April 14, 1936

MEMORANDUM TO: Mr. Rowe.

I am attaching hereto a revised draft of specifications and drawings covering the hand-operated cryptographic device which was originally forwarded to you about July 6, 1935, for the preparation of patent specifications.

William F. Friedman.

Attached:
Draft of specifications
Drawings

Copy for Mr. Friedman

This invention relates to cryptographic devices and has for its object the provision of a hand-operated device capable of affording a relatively high degree of security without involving the use of complicated mechanisms.

Another object is to provide a device useful in cryptographic and crypt-analytic investigations requiring the use of sliding alphabets.

The invention is explained in connection with four figures. Figure 1 is a front and side elevation of one embodiment of the device; Figure 2 shows a single section of another form of the device; Figure 3 shows a base; Figure 4 is a top view of a second embodiment of the device.

Referring to Figure 1, in this embodiment the device consists of a base, 1, on which are horizontally fastened a series of cylindrical rods, 2, forming a set of channel ways, 3, into which paper strips, 4, may be inserted and slid from left to right or vice versa. In the specific embodiment disclosed herein the device comprises 25 such channel ways, but the device is by no means limited to this number. The number chosen in this embodiment is merely a convenient number, and it may be increased or decreased within certain limits in other embodiments without materially departing from the basic nature of the device. A rule, or reading guide, 5, attached to a reading guide slide, 6, can be slid

to the left or right on a reading guide slide rail, 7. End bars, 8 and 9, serve as stops against which the reading guide 5 can be brought at the end of its travel to the left or right. To the back of the base 1 is fastened a hinged supporting frame, 10, which can be pulled out to support the device in a slanting position as it rests upon a table, desk, or other plane surface. Or, if the operator prefers to lay the device flat upon the table, the rubber feet, 11, at the four corners of the bottom of base 1 will support the device and keep it from sliding about on the table.

As stated above, into the channel ways 3 there are inserted strips of paper 4 hereinafter called alphabet strips, upon which appear sequences of letters of the alphabet, each sequence being repeated on the strip, and the letters being equidistant from one another throughout. The purpose of the duplication of sequence will appear presently. The letters on the alphabet strips may be in normal order or in disarranged order; if the latter, the various alphabets may or may not be different. Assuming, however, different alphabets are being used, each strip bears an identifying mark such as a number, 12, so that the alphabet strips may be inserted into the channel ways C according to some preagreed key. For example, in Figure 1

is shown a set of 25 channel ways into which 25 different alphabet strips 4 have been inserted according to the following key, reading from the top downward:

14-16-9-6-22-25-23-5-12-24-13-21-18-1-7-17-20-19-15-8-11-2-3-10-4

If another embodiment of the device should include more than 25 channel ways, additional alphabet strips may be inserted, according to a longer key.

Having inserted the alphabet strips into the channel ways in key order, the device is now ready for use either to encipher a plain language message or to decipher a cryptogram which has been enciphered by means of the device, alphabets, and key shown in Figure 1. Suppose this plain-text message is to be enciphered:

ACCORDING TO AN OFFICIAL REPORT FROM MILITARY AUTHORITIES . . .

Moving the reading guide 5 to the left, and bringing it against the left end bar 8, the operator proceeds to align, in a column immediately to the right of the reading guide, the first 25 letters of the message. This is most conveniently done by placing the eraser end of a pencil upon the successive desired letters as found on the successive alphabet strips 4

from the top downwards, and pulling or pushing the alphabet strips in their channel ways toward the reading guide so that each strip stops with the proper letter just to the right of the right-hand edge of the reading guide 5. When the alphabet strips are being aligned on the left-hand side of the device, as in the above procedure, the operator confines his search for letters to the left-hand half of the duplicated sequence on each alphabet strip.

When all 25 alphabet strips have been aligned as indicated, there is disclosed a multiplicity of columns of letters to the right of the plain-text column of letters thus aligned. All these columns of letters, except one, are columns of cipher letters, each column representing a cipher equivalent of the plain-text column. The single exception is the column which is the 25th removed from the plain-text column set up by the operator, and is merely a repetition of that plain-text column. One of these cipher columns is selected at random and is recorded in 5-letter groups. The reading guide 5 is useful in this operation, since by placing it alongside the column selected, reading of the cipher column is facilitated. Suppose that the reading guide 5

is moved so that its left-hand edge aligns a column of cipher text. These letters are recorded and constitute the cipher letters for the first 25 plain-text letters.

