The GEE System—V

~~*Top Secret Dinar*~~

Weaknesses in German Security

Summary

This is the fifth and final installment in the description of the GEE system. Several persons contributed to its authorship; Mr. T. A. Waggoner and Miss R. Jache are noted as having prepared the report for publication. Neither Mr. Waggoner nor Miss Jache is with NSA at present.

1. TICOM AND THE GERMAN ATTITUDE TOWARDS THE ADDITIVE GENERATOR.

In general, almost all responsibility for weaknesses in German security lies on the shoulders of the Foreign Office. Little or no progress was made in the solution of GEE from errors made by cryptographic clerks. The possibility of solution of GEE lay in the basic assumptions and misconceptions of the cryptographers in the Foreign Office (*das Auswaertige Amt*) in Berlin. From the TICOM material received on German cryptography, it is quite evident that the German office of cryptography was perfectly well aware of the mathematical limits, phases, cycles, and periods of all the elements of the additive generator which would be "unknown factors" to foreign cryptanalysts. In fact, many of the terms and conventions used by Herr Schauffler, the co-head of the cryptanalytic section of the German Foreign Office, were used by those working on the system during solution. One of his studies[1] makes clear not only that the limitations of the machine were well known, but that the machine was also trusted, in spite of its systematic nature, as giving sufficient security for the system. Part of this study, translated, reads:

> "*1. Description of the mechanism and statements of the problems.*
> "On an axle which goes from right to left, there are *r* wheels arranged so that they can turn. The smallest number of wheels possible is 2; in practice up to now *r* has been 5. The wheel farthest to the right is called wheel number 1. Around the outside of each wheel, 10 printing surfaces are embossed, i.e., the 10 digits in mixed order; the sequences may be different ones on different wheels. When a wheel turns, each digit comes in turn to 10 positions; one of the 10 positions is the "printing position," the position in which the digit is printed by the numbering machine. The change-over from one position to the next is called "step." On each of the wheel numbers 2 to *r*, one of the

[1]TICOM Document No. 3280: "Theorie eines Chiffrier-Numerierwerkes," Berlin, 3 December 1928, Section I.

10 digits has special properties and is called the "influence digit." The mechanism is so constructed that all r wheels turn step by step in a specified direction, and after each step, the digits which are in printing position are printed. Only when the "influence digit" of one of the wheel numbers 2 to r is in printing position does it happen that all wheels which are to the right of the digit under consideration stand still for the duration of one step. Thus the result is that only wheel number r turns uninterruptedly and uninfluenced with a period of 10, while all other wheels are brought to a stop at certain positions, thus printing the same digit two or more times in succession.

"This will be explained by means of an example. Figure 1 shows the sequences on the five wheels, i.e., the order of digits for each wheel as they come to printing position in uninfluenced succession. The influence digits are circled in black.

Figure 1

5	4	3	2	1
1	(1)	1	(1)	1
6	3	4	3	6
3	9	2	7	2
0	5	8	6	9
5	7	0	4	7
7	2	(6)	0	4
2	0	3	5	8
8	8	9	8	5
9	4	5	9	0
4	6	7	2	3

WHEEL NUMBERS

Figure 2

5	4	3	2	1
5	0	0	6	6
7	0	0	6	6
2	8	6	4	2
8	4	3	4	2
9	6	9	0	9
4	1	5	5	7
1	3	5	5	7
6	9	7	8	4
3	5	1	9	8
0	7	4	2	5
5	2	2	1	0
7	2	2	1	0
2	0	8	3	0
2	8	0	7	3

"Figure 2 shows the five-digit groups in the order in which they are printed if the starting group is 50066. The repetitions which are caused by the 'influence digits' are circled in red [here underlined].

The cipher numbering machine, then, has to some extent the inverse action of an ordinary numbering machine whose wheel number r also turns regularly with a period of 10, while one of its wheels, number to r-1, however, can step once *only* when all of the wheels to the left have the 'influence digit' 9 in printing position.

