THE KRYHA
CIPHERING MACHINE

A MATHEMATICAL OPINION

by

DR.PHIL. GEORG HAMEL

Professor of Mathematics at the Institute of Technology in Berlin-Charlottenburg.

MATHEMATICAL OPINION ON THE KRYHA CIPHERING MACHINES

by
Dr.phil. Georg Hamel,
Professor of Mathematics at the Institute of Technology in Berlin-Charlottenburg.

Reference to Designations used:

N number of letters, P number of stop points (groups of teeth) of ciphering wheel, $d_1, d_2 \ldots d_p$ number of teeth of a group.

$M = z_p = d_1 + d_2 + \ldots + d_p$ total number of teeth. $z_1 = d_1$,

$z_2 = d_1 + d_2, z_3 = d_1 + d_2 + d_3$ and so on, p whole part of P,

after p stop points the groups of teeth recur periodically, m possibly of the entire ciphering process.

I. INTRODUCTION.

We are starting from the simple system that N = 26 letters of the German language, including the space between words, but J = I, is coordinated to one each of N = 26 letters, here excluding the space and J not taken like I. The first system of N letters comprises the so-called clear or plain text, the second the ciphering text.

---

*) The computation were made by Dr. Engineer Sadowsky, Assistant of the institute for applied Mathematics of the institute of Technology Charlottenburg.

The totality of all these possible coordinations is N!=N. (N-1).(N-2)...2.1, hence in the special case 26 . 25 . 24 ...3.2.1. This computed results in

403 291 461 126 605 635 584 000 000*)

Figure 1

Proof: One might coordinate to A any letter whatever, resulting in N=26 possibilities, the to B another of 25=(N-1) letters (one of the letters having already been disposed of), then

to C still another letter with 24=(N-2) possibilities, for by now already two letters have been disposed of, and so on.

But a system of this nature would in spite of its tremendously large number of keys be comparatively easy to decipher, owing to the coordination of clear text and ciphering text being always alike, by making statistical investigations on the frequency of the letters and on separate words continually recurring. *This possibility does not exist with the "Kryha" system*, as here the regular recurrence of the coordination of *clear text* and ciphering text is hindered by the continual change of the key in the following way (see 2).

> Treating the *intervening spaces* of the clear text as letters results in the important advantage, that it further complicates unauthorized deciphering, as the length of the actual words cannot be seen from the ciphered text and because the space does not recur as regularly as a letter, for instance the e in the German language.

2. THE FUNDAMENTAL IDEA OF THE SYSTEM.

It is to be supposed that after the above coordination of the clear text and the ciphering text has been selected at random, the letter pairs, belonging together, have been arbitrarily divided over places with the figures 1 to N, in the present case therefore 1 to 26, and then have coordinated the N+1 or 17 again to the same letter pair as the 1, the N+2 or 28 to the same letters as the 2, and so on, so that all figures are periodically covered by letter pairs. The length of the period is N. We also refer to an arrangement of the letter pairs in differentiation as to their mutual coordination.

With the Kryha machine arrangement and coordination is secured by placing *interchangeably* the N letters of the ciphering text on a circular disk, and the N letters of the clear text on a

ring arranged around it. Then there will result N!(N-1)! possible coordinations of the letters of both systems with regard to each other and to the figures 1 to N. The factor (N-1)! Is added by it being apparently immaterial, where the A of the clear text is placed, - this place may always be marked 1 – but that in this case there may be placed on the adjoining space 2 any of the other 25 letters, on space 3 any of the still remaining 24 letters and so on. Periodicity results by itself from the circular arrangement. (See figure I. Placing both alphabets twice on the ciphering text disk is only of technical and not of theoretical importance).

In addition any numerical order of $z_1, z_2, z_3, z_4, ...,$ is now to be agreed upon, which may have any length and, theoretically, is unlimited. The figures z are nought or positively whole and smaller than, N or, if they are larger or equal to N, then they should be replaced by a figure resulting from keeping on deducting from N until a figure from 0 to N-1 is obtained.

The next step is: Begin at the first letter of the clear text with one of the above coordinations, that is, one of the many that have been selected, or, in other words, write into the ciphering text instead of the first letter of the clear text the letter which is opposite to it on the disk. Then, however, the coordination is to be altered by turning the ring against the disk by z_1 places in conformity with the numbering.