The reading guide 5 is now moved to the extreme right of the device, up against the right end bar 9; the next 25 letters of the plain text are aligned against the left edge of the reading guide 5. Again a set of columns of cipher letters are disclosed to the left of the reading guide. One of these columns is selected at random and again a set of 25 cipher letters representing the second set of 25 plain-text letters is recorded. If the message contains more than 50 letters, the foregoing procedure is repeated until the entire message has been enciphered. There is no need to indicate to the recipient of the message which column is selected for the cipher equivalent of each set of 25 plain-text letters, as will be noted presently.

To decipher the message, having the alphabets and the key according to which they have been arranged, the operator merely proceeds as in encipherment, aligning the alphabet strips in their channel ways so that the first 25 cipher letters of the cryptogram are in one column. He then

examines all the other 25 columns of letters, looking for one which contains intelligible text throughout its extent from top to bottom. There will be one and only one such column, and this will be the plain-text equivalent of the column of cipher text set up on the device. The reading guide 5 is useful in this search for the plain-text column, as it can readily be moved to scan the successive columns from left to right, or from right to left. The plain-text column thus found is recorded in word lengths and the operator proceeds to set up the next 25 cipher letters on the right-hand side of the device. Again he looks for a plain-text column and records it when found. He continues this process until the message has been completely deciphered.

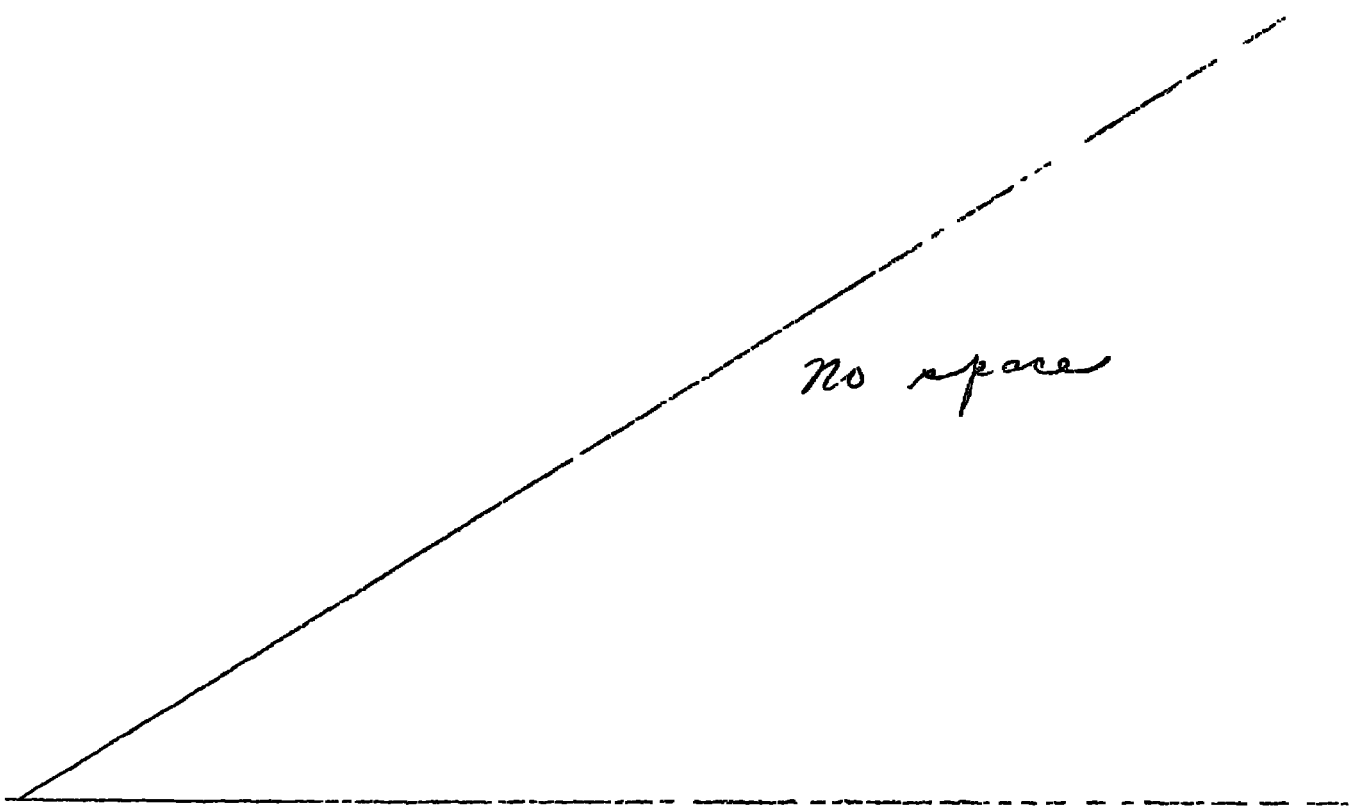
Although in the figures accompanying this description a device is shown in which cylindrical rods are riveted to a base at regular intervals from one another to form the channel ways into which the alphabet strips are inserted, it should be understood that any other means may be employed to form the channel ways. For example, a series of elongated metal strips known in the trade as "card holders", used ordinarily to hold narrow strips of paper bearing names of mail-box owners in apartment

