MATHEMATICAL SOLUTION OF THE ENIGMA CIPHER

MARIAN REJEWSKI

[TRANSLATED BY CHRISTOPHER KASPAREK]

[On March 1979 in Warsaw Poland Marian Rejewski died. He was the last of the great war time Polish geniuses. Henryk Zygalski died in England in 1978. Jerzy Rozycki died in military action in 1942 Before he died Rejewski wrote a study in Polish on the mathematical solution of the German machine cypher. His work was published in Polish by Dr. Władysław Kozaczuk in his book Enigma in Warsaw 1979. This is the first translation of Marian Rejewski's work.]

INTRODUCTION

Cryptology, the science of ciphers and codes, has long used mathematical methods. It was however only in the 1920s with the introducion of cipher machines. that the application of mathematics to cryptology expanded greatly. This was so especially with permutation theory. Application of the latter, along with other methods of cryptological analysis, contributed to the breaking in Poland, in 1932/33, of the German machine cipher, Enigma.

My two reports on the breaking of the Enigma cipher are to be found, the (first of 1942) at the Sikorski Historical Institute (Instytut Historyczny imienia Generała Sikorskiego) in London, the second (of 1967) at the Military Historical Institute ~~(Wojskowy Instytut Historyczny)~~ in Warsaw.

PART I. THE MACHINE

1. Description of the machine

Enigma was a device that served for the mechanical encipherment of "plain texts." Figure 1 gives an idea of the machine's appearance and permits an abbreviated description of its operation.

Enigma had a 26-letter keyboard and, beyond it, a panel with 26 letters illuminated by glowlamps beneath them. The main ciphering components were three cipher drums or rotors (Chiffrierwalzen) [1] and a fourth, stationary "reflector" or "reversing drum" (Umkehrwalze) set on a single axle; the reversing drum could be moved to or away from the rotors with a lever. The three rotors had the letters of the alphabet placed about their rims, the topmost letters being visible beneath little windows in a lid. Visible, to the side protruding somewhat, are serrated disks for manipulating the rotors. Each rotor had, on one face, 26 concentrically arranged fixed contacts, and on the other, 26 spring-loaded contacts. The fixed contacts

were connected with the spring-loaded ones in irregular fashion by insulated wires passing through the ebonite heart of the rotor. The reversing drum had, on only one face, spring-loaded contacts connected among themselves in pairs, likewise in irregular fashion The connections in these four subsystems constituted the essential ciphering part, and secret, of Enigma. The electric circuit of which the rotors formed a part is represented functionally in Figure 2.

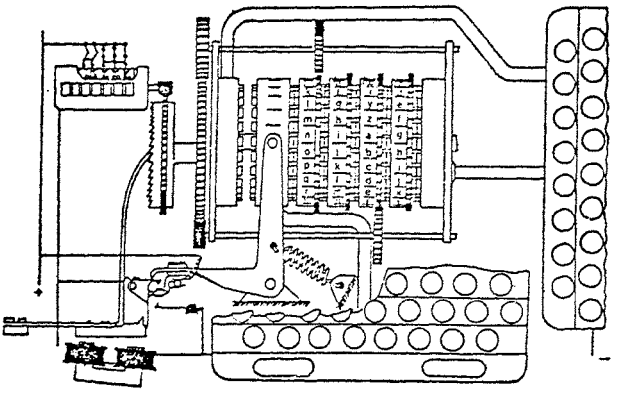

Figure 1. Diagram of an Enigma with four rotors (type M 4).

To the right of the rotors was a battery that powered the machine. In front of the keyboard was the commutator; six pairs of plugs connected with wires (Steckerverbindungen) made possible the interchange of 12 among the 26 letters of the alphabet.

Depression of an Enigma key caused the right-hand rctor to turn through 1126th of a revolution. At the same time, the circuit closed and current ran from the depressed key through the commutator, all three rotors, the reversing drum, back through the rotors, and once more through the commutator. A glowlamp lit under one of the letters, which was always different from that on the depressed key, If instead, in the previous position of the rotor, the key marked with the same letter as the glowlamp that lit up had been depressed, then the glowlamp marked with the same letter as appears on the key initially struck would have lit.

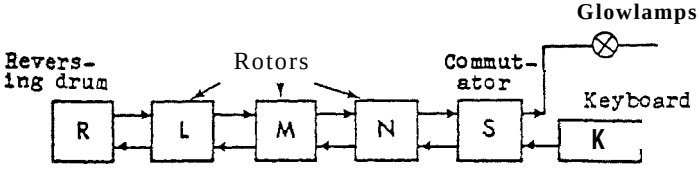

Figure 2. Enigma's functional circuit.

The Enigma machine thus served both for transforming plain text into cipher text and for the reverse operation, without any additional manipulations. Every successive depression of a key caused the right-band rotor to move through 1126th of a revolution and yet another glowlamp to light. The middle and left-hand rotors likewise turned, but much less often, in accordance with a built-in program.