The figure n belonged previously to the second letter of the clear text and to a letter of the ciphering text, but now there is coordinated to the second letter of the clear text the figure $n+z_1$, and then in the ciphering text the letter, which in the former order corresponded to this figure. Continue in this manner. As regards the third letter the figure z_2 is added to the former figure n belonging thereto, and then the letter is coordinated, which according to the original order belonged to this figure $n+z_2$, and so on. Conditions are further explained by the following table:

Clear text: $e_1, e_2, e_3, \ldots e_N, e_{N+1}, e_{N+2}, \ldots$

1 2 3 ... N, N+1, N+2, ...

Ciphering text: $E_1, E_2, E_3, \ldots E_N, E_{N+1}, E_{N+2}, \ldots$

Here the $e_1, e_2, e_3, \ldots$ indicate the letters of the clear text in anay arrangement ($e_{N+1}=e_1, e_{N+2}=2,$ and so on), the $E_1, E_2, E_3, \ldots$ letters of the ciphering text. If, for instance, the clear text reads $e_1, e_7, e_3, \ldots$ and if there is $z_1=4,$ and $z_2=5,$, and so on, the ciphering text will read E_1, E_{11}, E_8 and so on.

Hence there is a continual change of the key, depending on the numerical order of z agreed upon.

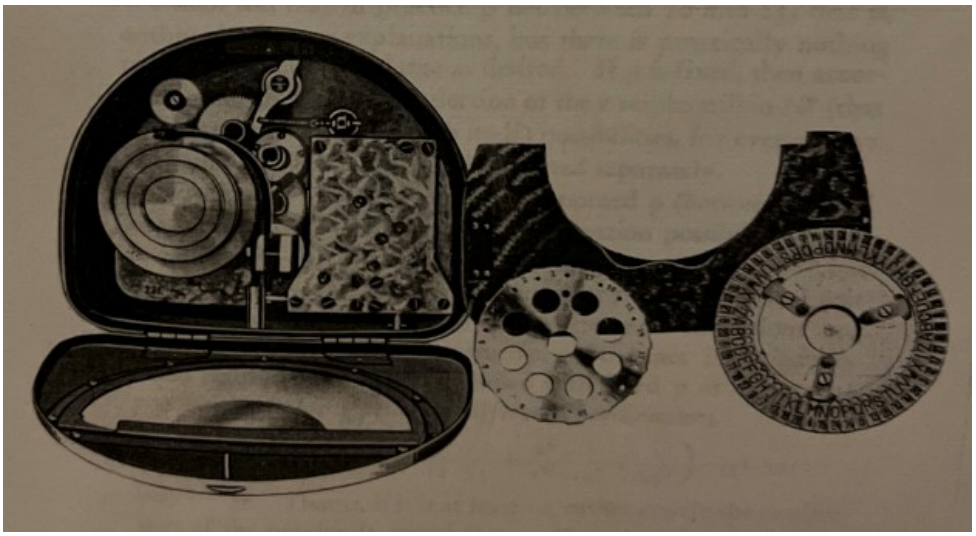

Figure 2.

3. THEORY OF THE SYSTEM

a) Number of Combinations.

As stated above, alone the arrangements and coordinations of the twice N letters on disk and ring permit of N!(N-1)! manipulations. This figure has with N=26 a value of 6 255 538 562 216 633 250 270 726 284 985 715 654 656 000 000 000 000 having 52 digits.

But the process is yet dependent on the selection of the z. Since the numerical order of the z is unlimited, the number of combinations is also theoretically unlimited.

But with the Kryha the numerical order of the z is made subject to a law. It is selected periodically. The z must be made to recur after m figures. Besides, the m figures are made dependent on only p independently selective among them. We shall see, that in practice p lies between 10 and 25,that is within the former explanations, but there is practically nothing to hinger making p as large as desired. If p is fixed, then according to the above the free selection of the z results still in Np (that is, N p times multiplied with itself) possibilities, for every z may as matter of fact be arbitrarily selected separately.