houses, etc., may be used to form the channel ways; these card holders may be riveted to the base, or spot welded to it, or attached in any other suitable manner. Or, the channel ways may be formed by milling grooves in the base 1 itself, which may be made of molded bakelite, for example. In such case the grooves are made by a rotating cutter which undercuts at the two edges, forming a channel way such as is commonly found in slide-rules. Figure 2 shows such a section in the form of a piece of bakelite or similar material, 13, in which five such channel ways 3 have been cut. Sections with equal or unequal numbers of channel ways may be easily provided and given identifying symbols such as letters, A, B, C, ...

In Figure 3 there is shown a base suitable for use with such sections of channel ways. Thus, instead of having all the channel ways on a single base, as is the case in Figure 1, the base is merely made in the form of a flat surface onto which sections of channel ways may be positioned and temporarily fixed, so that rearrangements of sections can be made according to subsidiary keys. Referring to Figure 3, the base 1 is a plane surface across which has been cut a slot, 14, for carrying a sliding clamp, 15, provided with a knurled thumb screw, 16, for fastening the clamp into position. End bars 8

and 9 elevated above the base by supports, 17, and back stop, 18, serve the same purpose as similarly designated end bars of Figure 1.

Using a base such as that shown in Figure 3, with several sections such as that shown in Figure 2, one method of operation of this embodiment of the invention is shown in Figure 4. In that figure there are five sections of 3, 4, 5, 7 and 8 channel ways, giving a total of 27. First, the sections are temporarily fastened to the base in the alphabetical order of their identifying symbols. Then the 27 alphabet strips would be



inserted in the 27 consecutive channel ways according to the predetermined numerical key already referred to above in connection with Figure 1. [illegible] To encipher a given message, there would then be a subsidiary or specific key, also arranged for in advance by means of an indicator in the message, which would direct that the sections be now placed onto the base in a mixed order, say E - D - A - B - C, as shown in Figure 4. The encipherment of a message would then proceed exactly as before. In another message, the indicator for the sectional arrangement might be different, say one calling for the sequence of sections D - A - C - E - B. Thus, with five sections there could be 120 different arrangements of sections on the base, even though only one set of [illegible] alphabet strips is employed. The purpose of this is, of course, to increase the keying possibilities of the device, and to impart uniqueness to successive messages, without going to the trouble of making a complete rearrangement of all [illegible] alphabet strips in the set of [illegible] channel ways.

~~In Figure 5 the sections of channel ways comprise equal numbers of~~ ~~[illegible] but this is, of course, not an essential feature. Sections~~ ~~containing [illegible] up to any [illegible] channel ways are perfectly~~ ~~possible, and would give increased cryptographic security by rearrangement.~~

The many uses of this device, with variable alphabets, in cryptographic or cryptanalytic studies will be apparent to all skilled in the art and nothing further need be said on this score except that there has existed for many years a hitherto unfulfilled need for a simple device of this type, suitable for the insertion of sliding alphabets.

1. A cryptographic device consisting of a base upon which is provided a plurality of channel ways in which strips of character-bearing material may be inserted and slid into alignment.

2. A cryptographic device consisting of a base upon which is provided a plurality of channel ways in which strips of character-bearing material may be inserted and slid into alignment, the channel ways being open at both ends.

3. A cryptographic device consisting of a base upon which is provided a plurality of channel ways in which strips of character-bearing

material may be inserted and slid into alignment, and a slidable guide rule for making excursions transversely across the channel ways.

