

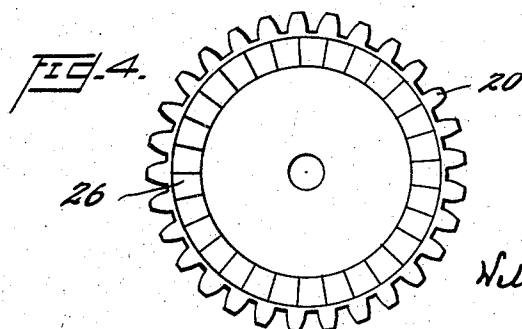
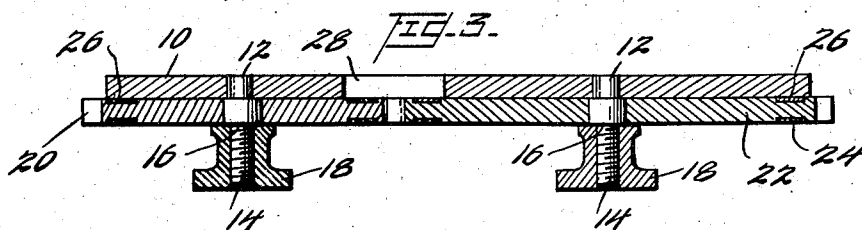
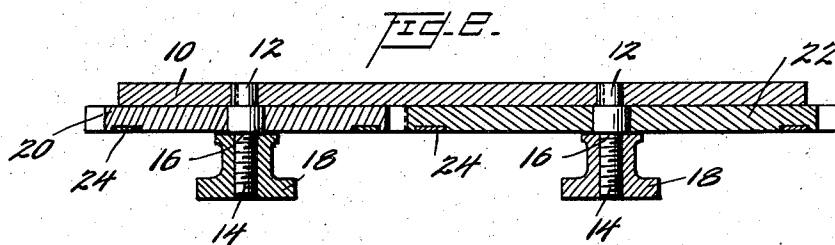
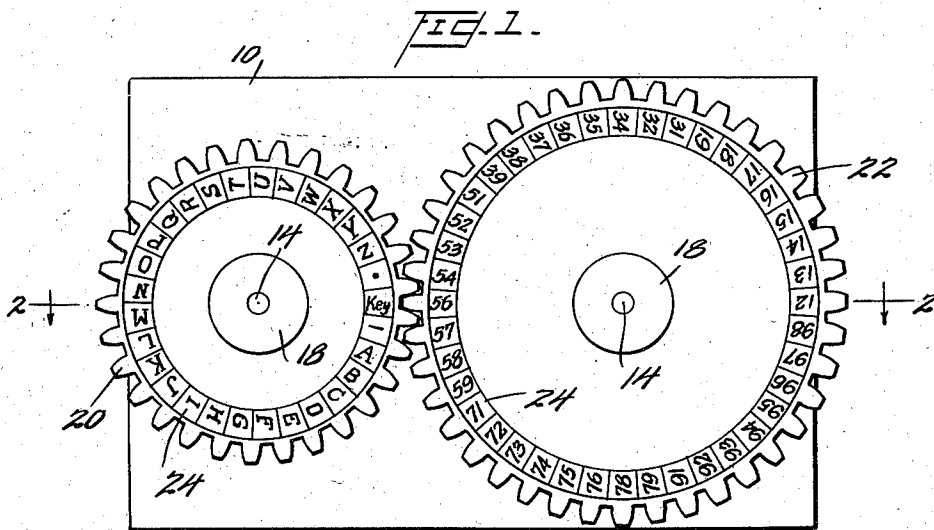
Dec. 13, 1938.

W. F. FRIEDMAN

2,140,424

CRYPTOGRAPHIC DEVICE

Filed June 7, 1937



Inventor
William F. Friedman

By L. R. Paris.

Attorney

UNITED STATES PATENT OFFICE

2,140,424

CRYPTOGRAPHIC DEVICE

William F. Friedman, Washington, D. C.

Application June 7, 1937, Serial No. 146,906

12 Claims. (Cl. 35—3)

The present invention relates generally to cryptographic devices for encyphering and decyphering messages, and one of the objects of the present invention is to provide a device of this type which is simple to manufacture and may be manipulated with great facility so as to provide for the rapid encyphering and decyphering of messages.

The simplicity of construction of the present device resides in that the device essentially consists of a pair of relatively rotatable toothed gears, the gears bearing on their faces indicia which take the form of message characters on one and the form of message symbols on the other. The device is even further simplified by disposing these indicia on the exposed faces of the gears in annular spaces immediately adjacent the teeth of the gears.

The facility and rapidity of encyphering and decyphering messages by the present device is enhanced by the disposition of the indicia on the faces of the gears in such a manner that such indicia are disposed on one gear immediately adjacent the spaces between the teeth and are disposed on the other gear immediately adjacent the teeth. Thus, it will be seen that each tooth serves as a pointer for any combination of message character and message symbol. It will be understood that if desired, the indicia on the latter gear may be disposed directly on the tooth, although it will be clear from an inspection of the accompanying drawing that the disposition of such indicia immediately adjacent each tooth, whereby the tooth serves as a pointer, practically eliminates the possibility of error in reading the device.

