REF ID:A521451

IN THE UNITED STATES PATENT OFFICE

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

Div. 53, Room 6897

December 5, 1934.

Hon. Commissioner of Patents,

Sir:

Responsive to Patent Office Action dated June 6, 1934.

Claims 11 and 13 are cancelled without prejudice.

Claim 17, line 3, after "bank" and before the semicolon insert - - , said sets of elements being electrically interrelated - - Line 4, cancel "connections" and substitute - - electrical relation - -

Claim 18, line 2, cancel "and" Line 3, after "bank" and before the semicolon insert - - , and including electrical connections between said sets of elements - -

Claim 19, line 2, cancel "and" ; substitute a comma after "keyboard " Line 3, after "bank" and before the semicolon insert -b- , and including electrical connections between said sets of elements - -

Claim 20, line 2, cancel "and " ; substitute a comma after "keyboard" Line 3, after "bank" and before the semicolon insert - - , and including circuit connections between said sets of elements - -

Claim 21, line 2, cancel " and" ; substitute a comma after "keyboard" Line 3 after "bank" and before the semicolon insert - - , and including circuit connections between said sets of elements - -

Confidential

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

Claim 22, line 3, after "bank ; " insert - - electrical connections between said sets of elements ; - -

Claim 23, line 3, after "bank ; " insert - - circuit connections between said sets of elements ; - -

Claim 24, line 3, after "bank ; " insert - - circuit connections between said sets of elements ; - -

Claim 25, line 3, after "bank ; " insert - - circuit connections between said sets of elements ; - -

R E M A R K S

Referring to the Examiner's statement "Hebern discloses mechanism for displacing the code wheels ", this is correct. But his statement that " this mechanism is in effect a cipher-key transmitter " is erroneous in two respects.

Looking into the meaning of the expression " cipher-key transmitter" , we have three things to consider : first, the meaning of the term "cipher key " ; second, the meaning of the term "transmitter" , and third, the meaning of the term resulting from combining "cipher key" with "transmitter" into one expression. It will be granted, presumably , that these terms must be examined in the light of cryptographical technique and terminology. Accordingly, having recourse to a reference source commonly accepted as authoritative, viz., the Encyclopedia Britannica,

B

14th Edition, Article "Codes and Ciphers " in Vol. 5, we find the following statement :

> "Every practical cipher system must combine (1) a basic method of treatment which is constant in character, with (2) a keying principle which is variable in character and employs specific keywords, phrases, or numbers, the individual compositions of which determine or control the exact results under the basic method. "

Considering the phrase "cipher key " as it appears in the applicant's specifications and claims, and bearing in mind that we are directing attention only to the mechanism for displacing the cipher wheels, it is quite clear that the cipher key here serves as the physical embodiment of the "keying principle " referred to in the foregoing citation, and that its sole purpose is to serve as the controlling element in effecting the displacements of the cipher wheels in a variable manner. Contrast this situation with that in Hebern. Referring now only to the mechanism for displacing the cipher wheels, in Hebern there is embodied no such thing as a cipher key which corresponds to a " keying principle which is variable in character " because the mechanism for displacing the cipher wheels is absolutely fixed. It is, in fact, the very antithesis of a keying principle variable in character and is strictly comparable to the mechanism of any indicating or recording meter for measuring gas, electric power, or water consumption. Certainly, no one could consistently argue that the mechanism actuating an odometer, for example, embodies a keying principle which is variable in character and which controls the movements of the wheels in a variable manner. Indeed, constancy is the fundamental basis of operation and functioning of such a device, and not variability. Since this is the same type of meter-like mechanism as is embodied in Hebern, it must be quite clear that the

REF ID:A521451

mechanism for displacing the cipher wheels in Hebern is positively not an embediment of a "keying principle which is variable in character " and therefore the Examiner is not correct in assuming that Hebern discloses a mechanism which embodies a cipher key as a controlling element in displacing the cipher wheels.

Coming now to the word "transmitter" , in the phrase "cipher-key transmitter ", this refers to a definite mechanico -electrical entity well known in the art of telegraphy as a specific mechanism operating in a specific manner to accomplish specific functions in electrical transmission of energy. In its essence, a transmitter of the character disclosed by applicant is a mechanism which permits of the establishment of one of a multiplicity of sets of electrical conditions for transmitting electrical impulses and of changing from one set to another set of conditions according to some variable factor such as a tape bearing perforations corresponding to a communication alphabet. Certainly Hebern discloses no such device, nor is the mechanism embodied therein even faintly similar to an electrical transmitter of this type, nor is the Hebern mechanism in affect a transmitter, as inferred by the Examiner.