From this it appears that with supposed p (between 10 and 25) the totality of the different combination possibilities seems to be N!(N-1)!Np, or in the case before use 26!.25!.26p, but and ciphering text may occur with different z successions and with different initial arrangements. An exact investigation, based on theoretical figures, shows with fixed p as totality of possibilities yielding actually different coordinations.

$$\left(\frac{26P-13P-2P+1}{12}+\frac{33P-1}{12\cdot 13}+\frac{2P-1}{2^{12}\cdot 12!}+\frac{1}{25!}\right)\cdot 25!\cdot 26!$$

for N=26. That is, if p is at least 10, rather closely the twelfth part of the previously stated figure 26p.25!.26!. As, for instance, already for p=14, the figure 26p is a figure of twenty digits, beginning with 6, the total figure is at the lowest a figure

of seventy one digits, beginning with 3. Its exact value is:

33 626 824 886 765 738 311 878 611 841 331 860 444
831 499 784 068 709 602 069 315 584 000 000.

However, with respect to the maximum p=25, technically possible for the time being, the *number of keys is, however,* $\frac{26!25!}{12}26^{25}$, *that is a figure of 87 digits, beginning with I.* Or to be more exact 123 400 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000. (Here the first four digits have been computed exactly.)

A summation covering all technically feasible p will result in an even somewhat larger, but yet as regards the order of quantity not very much differing *total number of keys*, and we shall see, that is may be somewhat lessened by a limitation of construction, but not be materially reduced in order of quantity.

b) Periods of Recurrence.

Of more importance than the large number of combinations is the question of periodicity, which is subdivided in two questions:

I. When does a previous coordination of the separate letters recur?

2. When does the entire system recur?

The first evidently only takes place if it happens that z is nought or equal to z having already occurred. *This recurrence will, however, be of minor importance with regard to deciphering by unauthorized persons, as it is not periodic and the ciphered text does not disclose when exactly a coordination recurs.*

The second question, however, is of much greater importance. After how many letters can the whole system of coordination recur? Such recurrence takes place in the event, and only then, of the figures z recurring. The length of this possibly exiting period we call m.

4. PRACTICAL CONSTRUCTION.
THE "KRYHA STANDARD".

As we already know, changing the coordination from clear text to ciphering text is effected by turning the ring in opposition

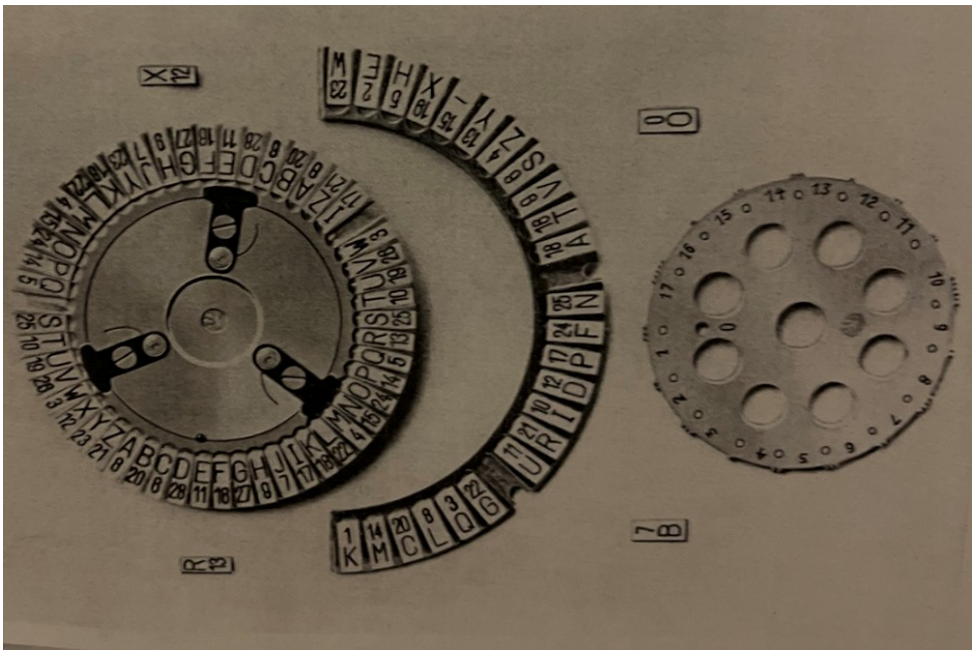

Figure 3

to the disk in succession by $z_1, z_2, z_3, \ldots$ against the initial seting. This turning is effected with the Kryha machine in the following manner:

A wheel, actuated by a clockwork, the ciphering wheel (figure 2 and 3) is provided at its periphery with M teeth, which are arranged in P groups to $d_1, d_2, d_3 \ldots d_p, d_1+d_2+d_3+\ldots P_p=M$. After each ciphering the catch of the clockwork is released and the ciphering wheel revolves further around a group of teeth, or a stop point, as we might also say, and thereby turns the disk with the ciphering text letters, or also the clear text ring, by so many places as there are teeth in the group. Therefore is $z_2=d_1, z_2=d_1+d_2, z_3=d_1+d_2+d_3,$ and so on; or, what amounts to the same $d_1=z_1, d_2=z_2-z_1, z_3-z_2$ and so on. A perhaps negatively computed d can and must be replaced by the positive d+N. In consequence of the circular form of the ciphering wheel the groups of teeth recur, and thereby also the d. Otherwise these d (number of teeth of a group) can be selected at random. Hence, *this period is the p used above in theory*. If one restricts oneself to such ciphering wheels, which cannot equivalently be replaced by wheels with less teeth, that is, if on does without a multiple periodic arrangement of the teeth on the ciphering wheel, which, as we shall see immediately, would reduce the period m of the system, then *p is the figure p of the groups of teeth or stop points*. This case is sure to always obtain, if the total number of the stop points is a prime number and if not all d are equal to one another. In general, p is a whole part of P.

How large now is the figure m? If the entire process recurs after m letters, then the d musts also recur, hence, p must be a whole part of m. But all z must also recur, or must have increased by a plurality of N. Thus, if $z_p=d_1+d_2+d_3+\ldots+d_p$ is divisible by N, then will be m=p; if z_p is divisible by a whole

part q of N (q largest common divisor of z_p and N) and if N =pQ, then is evidently

$$m = pQ,$$

for, after the p groups have been run off Q times, we have in Qz_p for the first time a figure divisible by N. If N equals 26 and z_p is divisible by 2, being an even number, the period is m=13p; if z_p is divisible by 13, then the period is m=2p. In all other cases it is (with N=26) equal to 26p. As the period should be as large as possible, we consider as "good" only such ciphering wheels, whose z_p is not divisible either by 2 or by 13, and hence not by 26 (general N or one of its whole parts). If it is avoided, that $M=z_p$ is divisible by 2 or 13, *then the ciphering wheel is considered as "good" in the sense of the above definition*.

Thus one obtains m=N.p, hence with N=26 and p between 14 and 25 a period m of t*he entire process, said period lying between 364 and 650 according to the p of the wheel. Not until so many letters have been ciphered does the whole system recur. Therefore, there can be used for a statistical investigation as referred to in the introduction only every 364th letter (in the most unfavorable case: p=14). But even this need not be considered because the deciphering party does not know the period. Besides, with long text the system (key) may be changed by agreement after some periods, which can be effected without any technical or operating difficulty*.

Such disturbance of the period may be especially successfully obtained by agreeing upon a *"lettre influent"*: it is agreed that when a certain letter shows in the clear text the operating key is depressed twice or three times, whereby one or two z of the order drop out of the order contrary to law and regularity, *so that a period does not exist any longer*.

ELEVEN

5. EFFECT OF LIMITATION TO A MAXIMUM NUMBER OF TEETH.

The following may still be pointed our with regard to the number of combinations: The circumference of the ciphering wheel and the width of the separate teeth fixed for practical reasons determines the highest possible total number of the teeth of a ciphering wheel, namely M=179. (This also determines the maximum 25 for p). While the total number of combinations is limited by the maximum number of the teeth M=179 as compared with the theoretical figure of 26^P yet *it is still inexhaustibly large*, as is shown by an investigation of but a fraction of all possibilities offered by a wheel with exactly 179 teeth. This is the mathematical figure showing how often 179 may be divided in p groups of figures between nought and 25, whereby, in addition, the arrangement must be considered. An exact investigation on theoretical numbers*) proves, that for M=179 the same coordination from clear text to ciphering text cannot continuously occur with any of the two thus counted possibilities. For the figure in question the following mathematical formular results:

$$\binom{M+p-1}{p-1}-\binom{p}{I}\cdot\binom{M+p-N-1}{p-1}+\binom{p}{2}\cdot\binom{M+p-2N-1}{p-1}-:+\ldots$$

until the row breaks off. In this, for instance, the symbol

$$\binom{179+10-1}{10-1}=\binom{188}{9}$$

means an abbreviation for $\frac{188\cdot187\cdot186\cdot185\cdot184\cdot183\cdot182\cdot181\cdot180}{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9}$

If this figure is computed for M = 179, p=14 and N=26, then a figure results, amounting to about $9\cdot10^{17}$, *that is, a figure with 18 digits*. But for M=179 and p=25 the result is about $10^{30}\cdot3{,}66$ ...

