IN THE UNITED STATES PATENT OFFICE

In re application of
W. F. Friedman, et al.
Filed Jan. 23, 1932,
Serial No. 588,344
Cryptographic System

Div. 53, Room 6897

July 31, 1934.

Hon. Commissioner of Patents,

Sir:

Responsive to Patent Office Action dated Feb. 15, 1934.

In the specification :

Page 6, line 20, cancel "the figure " and substitute - - Fig. 4 - - Lines 23 and 24 cancel " 2" and substitute - - 4 - -

Page 7, line 6, after "positions" insert - - , as in the case of pin 47 in Fig. 1 , - - Line 8, after "positions" insert - - , as in the case of pin 48 in Fig. 1, - - Line 27, after the numeral "50 " insert - - (see Fig. 6) Line 29 after "2, " insert - - (see Fig. 6)

Page 8, line 21 after "armature" insert - - 41 - - Same line cancel "41" and substitute - - 25 - - Line 23, cancel "methods" and substitute - - means - -

Page 16, line 7 after "tape" insert - - is - -

In claims 35, 36, and 37, line 5 in each instance, change " unequality" to - - inequality - -

R e m a r k s

Referring to page 6, lines 18 and 20, and to the Examiner's suggestion that Fig. 2 should show the pins; also referring to line 23 and the Examiner's suggestion that it is not clear how Fig. 2 represents

"permutations" , it will be noted that amendments have been directed on page 6, lines 20, 23 and 24 to bring out that it is Fig. 4 which shows the permutations. In said Fig. 4 the pins in their inactive positions are shown in dotted lines, while the pins in their active position are shown in full lines. With this correction in the text, it is not deemed necessary to correct Fig. 2, which figure shows the pins clearly enough when considered in connection with Fig. 4.

As to how the pins operate the levers, attention is called to amendments directed in lines 6 and 8, page 7 of the specification. When the text as here amended is considered in connection with Fig. 1, it is believed that the showing is quite clear and the Examiner is courteously requested to waive requirement for additional illustration in this regard.

As to line 13 wherein the Examiner raises the question of how the ratchet wheel of Fig. 3 is related to the cipher wheel and how the ratchets are related to member 24, etc., it is understood that the Examiner refers to line 13 of page 7. The operation questioned by the Examiner is quite fully described on page 9, beginning with the last paragraph and continuing on the following page. When this detailed description is considered in connection with the second paragraph found on page 7, it is believed that the description of the operation needs no further enlargement.

As to the Examiner's criticism of Fig. 3 and parts shown adjacent the elements 24 and 41, it is proposed to correct Fig. 3 in accordance with the attached print in which magnet 25 is indicated in red ink with the proper lead line from the reference numeral. In other respects,

it is believed that the essential parts will be clear by reference to Fig. 1. The numeral 24 designates the pawl (see Fig. 1), 25 designates the magnet and 41 designates the armature. In the same connection it is also desired to make a slight correction in Fig. 5 as shown in red ink in the same print. This correction consists in showing the armature 41 located back of ratchet tooth 23. By separate communication the Official Draftsman has been requested to incorporate these corrections subject to the approval of the Examiner. It is not seen why such an obvious and conventional structure need be shown more in detail than it is. The idea here is to make Fig. 1 largely schematic.

As to the criticism involving lines 22 and 28, page 7 of the specification, amendments have been directed in lines 28 and 29 to overcome the objection. In view of these changes, line 22 is correct as it stands.

Page 8, line 12, regarding the tendency of movement of wheel 52 due to the movement of wheel 48, the arrows shown in Fig. 6 are believed to indicate these movements correctly as described in the first paragraph of page 8. When the motor is in operation, the worm 52 fixed on shaft 58 tends to move to the right, while the wheel 48 is moving in a counter clockwise direction as indicated by the arrow. The predetermined arrangement is such that the movement of the worm carries the shaft to the right until the switching mechanism acts to stop the movement.

The correction required in line 23 of the word "methods" to the word - - means - - has been made.

Also the criticism noted by the Examiner applying to lines6 and 8 of page 16, an appropriate verb has been inserted to make the sentence complete.

The word " unequality" has been changed to - - inequality - - in claim 35 and the same amendment has also been made in claims 36 and 37.

The Examiner's query as to the significance of the word " unintelligible " in claim 36 is explained as follows: It is an established fact in cryptographic analysis that if the keying sequence consists of a series of letters having an intelligible meaning, solution of messages enciphered by means of such a keying sequence can be readily accomplished. Technically, therefore, the word "unintelligible" must be included to cover and support the claim or function of indecipherability of the proposed mechanism. Accordingly, it is thought that this claim should not be changed in the manner suggested by the Examiner.

Regarding the rejection of claims 34, 35, 36 and 37 as anticipated by Hebern, the limitation "means for angularly displacing the switching device in an aperiodic manner " clearly differentiates from Hebern. In the disclosure of said patent, the switching device is mechanically displaced in a perfectly periodic manner susceptible of no irregularity and this constitutes a fundamental weakness in the cryptographic principle underlying the operation of the device. Furthermore, as stated by the Examiner, in Hebern the enciphering elements bear the key, but in the present invention the key is contained in an instrumentality wholly external to the ciphering elements.

