

Telecrypto ApparatusType TKG 5/14A. General

The telecrypto apparatus has been developed in order to ensure secrecy in telewriting communications. In such cases the telewriters will not be connected directly to the line but over the telecryptos as per figs. 1 and 2.

The secrecy of the messages transmitted over the line is obtained in such a way that every and each of the impulse combinations, emitted from the telewriter on depressing keys on its keyboard will be modified in the telecrypto, and will be transmitted over the line in this modified (ciphered) form. At the receiving end the ciphered impulse combinations will be re-transformed through the action of the corresponding telecrypto apparatus and received by the telewriter in its original form, so that both telewriters will write the original text. When transmitting a message the telewriters are used in the normal manner, as if no additional apparatus were connected. The reading of the communications on the line by third parties will however not be possible, as the impulse combinations between both telecrypto apparatus are ciphered.

B. Telewriting system.

The telecrypto is constructed in such a manner that it can be used for both 5-pulse and (after reconnection) for the 14-pulse system.

1. Telewriting system according to the international 5-pulse-code. The different signs are composed and transmitted by 5-pulse combinations.

Declassified and approved for release by NSA on 11-19-2014 pursuant to E.O. 13526

DR. ING. E. GREENER ZÜRICH

Dat. 1949

17th Oct 49

Nn.

Main operating systems: closed circuit current
Double current
Audio frequency telegraphy

Maximum operating speed: 7 signs per second.

2. ETK-telewriting system (Dr. E. Gretener A.-G.).

The different signs are composed and transmitted by 14-pulse combinations. The respective signs are not printed, as f.i. with the 5-pulse system, in one operation, but combined from 14 different elementary signs. Each element corresponds to one of the 14 impulses.

Operating system :

Audio frequency telegraphy

Maximum operating speed : 5 signs per second

Advantages: A much simpler construction and smaller overall dimensions and weight than those of the 5 pulse system. Considerably smaller risks for faulty transmission, especially for radio communications.

C. Operating principles.

The telecrypto apparatus produces impulse series of the same character as those of the telewriting apparatus employed, i.e. 5-pulse combinations when used in conjunction with telewriters operating on the international system and 14-pulse combinations when used with ETK-apparatus. The crypto-impulse-series and the impulse combination of the telewriter (clear text-impulses) will be combined, i.e. converted in the manner hereinafter described so that the cipher-impulse series is obtained, and this impulse-series is then transmitted.

At the receiving end these ciphered impulse series are again converted with an identical cipher-impulse series and the original clear text impulse series will be reconstituted. The crypto-impulses materialize every time a key on the telewriter is depressed by the start impulse of the telewriter.

The composition of the crypto-impulse combinations varies from sign to sign and the series of these variations is to all practical purposes limitless. If one f.i. would always strike the key "A", then the ciphered impulse combinations in the line would change continuously.

Fig. 3 illustrates as an example the transmission of the letter "Y", according to the 5-pulse code. 1 - 5 are the five elementary impulses, + when current and - no current.

Line 1 shows the impulse combination, produced by the telewriter, line 2 shows a crypto impulse combination, in this example the combination for the letter "L". In the line 3 multiplied product of lines 1 and 2 is obtained of the elementary impulses. The conversion is done according to the following rule of a multiplication

$$\begin{array}{l} + \cdot + = + \quad + \cdot - = - \\ - \cdot - = + \quad - \cdot + = - \end{array}$$

It will be seen as a result of the ciphering operation that the letter "O" is obtained in this case. If the line is tapped with a telewriter (without telecrypto), there will be obtained the letter "O" instead of "Y".

From the lines 4 - 6 will be seen that the original sign combination, as produced by the sending telewriter, will be reconstituted by the multiplication of the ciphered impulse combination with the corresponding crypto impulse combination.

5-pulse system.

