Feb. 27, 1973 A. W. SMALL 3,718,349

CIPHER DEVICE AND METHOD

Filed April 6, 1954 2 Sheets-Sheet 1

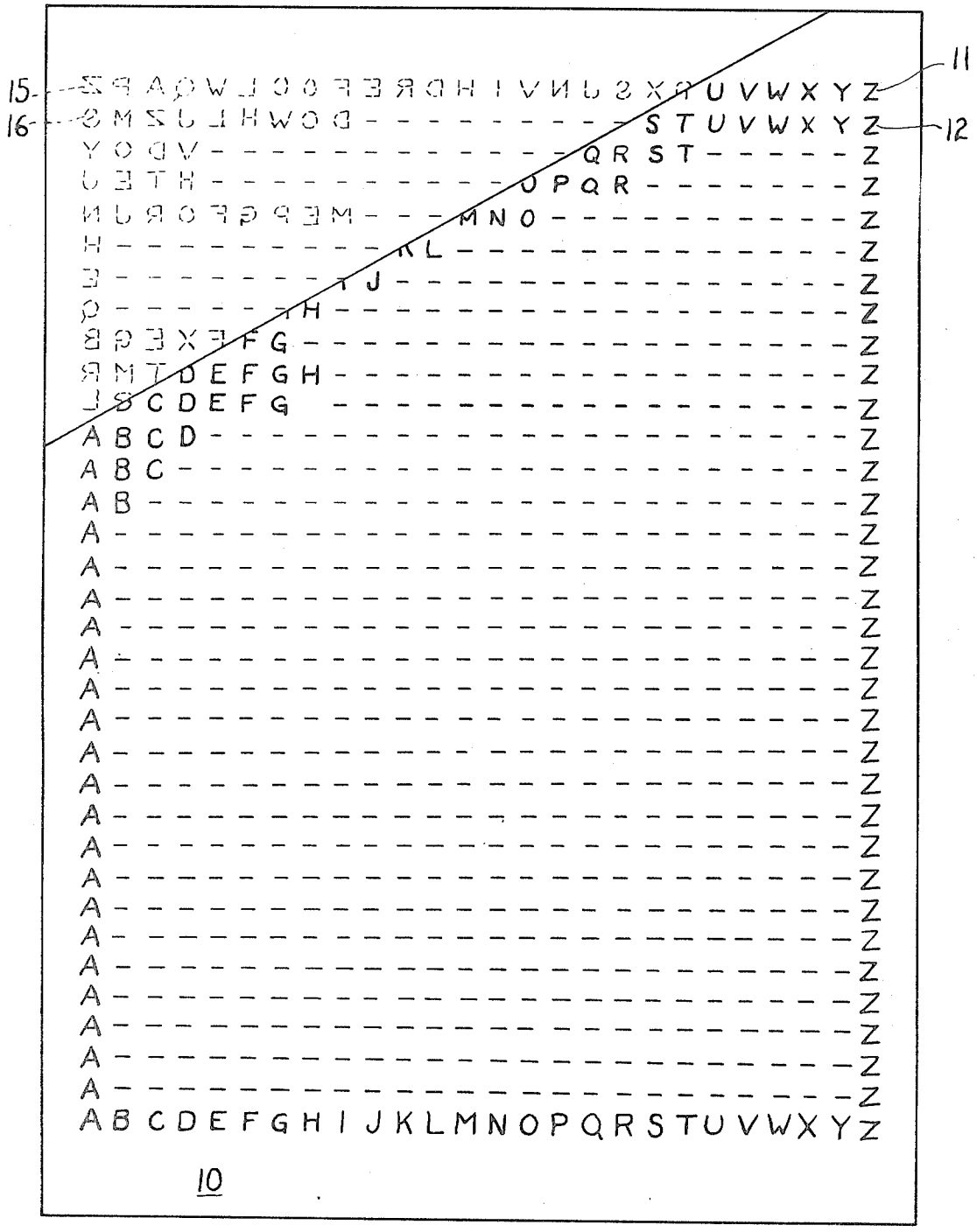

FIG 1

ALBERT W. SMALL

BY Henry K. Stauffer

HIS ATTORNEY

CIPHER DEVICE AND METHOD

Filed April 6, 1954 2 Sheets-Sheet 2

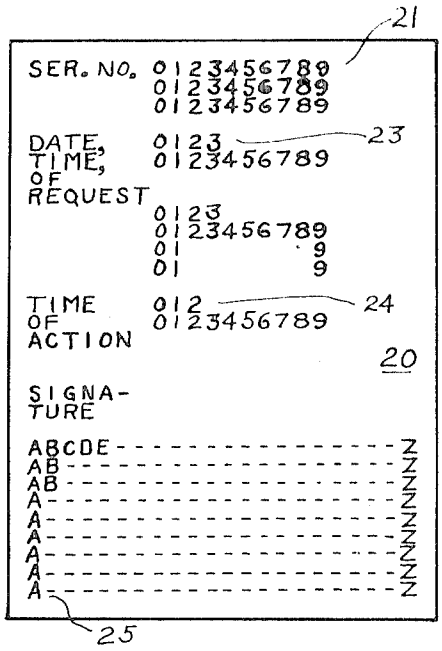

FIG. 2

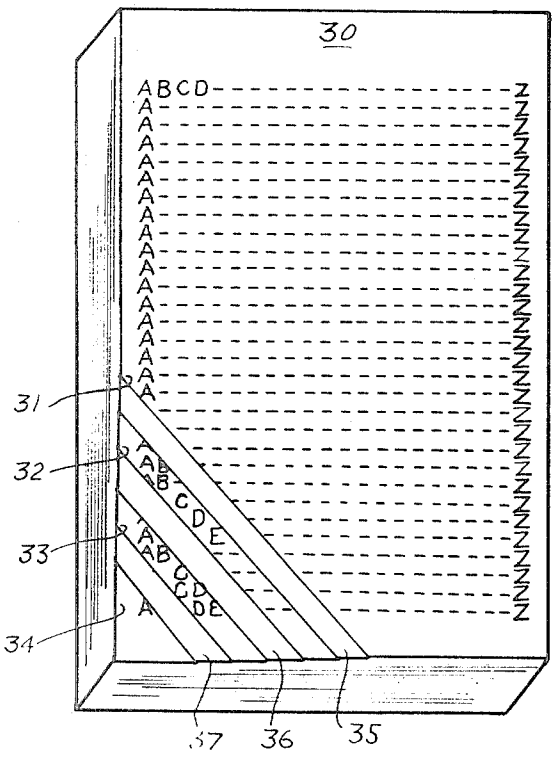

FIG. 3

ALBERT W. SMALL

BY Henry J. Stauffer

HIS ATTORNEY

United States Patent Office 3,718,349 Patented Feb. 27, 1973

3,718,349

CIPHER DEVICE AND METHOD

Albert W. Small, 5803 Greentree Road, Bethesda, Md. 20014

Filed Apr. 6, 1954, Ser. No. 421,459
Int. Cl. G09c 1/02, 5/00
U.S. Cl. 283—17 4 Claims

This invention is in cryptography and specifically is a device for simplifying certain crystographic operations.

Notwithstanding progress in the art of cryptography (as illustrated in many issued patents) whereby the bulk of secret communication is carried on by means of machines which more or less automatically encipher messages as the same are typed or fed into machines, and automatically decipher as cryptograms are fed thereinto, a field of usefulness remains for simple, hand-operated devices, or manual systems in which any paraphernalia necessary can be carried on the person or at worst stored or hidden in small compass. It is to this latter class of cryptographic devices that the present invention appertains.

The principal object of the invention is to provide simple and novel means and a method for performing certain cryptographic operations.

Broadly speaking, two principal schemes for encipherment of clear text are known: intransposition encipherment, the letters (or other indicia) of which the clear-text message is composed are shifted from place to place within the message according to some rule known to the addressor and addressee, so that their original order is not ascertainable to an interceptor, although their identities are not changed; in substitution encipherment, the order of the textual elements is not changed, but some or all of them have other apparently-unrelated textual elements substituted therefor before transmission.

The present invention has special reference to substitution encipherment.

