

Nov. 29, 1938.

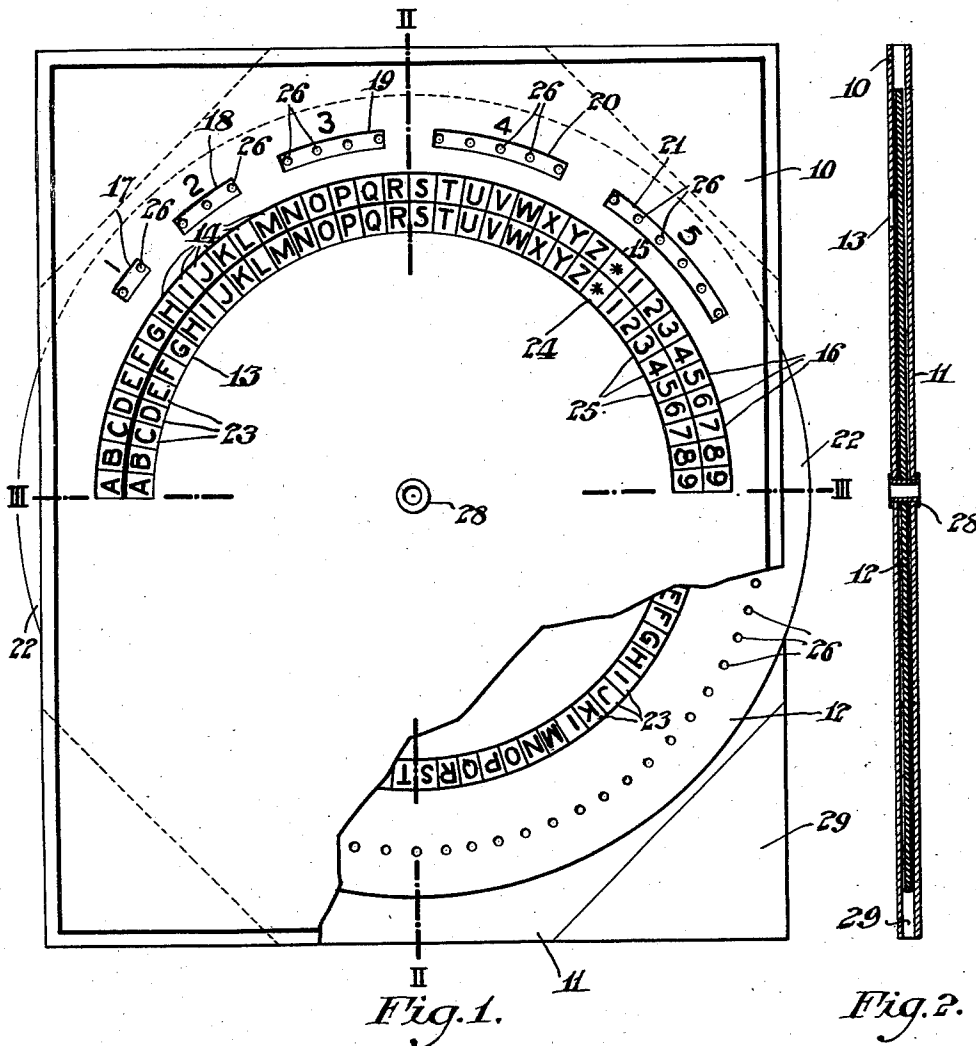
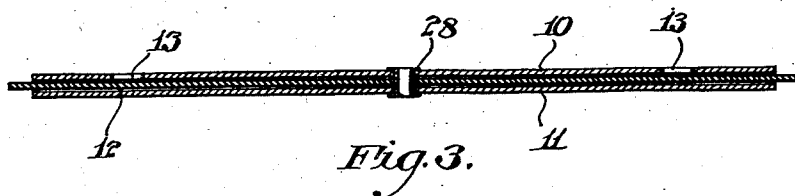
J. C. WOBENSMITH

2,138,532

CRYPTOGRAPHIC DEVICE

Filed Sept. 11, 1935

2 Sheets-Sheet 1



Inventor:
James C. Wobensmith,
By *3. T. Wobensmith*
Attorney.

Nov. 29, 1938.

