manufacturer of the Converter M-134-C (SIGABA), submitted a tentative specification for the Converter M-325 to Signal Security Agency on 17 August 1942. This specification was as follows:

General: The M-325 Converter (Authenticator) is to be a small manually operated electric cipher machine. The machine shall be simple, portable, reliable and light in weight. All parts shall be reasonably accessible, and the dry cells and bulbs capable of being changed without the use of special tools. The unit shall be made as weatherproof as possible. The ^{MACHINE} device is intended for intermittent service only. Provision shall be made to encipher only the 26 letters of the English alphabet. A water-repellant fabric carrying case with shoulder strap shall be provided.

Size: The size of the unit shall preferably be less than the following maximum dimensions - 4-1/2" x 5-1/2" x 8-1/2".

12

Mechanisms: The keyboard shall follow either of two designs -

(a) one is to have 26 push button contactors, and (b) the other is to have 26 contact surfaces, any one of which shall complete a circuit when touched by a stylus connected to the battery circuit by a removable cord.

Associated with each of the 26 push buttons or contact surfaces shall be a miniature bayonet type lamp bulb having a translucent lamp cap bearing a letter of the alphabet. The lamp bulbs shall be operated through a suitable electrical circuit by two No. 2 size flashlight cells connected in series.

The ciphering mechanism shall include a reciprocal maze and shall consist of (a) one fixed end plate having 26 contacts; (b) three removable rotating circuit changing elements with 26 mixed circuits each, known as "Code Wheels", (c) a manual stepping arrangement whereby the code wheels shall be stepped in metering fashion, (d) one removable end plate having 26 contacts with removable connectors arranged to allow convenient change of the reciprocal cross connections, and (e) a three-position counter, with reset, which shall be associated with the code wheel stepping arrangement so as to count each operation of the mechanism. The cover of the unit shall be arranged to provide easy access to the code wheels.

Operation: The various parts and the wiring shall be arranged so that when using a stylus to select the characters, a circuit shall be completed from battery through the stylus, through the selected contact, through the lamp associated with the selected contact and return to

13

battery. At the same time, from the selected contact, a parallel circuit shall be established through the code wheel maze to one other lamp and return to battery. Thus, two lamps will light - the one selected, and one other which will be determined by the position of the maze.

The operation of a unit having push buttons shall be similar to one having a stylus, except that the circuit which is completed by the stylus shall be completed by a push button.

When the Manual code wheel stepping mechanism is operated, a circuit shall be completed from battery to the "E" stylus contact or push-button contact, then through the code wheel maze circuit to a lamp and return to battery. The circuit shall be so arranged that the "E" lamp shall not light.

Approval was given by Signal Security Agency on 7 September 1942 for the above tentative specification except for two minor changes. These changes were: (1) that a sliding cover for the converter be provided and (2) that a sheet steel case be combined with the carrying case for protection.



24
After incorporation of these changes, the above tentative specification appeared in May 1943 as Specification No. 5-6107.

EARLY DEVELOPMENT

Signal Security Agency began investigating the possibilities of automatic stepping of the rotors (referred to as "code wheels" in the tentative specification) of the converter with each depression of the *KEY BOARD* push buttons.

This change was expected to increase the complexity of the ^{MACHINE} device. It was stated by the contractor that the development models of the M-325 were nearing completion and it was planned to demonstrate the converter in Washington 15 October 1942.

On 6 October 1942 the Army Communication and Equipment Coordination

15

Board, OCSigO, recommended that the Converter M-325 be adopted by the United States Army as an authenticator for use between fixed installations and by field forces above Army Corps for radiotelegraph messages. On 18 October, the Signal Security Agency suggested that this recommendation be amended to read "field forces down to and including division," as this would parallel the distribution of high-grade electric cipher machines.

(16)

At this time the Combined Communications Board considered the possible adaptation of the M-325 and the proposal was referred to the CCB committee on Codes and Ciphers. After reviewing the proposal, the Codes and Ciphers Committee concluded that the expense of manufacturing the ~~device~~^{MACHINE}, the amount of raw material involved, and the limited use of the ~~device~~^{MACHINE} in combined operations would not warrant its adaptation.

After representatives of Signal Security Agency had conferred with representatives of the L. C. Smith and Corona Typewriter Company, Syracuse, New York, manufacturer of the Converter M-209, it was decided by SSA on 11 February 1943 that the actual production of the Converter M-325, in quantity, would be turned over in its entirety to this company. Teletype Corporation, was then under contract to SSA to furnish only production models and drawings of the M-325.

Under terms of the agreement made between L. C. Smith and Corona Typewriter Company and SSA, Smith-Corona was free to discuss with Teletype Corporation all points of the M-325 model so that production models supplied by Teletype Corporation might be coordinated to meet the needs of Smith-Corona. In view of the fact that the Converter M-325 involved stamped parts, soldering, and assembling, it was suggested by SSA that the

(18)

rotors might present a major problem. Sheet metal parts, however, were in the Smith Company line of work; stamping and assembling thus presented no problem, nor did actual wiring of the rotors. It was only production of the rotors themselves that was beyond the scope of the Typewriter Company. To remedy this problem, Moulded Insulation Company, Philadelphia, Pennsylvania, was subcontracted by Smith-Corona to manufacture rotors and other plastic parts for the M-325.

Under the assumption that the necessary priorities could be obtained, Signal Security Agency requested of Smith-Corona an estimate on a first quantity of 5,000, and a second of 50,000; such estimate on production schedule was not to run currently with the Converter M-209 but subsequently.

Inasmuch as the Converter M-325 was classified confidential, action was taken to have the L. C. Smith and Corona Typewriter Company cleared for production of the ^{MACHINE.} ~~device.~~ To preserve the security of the converter, it was decided that there should be a minimum of discussion regarding the machine and that the model would be considered secret by the typewriter Company, regardless of Army Classification.

Converter M-325 was assigned the short title "SIGFOY" on 1 March 1943. Rotors used with the M-325 were assigned the short title "SIGNOAL".

The two development models of the Converter M-325, for which Teletype Corporation was under contract, were delivered to Signal Security Agency

19

On 5 May 1943 for official approval. One of these models was to be retained by the Signal Corps Laboratory and the other to be sent to Smith-Corona to be used as a production model.

MANUFACTURE AND DELIVERY, SECOND MODEL

Quantities of the Converter M-325 which would be needed for distribution to various type field headquarters and permanent installations in the remainder of 1943 and in 1944 were estimated by Distribution Unit, "C" Branch, on 19 April 1943, at a total of 11,991. As it was planned eventually to replace ^{ALPHABET} strip cipher systems with the M-325, this figure was calculated proportionate to the quantity of secret and confidential ^{alphabet} strip systems then held by each type of headquarters. For purposes of estimation one Converter M-325 was regarded as equivalent to one copy of ^{alphabet} strip system. However, since it would be operationally impractical for a ^{code} room to operate with one M-325, the number was increased to include two converters for those units which received only one copy of ^{alphabet} strip system. Distribution was planned as follows:

Armies	18	per Headquarters
Corps	12	" "
Divisions	6	" "
Air Forces	16	" "
Bomber Commands	8	" "
Fighter Commands	8	" "
Air Support Command	8	" "
Wings	2	" "
Military Attaches	2	" "
Posts	2	" "
Groups	2	" "
Companies	2	" "

25

As of 20 June 1944, converters received by SSA from the manufacturer numbered 1,995. Still on contract were 10,005 machines. Of the converters received, 302 had been distributed to the State Department;²⁴ five to the Navy Department;²⁵ two to the Assistant Chief of Staff, G-2; one to Chief, "C" Branch; one to Plans and Policies Officer, "C" Branch; ten to Cipher Machine Section, "C" Branch; and 50 to School Section,

On 1 August 1944 the following report was made by Smith-Corona on the number of Devices "B" and "B-2"²⁶ manufactured and shipped to SSA as of that date:

<u>Date</u>	<u>Device "B"</u>	<u>Device "B-2"</u>
3-21-44	35	35
5-1-44	500	500
5-25-44	760	760
6-15-44	1700	1000
6-29-44	1000	1100
7-18-44	<u>1000</u>	<u>1500</u>
	3995	4895

The above figures included Navy deliveries.

Later in August 1944, delivery of 5,725 converters and 1,787 sets of

-
24. One thousand Converters M-325 and 2,000 associated rotor sets had been requested by the Secretary of State on 4 May 1944 for use by the State Department in world-wide communications.
25. On 17 March 1944 an order was placed with the Chief Signal Officer by the Navy Department for 1,000 converters and 2000 rotor sets.
26. Designation used by Smith-Corona for SIGFOY and SIGNAL respectively.