As practically all the possible different impulse combinations in this system stand for signs (letters, numerals, punctuation signs), the ciphered impulse combinations will give readable signs during transmission. The action of the telecrypto apparatus consists in this case of the exchange of signs: The letter "Y", for instance, as written on the telewriter, may be exchanged for an "O" as shown in the example above. A person, who taps the line and has no knowledge of the crypto impulse series employed, will thus obtain letters and numerals in an absolutely arbitrary sequence.

14-pulse system

With the 14-pulse system about 16'000 impulse combinations can be obtained; of these only about 50 combinations (= 0,3%) give readable signs. By the conversion of the clear text combinations with those of the crypto series, there will generally be obtained unreadable impulse combinations in the ciphered impulse series, so that an "X" may for instance be changed into \boxtimes etc. A telewriter, branched on to the communication channel, and not equipped with a telecrypto apparatus, will here write unreadable signs.

D. The ciphering keys

The keying elements of the ciphering key serve to obtain the variable crypto-impulse series. As elements for the ciphering keys a number of wheels (f.i. 14) are used. These pin wheels carry a number of slidable or rotatable pins, which can be displaced individually, by hand, and can take two different positions. In one of these positions one or several contacts will be closed (or opened), and vice versa in the other position. Each pin is defined by a number on the circumference of the pin wheel (key number). These key numbers are also used to define the starting positions of the pin wheels. An operating mechanism acts on the pin wheels and moves them after each transmitted sign, in an irregular manner. The movement rhythms can be varied and can be changed arbitrarily by hand.

The pin wheel contacts are connected in accordance with a special system. The connections terminate at a collector, which has five sectors for the 5-pulse system and 14 sectors for the 14-pulse system. The individual segments are either electrically activated, or not, depending on the position of the pin wheels. When a collector brush passes all segments, a 5-pulse or 14-pulse combination, or the so called crypto impulse series, is obtained.

An exceedingly complicated "program" for the composition of the crypto impulse series is obtained on account of the

system used for the connection of the pin wheel contacts. If f.i. the first impulse element gives "current" or not may depend on the position of up to 12 pin wheels, and their position at that moment is dependent on the combinations used for the movement of the pin wheels up to that moment.

Additional keying elements are also used, in the form of ciphering (permutation) collectors, of which one is always supplied. This is adjustable by hand. On special demand one or two extra ciphering collectors, which obtain the same irregular kind of movement as the pin wheels, are also supplied.

The ciphering collectors are marked on their circumferences with numerals in order to define their starting positions. There are also supplied special connector plates, which can be exchanged in a very simple way.

The pin wheels and the two ciphering collectors with automatic movements PS 1 and PS 2 (Fig. 4) are mounted on a shaft at the front end of the apparatus, while the hand operated ciphering collector PS 3 is to be found at the right hand side of cover of the machine.

E. Composing the ciphering key settings.

We distinguish between interior and exterior settings. The interior settings are changed more or less frequently, depending on the intensity of the crypto service, while the exterior settings are composed when starting a communication series, or eventually every time a telegram is sent.

The TKG 5/14 allows the following key settings :

a) Interior key settings.

1. The positioning of the pins on the pin wheels, which total about 500.
2. Arbitrary arrangement of the movement program for the 14 pin wheels and the two ciphering collectors.
3. The choice of different connection plates for the ciphering collectors.

b) Exterior key settings

1. The starting positions of the 14 pin wheels at the beginning of the communication, about 35 different positions for each pin wheel are possible.
2. The starting positions of the three ciphering collectors, each collector can take 28 different positions.

Both the interior and the exterior keys can be set by hand without any tools.

To set the pin wheel pins, as well as the starting positions of the pin wheels, a plexiglass cover is opened with the aid of the lever "H", when a sufficiently large sector of each pin wheel will be uncovered.

In order to compose the movement program for the pin wheels and ciphering collectors, the protective cover "A" is opened. The changes can be made by varying the position of contact plugs.

It should be noted that the different key elements can be adapted within reasonable limits to the needs of the customers, with regard both to construction and wiring diagrams.