J. C. WOBENSMITH

2,138,532

CRYPTOGRAPHIC DEVICE

Filed Sept. 11, 1935

2 Sheets-Sheet 2

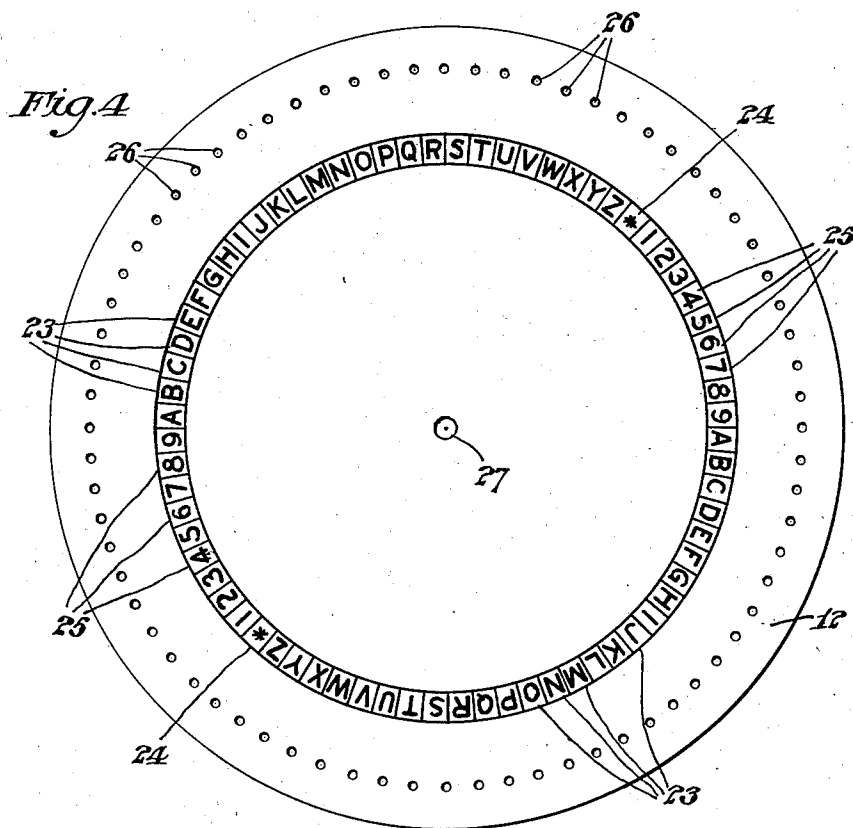
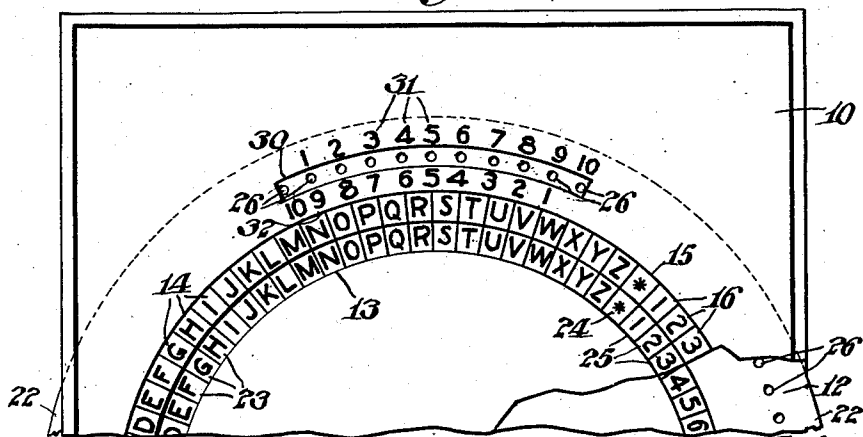


Fig. 5.



Inventor:
James C. Wobensmith
By *J. T. Wobensmith*
Attorney

UNITED STATES PATENT OFFICE

2,138,532

CRYPTOGRAPHIC DEVICE

James C. Wobensmith, Philadelphia, Pa.

Application September 11, 1935, Serial No. 40,170

15 Claims. (Cl. 35—2)

The present invention relates to cryptographic devices, and more particularly to an improved coding and decoding device which is simple in construction. The invention particularly contemplates a cryptographic device which may be used for coding and decoding messages with greater facility than has heretofore been possible, and by means of which cryptographic messages may be made up which are virtually impossible of solution without knowledge of the program used.

The invention further contemplates a cryptographic device which is adapted for use with a complicated program of character shifting. Other features will appear from the specification and claims.