32

rotors was made to SSA by Smith-Corona. The balance of the M-325 equipment under procurement was scheduled for delivery the end of November 1944. Of this delivery, 625 converters and 624 sets of rotors were turned over to the State Department. The balance of the rotors (376 sets) requested by the State Department were wired and ready for issue. At this time a request for the second thousand rotors desired by the State Department had not been received.

A recommendation was made to the Chief, "C" Branch on 31 August 1944 that immediate action be initiated to cancel delivery of 1,500 models of SIGFOY, 3000 sets of associated rotors, and the entire contract for spare parts. This action was requested because of revised requirements for the M-325 based on the theory that the possible cessation of hostilities in the European and Mediterranean areas was considered imminent and the Army's requirements for the M-325 would be diminished. The following day "C" Branch recommended to Security Division that "C" Branch be authorized to take necessary action to implement this recommendation.

The above requested authorization was received from Security Division and on 5 September, "C" Branch notified the Purchasing and Contracting Officer, SSA to initiate immediate action to cancel 1,500 Converters M-325, 3,000 sets of rotors for M-325, and the entire order for M-325 spare parts. All work in process at Smith-Corona on Converters M-325 and associated rotors be completed and accepted by SSA to be used as spare parts, thus making the purchase request for spare parts unnecessary. Cancellation of

33

contracts for the M-325 and associated rotors and the purchase request for spare parts would result in a saving of approximately \$75,000.

Operations Service Division, OCSigO, on 7 September recommended that the above cancellations be approved and two days later correspondence requesting that this equipment be cancelled was sent from SSA to Requirements Division, OCSigO.

However, on 18 September 1944 the Chief, Security Division notified "C" Branch that new prices had been received from Smith-Corona on the SIGFOY and associated equipment. Original prices quoted for this equipment when the contracts were signed were \$75 for each SIGFOY and \$60 for each set of rotors. The new prices quoted by Smith-Corona were \$51 each SIGFOY and \$47 each SIGNOAL with box.

In view of the decreased prices quoted above, the Chief, Security Division was in favor of continuing the current contracts for the M-325 with rotors and component spare parts, if "C" Branch concurred. "C" Branch agreed to have the contract continued in entirety.

The delivery schedule for the SIGFOY was changed on 29 September 1944 by a telegram from "C" Branch to the Commanding Officer, Philadelphia Signal Corps Procurement District requesting that Smith-Corona be notified to modify the delivery reference in their contract for 12,000 SIGFOYs as follows:

<u>Date</u>	<u>No. of SIGFOYs</u>
October 1944	1500
November 1944	1500
December 1944	1005

34

ASSOCIATED ENGINEERING PROJECTS

In September 1944 engineering tests were conducted on the visibility, battery life (number of operating hours that may be expected), and filament strength of the Mazda #45 bulb, furnished for use in the SIGFOY, and the Mazda #291 bulb. Tests were conducted with two machines, one equipped with a #45 bulb and one with a #291 bulb, from a 3-volt source of power.

On the basis of the above engineering tests, "C" Branch recommended on 21 September 1944 that the Mazda #291 bulb be procured in sufficient quantities to replace the Mazda #45 bulb. In operation the Mazda #45 bulb proved unsatisfactory inasmuch as the light given off was dim and made identification of characters difficult after a comparatively few operations of the machine. In addition, batteries deteriorated rapidly with the Mazda #45 type bulb due to their comparatively high current requirements. Mazda bulb #291, which has lower current requirements and includes all necessary characteristics for operation in SIGFOY, was chosen as a bulb likely to give better results.

The Mazda #291 bulb was approved in November 1944 and procurement initiated for 336,000 of the bulbs. As delivery of the bulbs could not be made by Supply Branch until 1 February 1945, it was requested that at least 84,000 bulbs be procured for use with the converters to be distributed to-

between 15 December 1944 and 1 February 1945 for operations tests.

Foot pedal operation for the stepping of the M-325, to relieve the operator of finger fatigue caused by pushing the rotor stepping button, was investigated by "F" Branch, at the request of "C" Branch, in September 1944.

The foot-
pedal mechanism was to be used for either desk or field. A wooden demonstration model was developed and examined by representatives of "C" Branch. It was decided that a second model, utilizing a flexible actuator to insure positive stepping action, should be developed. Accordingly, a demonstration model consisting of an operating lever, an actuator attachment, and flexible shafting was completed on 31 March 1945. (See Figures 5 and 6). The design of the attachment was such that it could be readily mounted or removed from the converter and could be stored in a relatively small space. Only a slight modification of the converter was required for use of the attachment. Normal use of the stepping button was not precluded by this modification.

required for a supplementary stepping attachment

device, and also

If, too, M-325s would have to be modified, the

44

Project No. 5024, "M-325

Operating Knobs (Misc.)," was set up by Equipment ("F") Branch to produce an improved operating knob. Twelve plastic knobs to be attached to the M-325 rotor stepping lever by means of a metal retaining band in such a way that it rode clear and enabled the operator to step the rotors of the M-325 by merely pressing down on the knob with hand or fist, relieving him of the necessity of actually grasping the machine with his fingers and pressing the knob with his thumb as was done on the ordinary M-325, (See Figures 7 and 8). The knobs were delivered to Mr. Friedman on 13 May 1944.

To ascertain the value of certain ideas proposed for improving the Converter M-325, it was requested by "C" Branch that "F" Branch make studies of the stepping pawl mechanism of the M-325 with the intention of improving the stepping action, and design a transformer to enable operation of the converter from a 110 volt A.C. line. In compliance, Project No. C-5059, "M-325 Improvements," was set up by "F" Branch in late October 1944.

42

*Partially typed
is typed on previous pages*

To ascertain the value of certain ideas proposed for improving the Converter M-325, it was requested by "C" Branch that "F" Branch make studies of the stepping pawl mechanism of the M-325 with the intention of improving the stepping action, and design a transformer to enable operation of the converter from a 110 volt A.C. line. In compliance, Project No. C-5059, "M-325 Improvements," was set up by "F" Branch in late October 1944.

A stepping difficulty in the M-325 was presented because the rotor covers supplied by Smith-Corona were larger in diameter than the specification provided for them. This was responsible for difficulties such as pawls getting out of the exact adjustment and frequent pawl breakage because of the crowding of the entire mechanism that resulted. At a conference held between "F" Branch engineers, members of "C" Branch, and a representative of the Smith-Corona Co. on 27 November 1944, it was decided that the rotor covers would have to be ground down to a smaller size. "F" Branch agreed to grind the covers available in "C" Branch and those to be returned from the Caribbean Defense Command where the device was being tested (totaling 12,000), and Smith-Corona would grind the balance to bring them within the required specification. The following day a telegram was sent from "C" Branch to the Philadelphia Signal Corps Procurement District requesting that no more sets of rotors be accepted until notification to ^{resume} ~~resume~~ acceptance was given by SSA.

On 1 March 1945 action was initiated by "C" Branch to procure 20,000

43

ground rotor covers from Smith-Corona. Purchase Request No. 45-721 covered this order. Accordingly, 8,800 of the 20,000 rotor covers desired were delivered to SSA on 6 April 1945 by Smith-Corona from their stock on hand. It was found that while the grinding process brought the rotor covers within the designed diameter, it resulted in an eccentric rotor once the ground covers were attached to the rotor body. This eccentricity approximated the oversized condition of the rotors in its overall effect.

It was also decided at the above-mentioned conference of 27 November 1944 that 1,000 pawls for the next batch of converters manufactured would be case-hardened to see if that would strengthen them in operation. However, tests made on the hardened pawls indicated that no appreciable improvement resulted from this treatment. At the time of the conference, the Smith-Corona Co. representative agreed to make a shield which would fit around the back side of the pawl assembly to keep the rotors from jamming the pawls at the time when the rotors were being inserted in the machine. This shield was provided by the company and installed on one of the converters.

The problem of developing and constructing a transformer to serve as an alternate source of power for the M-325 was turned over in entirety to Section F5 of Equipment Branch where it was set up as Project No. 5059 in February 1945. A transformer was developed which when inserted in the converter in place of the two dry cells, BA-30, normally used, permits

44

operation of the converter from a 115 volt, 60 cycle supply. The total development cost of one such unit was placed at \$160.50. It was decided to discontinue any further action on the matter pending the receipt of further recommendations and comments from field units to whom the SIGFOY was then being distributed for testing.

