~~SECRET~~
SECRET

R-176-54 CArmA - [redacted] 2

HAND-DRIVEN CIPHERING MACHINE, TYPE HC-4

1. During the first week in June, this office was contacted by the Foreign Liaison Section, [redacted] and requested to have a representative at a meeting to be held on 18 June 1954, in the office of the Chief of Signal, [redacted] Staff. The reporting officer, accompanied by the Military Attaches from [redacted] Inclosure 1, in English, pictures this machine and give a description of it.

[redacted]

3. The inventor stated that a sample would be available in 2 to 3 months at a cost of roughly [redacted] and that production of this machine would allow purchase of quantities made in [redacted] It is expected that this cost could be measurably reduced on large scale production.

4. This machine has apparently been well examined and tested by crypto analysts, [redacted] and has been, as far as could be determined, decided on as the tactical ciphering equipment for their Army. One representative of the office stated that he felt the machine was better than the [redacted] principle and that it was a secure piece of equipment for use at the battalion or lower levels provided that the SOI were changed frequently and that a maximum of approximately 40 groups were set for any one message before pin timbler changes were required.

5. The reporting officer asked whether they would welcome the visit by a specialist in this field from the U.S. in lieu of the possible purchase of one or more test models at a price of [redacted] each. They indicated that this would be acceptable, however they again reaffirmed the sensitivity of this project.

COMMENT: Although the reporting officer has very little knowledge of crypto equipment and has not used any tactical ciphering machine since early 1951 in Korea, this equipment appears to be handier and faster than that previously seen. It is apparent that the loaning of one machine to [redacted] It is also apparent that much thought was given to the manner in which this machine would be demonstrated to the Foreign Attaches representing NATO countries since there was ample notification of this meeting and the conference was rather obviously rehearsed with various questions ignored or referred to an additional meeting in the absence of the inventor following the demonstration. While the brochure, Inclosure 1, was not given a stamped security classification, it was handled to the Attaches and subsequently enveloped prior to departure from the building as though it were classified.

Distribution by originator: None

1 Incl - Brochure

~~SECRET~~

~~SECRET~~
~~S E C R E T~~

~~SECRET~~

R-176-54
Hand-driven Ciphering Machine, Type HC-4 1253175
CArmA- [redacted]
A-1
1

18 June 1954 21 June 1954
John E. Emerson, Jr. Maj GS Official

The report forwards a brochure and other information regarding a new hand-driven ciphering machine recently purchased by the [redacted]

~~SECRET~~

Hand-driven Ciphering Machine Type HC-4.

Description.

General.

This type has been designed with the intention of meeting the demands for a ciphering machine safe against cryptoanalysis, of small dimensions and of low weight, rapid, easy to handle and inexpensive. The dimensions are 135x155x150 mm (5 1/2"x6"x2"). Weight: 1.5 kg.

All steel details included in the machine are effectively treated against corrosion and it is so constructed that considerations are taken to prevent dust and humidity to enter into the interior.

Fundamental construction.

The machine is provided with 5 pin chains with the divisions 29,31, 33,34 and 35 (number of links and pins respectively in each chain).

The circulation (number of steps until the machine returns to the orginal position) is consequently equal to 25x31x33x34x35 = 35,303,730.

Each link is provided with a pin, which can be settled in either an active or a passive position, and is also supplied with a mark for identification.

The feeding of the pin chains is regular: 1 step at each advancement of the mechanism. The markings of the links are chosen in such a way that each chain contains the whole international alphabet besides a number of figures, thus:

29	division	ABCDEFGHIJKLMNOPQRSTUVWXYZ123
31	"	ABCDEFGHIJKLMNOPQRSTUVWXYZ12345
33	"	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567
34	"	ABCDEFGHIJKLMNOPQRSTUVWXYZ12345678
35	"	ABCDEFGHIJKLMNOPQRSTUVWXYZ123456789

In the key information only the alphabet markings are used, so that advantage is obtained that those not concerned can never reconstruct the divisions of the pin chains.

By each setting of the pin chains the pins of the actual links operate upon feeling levers, one feeling lever for each pin chain, and these feeling levers further activate a system of blinds. An active pin operates the feeling lever in a positive direction; a passive pin in a negative direction.

Each of the five feeling levers can consequently occupy one of two positions. The number of possible combinations of the positions of these feeling levers are consequently $2^5=32$.