2. Encipherment procedure

The Enigma cipher machine could be operated in a variety of ways. In German military formations to September 15, 1938, and in the SD. (Sicherheitsdienst) to July 1, 1939, the following instructions were in effect: The encipherer first set the rotors in the basic position (Grundstellung) established for that day, and changed the letters in the commutator by placing the plugs in the appropriate sockets. Then he independently selected the individual key for that message: three letters, which he enciphered twice. In this way, he obtained 6 letters, which he placed at the opening of the message. Next he set the rotors to the selected individual key and proceeded to encipher his message. The individual keys for a given day thus had the two following characteristics:

1. Encipherment of all individual message keys began from the same basic position, which was unknown to the cryptologist.

2. Each key was enciphered twice, and thus the first letter designated the same thing as the fourth letter, the second the same as the fifth, etc.

If we have a sufficient number of messages (about 80) for a given day, then in general all the letters of the alphabet will occur in all six places at the openings of the messages. In each place they form a mutually unique transformation of the set of letters into themselves, that is, they are permutations. These permntations, designated respectively by the letters A through F, are not known to the cryptologist, but the transitions from the first letters to the fourth, from the second to the fifth, and from the third to the sixth likewise form permatations, and these are known to the cryptologist. They are products AD, BE, CF of the previous permutations. They may be represented as disjunctive products of cycles and then assume a very characteristic form, generally different for each day, for example:

AD = (dvpfkxgzyo) (eijmunqlht) (bc) (rw) (a) (s)
BE = (b1fqveoum) (hjpswizrn) (axt) (cgy) (d) (k)
CF = (abviktjgfcqny) (duzrehlxwpsmo)

This kind of set of permntations obtained from the openings of messages constituted the starting point for solving Enigma. Using such sets from merely a few days, we managed to reconstruct the machine's internal connections. Thereafter, following the construction of the machine's doubles, each such set made possible, over a period of many years, the reconstruction of the daily keys (Tagesschlussel) and hence the reading of enciphered messages. Thus, in vier of the importance of this set, we shall devote some more attention to it.

We know from the machine's description that, if striking a given key, for example x, causes the y lamp to light, then conversely striking the y key

will cause the x lamp to light. The cause of this is, of course, the reversing drum. That is what causes all the unknown permutations A through F to consist exclusively of transpositions. From, now, the encipherer, proceeding with the double encipherment of his key, strikes in the first place the unknown key x and obtains the letter a, and by striking in the fourth place the same key x obtains the letter b, then by striking in the first place the a key he would obtain the letter x, and by striking in the fourth place the x key he would obtain the letter b. Thus there occurs a successive action, first of a on x, and then of x on b. The successive execution of such an operation is termed multiplication of permutations. Thus re see that, in writing the letters ab next to each other, we are writing a fragment of permutation AD, which is a product of the unknown permutations A and D.

Let us now consider the following example. Let

dmq vbn
von puy
puc fmq

designate the openings, that is, the doubly enciphered keys, of three of some 80 messages available for a given day. From the first and fourth letters we see that d becomes v, v becomes p, p becomes f. In this way we obtain a fragment of permutation AD: dvpf. Similarly, from the second and fifth letters we see that o becomes u, u becomes m, m becomes b. We obtain a fragment of permutation BE: oumb. And lastly from the third and sixth letters we see that c becomes q, q becomes n, n becomes y. We obtain a fragment of permutation CF: cqny. The openings of further messages would permit a complete assembly of the set of permutations AD, BE, CF. Because of its configuration and fundamental importance, we shall call this set the characteristio set or, simply, the characteristic for the given day.

3. The set of equations

As re know, after a key has been depressed and before the current causes a given lamp to light, it first passes through a series of the machine's components, Each of these components causes a permutation of the alphabet. If re designate the permutation caused by the commutator with the letter S, and that caused by the three rotors respectively (from left to right) with the letters L, M, N, and that caused by the reversing drum with the letter R, then the path of the current will be represented by the product of permutations $SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$. However, at the moment that the key is depressed, rotor N executes 1/26th of a revolution, and to take account of this movement re must introduce a special permutation of one cycle that transforms each letter of the alphabet into the next one; we shall designate it with the letter P:

P = (a b c d e f g h i j k l m n o p q r s t u v w x y z).

Figure 3, in which the rotors have been replaced with two-dimensional slides, enables us to follow the path of the current before and after the movement of rotor N

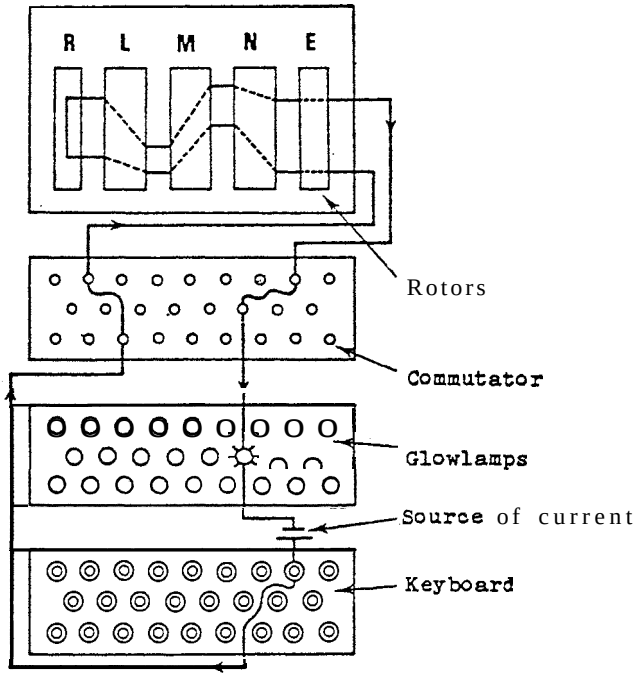

Figure 3. Path of electric current through Enigma's components.