Engineering projects covering later development of the M-325, on the basis of comments made following field testing of the ^{CONVERTER} device, are included in a subsequent section of this history.

45

STANDARDIZATION

Following receipt by Signal Security Agency of the two development models of the Converter M-325 from Teletype Corporation in May 1943, SSA on 14 June 1943 advised Equipment Coordination Branch, OCSigO, that the M-325 had been improved to the extent believed necessary to provide adequate security as an authenticator and that procedure leading to its standardization was under way. It was believed at this time that no new mechanical principle of authentication had been evolved which was superior to the M-325.

Nevertheless, Signal Security Agency was informed on 26 January 1944 by Requirements Planning Branch, OCSigO, that standardization of the Converter M-325 was not necessary at this time; the device could be standardized at a later date, after manufacture of the ^{MACHINE} device had begun, if SSA desired.

The tentative delivery schedule of the M-325 as per Purchase Plan 2107 requested delivery to start in February 1944. However, due to manufacturing difficulties, delivery was not begun until March 1944. Consequently, on 4 March 1944 action was initiated by SSA through Equipment Coordination Branch to the Signal Corps Technical Committee for standardization of the Converter M-325 as Required Type, Development Type, Limited Procurement

49

Type.³⁴ It was planned at this time by SSA that the M-325 would be used as an authenticator and ^{as a} cryptographic ^{MACHINE} device to replace the ^{alphabet} strip cipher device. Since the M-325 was to be a registered ^{and} cryptographic device used for special purposes, it was requested that it not be placed on the Tables of Basic Allowances so that control of issuance in accordance with War Department directives might be maintained. Army Service Forces, Army Ground Forces, and Army Air Forces had all given evidence of interest in the M-325. Later in March 1944, Equipment Coordination Branch recommended coordination with AAF and AGF before standardization of the M-325.

In September 1944 Signal Security Agency submitted a new request for standardization of the M-325 as Required Type, Adopted Type, Standard Article.³⁵ Before submitting the new request for standardization, SSA requested informal concurrence from Army Ground Forces. AGF concurred in October 1944 and on 23 November 1944 SSA recommended to Equipment

-
34. Required Type designates the ^{CONVERTER} device as an article of equipment for which there is an existing or expected need and from which military characteristics have been approved; Development Type is a Required Type being developed to meet approved military characteristics; Limited Procurement Type signifies that the item is suited for service, but requires refinement in design or further use in the hands of troops to determine definitely its suitability. Para. 14, AR 850-25, 30 June 1943.
35. Required Type, see footnote 34; Adopted Type signifies the item is a Required Type adopted as suitable for the use of the Army; Standard Article designates the item as the most advanced and satisfactory of the items adopted for a particular purpose and is preferred for procurement. Para. 14, AR 850-25, 30 June 1943.

50

Coordination Branch that the M-325 be presented to the Signal Corps Technical Committee for standardization as given above. It was stated in the recommendation to Equipment Coordination Branch that production of the device was started in March 1944 and would be completed by January 1945. To date, requirements requested by SSA had been met by the manufacturer.

As a result of the above action, on 22 December 1944 the Converter M-325 was classified as a Required Type, Adopted Type, Standard Article by the Signal Corps Technical Committee (SCTC Item No. 1279).

51

In addition to comments concerning the practicability and operating efficiency of the Converter M-325, the questionnaires filled in by using personnel and the trip reports made by observers after trial operation of the SIGFCY in the field included recommendations for improvement of the device. The following suggestions were made in the majority of the reports submitted:

1. The rotors should be reprocessed since many cases of faulty stepping could be traced to improperly manufactured rotors.
2. A form of foot pedal should be devised to step the rotors as the rotor stepping button is too hard on the finger of the operator.
3. A change in design and treatment of stepping pawls should be made.
4. An adjustment should be made in the machine so that an outside source of power could be used, in addition to batteries.
5. A print mechanism should be incorporated in the machine to eliminate the need for copying the text on paper during encipherment and decipherment.
6. The button panel and the light panel should be separated, with only one lamp, the encipherment or decipherment of the letter represented by the button, lighting. This has a two-fold purpose: (a) to lessen the confusion of having two lights lighted and the consequent possibility of writing down the wrong letter, and (b) to put all the lights where they will be immediately visible.

85

- 7. A circuit should be installed so that after a lamp has once been lighted, another one cannot be lighted until after the rotors have been stepped.
- 8. Alternately colored wires would help in the wiring of the intermediate rotors.
- 9. A screwdriver should be issued with the converter.
- 10. A more sturdy type of jackboard wire should be used and improved tweezers should be issued with the converter to make the wiring of the jackboard and reversing wheel easier.

Those of the above recommendations that were considered practicable were used as a basis for modifying the M-325 in an attempt to make the machine satisfactory for use. Suggestions concerning foot pedal operation, redesign of the stepping pawl mechanism, and use of an outside source of power had been studied previously by Equipment ("F") Branch and were set up as engineering projects. However, action on these projects had been discontinued pending the results of trial operation of the M-325.

In view of the unsatisfactory reports made on the M-325 following its trial operation, a conference was held at Signal Security Agency on 5 March 1945 to discuss future action concerning the converter. It was decided that no more introductory models should be sent out and that before general issue, the M-325 should be modified to meet its best possible form for use. Concerning converters held by military attaches, the M-325 would be replaced by strips or one-time pads, but the converters would remain in possession of the military attaches for the time being.

(86)

~~Modification of the SIGFOY was considered complete.~~ Actual changes in the SIGFOY during this period of modification were as follows:

1. No. 1 pawl was redesigned.
2. No. 2 and 3 pawls were redesigned, but remained interchangeable.
3. Counterlink was redesigned together with the counter operate bail.
4. New springs of different strength were designed for the operating pawls.
5. A new operating-bail spring was designed and produced.
6. A stronger spring was added to the rotor-lock bail.
7. New adjustments were determined for the old spring detents.
8. A new plug was designed for the plugboard and new colored wires provided for.
9. A special tweezer-like plug-removing tool was designed.
10. Colored reversing rotor clip cables were provided.
11. Emergency external battery connections were designed.
12. The battery compartment insert for use with a transformer or external battery was redesigned to allow its use with the back cover of the SIGFOY resting in a closed but unlocked position without damage to the wire.
13. The rotor pawl shaft was redesigned to allow an extra lock nut on its end.
14. Rotor pawl stop was redesigned.

97

15. The operating base had some redesign such as a new stop, fuses, and terminals instead of fixed connections, but due to contract termination the new design was never produced. (See Figures 9, 10, 11, 12, 13, 14, 15, and 16.)

The present SIGFOY modified according to the above procedures is the closest that could be reached to a reasonably good operating device without a complete redesign and manufacture of a new model. The construction is such as to minimize operating adjustments, permit accurate stepping operation, and to allow a proper count. Hand operational tests on the models indicated that stepping is consistently good. While the machine in its modified state is thoroughly operable, several of its original shortcomings are still present such as the very slow speed at which it may be operated (about two groups per minute), the tremendous concentration that is required to operate the device, and the finger fatigue that is caused from use of the machine on reasonably long messages.

It was considered that there was no object to further testing of the converter. The modified device includes all those improvements, requested by using personnel in the field following the trial operation of the M-325, that were considered practicable for inclusion in this model of the field device. Certain comments and suggestions, to be effectively included in the modified model, would have involved considerable redesign. An additional field test could only bring comments of accord on the changes already accomplished, and repeated requests for those changes previously suggested.

98

CANCELLATION OF PROJECT

A staff memorandum dated 24 August 1945 for the Chief, Signal Security Agency from the Chief, Security Division, stated that the cessation of hostilities had materially reduced requirements for all types of cryptographic devices. This conclusion was based on the facts that (1) the strength of the Army would be reduced to a peacetime level of 500,000 and (2) post-hostilities communications would have a much smaller percentage of classified messages. It was expected that the number of Converters M-134-C (SIGABA) in serviceable condition would be great enough to meet almost all of the peacetime cryptographic requirements. Consequently, it was believed that the requirement of strips as they were used at that time would be so small that expenditure of funds on another machine for the specific purpose of replacing strips could not be justified. At that time there was no replacement available for strips on the M-325. However, Converter MX-507()/U was under development; this device should eventually eliminate any need which would exist for strips for the M-325.