4. A cryptographic device consisting of a base with a hinged support rest attached to the reverse surface of the base; a plurality of members fixed to the obverse surface of the base at equidistant intervals to form a plurality of channel ways for the insertion of character-bearing strips bearing alphabetic sequences; solid members fixed at opposite ends of the channel ways and resting upon the members forming the channel ways; and a guide rule attached to a sleeve permitting the guide rule to be slid transversely across the channel ways.

5. A cryptographic device consisting of a base; a plurality of grooved members providing channel ways for the insertion of slidable, character-bearing strips, said grooved members bearing distinguishing symbols to differentiate one from another and containing one or more said channel ways; means for temporarily fixing said members to the base in linear juxtaposition to afford series of juxtaposed channel ways; end members attached to said base transversely to the direction in which the channel ways extend and raise above the ends of the channel ways so as to provide stops against

which an instrument is brought at the end of its travel in setting up letters for enciphering and deciphering; and a slidable guide rule movable transversely across the channel ways.

6. A cryptographic device of the character specified in Claim 5, in which said grooved members contain equal numbers of channel ways.

7. A cryptographic device of the character specified in Claim 5, in which said grooved members contain unequal numbers of channel ways.

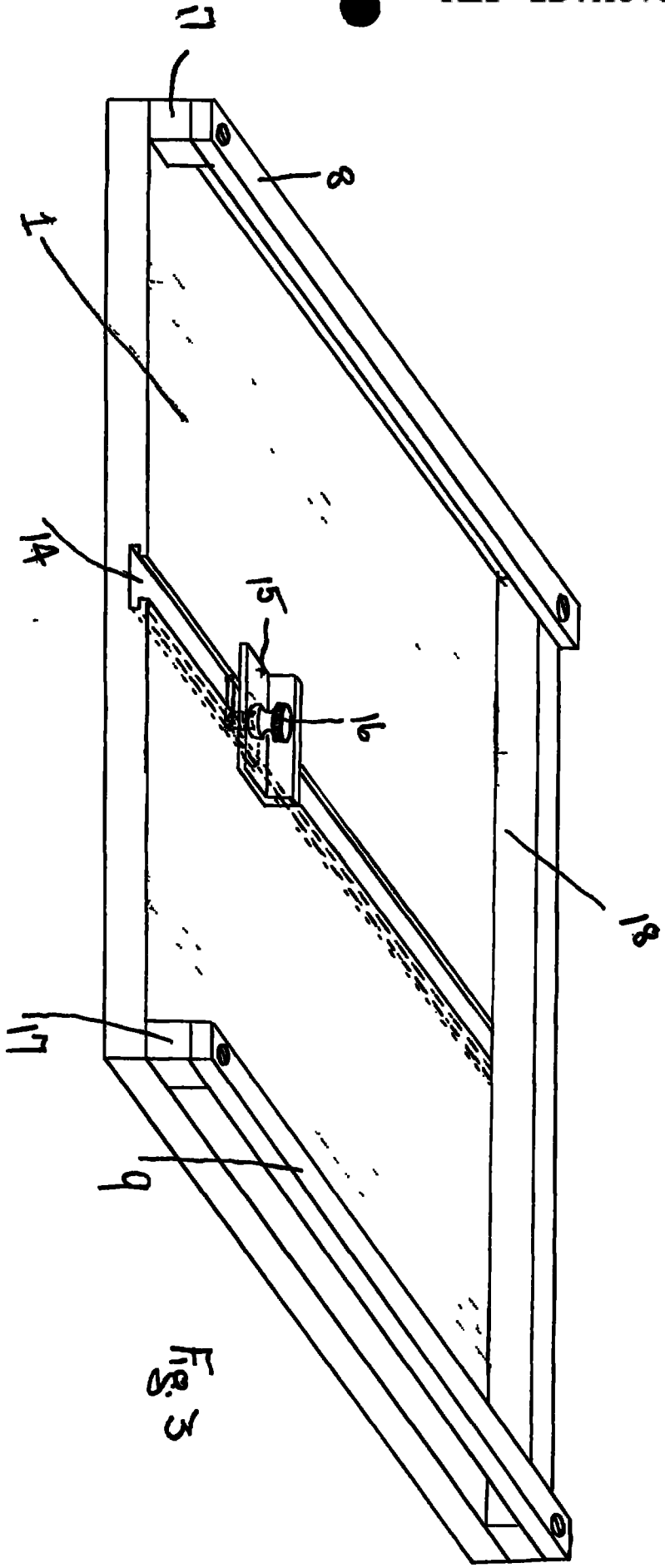
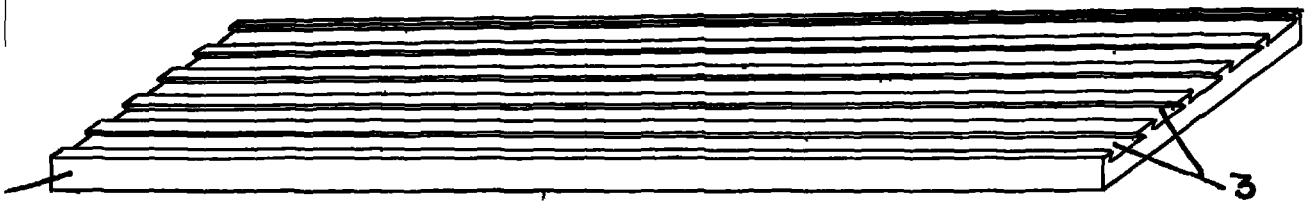