In the drawings, FIG. 1 illustrates one embodiment of my cipher device, FIG. 2 shows a modification thereof, and FIG. 3 shows a different form of my invention.

With reference to the drawing, and particularly FIG. 1 thereof, **10** represents a sheet of paper or other convenient material upon which indicia can be readily written, printed or in some other fashion inscribed.

Upon the obverse of sheet **10** may be seen a plurality of alphabets, **11** and **12**, for examples, the number thereof normally depending upon the size of the sheet, legibility requirements, etc., and not being otherwise critical.

Alphabets **11** and **12** as well as all the others, are shown in standard English, and this is the preferred arrangement, although alphabets in reversed or mixed order might be used without departing from the spirit of the invention.

The upper surface of sheet **10** has been removed at the top left thereof; this is for purposes of illustration only, and is not significant to the invention, although, as will be understood from the description, a sheet, as **10**, can in fact easily be formed of two sheets fastened together with suitable adhesive or by other means.

On the reverse of sheet **10** may be seen other alphabets, as **15** and **16**. These should be mixed, or reversed, relative to alphabets **11** and **12**, or at least many of them should be.

It is important that the alphabets on the reverse of sheet **10**, as **15** and **16**, be substantially in register with the alphabets on the obverse of the sheet, line for line and letter, for letter, although certain advantages will accrue if the registration is not in fact exact.

In performing an enciphering operation with this invention, the user employs a stylus of some description, conveniently a pencil point. If the first word of his clear

text message should be "ENEMY," he would normally utilize alphabet **11** (the first at the top of his sheet), and puncture the paper at the location of the "E" therein; he would then proceed to alphabet **12**, and puncture the paper at the location of the letter "N." He would continue down the sheet in this fashion until he had finished his message, and might, of course, have to use additional sheets of the same general nature.

He would then turn over sheet **10** and write out his enciphered message by inscribing the letters (or other indicia) occurring on the reverse thereof at the several puncture points.

Further complications can be introduced, of course, such as utilizing the alphabets on one side or the other of sheet **10**, or on both sides thereof, in something other than normal order; this would have to be according to prearrangement with an addressee.

Furthermore, it should be clear that, except for extremely brief communications, it will be desirable to prepare the sheets **10** in tablets or packages, and in such case, the sheets should reasonably be serially numbered.

The addressee of the message must be provided with an alphabet sheet identical with sheet **10**, or with a tablet like that used by the addressor. Assuming this to be the case, a message can readily be deciphered: the enciphered text is used as the control, and the sheet (or sheets) punctured from the back rather than the front. Clear text is then read from the front of the sheet.

Referring for a moment to the mention above made relative to registration of the obverse and reverse alphabets, it will be desirable in some circumstances to provide a deliberate offset. This will not be harmful in any case if the correspondence between alphabets is clear; it will be particularly helpful if the printing should be small, and the lines closely spaced.

This follows, of course, from the possibility otherwise that, in piercing through a small, printed, clear-text, letter (with a pencil point, for example), the cipher equivalent might be obliterated or obscured.

FIG. 2 shows a modified form of the invention wherein the sheet **20** (corresponding to sheet **10** of FIG. 1) is arranged for a particular kind of routine messages.

The sheet can be seen to include a group of lines of numbers, as **21**, a further group of lines of numbers, as **23**, a still further group of lines of numbers, as **24**, and a series of alphabets, as **25**. Each group of indicia is identified by a legend, as "Ser. No." Sheets made up in this fashion, particularly, should be bound into pads, and are especially useful when a large number of brief messages identical in form, are envisioned, since, by prearrangement between addressor and addressee, the various identifying legends can be disregarded, and the successive cipher groups deciphered by applying them to the successive categories on the sheet.

It will also be clear from FIG. 2 that the indicia utilized in my invention need not be in the nature of literal alphabets, that, on the other hand, they may be numerical; they may, in fact, be made up of arbitrary symbols.

FIG. 3 shows a pad **30** made up of a number of sheets, **31**, **32**, **33**, and **34**, for examples, each analogous to sheet **10** of FIG. 1, and each bearing a series of alphabets as already described. The reverse of each sheet, as before, bears a similar series of mixed alphabets (not shown). In this form of the invention the corresponding alphabets on obverse and reverse preferably are in exact registration, line for line, and letter for letter.