The nature and characteristic features of the invention will be more readily understood from the following description, taken in connection with the accompanying drawings forming part hereof, in which:

Fig. 1 is a top plan view, partly broken away, of a preferred embodiment of the invention;

Fig. 2 is a vertical central sectional view taken approximately on the line II—II of Fig. 1;

Fig. 3 is a vertical central sectional view taken approximately on the line III—III of Fig. 1;

Fig. 4 is a plan view of a disk or dial forming part of the present invention; and

Fig. 5 is a fragmentary plan view of a modified form of the invention.

It will, of course, be understood that the description and drawings herein contained are illustrative merely, and that various modifications and changes may be made in the structure disclosed without departing from the spirit of the invention.

Referring more particularly to the drawings, it will be seen that there is provided an upper cover sheet or plate 10, a lower sheet 11, and a disk 12. The upper cover sheet 10 has a semi-circular opening 13 extending therethrough. Characters corresponding to the letters of the alphabet as at 14, a space symbol or designation as at 15, and numerals as at 16, are disposed radially adjacent an outer edge of the opening 13. While these characters have been shown in their ordinary sequence, it will, of course, be understood that any other preferred arrangement or grouping may be employed. Each of the characters corresponds to an angular unit for cooperation with other indicia as hereinafter pointed out. A plurality of slots of predetermined angular length to correspond to the characters on the upper plate 10 and the disk 12, is also provided. The slot 17 is preferably one angular unit in

length, the slot 18 two angular units, the slot 19 three angular units, the slot 20 four angular units, and the slot 21 five angular units.

The disk 12 preferably extends beyond the edges of the upper and lower cover sheets, as shown at 22, for facilitating the turning of the disk 12 by hand. If desired, however, the disk 12 may be completely within the edges.

The disk or dial 12 is provided with characters which may comprise the letters of the alphabet as at 23, a space symbol or "stop" designation as at 24, and numerals as at 25, although it will, of course, be understood that if desired, the numerals 25 and space symbol 24 may be omitted and the characters may be arranged in any desired sequence.

The indicia on the disk 12 preferably are the same as those appearing adjacent the semicircular opening 13 except that they are repeated so that the characters in their desired sequence appear at least twice. The disk 12 is provided with a plurality of apertures 26 at a uniform distance from the center, the ring of apertures thus being concentric with the characters 23, 24, and 25. An aperture 26 is provided to correspond to each of the characters 23, 24, and 25 and thus with each angular unit, and is adapted to receive the point of a stylus or other instrument for turning of the disk 12. The disk 12 has a central bearing aperture 27 for rotatably mounting the same with respect to the top and bottom plates 10 and 11 by means of an eyelet, a rivet, or other suitable pivot device 28.

The upper and lower cover sheets 10 and 11 may be secured together in any suitable manner, but it has been found preferable to provide separating members 29 for insertion at the corners of the upper and lower sheets 10 and 11, these separating members 29 preferably being of greater thickness than the disk 12, and the sheets 10 and 11 being secured thereto by a suitable adhesive.

In the modified form of the invention, as illustrated in Fig. 5, in lieu of the plurality of slots 17, 18, 19, 20, and 21 in the top plate 10, a single slot 30 is provided, with suitable numerals and indicia disposed on either side thereof as a scale for guidance in shifting the disk 12. The numerals beyond the slot 30 may be arranged with the numbers 31 increasing toward the right and the numerals within the slot 30 may be arranged with the numbers 32 increasing toward the left.

The operation of the device will now be pointed out. In using the same for simple substitution cryptograms, the disk 12 is rotated to bring the characters thereon to the desired position with

respect to the characters on the upper plate 10. The message may then be encoded by substitution in the message of the characters on the disk 12 which are in radial alignment with the characters on the upper plate 10. A full set of the characters on the disk 12 may be seen through the semi-circular opening 13 in the upper plate 10. The decoding of such a message is effected by locating the character of the message on the disk 12 and then referring to the character corresponding thereto on the upper sheet 10.