Coming now to the whole phrase "cipher-key transmitter ", a transmitter of the type described by applicant is usually employed strictly for ordinary telegraphic transmission purposes. It is true that it has been employed for cryptographic purposes, as disclosed in Morehouse, Vernam, and others. But it has never before been employed in connection with a cryptographic device using rotatable cipher wheels, nor for the purpose of controlling the displacements of the cipher wheels.

In the light of the foregoing paragraphs it must be quite clear that the Hebern mechanism is not " in effect a cipher-key transmitter " as here described and that applicant's claims 1 to 4 are by no means met by the Hebern reference.

Referring to Examiner's statement "If the keying element is necessary to the functioning of the rest of the device, it cannot be said to be independent thereof " , it may be said that the tape is not necessary to the functioning of the device. Considered solely as a mechanico-electrical device which has moving parts actuated thus and so by interaction of its component elements, and not thinking of it as a device for enciphering and deciphering communications, it could operate perfectly satisfactorily without any tape at all. What would happen in this case is that once started in operation the displacements of the cipher wheels would be perfectly regular : all five wheels would step forward one space for each depression of a key of the keyboard. Cryptographically the result would be equivalent merely to the use of a set of 26 different alphabets. This, however, is wholly beside the point raised by the Examiner, viz:, whether or not the keying element, in this case the tape, is necessary to the functioning of the machine. It has been demonstrated that this is not the case and therefore the Examiner is in error in this regard. The keying element is in fact independent of the cryptograph. It was not intended that the fact that it can be replaced be used as an argument favoring its independency of the mechanism itself. That phase of the matter has nothing to do with the present argument. The essential idea here is that of a cryptograph employing rotatable cipher wheels the displacements of which are controlled by an external element, in contradistinction with a

device in which the displacements of the cipher wheels are controlled by an internal element. The applicant can only insist that claims 6 to 10 and 18 are accurate in description and in all sincerity requests the Examiner to reconsider his action in the light of the foregoing remarks :

As for the Examiner's statement that these claims are indefinite in the inferential inclusion of the tape as element of the machine, the applicant has earnestly endeavored to avoid any basis for such an inference. Again and again the specifications and the claims distinctly indicate that the tape is not an inherent element of the machine but on the contrary is an external element, independent of the cryptograph.

In support of the proposition that impositive inclusion of elements has often escaped criticism by the Courts, it is desired to refer to "Patent Claim Drafting " by Dr. Stringham (1930), Sec. 5455, page 211, wherein several cases are mentioned. In connection with one of these (Eibel v. Minnesota , 261 U.S. 45 ; 310 O.G. 3), it is said : "Eibel claim 7 and some of the other claims of the same patent consist exclusively of impositively included elements, except for the introductory nominative. " The Eibel patent in question is No. 845,224.

The Examiner then goes on to say that if the tape is directly included as a machine part, the claims would be subject to rejection on the ground of aggregation, or as an old combination of machine and tape. While not admitting the validity of including the tape as a part of the machine, even if it were admitted, it is difficult to see any basis for rejection on the ground that we have here an old combination

of machine and tape. The Examiner has failed to cite references wherein a cryptographic device employing rotatable cipher wheels is combined with a cipher-key transmitter using a tape. So far as the applicant is aware this combination is novel in the art. However, if the Examiner assumes that the use of a tape in the applicant's invention is merely another way of causing the cipher wheels to be displaced and that a means for such a displacement is inferentially present in Hebern, and that therefore it is merely an old combination, then it is hoped that the discussion in connection with claims 1 to 4 above will serve to clarify the structure and will lead to a change of opinion.

Again, it is desired to stress the point that the Hawley case cited by the Examiner would not apply to applicant's case, even assuming the inclusion of the tape as a positive element. In that case it was said "The substitution for an old element in a combination of an element performing a similar function, but constructed in a different way, does not render the combination itself patentable where there is no resultant change in the operation " In applicant's case the key tape or a plurality of key tapes in the combination as claimed does most emphatically produce a resultant change in the operation viz: that periodicity is prevented, and the elimination of predictable factors is made more effective by multiplying the number of keying elements or tapes, all as elaborated very fully in the previous argument and throughout the disclosure of applicant's case.

Reference Examiner's rejection of claims 11 to 16 on the basis of Hebern who, he contends, "shows mechanism for effecting adjustment of the commutators " , the discussion in connection with claims 1 to 4 above

is again pertinent. The explanation offered as to the distinction between the fixed, invariable, strictly meter-like mechanism in Hebern and the variable mechanism embodied in a true cipher-key transmitter as disclosed by applicant is believed to be quite sufficient to differentiate the applicant's invention and claims 11 to 16 from anything in Hebern.