Under the system of blinds there can be inserted a case with 16 interchangeable incoherent alphabets, only one of which will be exposed at each position of the pin chains.

The principle of selecting alphabets is based upon the fact that each incoherent alphabet that is exposed can be referred to one of two possible positions of the feeling levers, which positions are chosen in such a way that they have mutually reversed symbols.

The result will be that exposure of a certain incoherent alphabet can be caused when a feeling lever by a certain setting of the pin chains occupies a positive position, by another setting of the pin chains the same incoherens alphabet can be exposed with the same feeling lever in a negative position.

In other words, it is impossible to decide if the feeling lever in question has occupied a positive or a negative position.

On the uppermost of the blinds that expose the incoherent alphabets, there are applied direct(standard) alphabets, which correspond to the incoherent ones.

Example:

A	B	C	D	E		F	G	H	I	J		K	L	M	N	O		P	Q	R	S	T		U	V	W	X	Y	Z
P	D	K	B	X		N	Y	M	Q	U		C	S	H	F	R		A	I	O	L	Z		J	W	V	E	G	T

To render the reading from the direct alphabets possible by ciphering as well as by deciphering, the incoherent alphabets are reciprocal to the direct alphabets.

The machine can of course be used for other purposes than for the ciphering an deciphering of letters. (It is naturally indifferent what kind of signs are used). Thus the machine is eminently suitable for the ciphering of wheather codes in figures.

Since the ciphering alphabets are incoherent communications with the same key are not susceptible of the standard method of simultaneously decrypting several texts enciphered by the same unlimited Vigenere key.

Besides, all alphabets can be known by outsiders without inconvenience, as the number of alphabets (the regular equipment consists of 260 alphabets) gives such an enormous possibility of variations that no possibility of cryptoanalysis is present unless the setting of pins is known. In other words: The alphabet never have to be exchanged.

Shape and use.

Enclosed photos illustrate the exterior of the machine.

Fig.1 shows the machine closed.

Fig.2 shows the machine with the cover removed.

Fig.3 shows the back of the machine with the lid lowered and the alphabet case a little pulled out.

Fig.4 shows the alphabet case with one alphabet-stick half pushed in, and front and back of an alphabet-stick.

Fig.5 shows the inside of the cover with the keeping case.

Setting of pins.

In order to set the pins of the pin chains (in an active or a passive position) the blocking plate 1 (Fig.3) is to be pushed to the right. The feed wheels are now free from the advance mechanism and are free to be turned for setting the pins. The same procedure is used when a new key is to be set. The feed wheels are turned until the key combination is put into position.

When the feed wheels are to be coupled again to the advance mechanism, the blocking plate just mentioned is to be pushed to the left.

Through a window 2 (Fig.2) the position of the advance mechanism can be read on a step disc, numbered 1-5. When a new key is to be set the first measure is to advance the mechanism until the figure 5 appears in the window and after that to set the key and then advance the mechanism 1 step. The blind system will not be influenced by the setting of the key alone but only by the following advancement.

The advancement of the mechanism is to be done by catching the ears 5 and 6 (Fig.2) with the left hand index and thumb and moving the ear 6 to stop and then letting it return to ist starting-point. If, for any reason, it is desired to back the machanism to any previous position, the small arm 3 (Fig.2) is to be pushed to the right, and then the mechanism is moved backwards when the ear 6 is operated.

Alphabet-sticks.

The machine is equipped with 130 alphabet-sticks, which are provided with one incoherent alphabet on each side; thus there are 260 alphabets accessible for insertion in the machine. The alphabets are arranged according to the customer's desire.

For keeping these sticks there is in the cover an easily removable keeping case with 13 partitions, marked AB,CD,EF --------YZ, each containing 10 sticks. Each side of the sticks has in one of its ends an identification mark (see Fig.4): a letter and a figure. The letter indicates to which

partition the stick belongs and the figure the ordinal number in the partition.

The sticks chosen for a certain combination is therefor easily taken out of the keeping case and is inserted in the stick case (as shown in Fig.4), after which the stick case is inserted into the machine (as shown in Fig.3). An exposed incoherent alphabet appears at 4 (Fig.2).

The letter to be ciphered (or deciphered) is looked for in the direct alphabet, which is found immediately above or below the exposed incoherent alphabet. It is to be exchanged for that letter in the incoherent alphabet which is just above or below it. After each reading, the mechanism is to be advanced.