The manipulation of the present device is further facilitated by the construction shown in which the two gears are mounted on a plate, one or both of the gears having portions extending beyond the plate which serve to be engaged by a finger of the operator so as to rotate the gears.

In the present device the risk of unauthorized translation of a message is greatly decreased by the fact that in the present device, the number of teeth in the two gears are unequal and the number of indicia in the two gears are unequal, whereby in the same message one character is represented by various symbols. Preferably, the symbol gear is larger than the character gear and in the present system, the symbols each contain at least two digits or characters. This makes it possible to provide a symbol gear which has a much greater number of teeth than the other gear. In the present case, also, the mes-

sage character gear has twenty-nine teeth, whereas the symbol gear has forty teeth, this ratio being illustrative of a preferred arrangement in which the two numbers do not have any common factors. In the present organization, it will be seen that each message character may be represented by any one of forty message symbols.

Another object of the invention is to provide for the rapid setting of the device to any desired key. In the present device, this is preferably accomplished by providing readily manipulable means for disengaging the two gears and then setting the gears to the desired key position.

The drawing accompanying the present application and forming a part of the present specification illustrate one specific embodiment of the present invention, it being understood, however, that variations of the embodiment falling within the scope of the appended claims will be apparent to persons skilled in the art.

In the drawing:—

Fig. 1 is a plan view of the present device; and

Fig. 2 is a sectional view taken on line 2—2 of Fig. 1.

Fig. 3 is a sectional view, similar to Fig. 2, of a modified form of the invention.

Fig. 4 is a view of the obverse face of one of the gears and is designed to show diagrammatically a form of the invention in which the obverse face of each of the gears is provided with an annular space in which the characters or symbols may be inscribed by the purchaser. One or both of the gears may be provided with this annular space on the obverse face of the gear. This feature may be applied either to the form shown in Fig. 2 or to the form shown in Fig. 3.

The present device illustrated in the drawing comprises a base plate 10, which, although it may be of any suitable shape and construction, is preferably oblong. The plate may be made of any suitable material. A pair of studs 12, 12 are fixedly mounted on the plate 10, each of these studs having an exteriorly threaded reduced shank 14, thereby forming an annular shoulder 16 on each stud. Interiorly threaded knurled collar 18 cooperates with each of the studs to hold the gears 20 and 22 in freely rotatable position on the studs 12.

As shown in the present drawing, the gear 20 constitutes the character gear and the gear 22 constitutes the symbol gear. Gear 20 as shown has twenty-nine teeth, and the gear 22 has forty teeth. It is obvious, however, that the number of teeth may be varied as desired depending upon the number of message characters which it is

desired to employ and depending also upon the number of variations in the message symbols that one may desire. While it is preferred to use a pair of gears having an unequal number of teeth and in which the numbers have no common factors, it is obvious that for some purposes, the device may be just as effective without embodying this peculiar relation of the two numbers.

In the form of the invention shown herein each of the gears is provided with an annular inlay 24 bearing the character or symbol insignia. It will be understood, however, that if desired the insignia may be applied directly to the gear when the gear is made of material that will render the insignia readily legible. In the preferred form shown herein these annular inlays 24 are of white Celluloid upon which the insignia are inscribed so that the same are highly legible.

As shown, in the character wheel 20, the annulus 24 is divided into twenty-nine spaces, each immediately adjacent the space between a pair of teeth. These bear the letters of the alphabet, a period, a dash, which may be used for indicating the end of a word, and the word "key" which may be employed for the setting of the wheels or gears at the beginning of an encyphering and decyphering operation. It will be understood that the word "key" may be omitted if desired and any other character may be employed as a key to the setting.

The symbol wheel or gear 22 in the form shown has forty teeth, and the annulus is divided into forty spaces, one immediately adjacent each tooth, and each space bears a two digit symbol. It will be understood that other symbols may be employed if desired, such as letters of the alphabet, or combinations of such letters with digits.

Each of the two gears extend a little beyond the lateral edges of the base plate 10 and these extending portions may be engaged by the finger of the operator so as to rotate the wheels. While any key setting may be obtained by the rotation of the gears in their assembled or engaging position, the key setting may be obtained with greater facility by releasing one of the collars 18, moving the released gear axially out of engagement with the other gear and then rotating the two gears to the key position and then dropping the released gear into proper engagement with the other and bringing the released collar home.

It will be seen that in the organization and structure shown herein all the characters and symbols are in clear view and that the teeth on the symbol gear serve as pointers for each setting, thereby greatly facilitating the operation and use of the present device.

The present device permits the operation of the device in either of two directions, with the contacting teeth moving either up or down. This affords great freedom of operation which may be employed by persons in communication for further enhancing the secrecy of their communications.

