(No Model.)

A. VON SIMON.

CRYPTOGRAPHIC APPARATUS.

No. 407,425. Patented July 23, 1889.

Fig. 1.

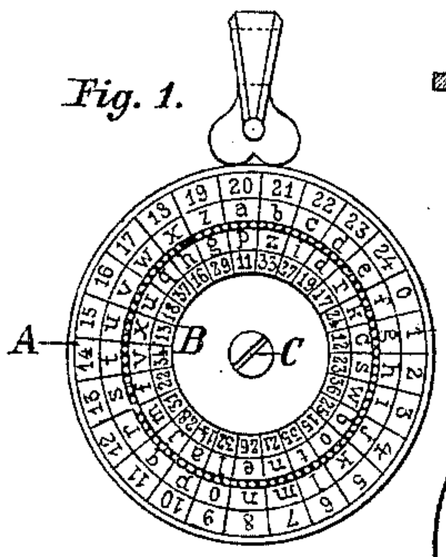


Fig. 4.

Fig. 3.

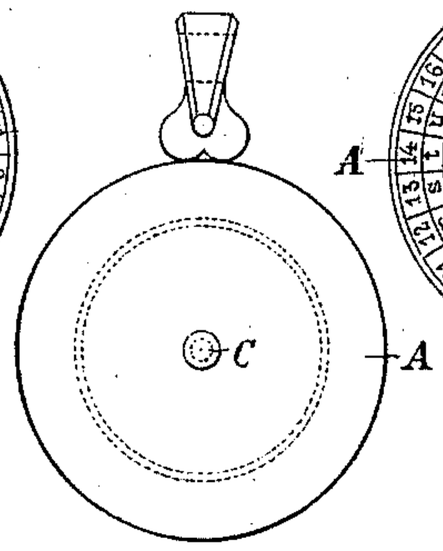


Fig. 2.

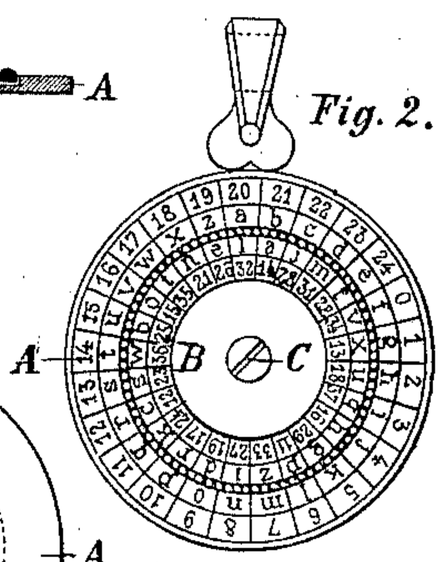


Fig. 5.

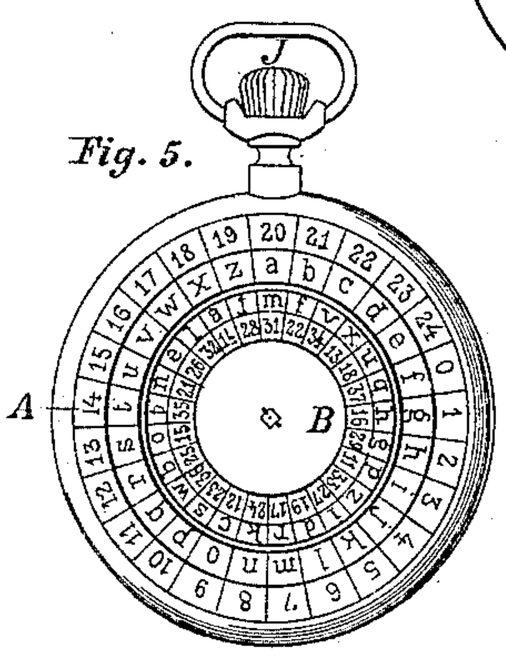


Fig. 7.

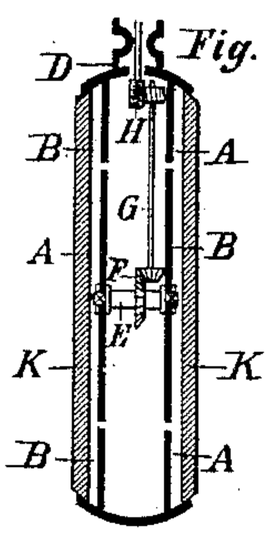


Fig. 6.