The construction of the TKG 5/14 apparatus offers an exceptionally high degree of safety, when fully equipped. In many cases the equipment can be simplified; the wishes of the customer can be taken into account.

The telecrypto will be built in such a way that the same apparatus can be used together with telewriters according to the 5-pulse or the 14-pulse system. The change-over from one system to the other is done by changing the position of a connecting plug "U", after removing the cover plate "P" (Fig. 4), and by the exchanging of two gear wheels.

The telecrypto apparatus will be built for

- | | | |
|---|---|----|
| <ol style="list-style-type: none"> 1. 5-pulse closed circuit current 14-pulse ETT | } | or |
|---|---|----|

- | | | | |
|----|--|---|---|
| 2. | 5-pulse double current
14-pulse ETT | } | or |
| 3. | 5-pulse ETT
14-pulse ETT | } | according to the wishes of
the customer. |

Wire or radio can be used as communication channels. In case of radio the smaller sensitivity of the 14-pulse system against perturbations should be noted.

F. Electrical dater.

The telecrypto apparatus can be used with :

1. 110, 125, 145, 220 and 250 volts alternating current,
50 cycles
Power consumption abt. 100 VA.
2. 12 volt direct current (Battery)
Power consumption abt. 70 Watts.

G. Mechanical construction, dimensions and weight.

The telecrypto apparatus consists, as will be seen on Fig. 4, of a frame of sheet metal UT, which contains the electrical elements such as vacuum tubes, transformer, resistances, condensers etc. and of an upper part OT, which contains the mechanical elements : motor, gears, ciphering collectors, pin wheels etc. The upper part is hinged on the base, and by tilting it up, all parts in the interior of the base will be easily accessible.

A carrying case is provided for the transportation of the apparatus.

The dimensions of the TKG 5/14 will be seen onf Fig. 4. They are :

Width	Depth	Height
410 mm	350 mm	225 mm

The weight is about 55 lbs. (25 kg.)

H. Operation.

After having connected the telecrypto to the mains, or to a battery, and to the telewriter, service communication is first established in clear text. The lamp L_1 indicates that the apparatus is connected. The switch S is set in the position "clear" which disconnects the ciphering mechanism of the telecrypto. In this position a red lamp L_2 warns that clear text is being sent. After having sent the routine messages, and after having made all key settings, the switch is changed over to "Crypto", after which the secret communications can start.

When the transmission conditions are poor, f.i. atmospheric disturbances when using radio channels, it may happen that the two telecrypto apparatus fall out of step. From this moment the deciphering at the receiving end will become faulty, so that the receiving telewriter will not write clear text any longer.

The operator at the receiving end will in this case strike the special key of his telewriter, which interrupts the transmission. Both operators then put their switches S in the "clear" position. In order to avoid the tedium of making new settings of the secret keys, a counter "Z" is provided for, which automatically counts the number of operations of the telecryptos. In order to put the two telecryptos into step again, the operator of that station, whose telecrypto got behindhand, has only to press the button D a number of times, until his counter shows the same number as his correspondents. When this is obtained, the switch S is put back into position "Crypto", and the transmission of the secret message can be continued.