The diagram makes it evident that the unknown permutations A through F may be represented in the form:

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$

$$B = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}S^{-1}$$

. . . . . .

$$E = SP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$

$$F = SP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

and the known products AD. BE, CF—in the form:

$$AD = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{3}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}S^{-1}.$$

$$BE = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{3}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$

$$CF = SP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{3}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}.$$

The first part of our task is essentially to solve this set of equations, in which the left sides, and on the right side only the permutation P and its powers, are known, while the permutations S, L, M, N, R are unknown.

In this form, the set is certainly insoluble. Therefore re seek to simplify it. The first step is purely formal and consists in replacing the repeated product $MLRL^{-1}M^{-1}$ (it may be interpreted as a fictitious reversing drum) with the single letter Q; we have thereby temporarily reduced the number of unknowns to three, namely. S, N, Q.

$$AD = SPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}S^{-1}$$

$$BE = SP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}S^{-1}$$

$$CF = SP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}S^{-1}.$$

4. Theorem on the product of transpositions

The next step is more **important.** Prom the **known** products AD, BE, CF we wish to obtain separately the **unknown permutations** A through F. As we have explained, these permutations consist solely of transpositions, and the expressions AD, BE, CF are their products. We may apply to them the following theorem:

If two permutations of the same degree consist solely of disjunctive trans; positions, then their product will include disjunctive cycles of the same length in even numbers.

Proof: As an example we designate the permutations to be multiplied by each other by the letters X and **Y,** and their degree by **2n.** If in permutation X there happens to occur a transposition identical with a transposition occurring in permutation Y, for example **(ab),** then in the product XY there will occur a pair of unilateral cycles **(a)** (b). With reference to transpositions identical in both permutations the theorem is therefore true. After rejecting these identical transpositions re may without prejudice to generality assume that

in permutation X there will occur the transposition	in permutation Y there will occur the transposition
(a_1a_2)	(a_2a_3)
(a_3a_4)	(a_4a_5)
.....	.....
$(a_{2k-3}a_{2k-2})$	$(a_{2k-2}a_{2k-1})$
$(a_{2k-1}a_{2k})$	$(a_{2k}a_1)$

because the letter a_1 must finally occur in permutation Y. When we proceed to execute the multiplication XY, **obviously** re shall always obtain **two** cycles of the same length $K \leq n$:

$$(a_1a_3.....a_{2k-3}a_{2k-1})\ (a_{2k}a_{2k-2}.....a_4a_2).$$

If in this manner we have not exhausted all the letters in the permutation, we continue our procedure until we have done so.

At the same time let us note that

1. the letters that enter into one and the same transposition, always enter into two different cycles, of the same length, of pennntation XY;

2. if two letters that occur in two different cycles, of the same length, of permutation XY, belong to the same transposition, then the letters adjacent to them (one to the right, the other to the left) also belong to a single transposition.

Especially important for us is the converse theorem: If a permutation of even-numbered degree includes disjunctive cycles of the same length in even numbers, then this permutation may be regarded as a product of two permutations, each consisting solely of disjunctive transpositions. It is unnecessary to supply a proof fox this converse theorem or to give a formula for the number of possible solutions for X and Y. It will suffice to mention that this theorem, when applied to the products AD, BE, CF, supplies for each of the expressions A, B, C, depending on the configurations of the products, between abont a score and several dozen possible solutions, whereas permutations D, E, F are in each case determined uniquely by them.

Thus for the whole characteristic set of three equations we obtain anywhere from several thousand to several dozen thousand possible solutions, and extracting the one true solution would be very difficult. Therefore the theorem on the product of transpositions does not bring us to our goal bat does bring us much closer to it. For let us suppose that we know that in their messages encipherers prefer as keys three identical letters, for example jjj. Having before us the characteristic set and the letters xqr gve as the enciphered message key, and assuming that in plain text these letters designate jjj, we may conclude that the opening of a message nfa qqb mast designate the letters ppp, and that the opening eug imf must designate the letters zzz, etc. Thus a knowledge of encipherers' habits, combined with the theorem on the product of transpositions, enables us to find the one correct solution so that finally in the set of equations

$$A = SPNP^{-1}QPN^{-1}P^{-1}S^{-1}$$

$$B = SP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}S^{-1}$$

.....

$$F = SP^{6}NP^{-6}QP^{6}N^{-1}P^{-6}S^{-1}$$

we may regard the left sides as known. Of course, before he has broken the cipher the cryptologist generally does not know the encipherers' habit, but he tries to compensate for this with protracted trials, imagination, and sometimes the proverbial ounce of luck.

