CLASS: Cipher Machine (Electro-mechanical)
SYSTEM: Combined Monographic Substitution and Simple Transposition
METHOD: Two Circuit-Rotor Mazes, Through Paths, Gear Motion Control

NAME: Koch Transposition-Substitution Cipher Machine

DEVELOPMENT:

Invented by H. A. Koch. Application for basic patent filed in the Netherlands, 7 October 1919. Assigned to Naamlooze Vennootschap Ingenieurs-bureau "Securitas", Amsterdam, Netherlands, a firm associated with Chiffriermaschinen Aktiengesellschaft of Berlin, who later developed the "Enigma". Never manufactured commercially.

PATENTS:

U. S. 1,533,252 (H. A. Koch, 14 April 1925, Cl. 197-4). One of three pneumatically operated machines described in this patent combines transposition and substitution features. Will not decipher.

Ger 38[illegible],682 (Naamlooze Vennootschap Ing. Bureau "Securitas", 27 November 1923, Cl. [illegible] 14). Improved electro-mechanical version of the machine described in U. S. Patent 1,533,252.

DESCRIPTION:

A keyboard-operated, page-printing cipher machine which combines both substitution and transposition features. A transposition of characters within each line of printed text is accomplished by means of a circuit-rotor maze which controls the linear displacement of a typewheel relative to the page on which cipher characters are printed. After the printing of a line of text (which must be of a definite length, determined by the number of exit points from the rotor maze), the rotors are stepped by a set of gap-toothed gears. The substitution process occurs in two phases. A given plain-text character is first enciphered through another set of circuit rotors which, like the transposition rotors, are stepped at the end of each line of cipher text. It is then re-enciphered through one of a group of relay banks before being printed. The selection of the particular relay bank used to accomplish this super-encipherment is determined by the position within the line to which the character is transposed. Therefore, the first substitution is monoalphabetic within each line and the second substitution is monoalphabetic in identical positions among the various lines of cipher text. To decipher, the direction of the circuit paths through both rotor mazes and through the relays must be reversed by means of an encipher-decipher switching arrangement (not shown in the accompanying drawing).

In order to simplify the illustration, a machine with only six different characters and a line length of six has been shown. The keyboard universal bar has two functions: When a key is depressed, this bar is activated, closing contact (1); also, pawl (3) is caused to engage a tooth of the ratchet wheel associated with commutator (4). Rigidly mounted on the same shaft with this ratchet wheel are the brush-arm of the commutator and the single-tooth pinion (5). When the key is released, the universal bar is returned to its normal position through spring action, contact (2) is broken,

and the ratchet-wheel assembly is stepped forward one position, causing the brush-arm to move to the next segment of commutator (4). Once during each revolution of the ratchet wheel, the single tooth of the pinion engages the cogwheel with which it is in register and the shaft carrying the gap-toothed gears is advanced one step. Through the action of these gears, the rotors in the two mazes are stepped irregularly.

The relay unit consists of as many banks as there are exit points from the transposition maze, each bank having as many contacts as there are exit points from the substitution maze. Current through a given lead from the transposition maze will energize one of the electromagnets (6), causing the bank of contacts associated with it to close. Current through another lead from the substitution maze will then be allowed to flow, via one of the closed circuits, to a segment of commutator (13). The contacts of the various relay banks are connected to the output leads in different orders, as shown.