In view of the above facts, it was recommended in this memorandum that with the installation of an improved stepping mechanism and the addition of a base and power transformer on two experimental models of the M-325, no further machines be

99

modified and no further effort be made to improve the machine. Then action should be taken to classify the M-325 as an Obsolete Type in accordance with paragraph 14, AR 850-25. The memorandum further recommended that when the Converter MX-507()/U became available, the Converter M-325 should be condemned as unsuitable for further use and quantities known to be excess should be disposed of in the proper manner. Action, as recommended in the above memorandum, was approved by the Commanding General, SSA, on 7 September 1945.

(100)

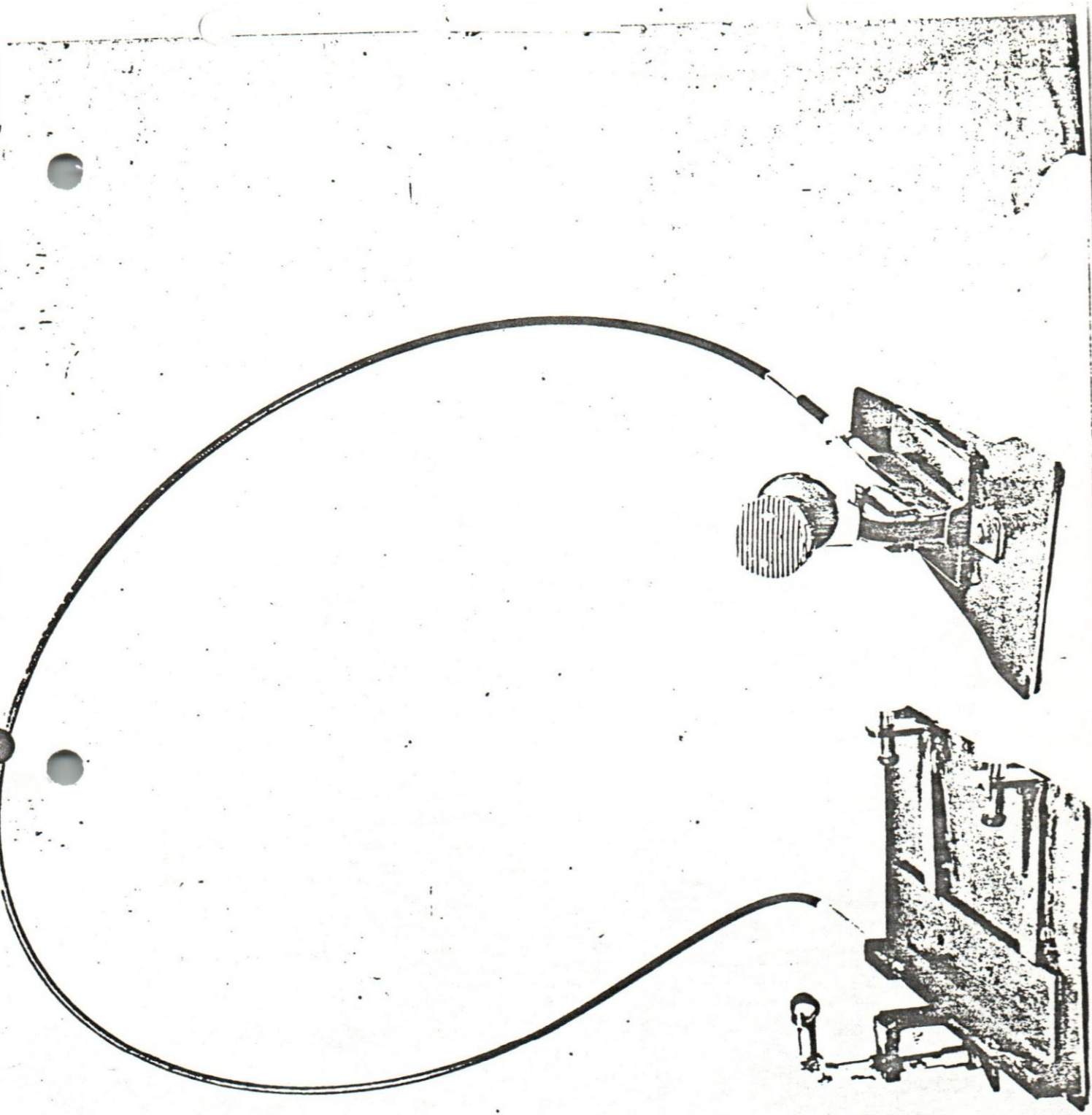
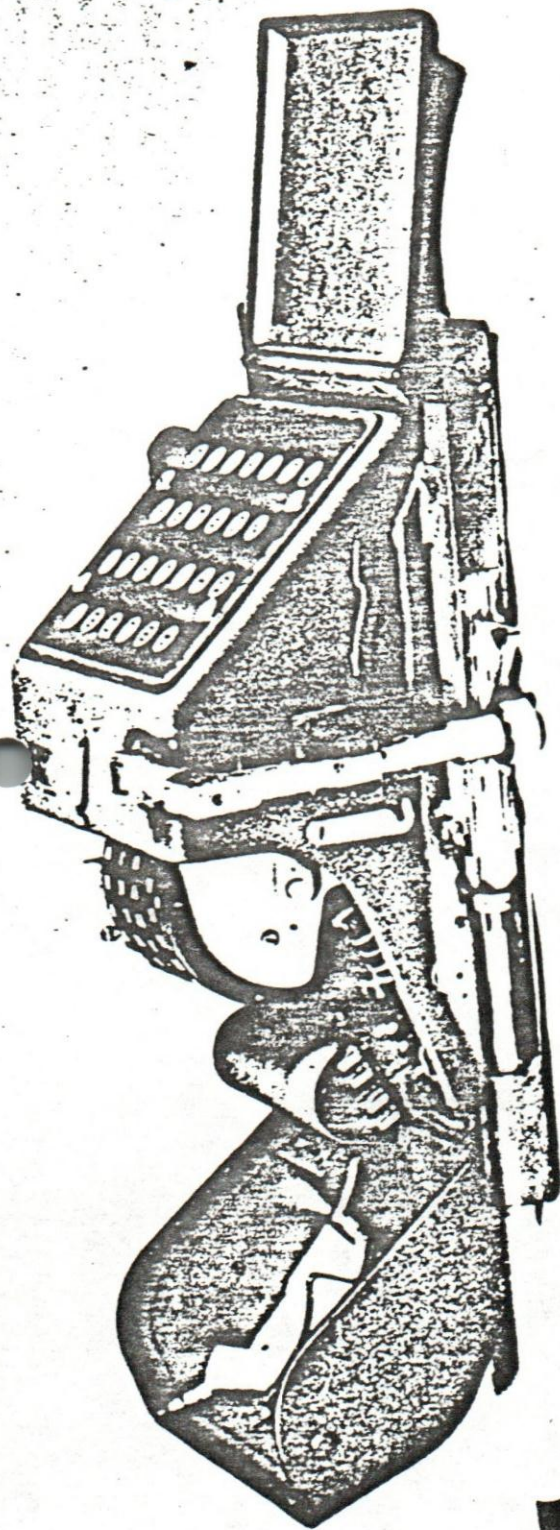
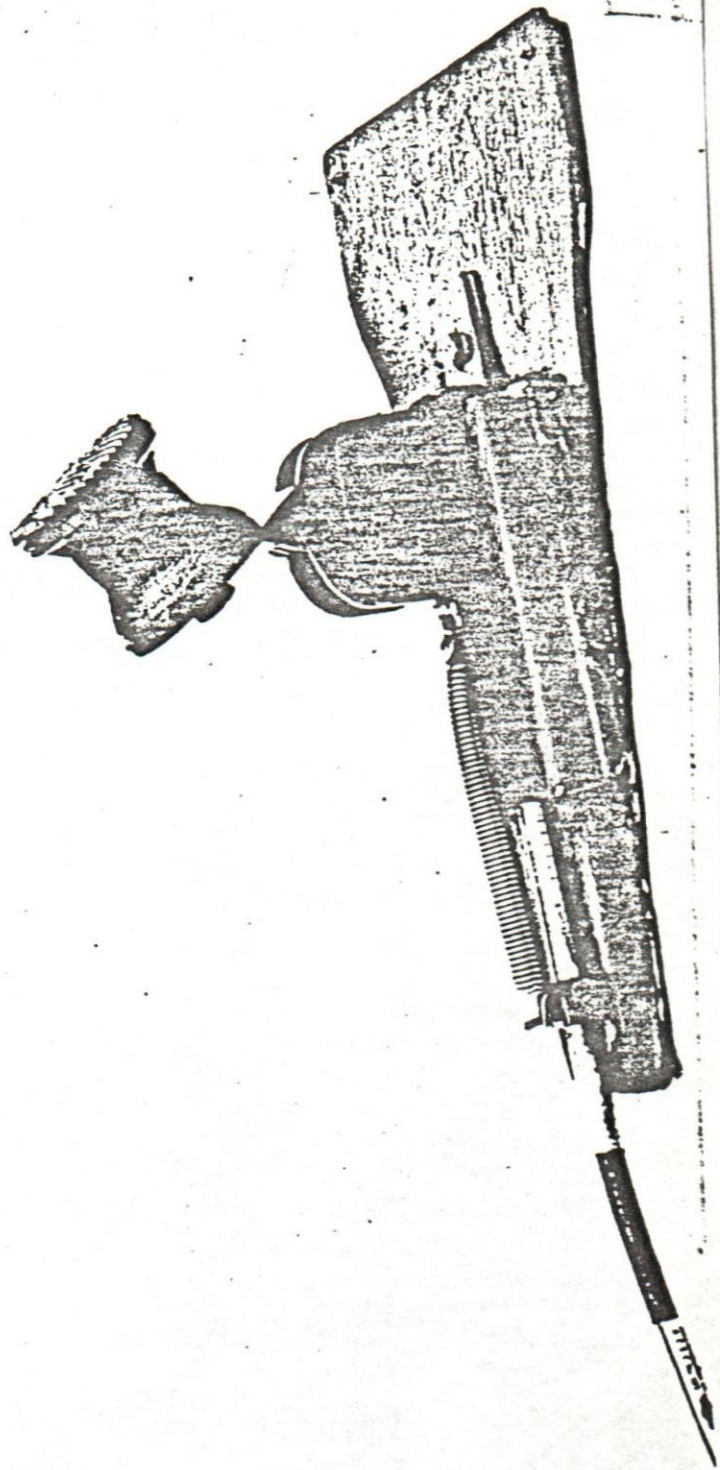