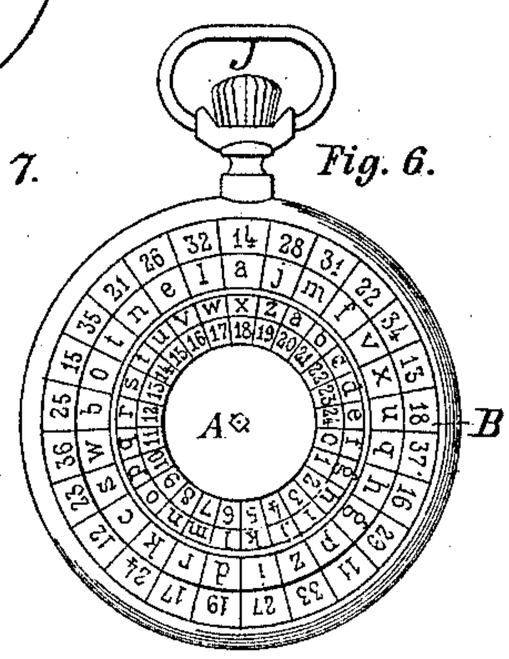


Fig. 9.

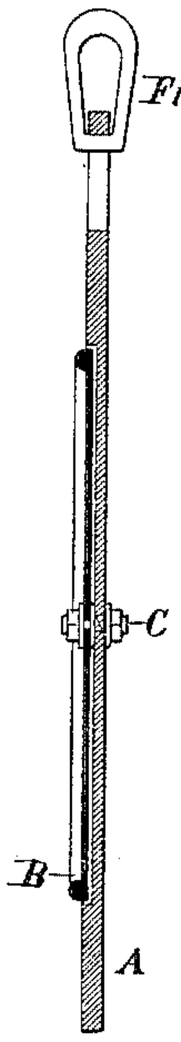


Fig. 8.

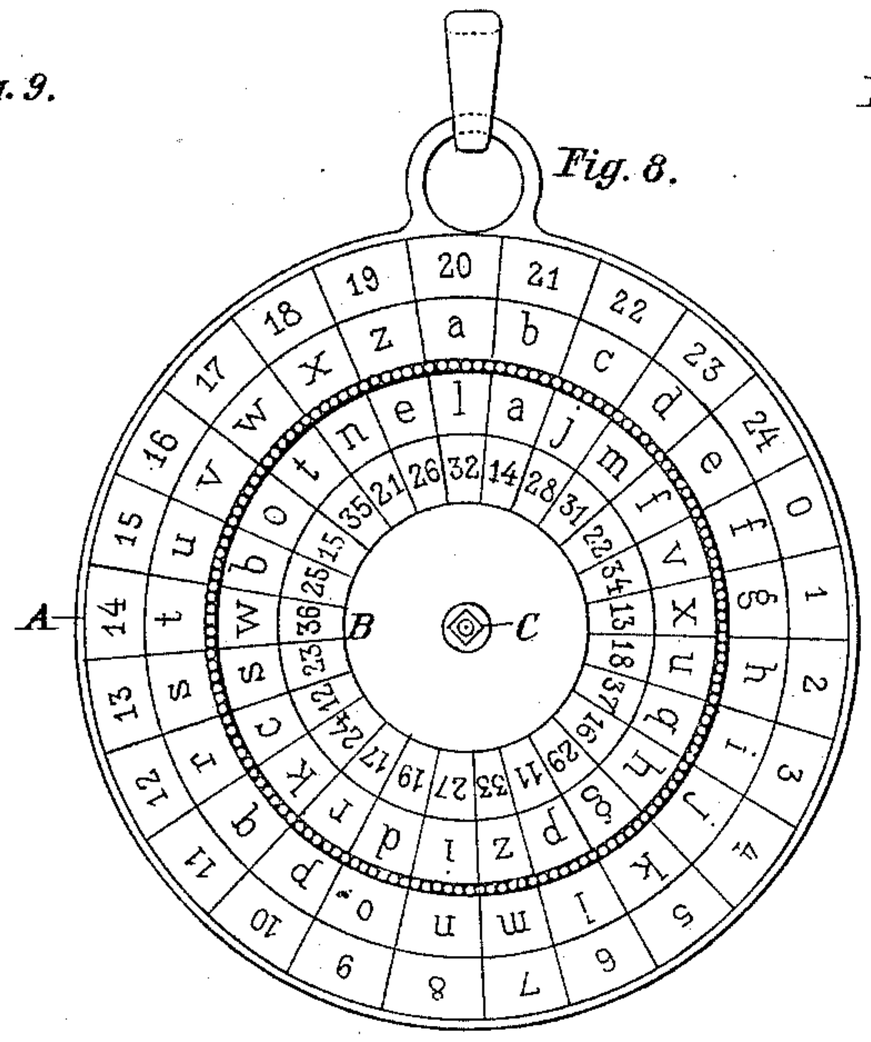
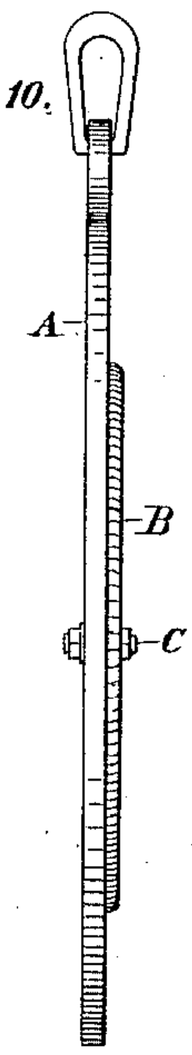