5. The connections in rotor N

Whether the foregoing set of six permutational equations with three unknowns S, N, Q is soluble without further, supplementary data, is not known to this day. However, it is known that this set would be soluble if the cryptologist had cipher material for two different days, with different

plug connections, but with the same or nearly the same setting of rotors. At first glance, such a demand seems utterly fantastic, inasmuch as the number of possible settings of the rotors is 6(26)(26)(26) = 105,456. Nevertheless, the laws of averages tell us that even within the span of several hundred, say 500, days one may expect a couple of days with the same setting of rotors. And such a pair may be recognized by the fact that both have the same characteristic (but not the other way around: the presence of the same characteristic gives no assurance that both days have the same setting or rotors). Bnt even having such a pair of days, the way to the goal would still be long and tedious, requiring the checking of many instances. In any case, a method of solving the set of equations existed, at least in theory. In reality, the necessary supplementary data were obtained by a different, far shorter way.

In December 1932, the French Cipher Bureau supplied the Polish Cipher Bureau with intelligence material containing German tables of Enigma keys, including the S commutator connections. Thus it now became possible to transfer the S permutation as a known to the left side of our set:

$$S^{-1}AS = PNP^{-1}QPN^{-1}P^{-1}$$

$$S^{-1}BS = P^2NP^{-2}QP^2N^{-1}P^{-2}$$

.....

$$S^{-1}ES = P^5NP^{-5}QP^5N^{-1}P^{-5}$$

$$S^{-1}FS = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

thereby obtaining a set of 6 equations with only 2 unknowns N and Q. This set is now soluble, but for various reasons, mainly in order to make certain whether within the six permutations A through F there does not occur a movement of rotor M, it is advisable to carry out certain transformations. Before we carry them out, we shall explain a certain question in permutation theory.

If we have three permutations G, H, T, such that $G = T^{-1}HT$, then we say that permutation G has been transformed from permutation H by the action of permutation T. As permutation theory demonstrates, it is not necessary to multiply permntation H on the left by T^{-1} and on the right by T in order to obtain permutation G. It is sufficient to execute in the elements of permutation H the changes indicated in permntation T. Hence it follows that the two permutations G and H are similar. It further follows that if we consider T to be unknown, then the equation $G = T^{-1}HT$ is soluble when, and only when, the two permutations G, H are similar, and that we will obtain as many solutions for T as there are ways of writing permutation G beneath permutation H without affecting the value of permutation G. But in the case when G (or H) consists entirely of transpositions, the number of solutions is very large, for example with 13 transpositions it amounts to 2^{13} (13!) = 51,011,754,393,600, and therefore is without practical importance. Yet that is precisely the case that we have before us, since each of the permutations A through F consists of 13 permutations. Hence we carry out certain transformations in order, among other things, to free ourselves from these transpositions.

First we transform both sides of the first equation by P, of the second equation by P^2, etc., and for short we designate the left sides by the letters U through Z:

$$U = P^{-1}S^{-1}ASP = NP^{-1}QPN^{-1}$$

$$V = P^{-2}S^{-1}BSP^2 = NP^{-2}QP^2N^{-1}$$

.....

$$Y = P^{-5}S^{-1}ESP^5 = NP^{-5}QP^5N^{-1}$$

$$Z = P^{-6}S^{-1}FSP^6 = NP^{-6}QP^6N^{-1}$$

Next we form products of each two successive expressions:

$$UV = NP^{-1}\ (QP^{-1}QP)\ PN^{-1}$$

$$VW = NP^{-2}\ (QP^{-1}QP)\ P^2N^{-1}$$

$$WX = NP^{-3}\ (QP^{-1}QP)\ P^3N^{-1}$$

$$XY = NP^{-4}\ (QP^{-1}QP)\ P^4N^{-1}$$

$$YZ = NP^{-5}\ (QP^{-1}QP)\ P^5N^{-1},$$

and by eliminating the common expression $QP^{-1}QP$ we obtain a set of four equations with only one unknown NPN^{-1}:

$$VW = NP^{-1}N^{-1}\ (UV)\ NPN^{-1}$$

$$WX = NP^{-1}N^{-1}\ (VW)\ NPN^{-1}$$

$$XY = NP^{-1}N^{-1}\ (WX)\ NPN^{-1}$$

$$YZ = NP^{-1}N^{-1}\ (XY)\ NPN^{-1}.$$

Proceeding in this fashion, we shall obtain from the first equation several dozen possible expressions for NPN^{-1}, depending on the configuration of permutation UV (or of permutations VW, WX, XY, YZ, as all of them must have the same configuration, unless we have made a computing error or there has been a movement of rotor M). But we will obtain the same number of solutions for NPN^{-1} from the second equation, and one of these solutions must be identical with one solution for the first equation. The final two equations are now superfluous.

To the solntion obtained for NPN^{-1} we apply the indicated method once again by comparing this expression with permutation P. We will obtain 26 possible solutions for N^{-1} that do not differ essentially, and after selecting one of them we will readily obtain N itself, the internal connections of the right-hand rotor.

6. Example

It seems appropriate to show how the foregoing theoretical deliberations were applied in practice to obtain the internal connections of rotor N. Let the characteristic already given in Part I, Section 2, serve as point of departure:

AD = (dvpfkxgzyo) (eijmunqlht) (bc) (rw) (a) (s)
BE = (blfqveoum) (hjpswizrn) (axt) (cgy) (d) (k)
CF = (abviktjgfcqny) (duzrehlxwpsmo).