The structure of the present invention is, however, capable of much broader use and a program involving a predetermined advance or retrogression of the disk 12 may be employed. The disk 12 is arranged at a predetermined position as for simple substitution cryptograms and thereafter the disk 12 is partially rotated through a desired number of angular units clockwise or counterclockwise, in accordance with the number of such units previously agreed upon. The character on the disk 12 corresponding to the character to be encoded may then be readily ascertained and written down. The turning of the disk 12 may be effected either by means of the portions 22 of the disk 12 which project beyond the upper and lower plates 10 and 11 or by inserting a stylus in an appropriate aperture 26 and moving the disk 12 the appropriate number of units, the length of the selected slot permitting this to be done rapidly and accurately.

A message thus made up may be decoded by locating on the disk 12 the character of the message and then referring to the corresponding character on the upper sheet 10 and then, after making the proper angular shift of the disk as in encoding, repeating the operation.

The structure of the present invention is, in addition, capable of use with a more or less complicated program which will render the cryptographic message virtually impossible to decode

without a knowledge of the program. The program will ordinarily comprise an initial setting, together with a sequence of different shifts to be made after each character is written down. The shifting may be done by inserting a stylus in the aperture 26 at one end of the appropriate slot and rotating the disk 12 in a predetermined direction through the requisite number of angular units.

In order to illustrate more clearly the manner in which the structure may be used for encoding a message, it will be assumed that a program has been agreed upon, which may be designated as "clockwise W-5-1-2", and that the message is as follows:

5.23 P. M. J. Q. Vandz struck my big fox whelp.

This message may, if desired, be analyzed prior to the encoding. The analysis in accordance with the program heretofore mentioned is as follows:

W512512 51251251251251251251251251251251
5.23 P. M. J. Q. Vandz struck my big fox whelp.

Such an analysis is not, however, essential since the program may be followed without specific reliance upon the analysis.

In following out the foregoing program, i. e. "clockwise W-5-1-2", the disk 12 is set with the character "W" thereof in radial alignment with

the character "A" on the upper cover plate 10. The character corresponding to the numeral "5" of the message is then ascertained from the disk 12 as "R". The disk 12 is now rotated five angular units clockwise by inserting a stylus in the aperture 26 at the left hand end of the slot 21 and moving the disk 12 around its axis until further movement is stopped by contact of the stylus with the right hand end of the slot 21. The character corresponding to the "period" or "stop" of the message is then ascertained to be "H".

The disk 12 is now rotated one angular unit by inserting the stylus in the aperture 26 at the left hand end of the slot 17 and moving the disk 12 clockwise on its axis until movement is stopped by contact of the stylus with the right hand end of the slot 17. The character corresponding to the character "2" of the message is ascertained to be "T".

The disk 12 is now rotated two angular units by inserting the stylus in the aperture 26 at the left hand end of the slot 18 and moving the disk 12 on its axis until movement is stopped by contact of the stylus with the right hand end of the slot 18. The character "3" of the message is ascertained to be "H".

The program is continued following the "5-1-2" clockwise sequence. To obtain the encoded character corresponding to the next character of the message the disk 12 is rotated five angular spaces by means of the stylus and the character corresponding to the space after the "3" is ascertained to be "9".

By following the program as heretofore set forth the message given above will appear in code, as follows:—

RH1H9X6N*YCSGLKDNZN44UQN018M3EEKQM1FMQSM2Y32C

If, in place of using the program heretofore given, the program given is "counterclockwise W-5-1-2" the message would appear in code as follows:—

RRUXZP2T8AYG8NOL5JB24Y438V4MDQUA117NYCGE42BKW.

It is preferable to leave the message in the form shown above but if desired, the characters of the coded message may be separated into groups, either of the same or a different number of characters, or to convey information as to the program, which will be more confusing to a person unfamiliar with the program. Such a separation will not make more difficult or affect in any manner the decoding of the message by one familiar with the program.

In decoding a message the program followed is very similar to that heretofore pointed out for the encoding. The initial letter setting is first effected and the characters of the message are located, after the proper angular movement has been made, on the disk 12 and from the disk 12, by reference to the corresponding characters on the upper sheet 10, the original message may be ascertained. The direction of rotation of the disk 12 for decoding is the same as for encoding and in the same sequence.

Of course, if desired, the agreed upon program may include certain movements of the disk 12 in a clockwise direction and others in a counterclockwise direction.