Fig. 6. - Foot pedal mechanism for SIGFOY

070 041 (057)



- Fig. 6. - Foot pedal mechanism attached to SIGFOY

070 942 (157)



Fig. 7. - SIGFOY, Second Model, showing operating knob
in place

153
0 0 044

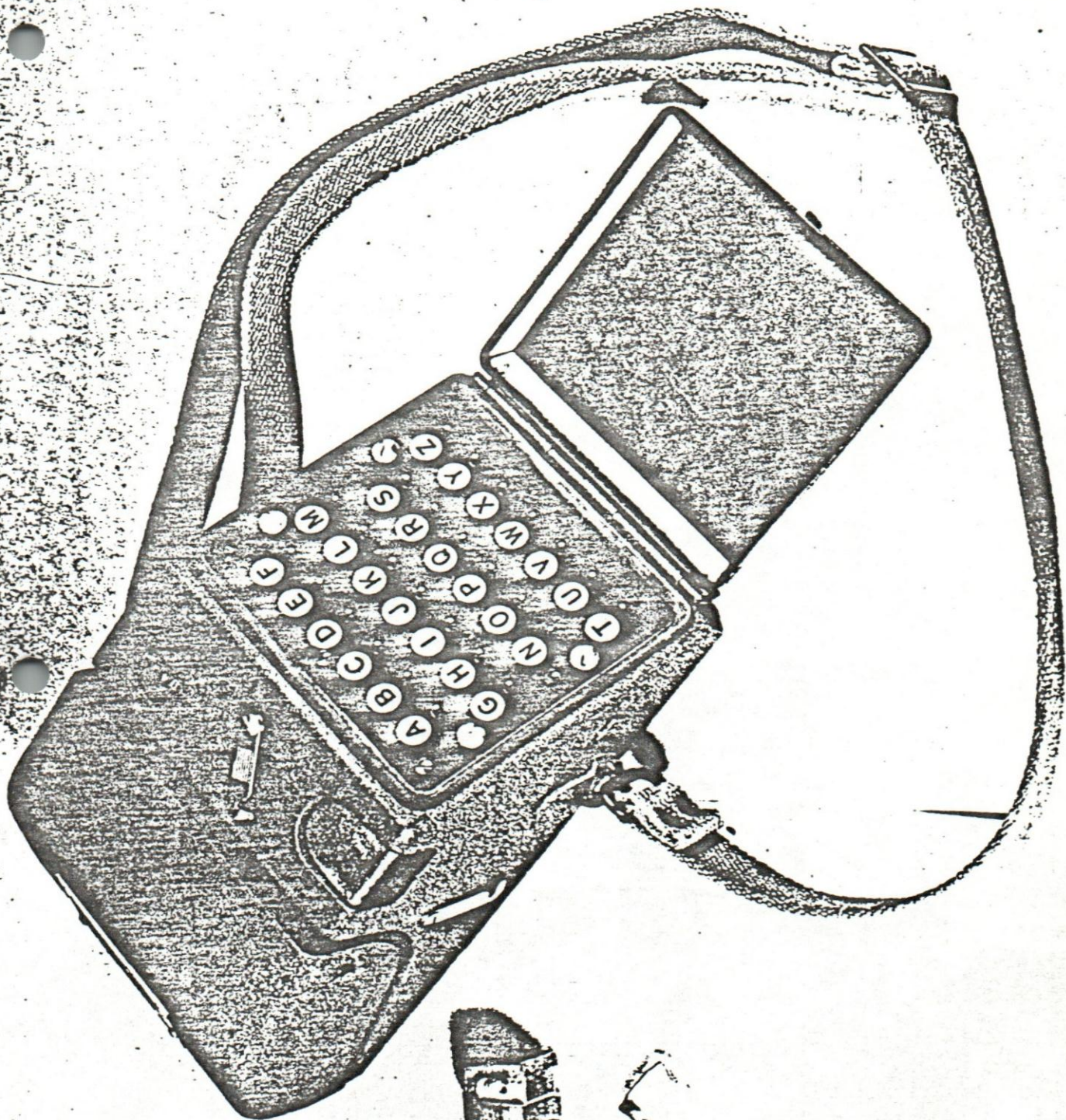
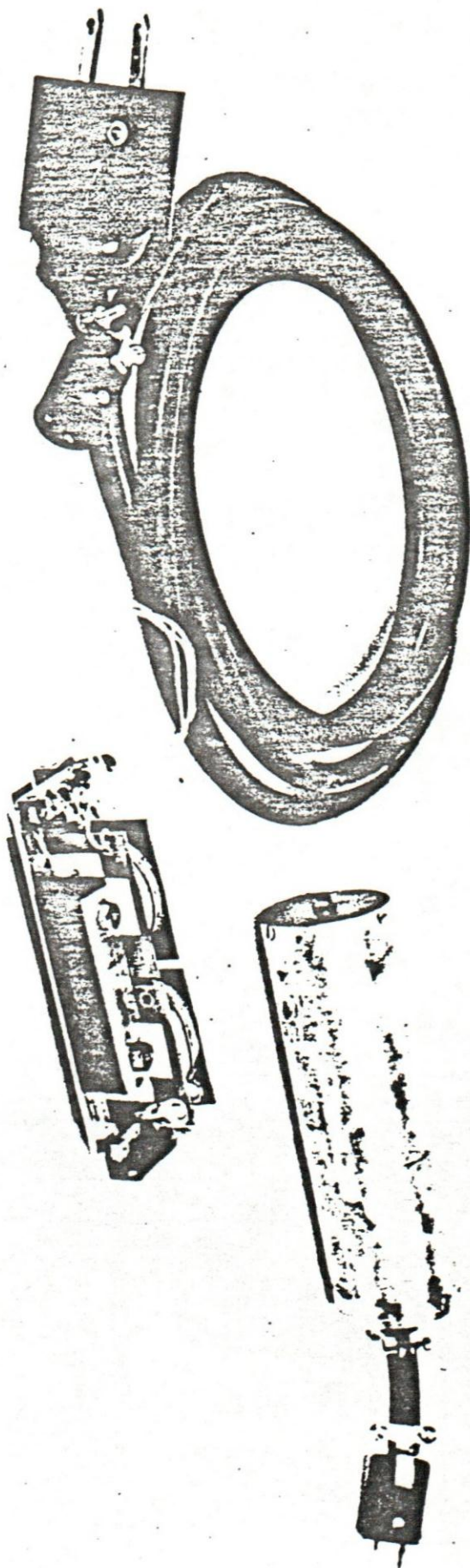