We assume that thanks to the theorem on the product of transpositions, combined with a knowledge of encipherers' habits, we know separately the permutations A through F:

A = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)
B = (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz)
C = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)
D = (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)
E = (ac)(bp)(dk)(ez)(fh)(gt)(io)(jl)(ms)(nq)(rv)(uw)(xy)
F = (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt)

Also known, thanks to materials obtained by intelligence, are the plug connections S for the given day:

S = (ap) (bl) (cz) (fh) (jk) (qu).

We, of course, also know permutation P and its powers:

P = (a b c d e f g h i j k l m n o p q r s t u v w x y z).

P^2 = (a c e g i k m o q s u w y) (b d f h j l n p r t v x z)

P^3 = (a d g j m p s v y b e h k n q t w z c f i l o r u x)

P^4 = (a e i m q u y c g k o s w) (b f j n r v z d h l p t x)

.....

Thus we may carry out the operations indicated in Part I, Section 5, to form the expressions U, V, W, X (expressions Y and Z will not be needed):

U = (ax)(bu)(ck)(dr)(ej)(fw)(gi)(lp)(ms)(nz)(oh)(qt)(vy)

V = (ar)(bv)(co)(dh)(fl)(gk)(iz)(jp)(mn)(qy)(su)(tw)(xe)

W = (as)(bz)(cp)(dq)(eo)(fw)(gj)(hl)(iy)(kr)(mu)(nt)(vx)

X = (ap)(bf)(cu)(dv)(ei)(gr)(ho)(jn)(ky)(lx)(mz)(qs)(tw),

and next their products:

UV = (a e p f t y b s n i k o d) (r h c g z m u v q w l j x)

VW = (a k j c e v z y d l w n u) (s m t f h q i b x o p g r)

WX = (a q v l o i k g n w b m c) (p u z f t j r y e h x d s)

We see that the prodncts have the same configuration of cycles--which is as it should be. Now we should (consistently with what we wrote in Part I. Section 5) write product VW beneath product UV in every possible way, and likewise product WX beneath product VW. Of all these possible ways, one will give the same result in both cases. That will be the expression NPN^{-1} that we need. Writing VW beneath W, and WX beneath VW, in every possible way is rather tedious. However, there are various tricks and technical means that make this subscription unnecessary, but whose description and, especially, justification would take us too far afield. It will suffice to say that products UV, VW and WX should be subscribed in the following way:

UV = (a e p f t y b s n i k o d) (r h c g z m u v q w l j x)

VW = (y d l w n u a k j c e v z) (i b x o p g r s m t f h q)

VW = (y d l w n u a k j c e v z) (i b x o p g r s m t f h q)

WX = (u z f t j r y e h x d s p) (c a q v l o i k g n w b m).

For in both cases we obtain for NPN^{-1} the same expression:

NPN^{-1} = (a y u r i c x q m g o v s k e d z p l f w t n j h b).

The rest is simple. Subscribing beneath permutation NPN^{-1} permutation P in all possible ways, of which there are 26, we will obtain 26 variants for permutation N. For example, one variant is:

$$N = \begin{pmatrix} a\ y\ u\ r\ i\ c\ x\ q\ m\ g\ o\ v\ s\ k\ e\ d\ z\ p\ l\ f\ w\ t\ n\ j\ h\ b \\ a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z \end{pmatrix};$$

after the upper row has been placed in alphabetical order, we obtain:

$$N = \begin{pmatrix} a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z \\ a\ z\ f\ p\ o\ t\ j\ y\ e\ x\ n\ s\ i\ w\ k\ r\ h\ d\ m\ v\ c\ l\ u\ g\ b\ q \end{pmatrix}.$$

All the other solutions do not differ essentially from the above. The only consequence of adopting one or another solution is that the right-hand face of rotor N is turned by a greater or smaller angle with respect to the left-hand face. Which version of permutation N we accept as the true one, will depend on such elements as the moments of rotation of the various rotors. But those details may only be established following the basic reconstruction of the connections in all the rotors.

7. Concluding remarks to Part I

The description of the machine given at the beginning was purposely simplified in order to show as clearly as possible the process of reconstructing the connections in rotor N. In reality, the machine and its operation were

considerably more complicated. For example, in addition to the three rotors and the reversing drum, Enigma also had an entry ring (Eintritts-walze) which made the breaking of the cipher much more difficult. Moreover, the rings on the rotors with the letters of the alphabet engraved on them, may be moved with respect to the remaining part of the rotors, and consequently a knowledge of the basic position said nothing about the actual position of the middle part of the rotors. Not only rotor N rotated but so also, at less frequent intervals, did rotors L and M, a fact that also caused various complications. Finally, the order of the rotors could be changed, and as a result the number of possible combinations rose, give three rotors, six-fold, and given five rotors, sixty-fold.

The last of the above-mentioned complications carried an implication not foreseen by Enigma's designers. It caused each of the three rotors to be located every so often on the right-hand side of the rotor set. As a result, the method described above for reconstructing rotor N could be applied by turns to each rotor, and thus the complete inner structure of the Enigma machine could be reconstructed.

PART II. KEYS

1. The cyclometer

Reconstruction of the machine was a necessary, but not a sufficient, condition for mastery of the Enigma cipher and for continaoas decryptment over a period of many years. Methods also had to be devised for rapid reconstruction of the daily keys. In other words, the problem was the opposite of that presented in Part I. Whereas in Part I the task was to reconstruct the machine's works, given a knowledge of the keys for a certain period of time, now we wish to show how--having the machine--one can reconstruct the keys. Here, once again, permutation theory came to oar help.