Beneath sheet **31** of the pad **30** is a sheet of carbon paper **35**, and similar sheets, as **36** and **37**, may be seen similarly arranged beneath the other alphabet sheets.

The several sheets of carbon paper, it should be understood are not utilized in accordance with normal practice, but are instead turned over, or reversed, so that the pigmented side lies uppermost, and thus in contact with the reverse of the various alphabet sheets.

In this embodiment of the invention a user does not puncture the paper as above described, but instead merely encircles, cancels, or makes some other appropriate mark adjacent the various clear text symbols. It will immediately be understood that the cipher text symbols, due to the reversed carbon paper beneath, are encircled, cancelled, etc.

A desirable arrangement under some circumstances is to use but one sheet of carbon paper, repositioning the same after each alphabet sheet is used; otherwise, if the sheets are of light weight paper, more than one may be marked as a result of pressure on the uppermost sheet.

Decipherment can be accomplished as described in connection with FIG. 1, that is, by puncturing from the reverse of a pad, or an appropriate sheet of alphabets may be laid face down upon a reversed sheet of carbon paper and treated in the fashion of FIG. 3.

Advantageously, however, reciprocal alphabets can be utilized in all forms of the invention, it being understood that reciprocal alphabets are those in which the plain and cipher equivalents are not randomized but are prearranged in the following fashion:

(PLAIN) ABCDEFGHIJKLMNOPQRSTUVWXYZ
(CIPHER) CNAYJWSUTEMXKBQROPGIHZFLDV

An inspection will show that in this pair of alphabets, C (plain) equals A (cipher) and also that A (plain) equals C (cipher), and that all other plain and cipher equivalents are similarly related.

If such alphabets are used, the various sheets of any of the embodiments above described may be used for decipherment as well as for encipherment by puncturing, encircling, etc. from the obverse side, that is, just as the sheets occur on the pads, and need not be torn off before hand and reversed.

The invention has been described in specific terms and modifications will occur to those skilled in the art. For the true scope of the invention, therefore, reference should be had to the appended claims.

I claim:

1. A cipher device comprising a sheet having obverse and reverse surfaces, a plurality of plain text alphabets comprising characters on one surface thereof and a plurality of cipher test alphabets comprising characters on the other surface thereof each character of each alphabet on said one surface having a substantially registering character of an alphabet on said other surface.

2. A cipher device comprising a plurality of sheets each bearing a plurality of alphabets on one side thereof and a plurality of reciprocal alphabets on the other side thereof in character-for-character registration therewith and duplicating means for marking the reverse of each sheet responsive to pressure on the obverse thereof.

3. The method of preparing a cryptographic message which includes inscribing on one surface of a sheet a succession of plain text alphabets, inscribing on the other surface of said sheet a succession of cipher text alphabets the characters thereof being in registration with the characters of said plain text alphabets, backing said sheet with a reversed sheet of carbon paper, and marking successive characters of clear text on the successive alphabets on said one surface of the sheet thereby to indicate by corresponding marks on the reverse of the sheet successive cipher text characters.

4. The method of preparing a cryptographic message which includes inscribing on one surface of a sheet a succession of plain text alphabets, inscribing on the other surface of said sheet a succession of cipher text alphabets in registration with said plain text alphabets, and marking by perforation successive letters of clear text in the successive alphabets on said one surface of the sheet thereby to indicate on said other surface of said sheet successive letters of enciphered text.

References Cited

UNITED STATES PATENTS

1,579,471	4/1926	Capony	283—62
1,586,628	6/1926	Lautherbach	35—48
1,705,657	3/1929	Clapp	35—48
1,984,726	12/1934	Brownlee	35—12
2,060,190	11/1936	Foster	41—31.5
2,614,338	10/1952	Clark	35—42

FOREIGN PATENTS

745,578	2/1933	France	283—17

SAMUEL FEINBERG, Primary Examiner

J. M. HANLEY, Assistant Examiner

U.S. Cl. X.R.

35—2; 283—6, 11