While it is contemplated that the present device be manufactured and sold with the insignia inscribed thereon as shown or in any other similar manner, it is also contemplated to permit the purchaser to devise his own cypher and employ the same device. For this purpose the lower face of each wheel or gear may have an annulus 26 which is spaced off in the same man-

ner as the annulus on top of the gear by means of radial lines as shown in Fig. 4. The purchaser can then inscribe his own characters and symbols on these annular members. He may then turn the gears over so as to expose to view his own code.

Still another form of the device is shown in Fig. 3. In this form an oblong opening 28 is provided in the base plate 10, the opening being disposed over the point of engagement of the gears. In this form the annular members on both faces of the gears bear inscribed thereon characters and symbols, respectively, and by this means, both codes on the opposing faces of the gears are available and may both be used in the same message.

Moreover, when each disc or gear bears characters or symbols on both faces, four code systems are made available by the following combination: upper 20—upper 22; upper 20—lower 22; lower 20—upper 22; lower 20—lower 22. If desired, all of these codes may be employed in the transmission of one message or group of messages, particularly where the communications are prolonged.

It is recognized that cypher experts can decypher a series of messages in which the present device may be employed without having the key available to them. This is, however, a time consuming process. The present device may, therefore, not be highly useful where permanent secrecy or secrecy for a long time may be desired. It is, however, useful where secrecy for a relatively limited time is essential and particularly where secrecy is desired in communications between persons and under circumstances where cypher experts are not readily available.

The present device is particularly useful as a source of amusement by children who wish to communicate with each other in secrecy.

Having thus described my invention, I claim:

1. A cryptographic device for encyphering and decyphering messages comprising a pair of relatively rotatable engaging toothed gears, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols.

2. A cryptographic device for encyphering and decyphering messages comprising a pair of relatively rotatable engaging toothed gears, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols, the indicia on one of said gears being disposed adjacent the space between the teeth, and the indicia on the other gear being disposed immediately adjacent each tooth, whereby each such tooth serves as a pointer for encyphering and decyphering messages.

3. A cryptographic device for encyphering and decyphering messages comprising a pair of relatively rotatable engaging toothed gears, one of said gears bearing in an annular space immediately adjacent the teeth, indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher

symbols, the indicia on one of said gears being disposed adjacent the space between the teeth, and the indicia on the other gear being disposed immediately adjacent each tooth, whereby each such tooth serves as a pointer for encyphering and decyphering messages.

4. A cryptographic device for encyphering and decyphering messages comprising a plate, a pair of engaging toothed gears rotatably carried by said plate, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in the annular space immediately adjacent the teeth, indicia in the form of cypher symbols.

5. A cryptographic device for encyphering and decyphering messages comprising a plate, a pair of engaging toothed gears rotatably carried by said plate, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols, the indicia on one of said gears being disposed adjacent the space between the teeth, and the indicia on the other gear being disposed immediately adjacent each tooth, whereby each such tooth serves as a pointer for encyphering and decyphering messages.

6. A cryptographic device for encyphering and decyphering messages comprising a plate and a pair of engaging toothed gears, rotatably carried by said plate, one of said gears having a portion extending beyond the plate, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols.

7. A cryptographic device for encyphering and decyphering messages comprising a plate and a pair of engaging toothed gears, rotatably carried by said plate, one of said gears having a portion extending beyond the plate, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols, the indicia on one of said gears being disposed adjacent the space between the teeth, and the indicia on the other gear being disposed

immediately adjacent each tooth, whereby each such tooth serves as a pointer for encyphering and decyphering messages.

8. A cryptographic device for encyphering and decyphering messages comprising a plate, a pair of spaced shouldered studs mounted on said plate, each of said studs having a threaded end of reduced diameter and carrying an interiorly threaded collar, a pair of engaging toothed gears rotatably carried by said studs, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols.

9. A cryptographic device for encyphering and decyphering messages comprising a plate, a pair of spaced shouldered studs mounted on said plate, each of said studs having a threaded end of reduced diameter and carrying an interiorly threaded collar, a pair of engaging toothed gears rotatably carried by said studs, the number of teeth on the two gears being unequal, one of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of message characters, and the other of said gears bearing, in an annular space immediately adjacent the teeth, indicia in the form of cypher symbols, the indicia on one of said gears being disposed adjacent the space between the teeth, and the indicia on the other gear being disposed immediately adjacent each tooth, whereby each such tooth serves as a pointer for encyphering and decyphering messages.

10. A cryptographic device for encyphering and decyphering messages, comprising a base plate, a pair of spaced studs mounted on said plate, and a pair of engaging toothed gears rotatably carried by said studs, one of said gears bearing in an annular space immediately adjacent said teeth on both faces thereof message characters, and the other of said gears bearing in an annular space immediately adjacent the teeth indicia in the form of cypher symbols on both faces thereof, said plate having an opening in registry with the contacting teeth and adjacent insignia.

11. A cryptographic device as set forth in claim 8 in which each gear has on its lower face an annular portion, immediately adjacent the teeth, said portion having a surface capable of receiving inscriptions of characters or symbols.

12. A cryptographic device as set forth in claim 1 and in which each of the cypher symbols comprises at least two characters.

WILLIAM F. FRIEDMAN.