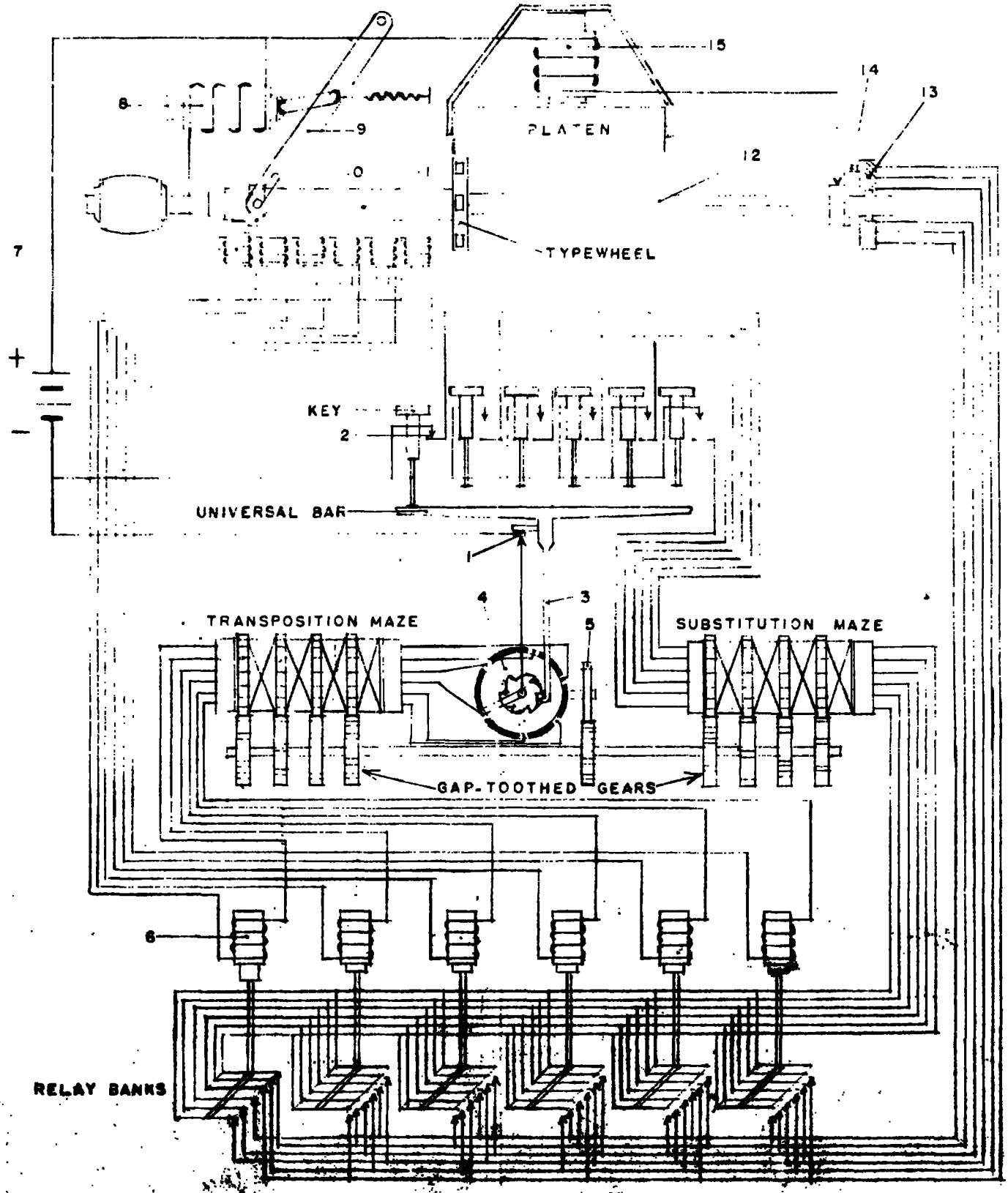
The printing mechanism operates as follows: The typewheel is mounted on a four-sided shaft (12) along which it can slide laterally. This shaft is rotated continuously by a motor. Attached to the typewheel is a cylindrical member (11) which fits over the shaft as a sleeve and on which a ring (10) is mounted so that, although it is fixed in position on the sleeve (11), the latter may rotate freely within it. Through the linkage shown, the lever (9) is capable of displacing the typewheel assembly laterally along the shaft (12). When the magnet coil (8) is energized, its movable core is pulled in and the typewheel is moved to the left; when it is de-energized, the typewheel is returned to its extreme right-hand position by spring action. When one of the magnet coils (7) is energized, its core is raised and the leftward movement of the typewheel is blocked by the engagement of ring (10) with this projecting core. Brush-arm (14) is rigidly mounted on the square shaft (12) and as the latter rotates the brush-arm passes over the mutually insulated segments of commutator (13). When the brush-arm reaches a conducting segment, current is transmitted to magnet coil (15) which, when energized, causes the platen to strike against the typewheel and so print the character associated with the segment of commutator (13) through which current has passed.

When a key is depressed, two circuits are completed successively: First, contact (1) is closed by the universal bar action and current flows from the positive pole of battery via commutator (4) through the transposition rotor maze to one of the magnets (6) which, when activated, closes the bank of relay contacts associated with it; thence through the coil of one of the magnets (7) to coil (8) which interact to displace the typewheel laterally as described above; and back to negative battery. Then, immediately after the closing of contact (1), the contact (2) of the particular key depressed is closed and current flows from battery via the substitution rotor maze to the relay banks and from there, through the path made available by the action of magnet (6), to a segment of commutator (13), from whence it is transmitted via brush-arm (14) to coil (15) and back to battery.

As described in the patent, variable keying elements include only the rotor order within the two mazes and the relative alignment of the rotors for a particular message encryption. No provision is made for interchanging, replacing or otherwise varying the relationships among the gap-toothed gears, but the possibility of changing the circuit paths through the different relay banks by means of a plugging arrangement is suggested.

Note: In the first patent on this machine pneumatic instead of electrical circuits are used, the relay banks have been omitted and the gears controlling the motion of the substitution rotors are stepped each time a key is depressed,

thus making decipherment in a single operation impossible. The inventor apparently overlooked the fact that it would be necessary first to replace the cipher characters in their proper order through the transposition maze, and then to decipher this correctly arranged sequence through the substitution maze in order to obtain the original plain text. In the later patent, another version of the machine is described in which the relay banks are omitted and the stepping of one of the rotors in the substitution maze is controlled, through a rather crude wire and pulley linkage, by the lateral movement of the typewheel assembly. Thus, the position to which the typewheel is displaced by the transposition unit determines the substitution alphabet used to encipher a given character.



KOCH CIPHER MACHINE