As to the rejection of claims 35, 36 and 37 as being intangible, the invention consists in the association of a ciphering mechanism with a key which is not an integral part of the ciphering mechanism itself, being something which can be fed into the ciphering mechanism to control its action in enciphering or deciphering in a manner analogous to that in which a perforated sheet controls

the music produced by an automatic piano. The combination of a ciphering mechanism of the type disclosed with a cipher key that is external to the cophering mechanism and is not an integral, mechanical part of the ciphering mechanism is novel.

It is noted that the Examiner also objects to claims 36 and 37 as intangible in the word "sequence". In this connection it is explained that the order in which the ciphering characters are arranged on the cipher key in cases of this nature is vital to the security of the cyrptographic system. The statement " a sequence cannot produce physical changes " does not appear to be strictly true in this specific case because the nature of the cryptographic results of the action of the device can be and are varied by the order in which the ciphering characters are brought into play. For example, the word "Enemy", enciphered by the sequence of keying elements ABCDE, may yield the cryptographic sequence VWXYZ; but the same word, enciphered by the described mechanism by the sequence BACDE would yield a wholly different cipher result. Here a very definite physical change has been produced by the sequence of ciphering characters involved.

The Examiner's grounds for rejection of the group of method claims 40 - 50 are duly noted.

Exception must be taken to the position that no changes of character or condition are effected by the practice of the present method. A system which so changes the cipher equivalents representing plain text characters as to prevent periodicity in the relationship, and one which changes the relationship to such an extent as to achieve practical aperiodicity is certainly making a very decided change of character or condition.

In this invention the fundamental concept contemplates the elimination of predictable factors by the method which varies the cipher resultant of a plain text character by externally and aperiodically controlling switching devices. This step of external control depends upon an external element viz: a key tape for example, which can be varied at will. Instead of a key tape it may be conceived that a kind of chain could be substituted in which the size or length of the links would be varied to function as a controlling external element. When the inventive concept is understood, it is urged that such an element is aptly and correctly described as an external element. Particular attention is called in this connection to such claims as numbers 46 and 47 in which the idea of a two phase control is defined, one phase of control being internal and the other phase of control being external. Such a concept is not found in any of the art of record or known to the applicant and the novelty of this inventive concept is insisted upon and moreover, it is contended that operations comprising steps such as recited in the group of method claims are clearly method steps in as full a sense as the steps defined by method claims found in Vernam patent 1,416,765. The method also involves the further step of so controlling the cipher elements as to eliminate from the final cryptogram six extra permutations representing the difference between the 32 permutations of a plural unit code such as the Baudot Code and the usual 26 characters of the alphabet or the standard equivalents of the Morse Code.

It is contended that a system comprising the steps discussed above which starts with a message composed of plain text characters and so changes the relationship of such a message in respect to the final cryptogram as to finally eliminate the predictable or periodic factors, brings about a

change of character and condition which certainly satisfies this requirement of what constitutes a method.

It is further contended that here we have a true method which is more than the mere function of the apparatus disclosed. That this is so is evidenced by the fact that the method does not depend upon a single mechanism. That the mechanical set up or assembly of coordinated mechanisms may be varied considerably in respect to the individual components can be readily shown. In other words, the method does not depend upon one single assembly of individual components.

Again, it is contended that true method claims may be predicated upon a recital of structure in the preamble sufficient to define and give meaning to the method steps, all of which is well established by the practice. The present method is one which justifies the use of a certain introductory or antecedent recital of structure. In principle, this is supported by numerous patents, among which may be mentioned the patent to Vernam identified above. Several decisions in support of the practice in this regard will be cited below.

The proposition that a mechanical method is entitled to patent protection is supported by the following decisions:

Ex parte Chase (Patent 1,637,138) - 2 U.S. Daily 1669

Ex parte Weston - 17 Ct. App. D.C. 449; 1901 C.D. 417

Expanded Metal Co. vs. Bradford - 214 U.S. 366; 1909 C.D. 521

American Graphaphone Co. vs. Universal Talking Machine Mfg. Co. 151 F. 595-601 (2nd Cir. 1907)

Buffalo Forge Co. vs. City of Buffalo - 246 F. 135

That a recital of structural elements is permissible in method claims is supported by the following decisions: -

Ex parte Murray (Ct. App. D.C. 1928) - 372 O.G. 442

Ex parte Astor and Beale - 15 Pat. Q. 292 (Bd. of Appeals, 1932)

Ex parte Gustavson - 14 U.S. Pat. Q. 332 (Patent 1,870,955)

All of the grounds of rejection have been discussed in detail and favorable reconsideration is courteously asked in the light of the foregoing. At a later date applicant desires to have an opportunity to demonstrate working models both of the machine embodying the present invention and also a machine embodying improvements forming the subject matter of a later application, Serial No. 682,096.

Respectfully submitted,

W. F. Friedman, et al.

By:

Attorney

IN THE UNITED STATES PATENT OFFICE

In re application of
W. F. Friedman, et al.
Filed Jan. 23, 1932,
Serial No. 588,344
Cryptographic System

Div. 55, Room 6897

July 31, 1934.

Hon. Commissioner of Patents,

Sir:

Referring to amendment of even date herewith and subject to the approval of the Examiner, the Official Draftsman is requested to correct Figs. 3 and 5 of the drawings in this case in accordance with red ink indications found in the attached print.

The corrections consist in the case of Fig. 3 in showing in dotted lines the magnet with appropriate lead lines to the reference character 25.

The other correction consists in showing the armature 41 back of the tooth 28, Fig. 5.

The cost of making corrections is chargeable against the account of the Army Air Corps.

Respectfully submitted,

W. F. Friedman, et al.

By:

Attorney