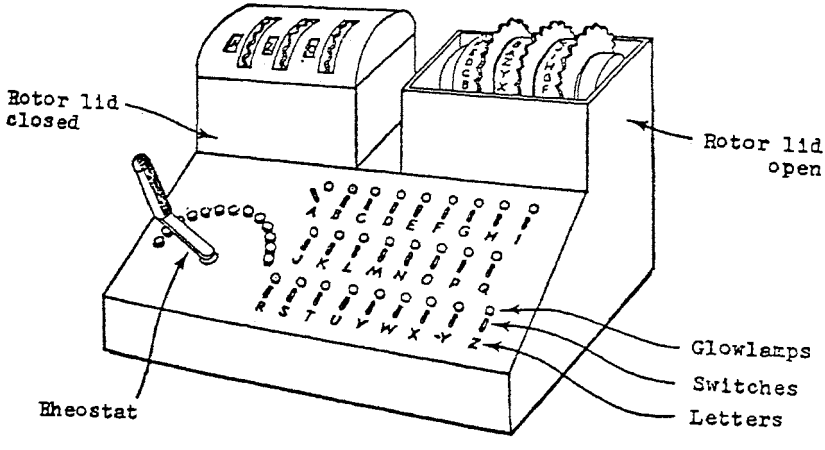

Figure 4. Cyclometer

As the formulas for AD, BE, CF show, **permutation** S as a transforming permutation inflnences solely the letters within cycles comprising **permutations** AD, BE, **CF, but** does not influence the actual configuration of these cycles. Furthermore, permutations AD, BE and CF have a characteristic form (see Part **I,** Section **2),** and a set of three **such permutations** with the same confignration of cycles recurs infrequently.

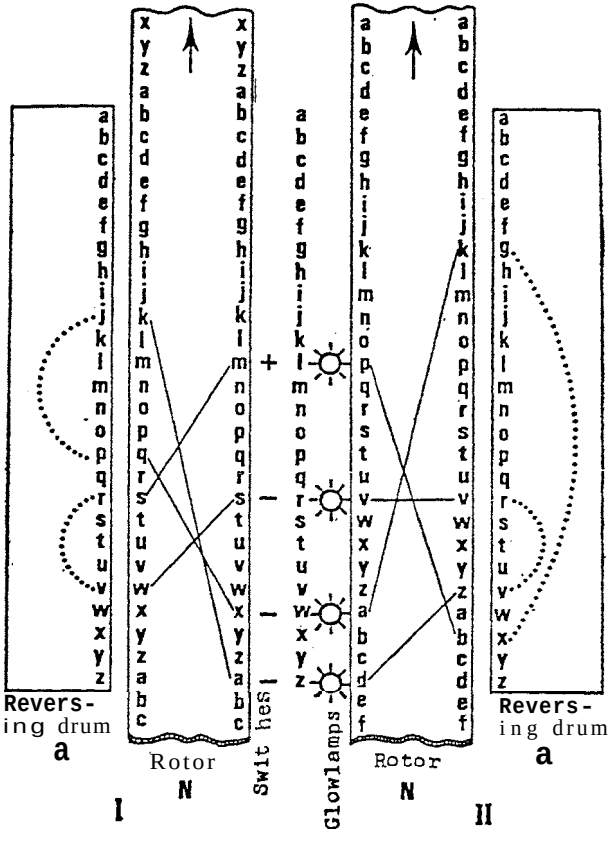

Figure 5. Diagram of cyclometer.

Three rotors can be placed on an axis in six different ways, and the rotors themselves can assume **(26)(26)(26)** = 17,576 different positions. Therefore. if **it** were possible to design a device that gave the length and number of cycles in the characteristic for each position of the rotors, and if next the lengths and numbers of cycles were cataloged, then **it** would suffice to compare the products AD, BE, CF for a given day with products **with** the same configuration in the catalog, to at once obtain the order of rotors and permutation S, while the remaining components of the daily key would be obtained by other methods.

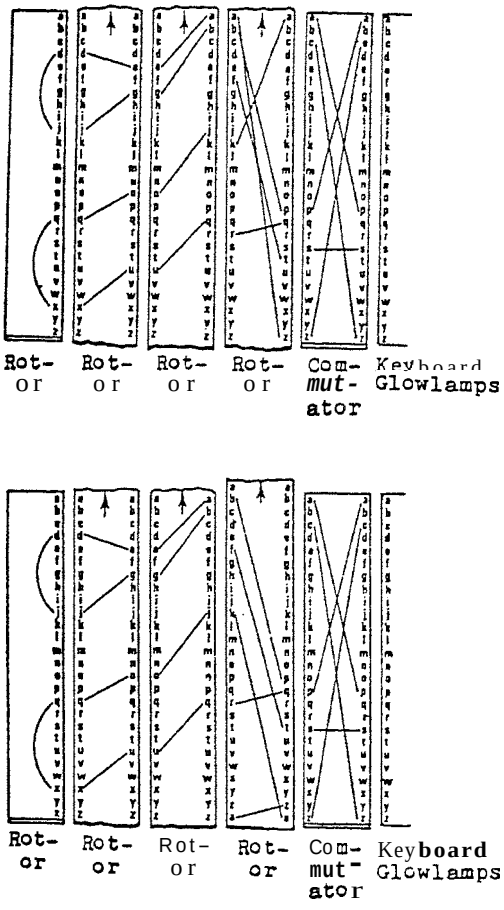

Figure 6. Path of electric current through Enigma upon revolution of rotor N.