Fig. 3

Fig. 2

13


3

REF ID:A67560

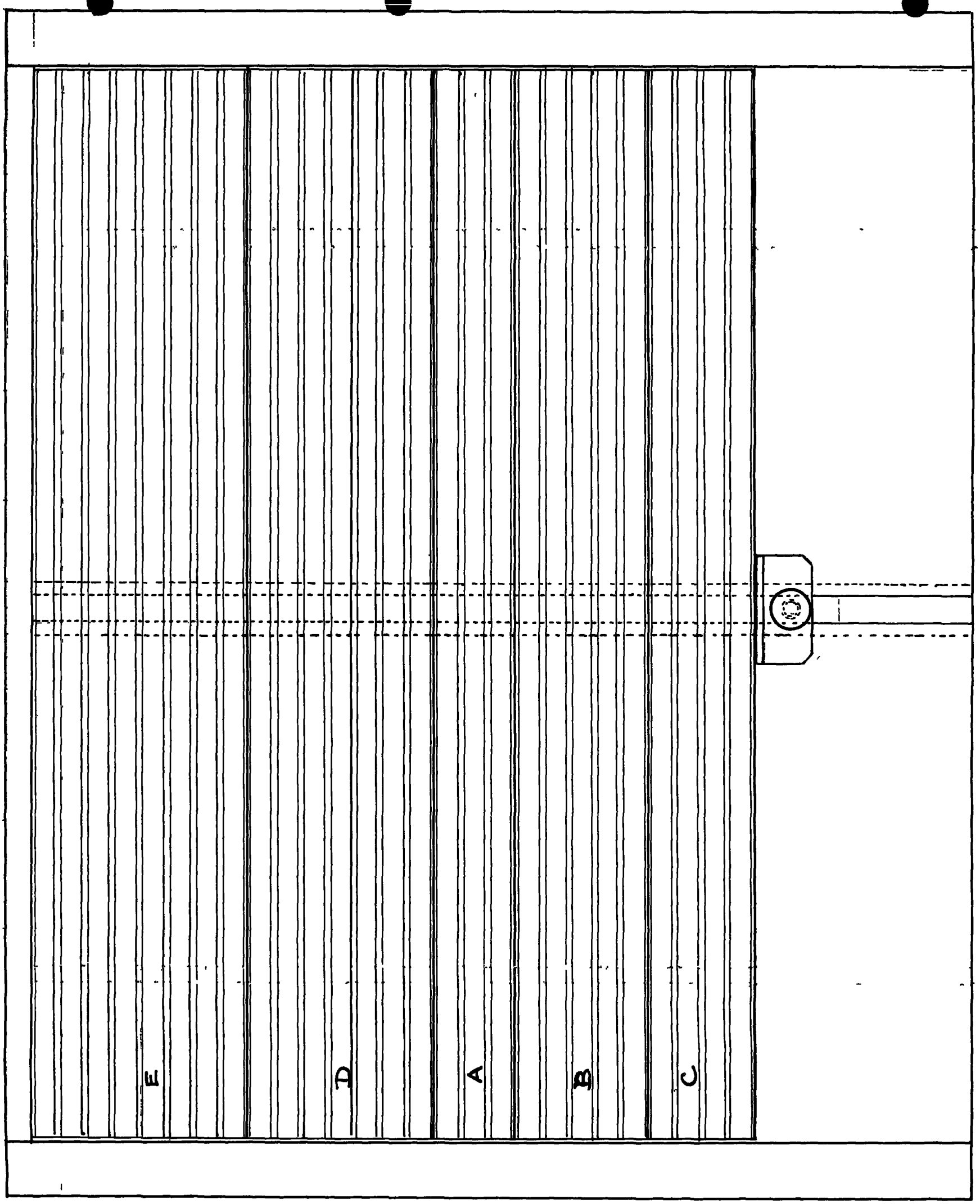