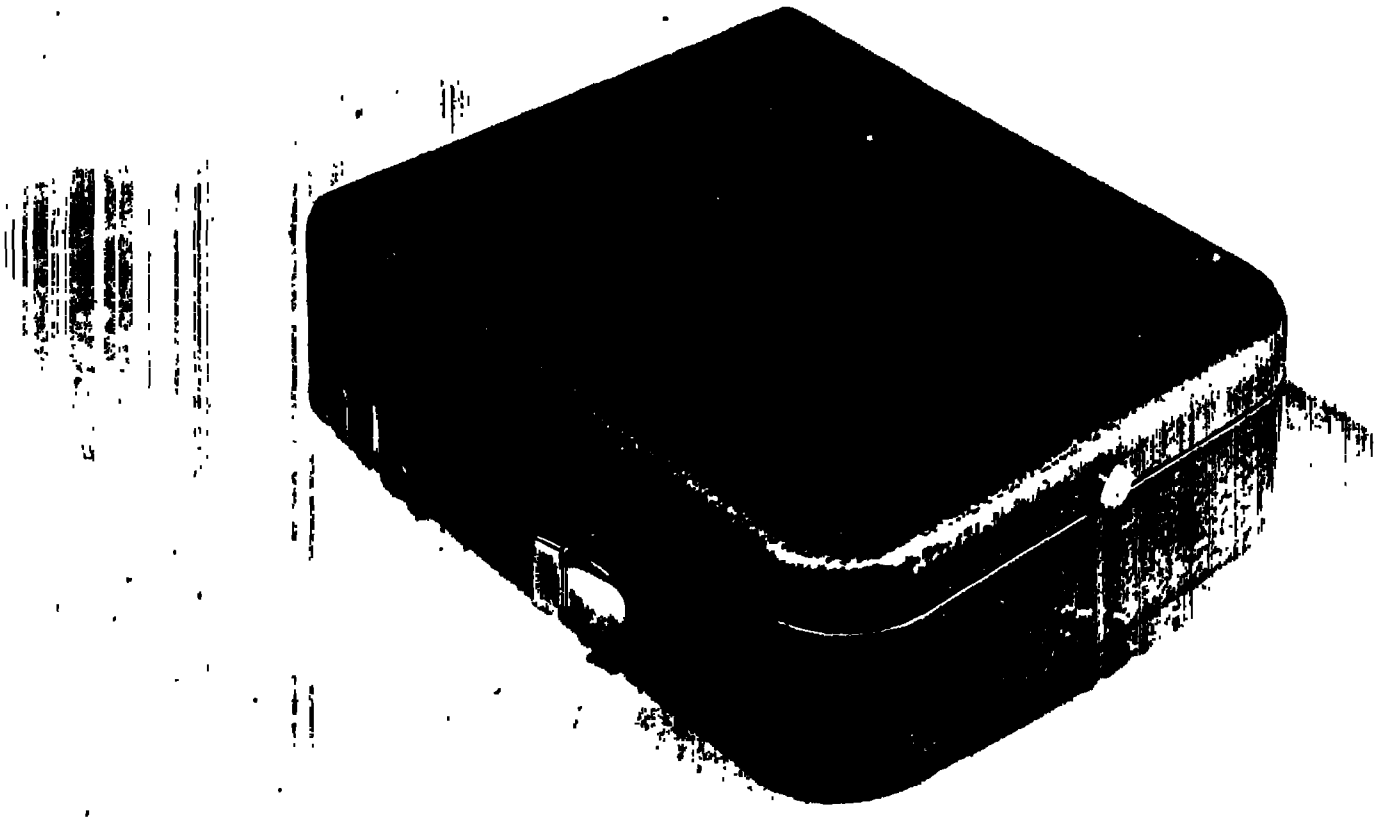


Fig. 1