In the use of the device as shown in Fig. 5 of the drawings, instead of inserting the stylus

in the aperture 26 at one end of one of the slots 17, 18, 19, 20 or 21, as in Fig. 1, it is inserted in the aperture 26 opposite the number 32 corresponding to the desired shift, on the inside of the slot 30 if the disk 12 is to be shifted in a clockwise direction, and then shifting the disk 12 until the stylus encounters the right hand end of the slot 30. If the disk 12 is to be shifted in a counterclockwise direction, the stylus is inserted in the aperture 26 opposite the number 31, corresponding to the desired shift, on the outside of the slot 30, and then shifting the disk 12 until the stylus encounters the left hand end of the slot 30.

I claim:

1. A cryptographic device comprising a fixed member and a member movable with respect thereto, one of said members having character indicia thereon, the other of said members having an opening with character indicia therealong for alinement with said other character indicia, said last named member also having a slot of a length to correspond to a predetermined number of said characters, said first named member also having apertures corresponding to said characters and in alinement with said slot.

2. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, one of said members having character indicia thereon circularly disposed, the other of said members having an arcuate space with character indicia therealong for alinement with said other character indicia, said last named member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said characters, said rotatable member also having a plurality of apertures corresponding to the characters thereon and in alinement with said slot.

3. A cryptographic device comprising a fixed cover member and a member therebelow and rotatable with respect thereto, said rotatable member having character indicia thereon circularly disposed, said cover member having a semi-circular opening concentric with said character indicia and having character indicia therealong for alinement with said circularly disposed indicia, said cover member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said characters, said rotatable member also having a plurality of apertures corresponding to said characters thereon and in alinement with said arcuate slot.

4. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said first named member having an arcuate space therein with character indicia therealong, said rotatable member also having character indicia thereon disposed for alinement in said space with said first mentioned character indicia.

5. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said first named member having an arcuate opening therein with character indicia therealong, said rotatable member also having character indicia thereon circularly disposed for alinement in said opening with said first mentioned character indicia.

6. A cryptographic device comprising a cover member and a member rotatable with respect thereto, said first named member having an arcuate opening therein with character indicia therealong, said rotatable member also having char-

acter indicia thereon circularly disposed for alinement in said opening with said first mentioned character indicia, said latter character indicia including a repetition of said first mentioned character indicia.

7. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an opening with character indicia therealong for alinement with said other character indicia, said first mentioned member also having a slot of a length to correspond in angular relationship to a predetermined number of said characters, said rotatable member also having a plurality of apertures corresponding to the characters thereon and in alinement with said arcuate slot.

8. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an opening with character indicia therealong for alinement with said other character indicia, said first mentioned member also having a plurality of arcuate slots each of a length to correspond in angular relationship to a predetermined number of said characters, said rotatable member also having a plurality of apertures in alinement with said slots.

9. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an opening with character indicia therealong for alinement with said other character indicia, said first mentioned member also having a plurality of slots each of a length to correspond in angular relationship to a different predetermined number of said characters, said rotatable member also having a plurality of apertures corresponding to the characters thereon and in alinement with said slots.

10. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said first named member having character indicia thereon, said character indicia comprising the letters of the alphabet, a space indicator and the unit numbers, said rotatable member having character indicia thereon, the indicia on said rotatable member including the same characters as those on said first named member and also a repetition thereof.

11. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said first named member having character indicia thereon arcuately disposed, said character indicia comprising the letters of the alphabet, a space indicator and the unit numbers, said rotatable member having character indicia thereon, the indicia on said rotatable member being circularly arranged and including the same characters as those on said first named member and also a repetition thereof.

12. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an arcuate opening with character indicia therealong, said fixed member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said characters, and a set of movement indicating indicia along said arcuate slot.

13. A cryptographic device comprising a fixed

- member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an arcuate opening with character indicia therealong, said fixed member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said characters, and a plurality of sets of movement indicating indicia along said arcuate slot.
- 10 14. A cryptographic device comprising a fixed member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said fixed member having an arcuate opening with character indicia therealong, said fixed member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said char-
- 15

acters, and two sets of number indicia for indicating movement oppositely arranged in increasing order along said slot.

15. A cryptographic device comprising a cover member and a member rotatable with respect thereto, said rotatable member having character indicia thereon, said cover member having an arcuate opening with character indicia therealong, said cover member also having an arcuate slot of a length to correspond in angular relationship to a predetermined number of said characters, and movement indicating indicia, said indicia including a set of numbers along said slot with the numbers increasing in one direction and a set of numbers along said slot with the numbers increasing in another direction.
- 5 10 15

JAMES C. WOBENSMITH.