IN THE UNITED STATES PATENT OFFICE

In re application of
William F. Friedman,
Filed July 25, 1933,
Serial No. 682,096,
Cryptographic System,

Division 53, Room 6897

Hon. Commissioner of Patents,

Sir:

Responsive to Patent Office action dated October 9, 1933.

It is desired to amend the claims as follows:

Claim 5, line 6, change " a magnet " to read - - an electromagnet - - Same line before "associated " insert - - an - - Same line, after "pawl, " insert - - each ratchet and pawl actuating its associated commutator, - -

Claim 6, last line change the period after "cryptograph " to a comma and insert - - said element comprising a perforated tape bearing ciphering characters in a plural unit code . - -

Claim 21, line 8, before "non-repeating " insert - - practically - - Same line cancel "sequence " and substitute - - series - - Last line change the final period to a comma and insert - - said characters being represented by perforations permuted in accordance with a plural unit code . - -

Claim 22, line 8 before "non-repeating" insert - - substantially - - Same line, cancel "sequence " and substitute - - series - -

Claim 23, line 8, cancel "bars" and substitute - - keys - -

Declassified and approved for release by NSA on 12-16-2013 pursuant to E.O. 13526

# REMARKS

It is noted that claims 1 to 4 inclusive are rejected on the patent to Hebern, and the same patent is mainly relied upon for the rejection of claims 6, 7, 8, 9, 10 and 11 to 21 inclusive. It is desired to emphasize the point that nowhere in Hebern is a cipher key transmitter disclosed. This is an important and fundamental distinction in favor of applicant's invention. In Hebern the movements or displacements of the code wheels are purely mechanical; these movements are regular or periodic in character, and controlled by ratchet mechanisms internal to the device itself. In the present invention, these movements are controlled by the cipher key transmitter in an aperiodic manner, and by a tape or plurality of tapes external to and not a part of the device itself. Due acknowledgment has been made of the said Hebern patent on page 5 of the specification in this case, and a basis has there been established for the important distinction which is now brought out. It will be recognized that the Hebern structure has the inherent weakness of all such devices where the keying mechanism is a part of the device itself. Periodical recurrence of movements is a natural characteristic of all such mechanisms and the predictable factor thus introduced defeats the essential purpose. Thus we have a distinction which is material and inobvious, and which is supported by a material advantage. Claims 1 to 4, as well as the other claims above mentioned, each includes this distinctive element in one way or another and are clear of Hebern.

Claim 5 has been amended and in its present form is believed to avoid the objections as to form noted by the Examiner.

As regards claims 6, 7, 8, 9 and 10, the Examiner fails to distinguish between those parts of the mechanism which are internal to the cryptograph itself, viz: the keyboard, the commutators, the cipher key transmitter or transmitters, the indicating mechanism on the one hand, and the external element which is the key tape itself, on the other hand. It is not contended that the cipher key transmitter is the external element - this part of the mechanism is controlled by a perforated tape; it is the latter element which is wholly external, can be removed, changed and varied at will. In other cryptographs known to applicant in which rotatable circuit changers are employed, the keying mechanism is internal to and a part of the cryptograph itself and, therefore, inherently presents the weakness from a cryptographic standpoint that periodicity cannot be prevented, since whatever the keying mechanism may be (whether gearing, cams or the like ), the parts must operate upon mechanical principles giving rise to phase recurrences, or cycles, or periods. It is believed that the five claims are correctly and accurately phrased and are entirely clear in the light of the specification and drawings.

