CIPHER DEVICE 39
(Precise acquaintance with the Enigma cipher machine is assumed)

I. General

Device 39 is a further development of the Enigma cipher machine in mechanical and crypto-technical respects as well as in regard to operation. It is a completely automatic cipher machine, i. e. by pressing a letter-key the mechanism of the device is set in operation, the corresponding letter (letter on the key board) is enciphered or deciphered and the plain and the cipher letters are printed on separate paper tapes by means of a double type-wheel printer. The cipher text is automatically divided into groups of five letters. Independent of the printing device the cipher letter may also be read off the lamp field.

In this paper only the crypto-technical part is treated.

II. Drive Mechanism[1]

The three pin wheels (Nockenraeder) A 1, 2,3 are mechanically coupled with the three cipher wheels B1,2,3. Mechanical provision is made that the pin wheels A1,2,3 and the cipher wheels B1,2,3 move one step each time a key is pressed. The cipher wheels however are prevented from executing the step, if at the feeler lever C1,2,3 of the associated pin wheel there is a positive pin. The cipher wheels have 26 divisions, pin wheel A1 has 23, pin wheel A2 has 25 and pin wheel A3 has 27. On each pin wheel an odd number (excluding the number 13) of pins is set in the usual way as daily key. The period (Frequenz) of the individual pin wheel corresponds therefore exactly to the number of divisions. That means 23 steps for A1, 25 steps for A2, and 27 steps for A3. The common period of the three pin wheels is the product of the number of divisions 23 x 25 x 27 = 15,525 steps. The period of the cipher wheel is 26 steps when uninfluenced by the pin wheel. The movement of the cipher wheels is dependent however upon the associated pin wheel period. With 23 steps pin wheel A1 makes a full revolution, cipher wheel B1 however makes only 23 steps less the number of positive pins. Since the number of divisions of the pin wheel and the

1. See Supplement.

number of positive pins[2] are prime to 26 (number of divisions of the cipher wheels), we get for A1 - B1 a period of 23 x 26 = 598 steps, for A2 - B2 25 x 26 = 650 steps and for A3 - B3 27 x 26 = 702 steps. Since the position of all three cipher wheels with respect to one another is decisive for the ciphering procedure, the function of the cipher wheels must be considered as a whole. The period of the cipher wheels without the influence of the three pin wheels is 26 steps. Taking into account the 26^3 possible settings and eliminating the cyclic period displacements there are from a crypto-technical point of view 26^2 effectively different basic periods of 26 steps.

Under the influence of the pin wheel functions A - C1,2,3 the basic period of the cipher wheels is lengthened by the product of the number of divisions in the pin wheels A1,2,3. Hence there are 26^2 effectively different periods, whose constant lengths are given by the product of the number of divisions of A1, 2, 3 and B (1,2,3). If the number of divisions A1,2,3 and B1,2,3 are broken up into prime factors, then the product of the different prime factors gives the length of the period and the product of the like prime factors the number of effectively different periods. Hereby the repetitions of prime factors which occur within the number of divisions of one wheel (A2 and A3) must be regarded as different factors because here the unsystematic pin settings (positive and negative position of the pins) is decisive.

	A1	A2	A3	B1	B2	B3
	23	25	27	26	26	26
Prime factors:	23 · 5·5 · 3·3·3 · 2·13			·2·13	·2·13	· 2·13
Length of the period:	23 · 5·5 · 3·3·3 · 2·13 ..... = 403,676 steps					
Number of periods:	..... 2·13·2·13 = 676 periods					

In the development of Device 39 it was necessary to provide for correspondence with the Enigma when the pins on the pin wheels are put in the negative position.[3] This mechanical function will not be described here because it

2. The difference must be prime. See page 15. [Editor's note]

3. This was demanded by the German Navy. [Editor's note]

represents a purely mechanical demand rather than a crypto-technical necessity. Through this mechanical demand it did come about of course that the 676 periods passed over into one period. In regard to security it appears to be immaterial whether a cipher device yields 676 effectively different periods of 403,676 steps each or one period which is equal to the product of these two factors.

The three cipher wheels are mounted between the entry wheel B7 and the reversing wheel B8. On the sides of the cipher wheels B1-8 are mounted 26 contacts. These contact points are constructed as disk spring contacts. Within each of the cipher wheels B1-8 the 26 contact points on the one side are connected in any desired order with the 26 contact points on the other side. The contact points of the entry wheel B7 are connected to the 26 A-jacks D1 of the plugboard and the 26 contact points of the reversing wheel B8 are connected to a 26 part plugboard E1. These 26 jacks are united in pairs by interchangeable one-pole plug connections E2 (according to key).

With the mechanical rotation of the cipher wheels the contact points necessarily perform a switching function. The 26 A-jacks D1 are united with one another in pairs via the contact points B7, B3, B2, B1,[4] B8, E2, B8, B1, B2, B3, B7. Due to the differing internal circuits of the cipher wheel, which are subject to no particular rule, constantly new combinations result with the 26^3 positions of the cipher wheels.

In contrast to the Enigma two essential advances may be noted in the development of Device 39 in respect to cryptographic technique:

a. The non-uniform and variable stepping of the cipher wheels.

b. The combinations made possible by the variable reversing wheel E1, which moreover is readily changed since it is pluggable.

By these two improvements on the Enigma principle it has become virtually impossible to make Hollerith studies of the constants of the device which would favor the possibility of cryptanalysis.

The following disadvantages, however, are retained which are related to the Enigma principle and which involve an as yet unknown possibility of solution:

---

4. Order of wheels is reversed by error. See Supplement. [Editor's note]

a. The reciprocal structure of the cipher alphabets which is produced by a function of the reversing wheel E1.

b. The two-pole combinations of the plug connections D3, which have a limiting effect on the designations of the keys.