Fig. 8. - SIGFOY, Second Model, showing parts
of operating knob

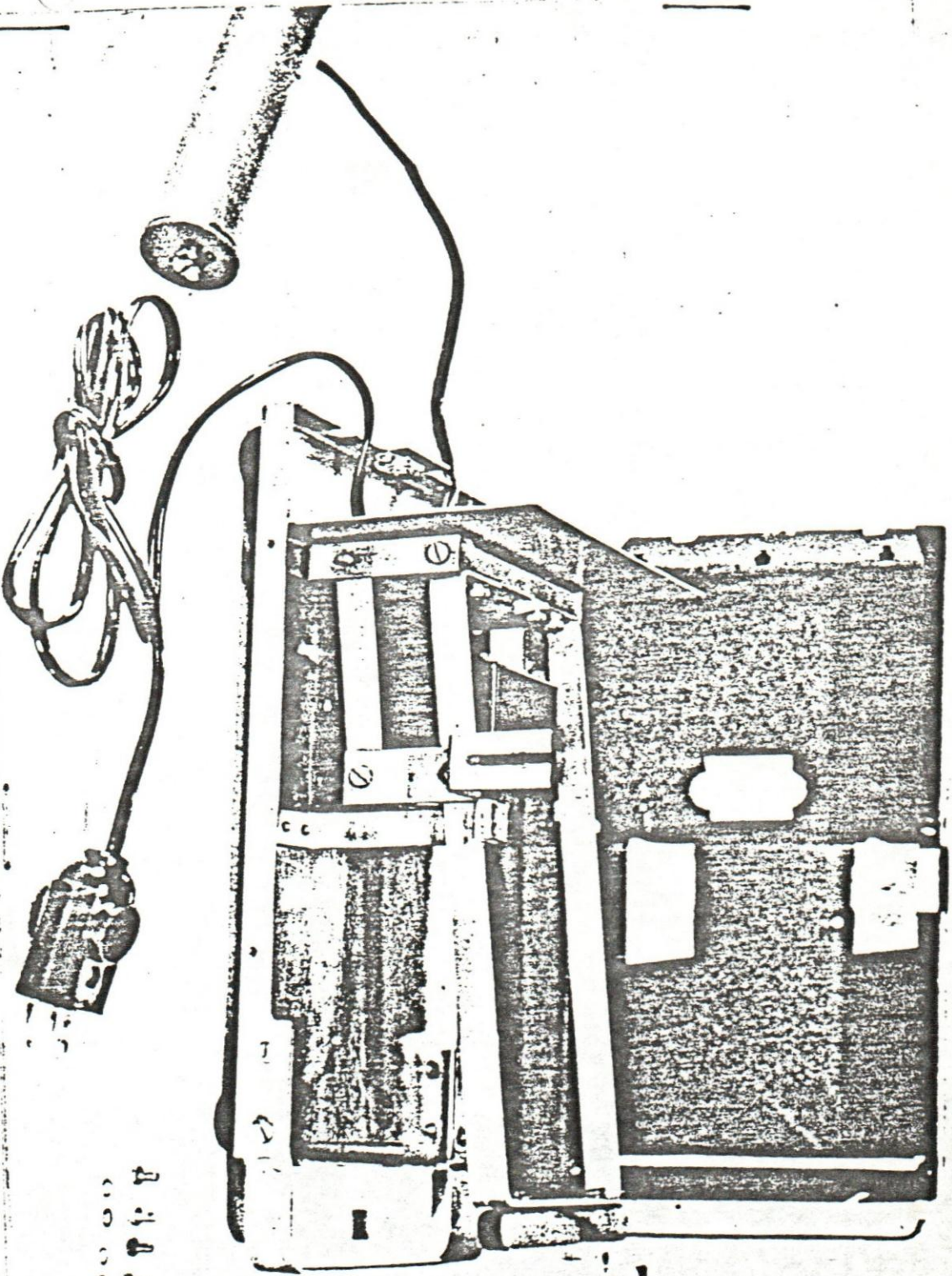
132
00045

FIG. 9. - Parts of transformer before final assembly in modified SIGFOY



203

Fig. 10. - Inside view of operating base for modified SIGFOY
showing mechanical linkages



A
A
A
A
A
A
A
A
A
A

204

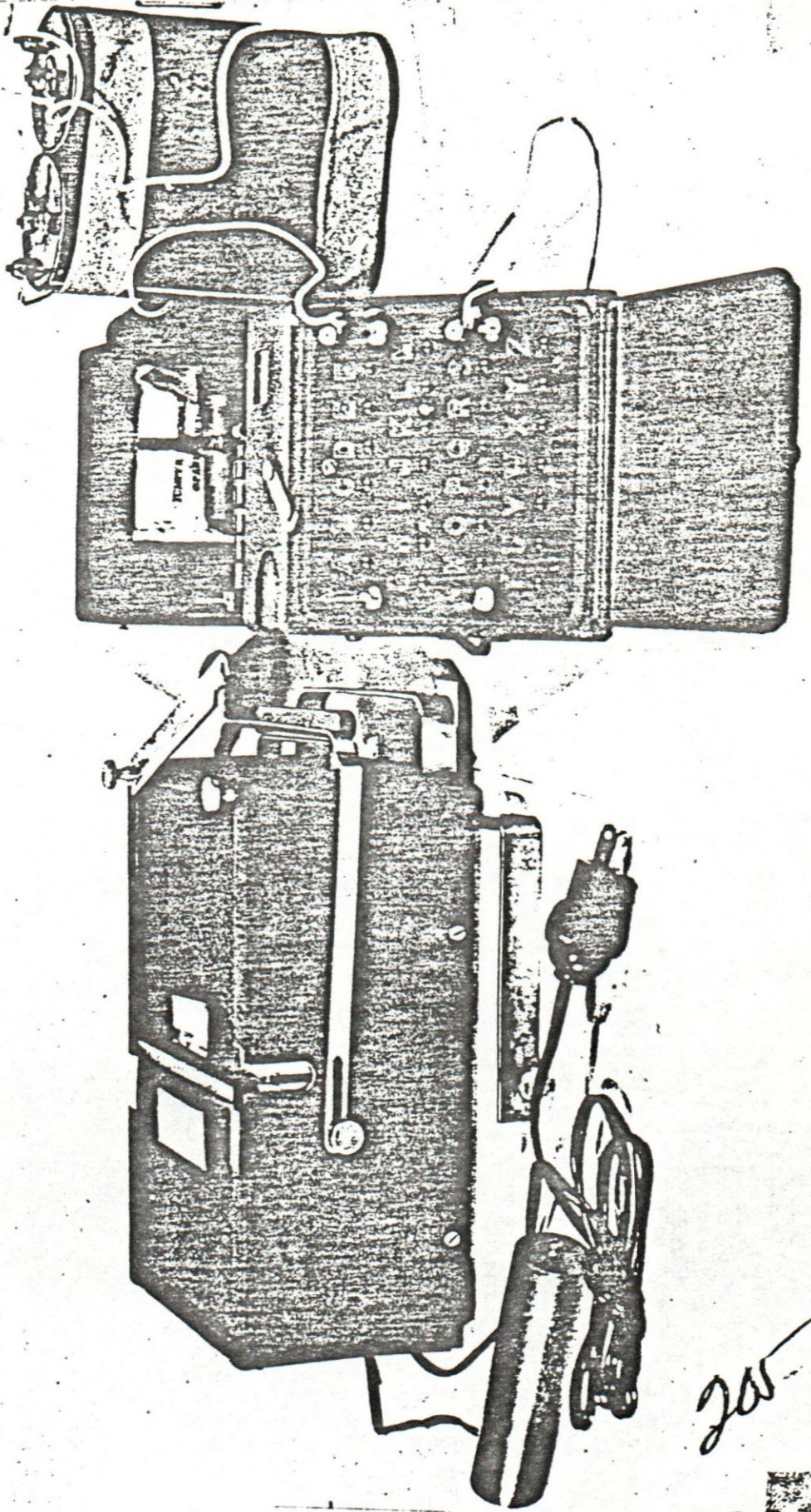
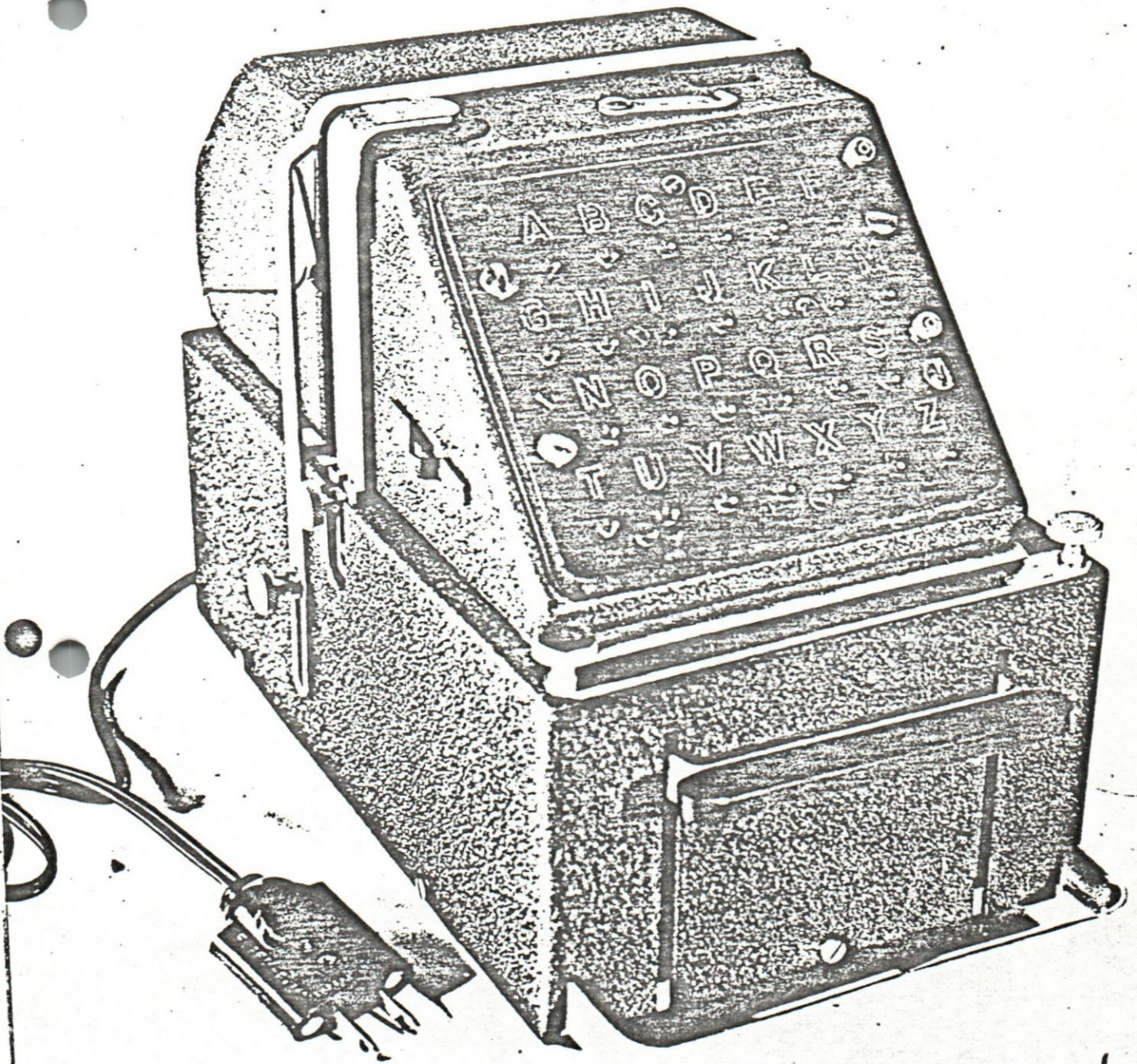