FS : Telewriter

- 9 -

TC : Telecrypto

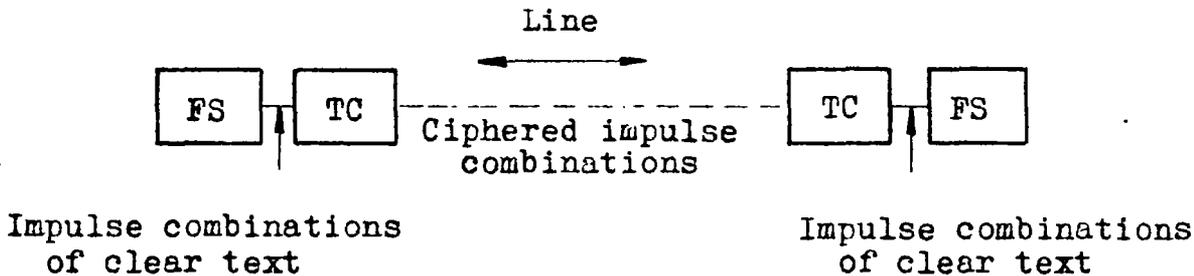


Fig. 1

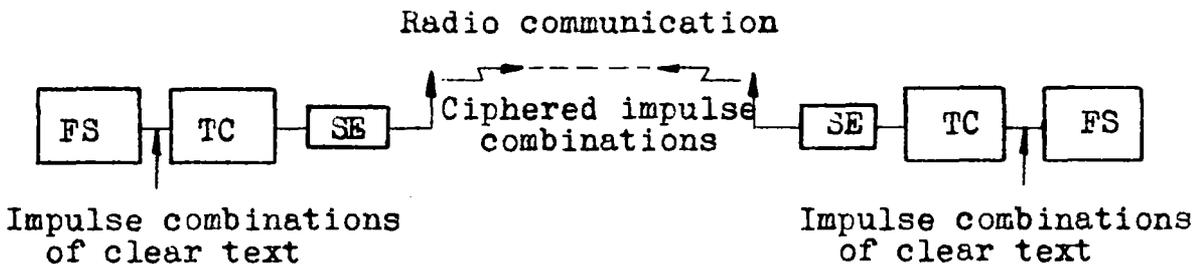


Fig. 2

	1	2	3	4	5	
Y	+	-	+	-	+	Impulse combination of the telewriter
L	-	+	-	-	+	Ciphering combination of the transmitting telecrypto apparatus
O	-	+	-	+	+	Ciphered pulse combination (transmitting side)
						Transmitting Channel
O	-	-	-	+	+	Ciphered pulse combination (receiving side)
L	-	+	-	-	+	Ciphering combination of the receiving telecrypto apparatus
Y	+	-	+	-	+	Clear pulse combination on the receiving side.