The principle factor of insecurity in all cipher systems remains here, namely, that in spite of all the highly developed mechanical cipher devices, the security of the systen is dependent on the choice of the message key. We shall return to this point later.

III. Cipher Process

The cipher process is carried out by means of the 13 circuits which have their beginning and their end in the 26 A-jacks of the plugboard D1, the 26 keys G and lamps F to each of which one letter of the alphabet is associated. The key board and lamp field (type wheel printing system) take over alternately the function of the plain and cipher alphabet. Since the alphabets are reciprocal no change in the wiring is required.

By pressing one of the 26 keys G a set of springs is activated. In so doing two contact springs are opened and two others closed. The one set of contacts H controls the type wheel (represented only by the terminals in Supplement 1). The other circuit, which is controlled by the second set of contact springs, switches in the circuit which makes possible the cipher process by means of the lamp field and the three cipher wheels.

Device 39 is to be set according to the daily key. The daily key consists, for instance, of the following data:

Wheel position: III IV I

Plugboard connections: bh qv do gm ac wy fl tx ei kr pz jn su

Reversing wheel: pn dh io at hs br jq cz fy gx ew lv ku

Pin wheel A1 acegiknprtu (11)

Pin wheel A2 bceghlmprtu (11)

Pin wheel A3 acefhjlmprsuvxz (15)

Before ciphering a text the three cipher wheels and the three pin wheels are to be set in an initial position which hereafter will be called the message key setting. The message key setting is to be treated quite individually because a great part of the security of the cryptogram depends on its selection. (10 messages in phase can be solved, whereby it does not matter which Enigma principle has been employed.)

The 6 letters of the message key are disguised in the usual form and prefixed at the beginning of the cipher text. To agree upon a different position has no significance as far as security is concerned because the letters will be recognized as a kind of indicator group in any case. Beginning with the message key setting, the letters of the plain text are enciphered by pressing the corresponding keys and the appropriate cipher letters are printed by the mechanical printing device. When deciphering the process is analogous.

IV. Choice of the Message Key and Its Consequences

On the basis of the experiences of the last fifteen years an attempt must sometime be made to determine why the analysis of cryptographic systems, some of which were very complicated and diverse, has been successful. Two essential types are noted in this connection:

(1) Cryptanalysis by the aid of compromises of all sorts

(2) Cryptanalysis with the aid of repeated periods (lining up or matching).

The possibilities of cryptanalysis which fall under point (1) can be counteracted in the case of substitution systems by the requirement that reconstruction of the daily key be impossible even with any technical aid. The requirement usually cannot be exactly proven; therefore, here only the most essential studies will be suggested. In this connection, it is naturally assumed that the usual security requirements have been fulfilled.

The possibilities of cryptanalysis which fall under point (2) are *per se* only special compromises of the cryptographic system. However, this method will be emphasized because it can be employed and can lead to success without any previous knowledge of the cryptographic systems. If, for instance, from a lot of homogeneous traffic single messages are put together which contain more parallel passages or other characteristics than would be expected by the laws of probability, then it may be assumed on the basis of experience that they are in the same key and in the same phase. In the case of the Enigma cryptograms are termed alike in key and phase which were produced by the use of the same daily key and the same setting of the three cipher wheels. In this connection it must be remembered that, due to the cyclic course of the period, only fragments of two cryptograms need be in phase.

Example: 1st cryptogram: dreurntosmnbvcxyasdfghjklääü

2nd cryptogram: poiuztrewqasdfghjklmnbvc

If ten cipher texts in phase can be thus lined up, then solution can be accomplished by the aid of column frequencies, etc. Theoretically this possibility of solution is limited by the fact that the relation between the total length of the machine's period and the maximum length of the intercepted messages is so determined that on the basis of probability no repetitions are to be expected. However these considerations are valid only when the appropriate regulations have been observed exactly in the choice of the message key (starting point in the period). The experience of the past fifteen years has shown however that regulations regarding the choice of message keys are quite generally disregarded. The cause is not the evil intent of the responsible person but rather convenience.

Consequently some reflection is in order as to how in the choice of the message key convenience can be furthered and at the same time the entire period exhausted in order to suppress the occurrence of messages in phase. Because experience shows that manual means are inadequate, the solution is to be attained by technical means.

Every cipher device gets a specially developed message key indicator which must at sometime show every message key which can be set up on the cipher device and which is permanently attached to the cipher device. The mechanical course of such a message key indicator must be so constituted that coincidence is ruled out, no matter how many machines are employed. Such a device will be described here, one which fulfills the conditions, is the size of a counter, and is conceived for Device 39 . It may be remarked that the idea is new and has never been put into practical use in crypto-technology.

Six wheels with the divisions 26, 26, 26, 23, 25 and 27 are to be so driven that each wheel takes on the average 13 steps to every 26 drive impulses and collectively yield a period equal to the product of the divisions of the 6 wheels. The drive is by means of a spring which is put under tension when the keys are pressed and can relieve itself of tension

by the unimpeded stepping of the six counter device disks. Using these mechanical principles, the number of steps of the six counter device disks is dependent on the key pressure from each depression of the key to the next and is therefore not subject to control. Each counter disk is inscribed with a random alphabet. In this connection care must be taken that no disk inscription is repeated in any message key indicator among all the cipher devices. By pressing a button the message key indicator can be stopped. The six letters then visible are to be used as message key.

The use of such a message key principle guarantees:

(1) that no message key combination will be repeated for a long time in any one cipher machine,

(2) that the occurrence of cipher texts in the same key and in phase will only be possible by pure chance. Chance, however, can be properly taken care of when constructing a cipher device through the ratio of the period length to the amount of enciphered traffic.