Fig 4

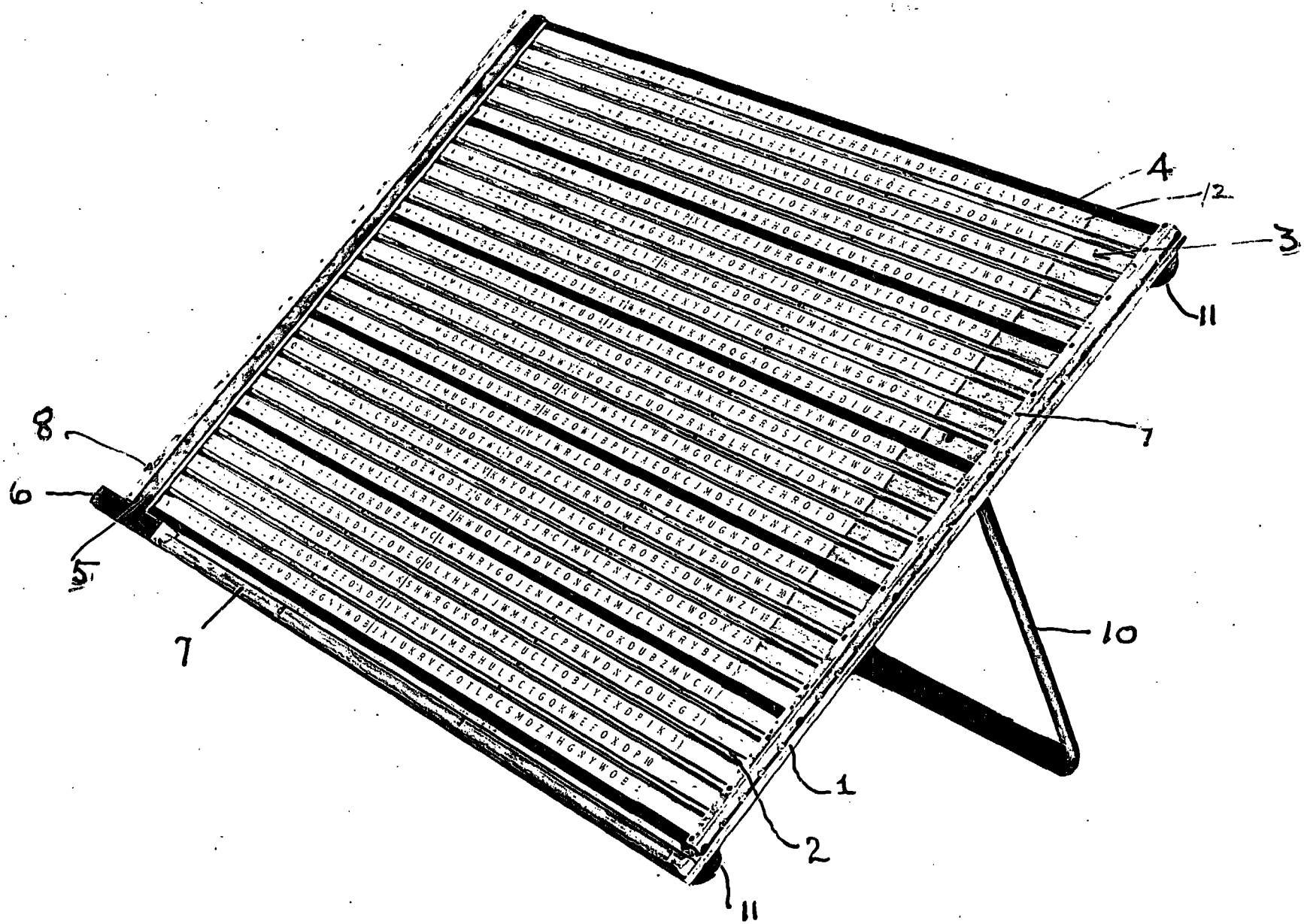


Fig. 1.