The total figure with all technically possible constructions $(14\leqslant p\leqslant25)$ with exactly 179 teeth is of course still higher, but

*) See Georg Hamel „Application of the elementary Theory of numbers to the Theorie of a Ciphering Machine“ Minutes of the meeting of the Berliner Mathematischen Gesellschaft XXVI. 1927.

by order of quantity just about the same. If we conservatively confine ourselves to M=179, p=25, *then the entire number of keys is* $10^{30} \cdot 3{,}66 \cdot 26! \cdot 25! = 10^{82} \cdot 2{,}29\ldots$

Thus, if every person on earth (say 2 000 000 000 people) buys the "Standard" then each of them can obtain the *inconceivably large number* of key changes of $10^{79} \cdot 1.14$ = about 11 400 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 without two persons ever having the same system.

(In order to comprehend the magnitude of this figure one must realize that a million is 10^6 , a milliard 10^9 , a billion 10^{12} and therefore 10^{24} is a billion of billions.)

Since each ciphering wheel contains 25 of theese combinations, within which with each group of teeth may be commenced, there would be, indeed, $10^{30} \cdot 3{,}66 : 25$, that is about $10^{29} \cdot 1{,}46$ ciphering wheels required. But every purchaser of a Kryha machine need not buy, apart from the machine proper, all the ciphering wheels necessary for producing all changes. By a *new and important advance in the construction* each ciphering wheel of p stop points is divided in as many segments with one group of teeth each. These p segments can be put together in any order and form thereby each time a new ciphering wheel, at any rate, if no segments with a like number of teeth occur. Presuming this to be the case, then p segments of a ciphering wheel permit of producing p! possibilities. Hence, *the number of keys which a single purchaser of a Kryha machine and a ciphering wheel with p=19 segments has at his command* (provided that the single segments have differing teeth numbers and the total number M of the teeth does not exceed 179 and is not divisible by either 2 or 13) *amounts to 26! 25! 19! This is about* $10^{68} \cdot 7{,}609556$, *or a figure with 69 digits, beginning with 7*. If M is divisible by 2 or 13, then this figure is slightly decreased and M is maintained in the order of quality for practical use.

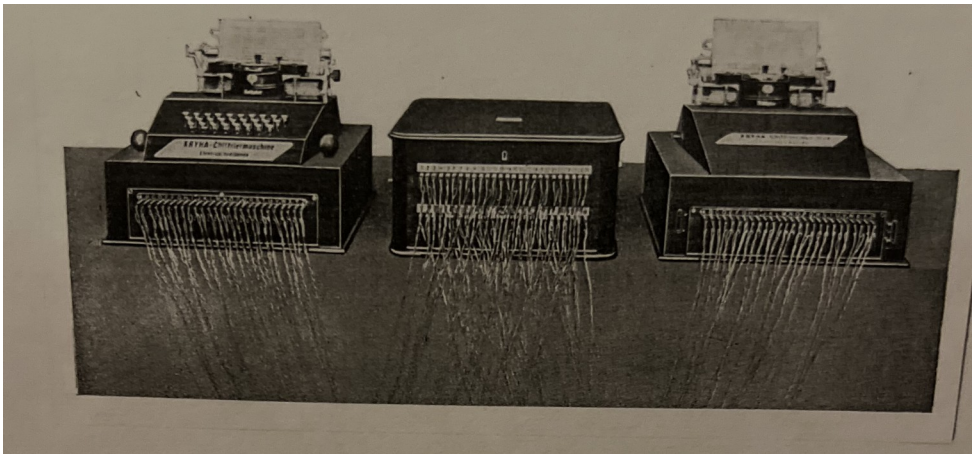

Figure 4

6. THE ELECTRICALLY RECORDING MACHINE "KRYHA ELECTRIC".

The electrically recording machine "Kryha Electric" operates according to the same system. It is based on the same mathematical principles as the "Standard" and presents the same possibilities of combinations and thereby the same safeguarding features as the "Standard". The only difference is, that ciphering and deciphering is effected automatically by electrical means. One of the texts is written on a typewriting machine and a second typewriting machine writes the other text automatically by means of electric transmission. (Figure 4.)

Berlin, June 24. 1929