Fig. 11. - Operating base and transformer for modified SIGFOY. The SIGFOY is shown connected to two BA-30 batteries.

205



906

Fig. 12. - Modified SIGFOY mounted on operating base with transformer.

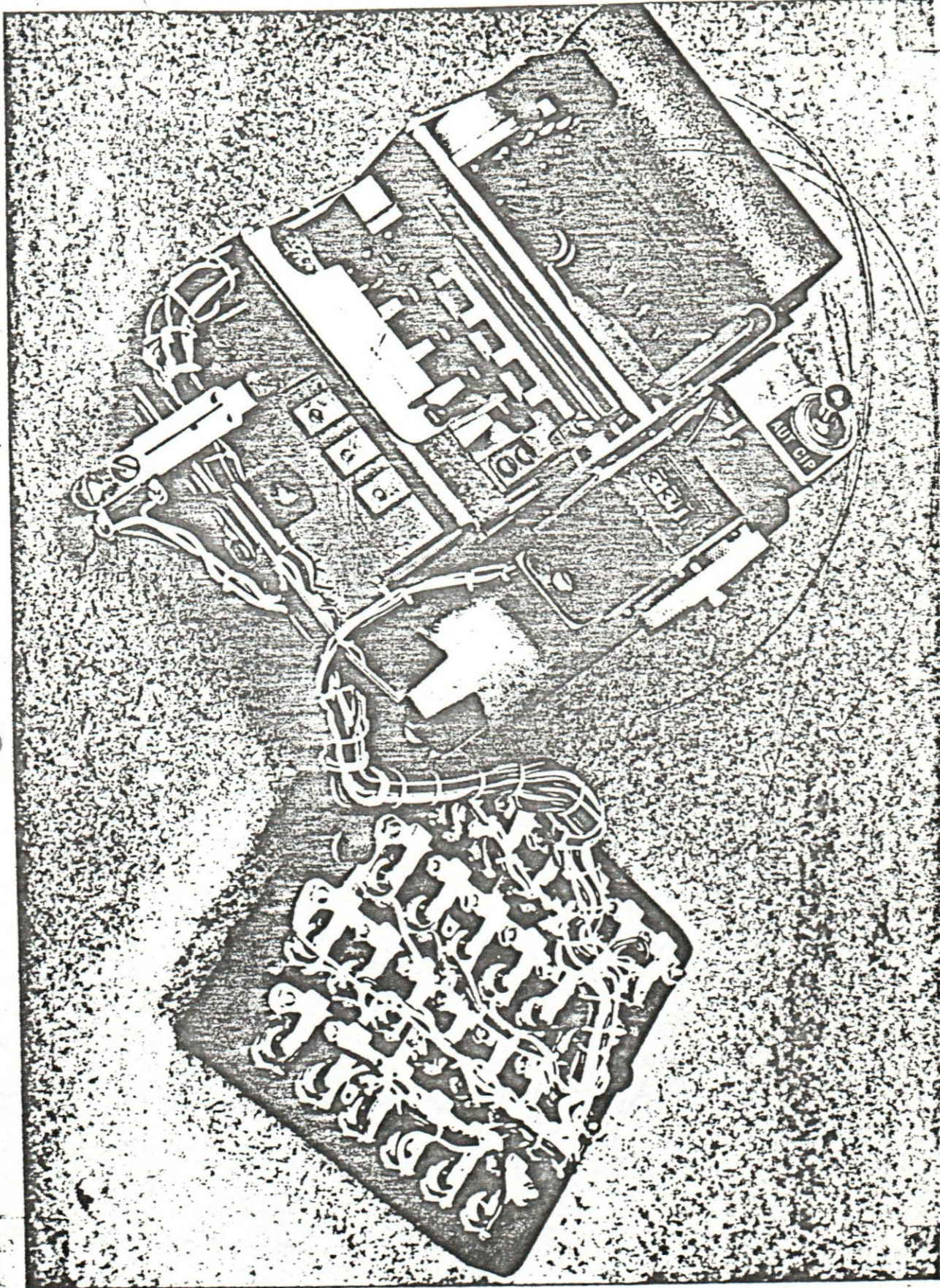


Fig. 13. - Modified SIGFOY dismantled to show guard for keeping rotors from jamming.