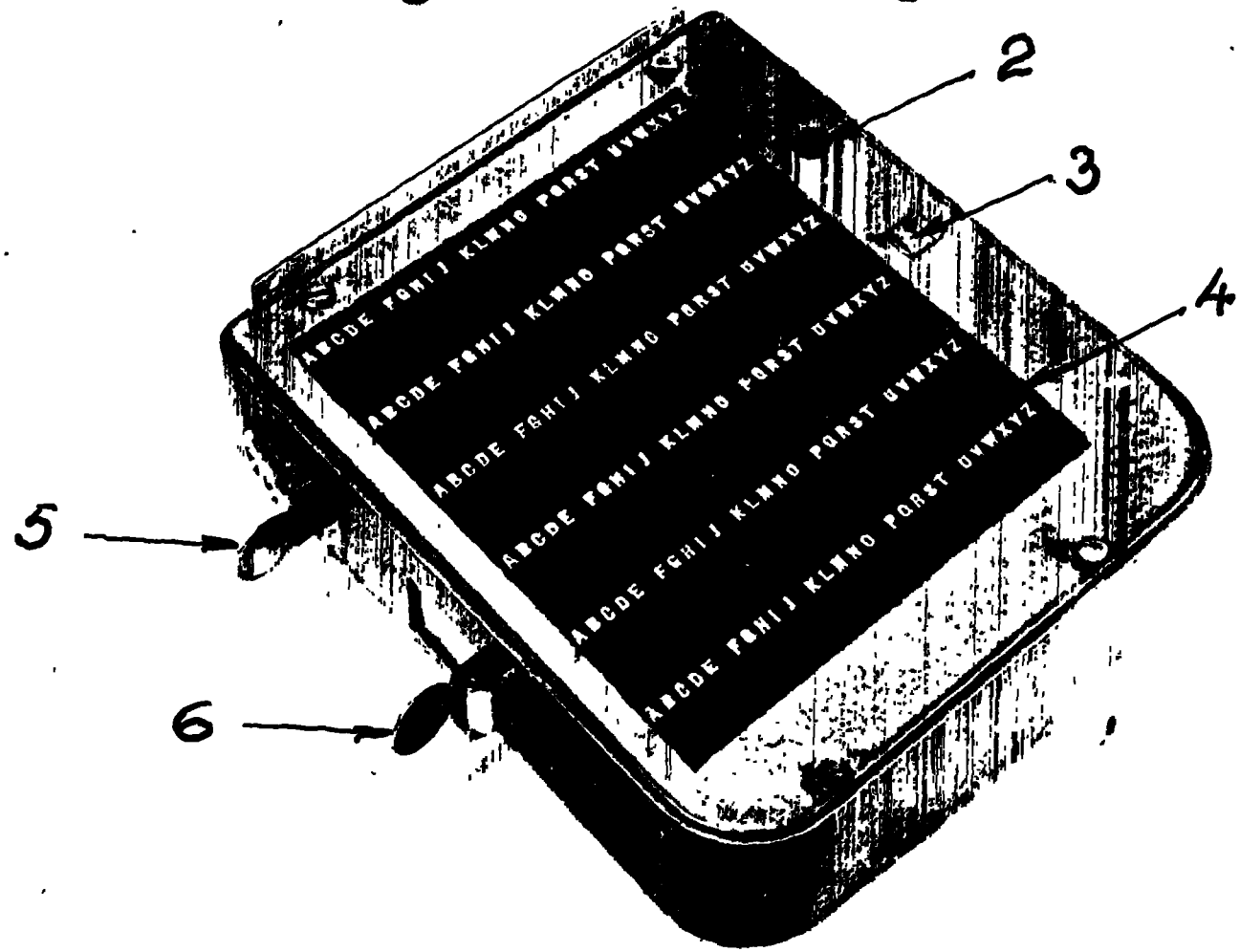


Fig. 2

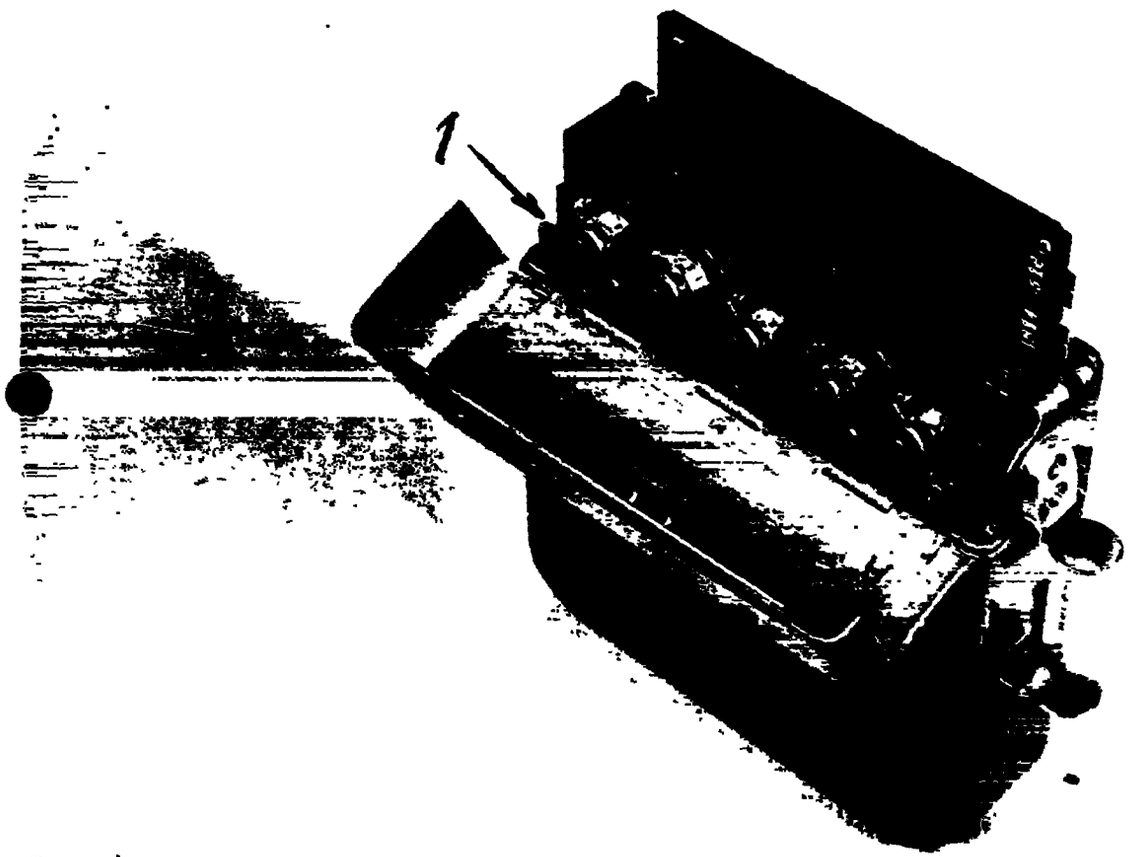