Fig. 10.



Witnesses:
J. A. Criswell
L. K. Fraser.

Inventor:
Alexis von Simon,
By his Attorneys,
Arthur C. Fraser & Co.

UNITED STATES PATENT OFFICE.

ALEXIS VON SIMON, OF VIENNA, AUSTRIA-HUNGARY.

CRYPTOGRAPHIC APPARATUS.

SPECIFICATION forming part of Letters Patent No. 407,425, dated July 23, 1889.

Application filed September 3, 1888. Serial No. 284,487. (No model.)

To all whom it may concern:

Be it known that I, ALEXIS VON SIMON, a subject of the Emperor of Austria, and a resident of the city of Vienna, Austria-Hungary, have invented a new and Improved Cryptographic Apparatus, of which the following is a specification.

This invention concerns an improved simplified cryptographic instrument whose cryptographic disk is so placed in a groove of the alphabet-disk that the upper surface of both disks lie in one level, whereby the instrument is simplified in its shape and made more durable than hitherto existing cryptographic apparatus, because projecting and easily displaced and injured parts are avoided. The instrument can also be produced in watch form, and is then combined with a decipherer. With my instrument I cipher the letters not only by themselves, but also by double figures, whereby any false or doubtful deciphering is avoided, because the person who is charged with the latter work will recognize and understand that every double figure is a letter, but every single figure is only a figure.

The accompanying drawings explain the improvements made, and show in Figure 1 a cipherer in shape of a watch or locket. Fig. 2 illustrates the same kind of instrument set for another reading. Fig. 3 is a rear view of the instrument shown in Figs. 1 and 2. Fig. 4 is a cross-section of the instrument. Fig. 5 shows the instrument in watch form. Fig. 6 shows the decipherer, being the rear side of the instrument represented in Fig. 5. Fig. 7 is a vertical section of the instrument shown in Figs. 5 and 6 and shows the mechanism for moving. Fig. 8 shows an instrument of the same form as in Figs. 1 and 2, but on a larger scale. Fig. 9 is a vertical section, and Fig. 10 a side view, of the instrument shown in Fig. 8.

A is the alphabet-disk; B, the cryptographic disk; C, the rivet fixed in the disk A by a square shank, or otherwise, which forms the axis for the cryptographic disk B and around which said disk B revolves freely. The several parts are made of metal, bone, or other suitable material. As before mentioned, the disk B lies in a depressed portion of the disk A, beyond which only the milled rim of the disk B projects for the purpose of turning it.

In Figs. 5, 6, and 7 both disks A B are inclosed in a watch-case D in the same plane. In this form a special decipherer is applied, which is distinguished from the cipherer in this, that the alphabet-disk A lies inside of the cryptographic disk B, Fig. 6, while the reverse is the case in the cipherer Fig. 5.

The cryptographic disk B of the cipherer and the alphabet-disk A of the decipherer are fastened on the hubs of the axle E, which is mounted in the case D in the same way as in a watch, Fig. 7. Pins hold the disk fast upon the axle. The turning mechanism is indicated by a pair of small conical shells F, by an axle G, arranged in the watch-case in an ordinary way, and by a cog-wheel H. The smaller wheel is mounted upon the axle of the winding-button J, which is turned by hand, like that of a watch. The watch-case is covered on both flat sides by the watch-crystal K.