207

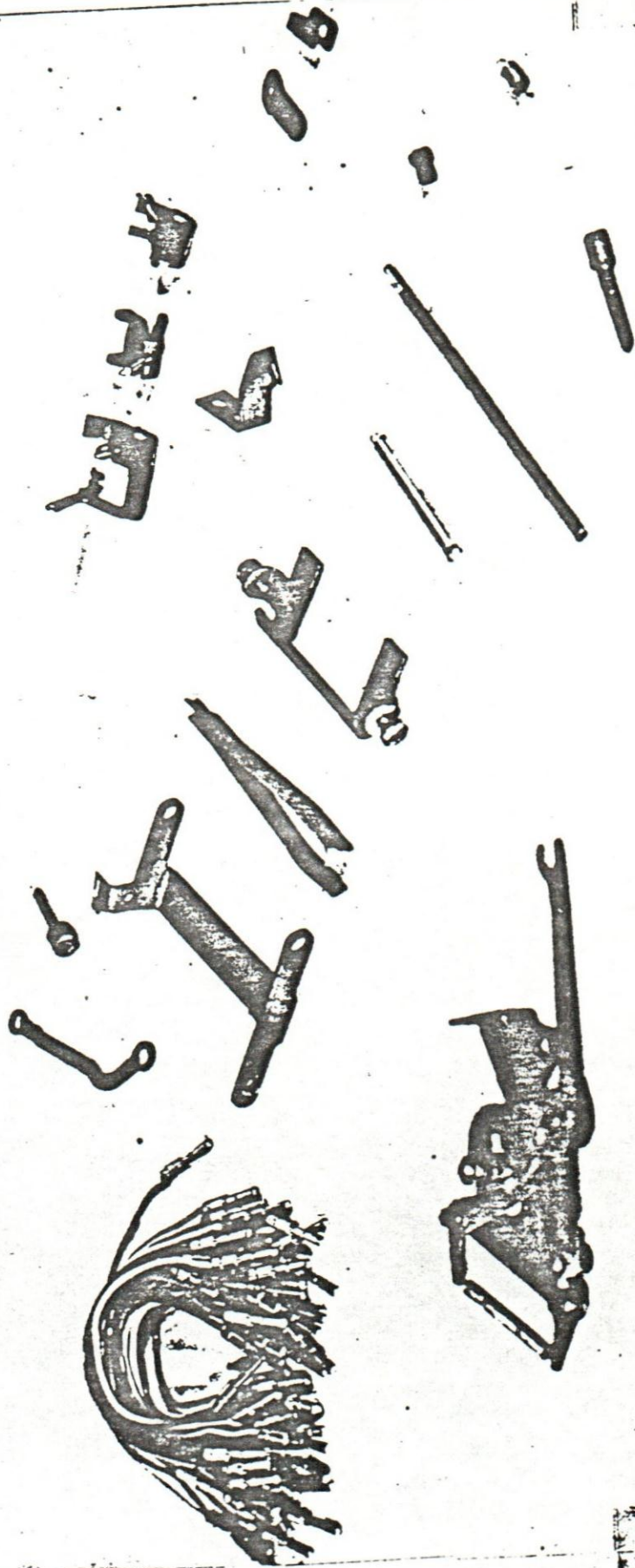


Fig. 14. - Modified parts for final model of SIGFOY.

208

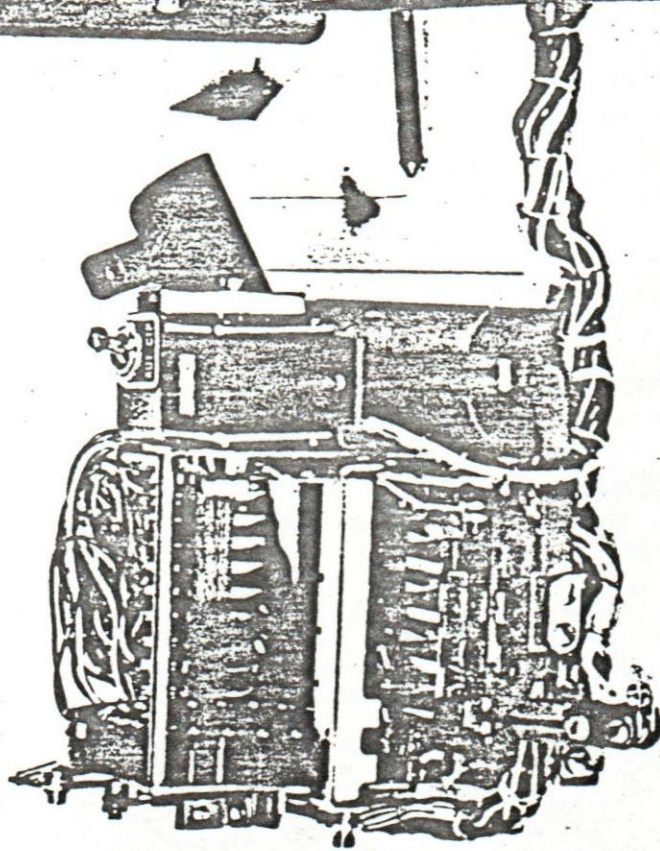


Fig. 15. - Modified parts installed in final model SIGFOY.

209

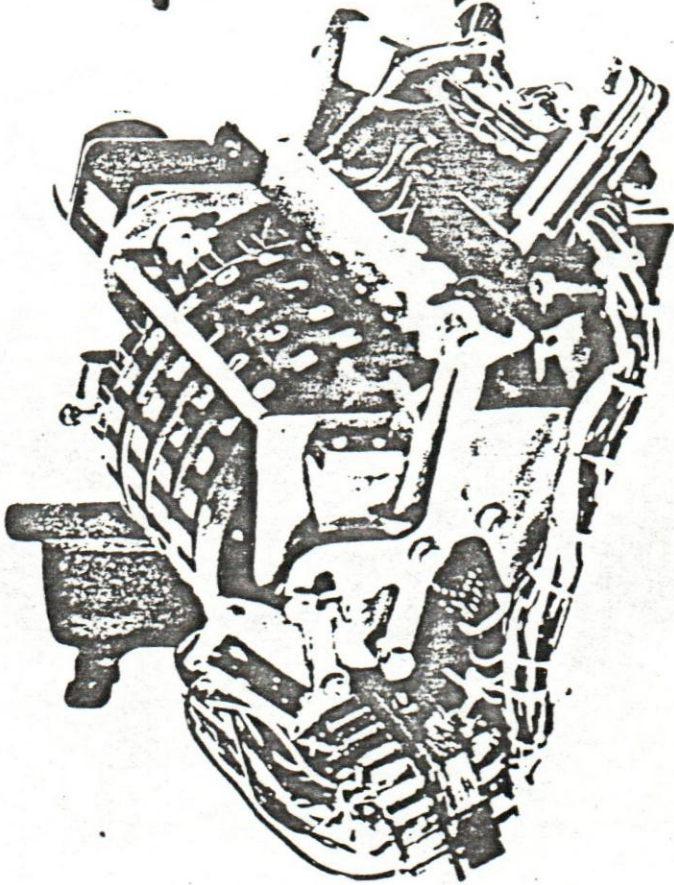
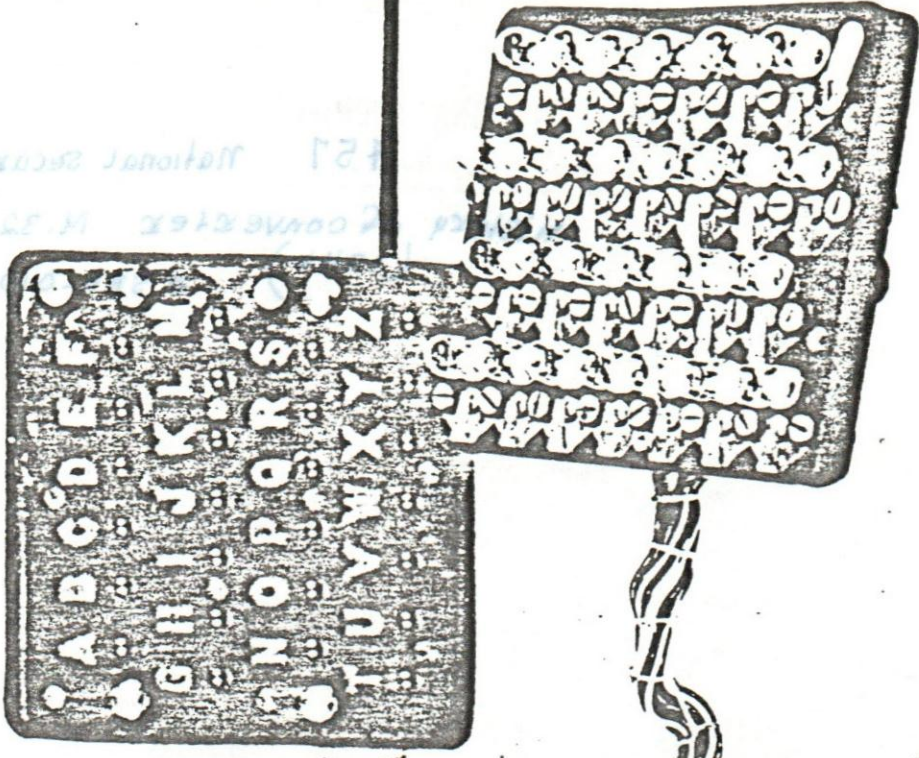


Fig. 16. - Assembled modified SIGFOY outside of carrying case.

(210)