It proved possible to design such a device, called a cyclometer. Figure 4 will give a general idea of its appearance. The main part of the cyclometer comprised two sets of rotors suitably connected by wires through which electric current could run; rotor N in the second set was three letters out of phase with respect to rotor N in the first set, whereas rotors L and M in the second set were always set the same ray as rotors L and M in the first set. The operation of the cyclometer is depicted in Figures 5 and 6. For greater clarity, the order of the rotors in set II has been reversed in the diagram, but that does not alter the essentials of the matter. The reversing drums have been marked with the letter Q. They replace (in the diagram only) rotors R, L and M. Between the two sets of rotors is a system of glowlamps with switches. If a source of current (symbolized in the drawing by the sign +) is turned on at any of the lamps. e.g. 1, then current will flow by turns through set I and set II of the

cyclometer, antil after a certain number of passes it returns to lamp 1. At the same time, the lamps that lie in the current's path will light. Their number, always even, equals doable the number of letters in one of the cycles of permutation AD. After a different switch has been thrown, that is, after the source of current has been turned on to a lamp that has not yet lit, further lamps will light, from whose number may be deduced the length of succeeding permutation cycles. In this fashion, with the help of the cyclometer, turning the rotors one by one and counting the lamps that light, one can determine the length and number of cycles in the characteristics for all 17,576 positions of the rotors for a given sequence of rotors.[2] And since there were six such possible sequences, the catalog of characteristics encompassed a total of (6)(17,576) = 105,456 entries.

2. Perforated sheets

The cyclometer, or rather the catalog of characteristics based on it, fulfilled its task until September 15. 1938. Beginning on that date, in all German formations and units that used Enigma except for the S.D., completely new rales for enciphering message keys were put into effect. Henceforth the Enigma operator himself selected the basic position, a new one each time, for enciphering the individual message key (Spruchschlussel) and placed this basic position unenciphered (in clear, or plain text) at the head of the message. The individual message key, however, as before. was enciphered twice. Thus the first letter of the key continued to designate the same thing as the fourth letter, the second the same thing as the fifth, etc.. while the basic position was now known to the cryptologist but was different for each message. Therefore, now there were no products AD, BE, CF, characteristic for each day, whose configuration could be found in the catalog. Nevertheless, there continued to be a relation between the first and fourth, second and fifth, third and sixth letters of the key, and that relation had to be exploited.

It was sometimes the case that the individual message key selected by the encipherer assumed, upon encipherment, a form such as: pst pwa. This meant that the first letter was identical with the fourth (or the second with the fifth, or the third with the sixth), that is, in the language of permutations it meant that in product AD, or perhaps BE or CF (if that were the case), here were unilateral cycles, also called constant points of the permutation. Since the length of the cycles in products AD, BE, CF was invariable with respect to the transformations produced by permutation S, the occurrence or nonoccurrence of constant points in the products was invariable with respect to those transformations.

Therefore what was needed, instead of a catalog of the cycle lengths of the products, was to create a catalog of constant points for all the 17,576 possible products (for each arrangement of rotor sequence) and to compare them with the constant points appearing in the individual message keys during the given day. The difficulty lay in carrying out the comparison. To be sure, the basic positions for each key were known, because the encipherer now gave them in clear at the head of each message, but since the rings on the circumferences of the rotors were adjustable and their settings unknown for a given day, the only thing in fact known was the relative distance of the constant points appearing in the keys for the given day.

Constant points occurred in the catalog in about 40% of all permutation products and, if transferred to a long tape, would have formed a distinct pattern. The constant points appearing in the keys for a given day, if transferred to another tape in accordance with their basic positions, would also form a pattern, and the task would be to find the place where all the constant points on the second tape coincided with the constant points on the first tape. But that task, at least with the existing technology, involved great difficulties. Besides that, the first tape would have had to be made doable length so that the second tape could be moved over it. A different way was found, however (by Henryk Zygalski).

Fairly thick paper sheets, lettered a through z, were prepared for all 26 possible positions of rotor L, and a square was drawn on each sheet, divided into 51 x 51 smaller squares. The sides, top and bottom of each large square (it could as well be a rectangle) were lettered a through z and then again a through y. This was, as it were, a system of coordinates in which the abscisses and ordinates marked successive possible positions of rotors M and N, and each little square--permutations, with or without constant points, corresponding to those positions. Cases with constant points were perforated. Such a sheet (reduced in size) looked more or less as in Figure 7.