With this improved cryptographic device, which allows the most manifold combinations, two persons may communicate without a third person, even if in possession of a similar instrument, succeeding in solving the messages.

The use of the instrument is as follows: A person "x," who wishes to send to a second person "y" a cipher communication, selects two letters as keys and prefaces his communication with them. The first letter applies to the alphabet-disk A and the second to the cryptographic disk B. The rotating disk is then turned until the two selected letters are brought into one line. For examples, if "b" is selected for the alphabet-disk and "z" for the cryptographic disk, "z i d v," &c., are the ciphers for "b c d e," &c. The sender of the message then substitutes for the letters of the alphabet-disk corresponding with those of the message sent the letters of the cryptographic disk, which will thus constitute the cipher-message. For example, (see Fig. 1,) suppose the message to be sent and its cipher to be "I start to-morrow" "bzw fvpmv vl nlmmlq." The person "y," who receives the dispatch, will first give his attention to the first two letters "bz" as keys. The first letter (in the case "b") must be sought in the alphabet-disk and the cryptographic disk must be turned until its "z" stands under "b." Thereupon the instrument is set for every letter. In this

instance "w" stands for "i," "s," "v" for "t," "p" for "a," &c. If figures only are selected for the cipher, the proceeding is as in the example just given, the first figure being a key applying to the alphabet-disk, and the second figure the key for the cryptographic disk—for example, Fig. 8, "Business done," "203 21425233727222323311927 22." In deciphering the four first figures are separated, the first two figures standing for the alphabet-disk, the second two for the cryptographic disk, and the interlying letters on the alphabet-disk being substituted therefor; but, if so preferred, the key letters or figures need not be included in the message, but can be agreed upon in advance—as, for instance, for all dispatches the initial letter of the christian name of the sender must be looked for in the alphabet-disk and the initial letter of the given name of the receiver in the cryptographic disk, which thus constitute the key. For instance, if a Karl and a Wilhelm have selected this mode and the former desires to send a message, the cryptographic disk must be turned until the "W" (the initial letter of the receiver) comes in line with the "K" (initial letter of the sender) of the alphabet-disk.

The combinations which may be seleted for the key are without number. For instance, the initial and end letter of the day on which the dispatch was set can be selected—"Wednesday," "W" alphabet-disk, "y" cryptographic disk—or the initial and end letter of the month in which the message is sent may be used as the key; or the alphabetic order of the letters may be selected as follows: In the first dispatch "a b," in the second dispatch "c d," in the third "e f," &c.

In every case the first letter always stands for the alphabet-disk, and the second letter always for the cryptographic disk; but an understanding can be had not only about the key of a dispatch, but also about a change of the key within the same dispatch. Somebody might think, for instance, that a word might be deciphered by chance and then the key found for the entire contents. To overcome this objection, it can be previously understood that the key will be changed after each word. Then to the first word applies the key agreed upon for all dispatches. The correspondents Karl and Wilhelm having selected, for instance, the initials of their names—viz., "K" and "W"—agree that the key shall be changed from word to word by letting the two last letters of each word of the text of the dispatch always form the key for the next word. For example, take the sentence "Everything quiet on the ship." The receiver must in deciphering take the letters "K W" as the first key, and after having deciphered the first word use the two last letters of the deciphered word as the key for the next word. The keys for the foregoing example would, therefore, be "K W, N G, E T, O N, H E." A word consists of one letter only. Such letter stands for both disks. The cipher dispatch may also consist of alternate letters and figures, so that for each letter the corresponding figures can be substituted, for instance, using the arrangement shown in Figs. 5 and 6, "Arrived to-day," "m25B11E 18X 35C 13M11." By this method the repetition of two identical successive letters in one word is avoided, and deciphering from this clue is rendered impossible.

From the foregoing it can be seen that the combinations as to the key and its changes are numberless, and that therefore deciphering is an impossibility for the uninitiated.

It may be mentioned here that in the place of the letters and figures mentioned any other letters and signs may be used and that the cryptographic disk B need not be depressed.

I claim as my invention—

A cryptographic apparatus comprising, in combination, two parallel annular fixed ring-disks and two rotary circular disks on the same axis concentric with said annular disks, respectively, said circular and ring disks having on their exposed or reading surfaces visible characters, the characters on the circular disk on one side being repeated on the annular disk on the opposite side, substantially as set forth.

ALEXIS VON SIMON.

Witnesses:

EDMUND JUSSEN,

OTTO SCHIFFER.