Referring to the rejection of claims 9 and 10 on Morehouse, it is pointed out that this citation does not disclose applicant's fundamental concept of aperiodically controlling switching devices by an external keying element, and Morehouse fails to show or to teach this fundamental concept. Now, since these claims each covers the said fundamental concept in combination with the feature of a plurality of cipher key transmitters, an attempt to build up a mental anticipation of said claims in view of Morehouse alone cannot be maintained. In Morehouse the character symbols of the two tapes are employed successively, and the

collective or multiple action contemplated by the applicant's invention is not possible. Moreover, in applicant's invention, the numbers of such characters in the respective tapes being prime to one another constitutes another important distinction over Morehouse from a cryptographic standpoint, which distinction is brought out in claim 10. Study has shown that if these numbers are not prime to one another, the full combinational potentialities of the respective keys cannot be realized in practice. For example, if there are two tapes, one containing 1,000 characters, the other 500, then after two revolutions of the longer tape, the combination of the two tapes produces a resultant which coincides with the resultant of the first revolution. In other words, instead of having a single resultant key of 1,000 x 500 = 500000 characters the resultant is only 2,000 characters in length. In the case of keys whose length is prime to each other the resultant has a latent length that is the product of their individual lengths.

As to the blanket rejection of claims 11 to 21 on Hebern, this patent has been discussed at length and it will be noted that each of these claims includes the cipher key transmitter or a plurality of such transmitters defined in one way or another for which there is no counterpart in Hebern.

Claims 17 and 19 are believed to define sufficient structure when interpreted in the light of the disclosure without introducing unnecessary limitations.

As to claim 18, it is believed that the significance of the words "external" and "independent" is quite clear and fully justified

by the disclosure, all as elaborated above in discussing the distinctions over Hebern and in explaining the meaning of said terms. The perforated tape is the external element.

Claims 21, 22 and 23 have been amended and in their present form are thought to be clear of the objections noted by the Examiner.

The grounds for rejecting claims 23 to 25 inclusive are not understood. The essence of the invention is defined in such terms in these claims as are employed in the other claims and the meaning is thought to be entirely clear in the light of the disclosure.

The Examiner's rejection on the ground of multiplicity is noted. The effort has been to draft a sufficient number of claims to cover a fair range of equivalents bearing in mind the importance of blocking possible future infringements, but not overlooking the importance of validity. Referring to claims 1 and 2, these two claims are phrased in different terms and are believed to be patentably distinct. For example, claim 1 recites " a cipher-key transmitter" while claim 2 recites " a cipher-key transmitter mechanism " . A cipher key transmitter is one element - a cipher key transmitter mechanism has a different and broader significance. Referring to claims 11 and 12, it will be noted that claim 12 is somewhat more specific than claim 11 and should claim 12 be found allowable, applicant would be willing to drop claim 11. Applicant would of course be willing to make some reduction in the number of the claims provided this would not involve any sacrifice in protection upon his invention.

The Examiner's grounds for the rejection of the method claims Numbers 26 to 34 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.

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 which can be varied at will. In the present method, elimination of predictable factors is made more effective by multiplying the number of external keying elements to produce a collective action. The method also includes the further step of so controlling the cipher elements as to eliminate from the final cryptogram six extra permutations representing the difference between the thirty-two permutations of a plural unit code such as the Baudot Code and the usual twenty-six characters of the alphabet or the standard equivalents of the Morse Code.

First, 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 practically eliminate the predictable or periodic factors, brings about a change of character and condition which certainly satisfies this requirement of what constitutes a method.

Secondly, it is 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. It will be noted that the drawings in this case is largely diagrammatic in character and the mechanical set up or assembly of coordinated mechanisms may be varied considerably in respect to the individual components. In other words, the method does not depend upon one single assembly of individual components.

In the third place, it is contended that true method claims may be predicated upon a recital of structure in the preambles 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 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 No. 1,416,765. Several decisions in support of the practice in this regard will be cited below, and it is significant that a number of these are comparatively recent.

A long line of decisions may be cited to show that in general, a mechanical method is entitled to patent protection. In this category the following decisions are mentioned:-

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

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

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

REF ID:A521456

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 ) - 379 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 )

It will be noted that nearly all of the decisions above cited are much more recent than thos relied upon by the Examiner, and those in the second group are for the most part quite recent, which may be regarded as persuasive of a more liberal practice both by the Courts and the Patent Office in favor of mechanical method claims and permitting the recital in such claims of sufficient structure to support the method steps.

Favorable reconsideration is courteously solicited in the light of the foregoing.

Respectfully submitted,

William F. Friedman,

By:

Attorneys