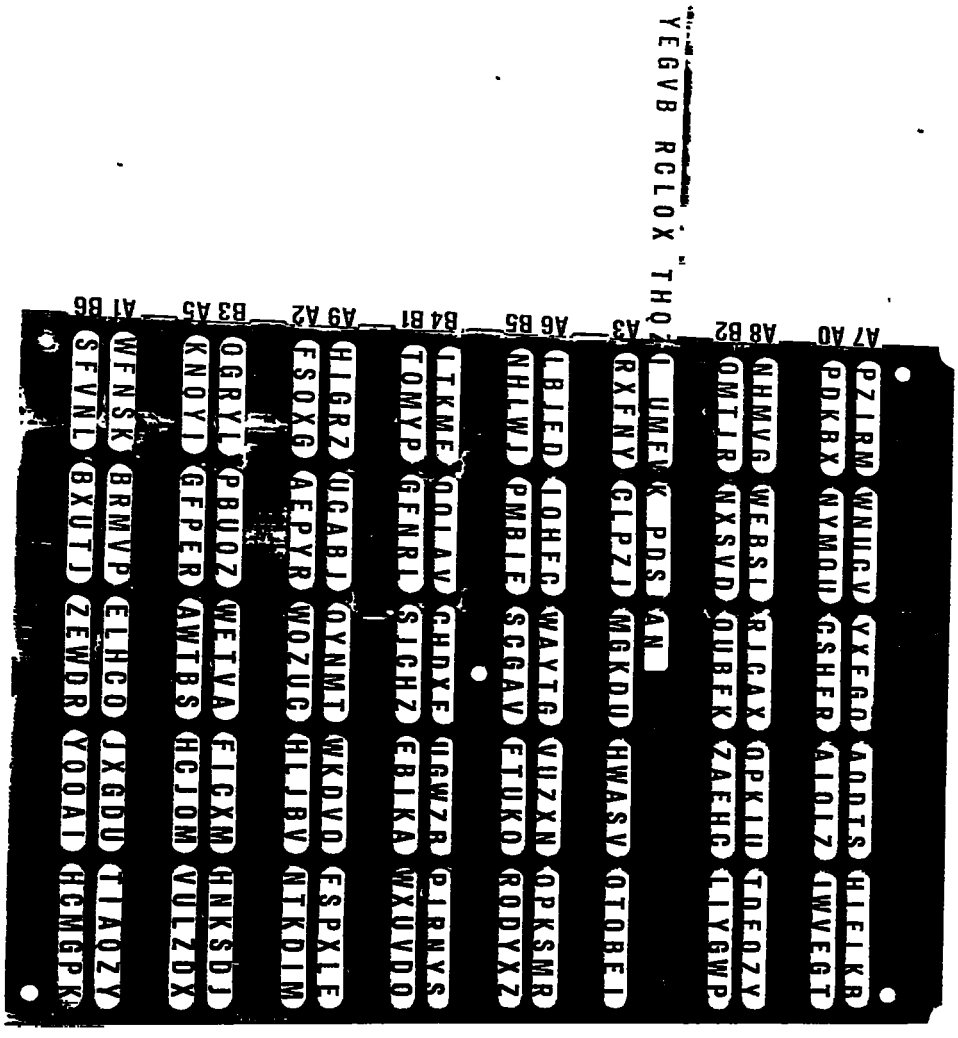