The ordinary numbering machine has a period of 10 (for a five-wheel machine, the period 100,000). We shall now prove that the cipher numbering machine has the same period and compute the periods which the individual wheels receive under the influence of the other wheels. For this purpose, in the next section, we will set up a formula which applies to the ordinary numbering machine, the cipher numbering machine we are describing and many similar mechanisms. In the third section, we will apply the derived formula to numbering machines and solve the problem just proposed. The last section will discuss the cipher numbering machine frame."

This extract shows how clearly the limits of the additive machine were understood by the Foreign Office. The conclusions drawn concerning the security of the machine were put in terms of a statistical

comparison with the Enigma machine: A translation of Section IV of Herr Schauffler's paper follows:

IV. Cipher Numbering Machine Frame

n cipher numbering machines, all of which have the same number of wheels, r, and all of which run in phase are put into a printing frame. A practical example, to which we will return several times, is $n = 48$ machines, each with $r = 5$ wheels. These machines print variations of the numbers 0, 1 . . . 9 to the $(n \cdot r)$ power; the number of different variations possible is:

$$V = 10^{240} = 10^{n \cdot r}$$

In the example at hand, therefore, the number of different variations which can be printed is:

$$V = 10^{240}$$

That is, the number which, written in the usual manner, is 1 followed by 240 zeros.

Since the separate cipher numbering machines in the frame all have the same period, Q, the frame, too, has the period:

$$Q = 10^{r}$$

Therefore, in the practical example, the period Q = 100,000, i.e., after 100,000 sheets have had 240 digits printed on them, the numerical variations will start to repeat.

Each of our variations to the $(n \cdot r)$th power belongs to a "period series," i.e., to a series of Q variations which result from the moving ahead of the machines. There are, therefore,

$$S = \frac{V}{Q} = 10^{n \cdot r - r}$$

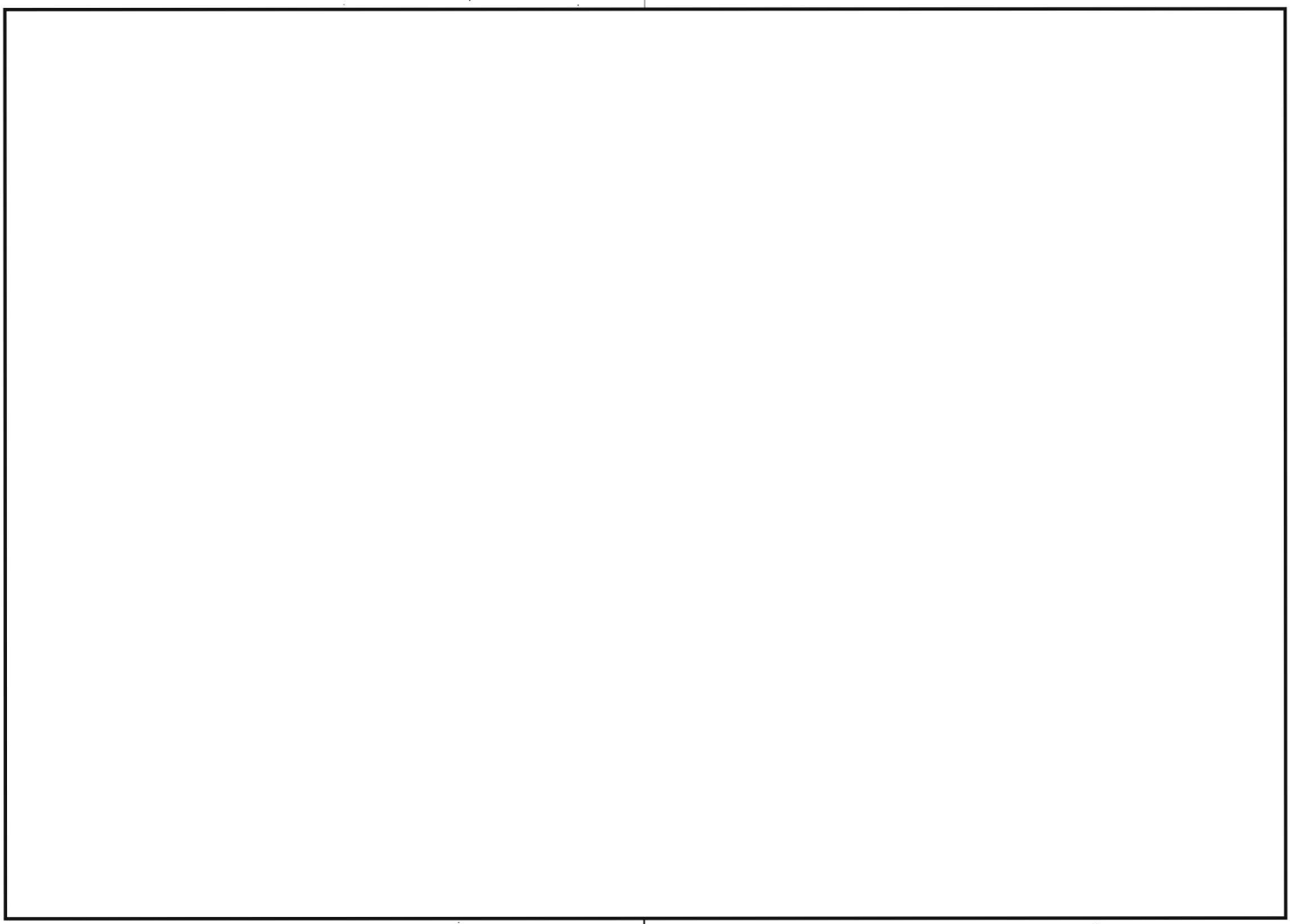
different period series which have no variations in common. In the example $S = 10^{235}$.