Fig. 3

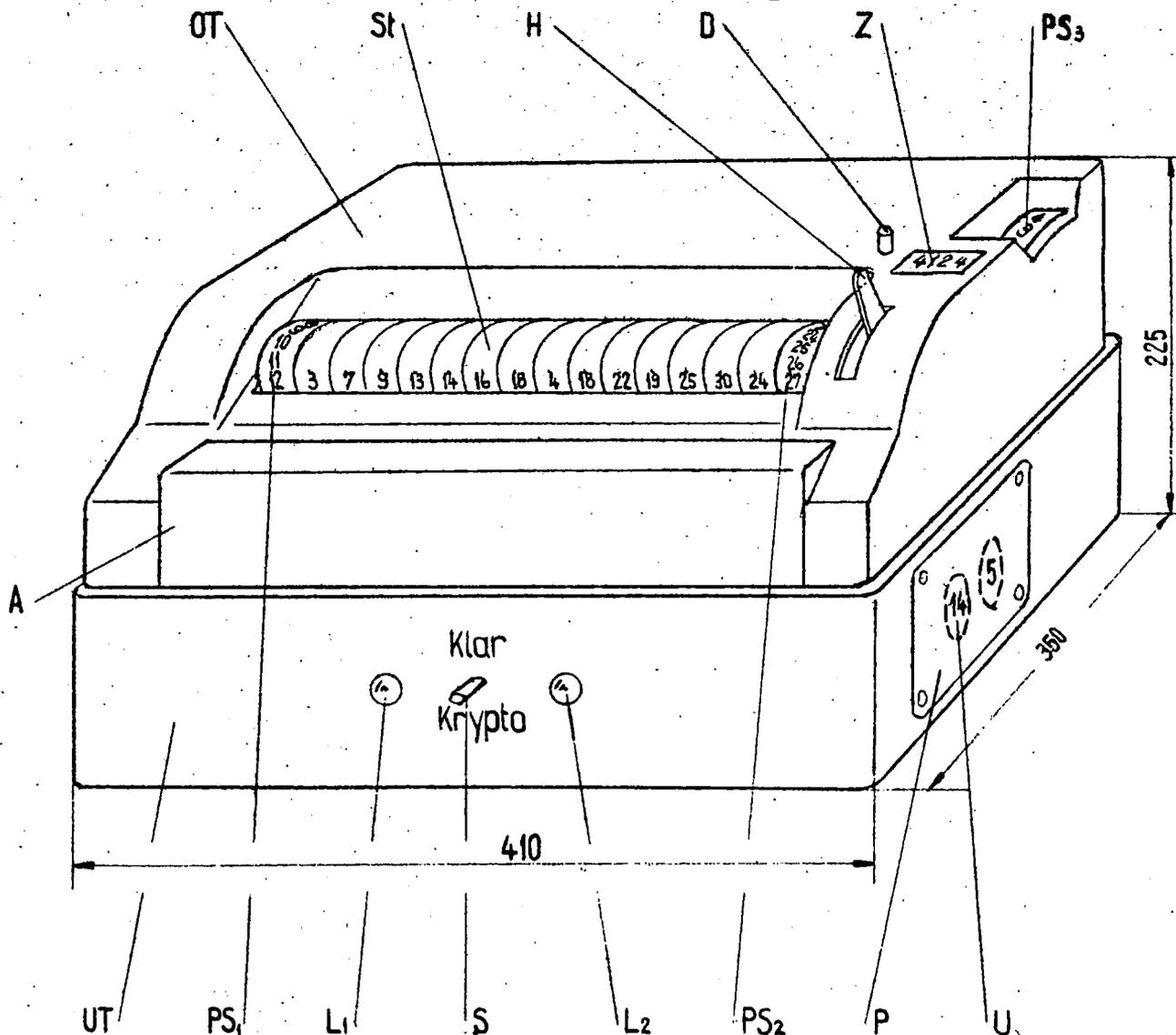
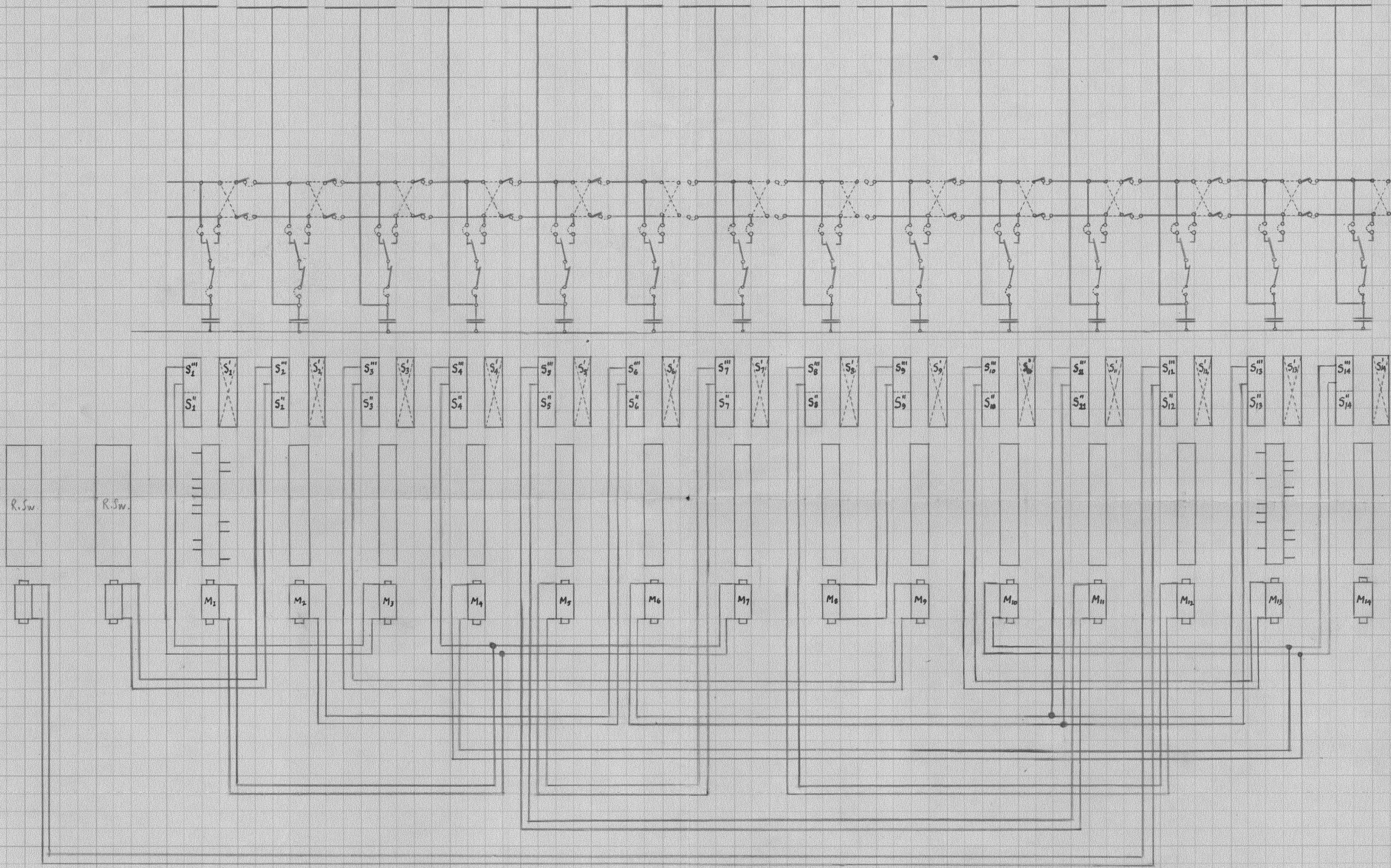