Fig. 3



A2 FSOXG AEPYR WQZUC HLJBV NTKDIM

B2 QMTJR NXSVD OUBFK ZAEHC LIYGWP

Fig. 4

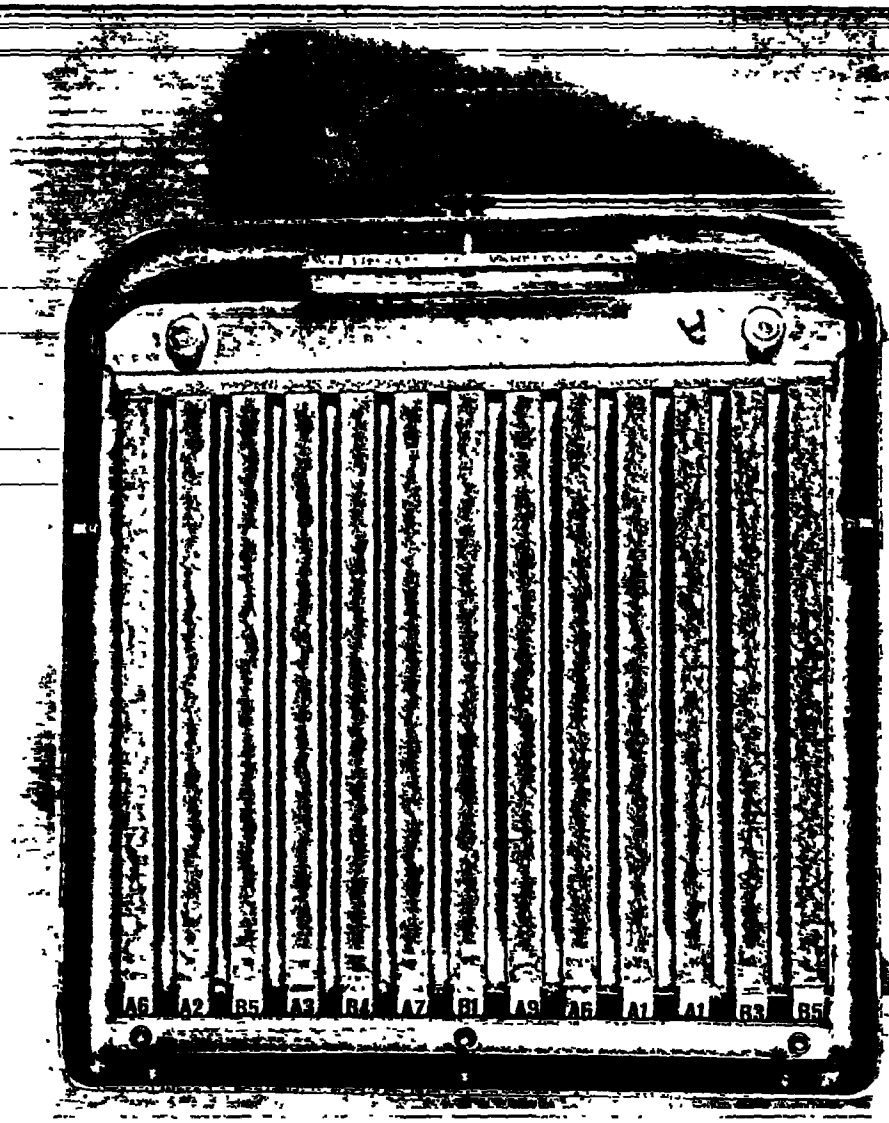


Fig. 5