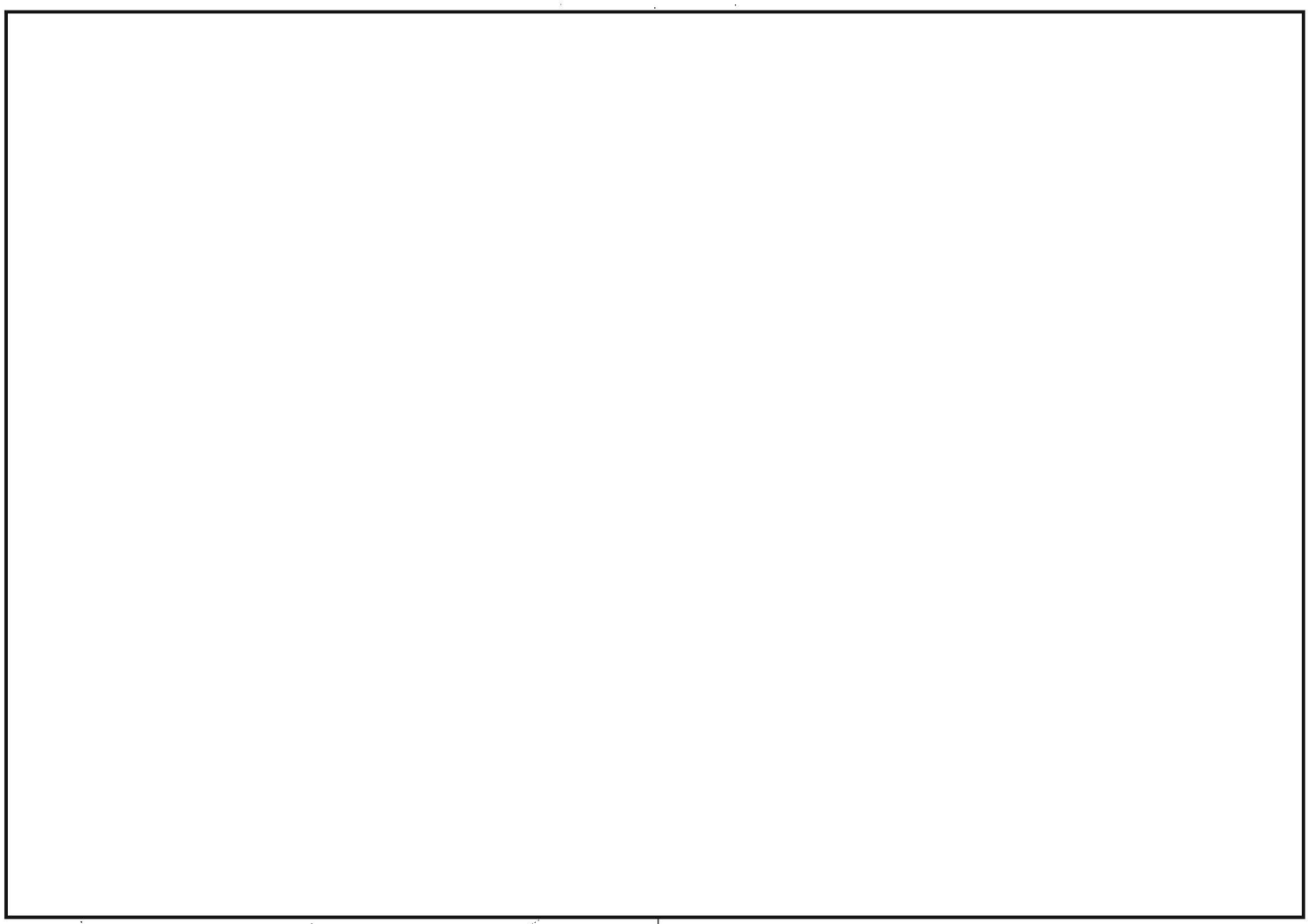
To compare the possibilities of combination, the *Enigma* may be referred to (see Patent Document DRP No. 429122). We ask: How many keys 240 digits long will the *Enigma* produce? The answer for the performance of the *Enigma* in the Patent Document mentioned is:

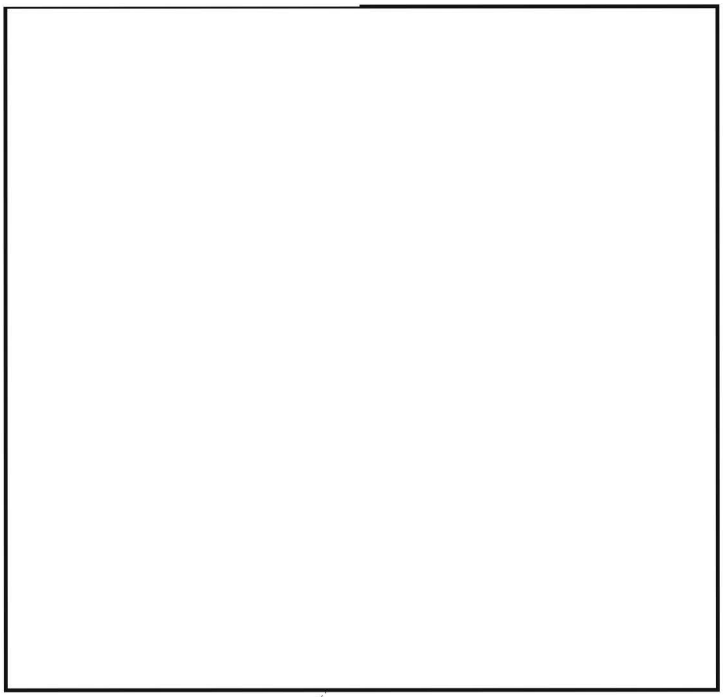
$$V = 11 \times 15 \times 17 \times 19 \times 26 = 24{,}350{,}000{,}000$$

therefore, an eleven-digit number, while the corresponding number for our present example of the cipher numbering machine frame is a 240-digit number.

Thus, with rather arrogant confidence, Herr Schauffler convinced himself and the Foreign Office of the security of the one-time pad system. But he was thinking of security in terms of pure statistics rather than in terms of foiling completely the enemy cryptanalysts.







(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36