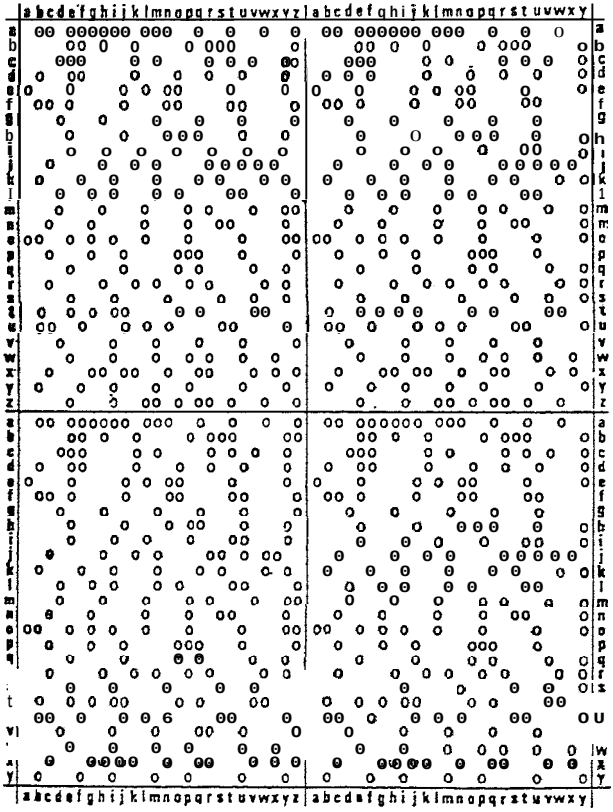

Figure 7. Perforated sheet.

We see that each constant point had to be perforated as many as four times. This was a very time-consuming job. When the sheets were superimposed and moved in the proper sequence and the proper manner with respect to each other, in accordance with a strictly defined program, the number of visible apertures gradually decreased. And if a sufficient quantity of data was available, there finally remained a single aperture, probably corresponding to the right case, that is, to the solution. From the position of the aperture one could calculate the order of the rotors, the setting of their rings, and by comparing the letters of the cipher keys with the letters in the machine, likewise permutation S: in other words, the entire cipher key.

3. Concluding remarks to Part II

In addition to these two methods of reconstructing keys, still other methods and devices were used as needed in various circumstances and periods, often to supplement the cyclometer or the perforated sheets: some simple, for example a method called the grill method (metoda rusztu), others mechanized and expensive, such as the cryptologioal bomb (Figure 8). These methods have not been described here, since they were not based on permutation theory but on the fact that the commutator connections did not change all, but only part, of the letters of the alphabet. It will suffice to say that the grill method, manual and tedious, was used primarily in the initial period, before the advent of the cyclometer: later it was used rather sporadically. The bomb method, invented in the fall of 1938, consisted largely in the automation and acceleration of the process of reconstructing the daily keys. Each cryptological bomb (up to September 1939, six were built in Warsaw for the Cipher Bureau) essentially constituted an electrically powered aggregate of six enigmas; it took the place of about 100 workers and shortened the time for obtaining a key to about 2 hours.

A variety of methods and stratagems were also devised, of limited scope, to be sure, but which sometimes made possible great savings in time and effort. For example, there was the "clock" method (invented by Jerzy Rozycki) which sometimes made it possible to determine which rotor was in the N rotor's place, that is, at the right-hand side, on a given day.

The German cipher service (Chiffrierdienst, or Chi-Dienst for short) continually introduced new difficulties designed to frustrate attempts at reconstructing keys. These moves had to be countered.

Thus, on November 1, 1937, the reversing drum was exchanged. The number of connections in the commutator was gradually increased from 6 to 13 pairs. On December 15, 1938, the number of rotors was increased from 3 to 5. From year to year the number of German radio communications nets also grew and, while each used the same Enigma devices, they used different keys.

In September 1939, nearly all the Cipher Bureau's equipment and most of its records were destroyed prior to and during evacuation. But at a meeting of Polish, French and British cipher bureau representatives held in Warsaw on July 25, 1939, the Polish side had made all its methods and devices for Enigma decryptment available to the future war allies, turning over to each as well a copy of the German cipher machine that had been reconstructed in Poland on the basis of the theoretical work that has been described here,

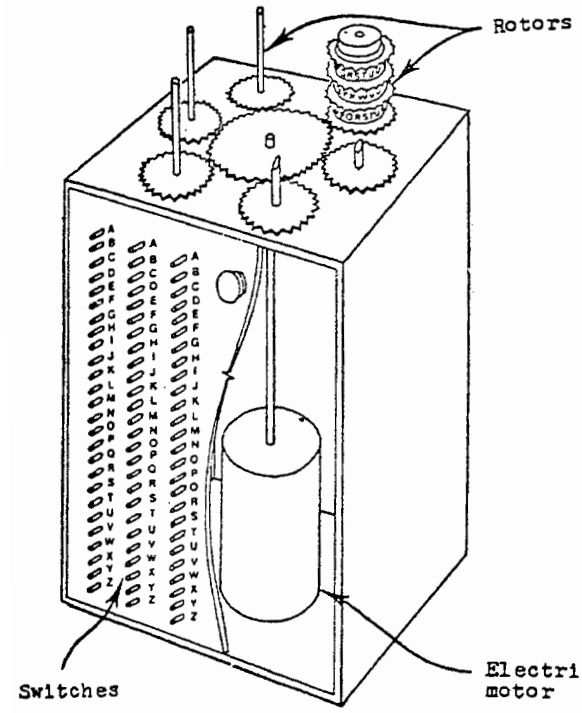

Figure 8. Cryptological bomb. (For clarity, only one set of rotors is shorn in the upper part of the bomb.)