The suggestion of the Examiner found in the first paragraph, page 2 of the rejection, that " an arbitrary phrase " is used " to designate such mechanism " , must be traversed. Supplemental to what has been said above, attention is called to the repeated use of the term "cipher key " in the Morehouse patent of record in this case. Here an example is found in the patent art for the terminology properly used by applicant. Surely, such patents as Vernam and Morehouse will serve to confirm what has been said above, and give authority and sanction for the use by applicant of such terms as "cipher key ", "cipher key transmitter " , and "cipher key transmitter mechanism ". Moreover, the meaning of these terms in the instant case is well supported by the specification and drawings, always keeping in mind that the specification is to be regarded as the dictionary for the claims in every case.

As to the term "cryptograph " used to designate the machine. The terminology officially adopted by the War Department in its publications dealing with cryptography distinguishes between "cryptogram ", which is the secret writing or message itself and "cryptograph" , which is an instrument, device, or apparatus producing such a writing or message. These terms are strictly analogous to the terms "telegram " and "telegraph".

Moreover, the Encyclopaedia Britannica, article referred to above, follows this terminology. It should be recognized that dictionaries are as a rule unable to keep abreast of advances in highly specialized fields, and one must look to the latest texts and current publications for up to date terminology. The term cryptograph used as a noun to designate a cryptographic device, instrument or machine is found only in the Encyclopedia Britannica of 1929, and in recent texts and publications on cryptography.

Referring now to the decision in Berardini v. Tocci relied upon by the Examiner in repeating his rejection of the method claims Numbers 26 to 34, it is urged that said case is surely insufficient to support the contention that a method of enciphering and deciphering is not entitled to patent protection as a true method or mechanical process. In the cited case, the Court apparently went no further than to hold ~~that~~ in the instance of one of the patents in suit (No. 889,094) that the invention, if any, resided in a "system " , or "art " (using these words as more or less synonomous with method or process) ; but the decision goes on to assert that the art or method as such was not claimed. The claims were, in fact, directed to a "code message " and were in that particular case held void for lack of invention. As just stated above, this case is assuredly not to be regarded as a controlling authority to support the position that no method of enciphering or deciphering is entitled to protection as a true method. The Vernam patent No. 1,416,765 and the Morehouse patent cited in this case No. 1,356,546 , are both in this same art and both include method claims.

As to the inclusion of a recital of structure in method claims, patents of this character are too numerous to mention. Applicant's

position on this point was quite fully discussed in the last argument. Examples of claims directed to methods of performing particular operations, and for methods of manipulating machines, may be cited in large number . In many such examples a recital of structure is necessary to clearness and intelligibility. Surely it must be conceded that the inclusion of structural elements in such cases does not vitiate the method, nor does it follow that the method steps in such cases are merely statements of function of any given machine. It must be remembered in the present case that we have an example of a method of manipulating certain instrumentalities, but obviously these instrumentalities are susceptible of considerable variation so that the essential method steps which applicant is seeking to protect in his method claims require a certain recital of structure for the sake of clearness but this does not preclude the idea of changes and variations in the mechanical instrumentalities. In support of applicant's contention in this regard, it is desired to add to the record several cases listed as follows:

Hazeltine Corp. v. Wildermuth, 34 F.R. (2nd) 635
Ex parte Van Kirk, Pat. No. 1,658,796
Ex parte Trinks, 17 U.S. Pat. Q. 139 , Pat. 1,902,532
Century Elec. Co. v. Westinghouse E. Mfg. Co., 1914 C.D. 267 ; 207 O.G. 1249 ; 191 F.R. 350, Pat. 511,915.

Reconsideration is requested of claims 1 to 4, 6 to 10 and 18, also claims 11 to 16 for reasons fully set out in the foregoing argument. The criticism of claims 11 to 16 on the ground that they include indefinite and functional limitations is thought to be entirely unwarranted since all these claims recite ample structure to support every functional statement there included. Applicant has endeavored in the foregoing argument to show

that the phrasing employed to designate the cipher key transmitter or cipher key transmitter mechanism is not in any sense arbitrary. On the contrary, the terms are well known in the art and are fully supported in the disclosure of this case.

Claims 17 to 25 have been amended to overcome the Examiner's objection as to the inferential inclusion of the "connections ".

The criticisms with regard to claims 18, 21, 22, 23, 24 and 25 have been dealt with in the foregoing argument.

It is believed that there is ample authority for using the word "cryptograph " to designate the machine, and this point has been treated at length in a preceding paragraph.

Further and favorable action is courteously solicited in the light of the foregoing.

Respectfully submitted,

William F. Friedman

By: (Sgd.) F. H. Vandervenner
" Shares O. Roses

Attorney