Fig. 4

St	=	Pin wheels
H	=	Lever
PS 1	=	Ciphering collector automatically driven
PS 2	=	" " " "
PS 3	=	Ciphering collector driven by hand
S	=	Switch
L 1	=	Red lamp
L 2	=	Green lamp
Z	=	Counter
D	=	Button of correction key
U	=	Connecting plug 5-pulse to 14-pulse system
P	=	Cover plate for the elements to change the movement program of the pin wheels.
OT	=	Upper part
UT	=	Below part.



INTERLOCKING PIN ROTOR ARRANGEMENT

14	
10	4
13	1 7
6	3 5
2	9 11
R.S.W.	8 6
	12
	R.S.W.

THIS DRAWING REPRESENTS AN ARBITRARY INTERLOCKING STEPPING ARRANGEMENT AMONG THE 14 PIN ROTORS AND THE ROTARY FEEDER AND SEPARATOR SWITCHES. PIN ROTOR 14 MOVES REGULARLY. ABSENCE OF A PIN AT READING POSITION ON ROTOR 14 WILL NOT ACTIVATE ITS ASSOCIATED MAGNETS, THEREBY ADVANCING ROTORS 4 AND 10. PRESENCE OF A PIN WILL CAUSE ACTIVATION OF THE TWO MAGNETS, THEREBY PREVENTING MOVEMENT OF ROTORS 4 AND 10. IN TURN, ABSENCE OF A PIN AT READING POSITION ON ROTOR 10 WILL ADVANCE ROTOR 13. ROTOR 13 WILL ADVANCE, THEREFORE, SO LONG AS NO PIN IS READ ON ROTOR 10, REGARDLESS OF MOTION OF ROTOR 10. THE MOTION OF THE MACHINE IS THEREFORE COM.

HAGELIN-GRETENER CIPHER TELEPRINTER
TYPE TKG 5/14
1949