

INTEROFFICE ROUTING AND/OR CARRIER SHEET HQ ASA

MUST REMAIN WITH ATTACHED PAPERS

NUMBER EACH MEMO OR REPLY IN LEFT BORDER, PLACE NAME, RANK AND TELEPHONE NUMBER BOTTOM OF EACH ACTION DRAW LINE UNDER EACH ACTION

~~SECRET~~ ENTER FILE CLASSIFICATION ADJUTANT _____

TO	FROM	DATE	SUBJECT
AS-76	AS-76C	1947 22 Apr	Studies Involving Multiple Stepping
			<p>1. Forwarded herewith is a paper listing references to multiple stepping in reports made by WDGAS-76C, and a memorandum from Cryptologic Research Subsection giving examples of other types of multiple stepping studied by them. These two papers do not accurately reflect the amount of thought that has been devoted to this problem, because the feature of multiple stepping has been considered in many embodiments that have been discarded later.</p> <p>2. Solutions Subsection has studied the German Cipher Machine SG-41, which involves multiple stepping. Some of these studies are now being written up and will be forwarded when complete.</p> <p style="text-align: right;"><i>Robert E. Gordon</i> ROBERT E. GORDON CIC, Projects Section</p> <p>Enclosures: 1. References to multiple stepping. 2. Examples of Multiple Stepping.</p>
2. THRU: AS-70 TO: AS-14	AS-76	24 Apr	<p>1. Forwarded for your information in response to your recent question on the subject.</p> <p>2. Keep one copy for your file.</p> <p style="text-align: right;"><i>Arnold I. Dume</i> ARNOLD I. DUMEY Chief, Cryptologic Branch Ext. 329</p>
2 Encls. n/c			<p style="text-align: center;">SECRET</p>

70-524547

WDGAS-76C

22 April 1947

References to Multiple Stepping

The following paragraph is from a paper entitled "Projected Random Tape Cipher Machine (suggested modifications for Mr. Friedman's device). 2 July 1946.

"A further modification of this last proposal has been suggested, in which the rotor would be in continuous motion, and the necessity of stopping and restarting its rotation during encipherment completely eliminated. The major problems here, of course, are the difficulties involved in synchronization and in adjusting the machine to irregularities in the speed of keyboard operation, the idea has, however, been discussed with the engineers and the possibility of such a design is being considered."

The following references to research done on Multiple Stepping Cipher devices have appeared in the weekly reports of Projects Section of Research Laboratories Division.

24 October 1946 - Thinking on the MX-507 and 508 has been proceeding along with the work on the 519. The main effort has been directed toward evolving a totally new cryptographic principle, or, alternatively, if a rotor maze is used, to cut down the number of rotors necessary, and to maintain the necessary level of security by adding new principles to the rotor maze. For different principles involving a rotor maze the following are being considered:

1) Multiple stepping of rotors, i.e. instead of a rotor stepping one place or not all, it would step either 0, 1, 2, or 3 places between encipherments.....

16 January 1947 - The cycle of a multiple stepping device with the following motion control has been examined

"In a w-wheel device a specified subset of the wheels move according to the rule of motion, (a);

a. The wheel moves one step when a notch appears for the first time in the effective position of its controlling wheel, otherwise it remains stationary.

The rest of the wheels move according to rule (b).

b. The wheel receives at every encipherment one impulse to move; it receives an additional impulse to move if a notch appears for the first time in the effective position of its controlling wheel. The wheel then moves as many steps as it has received impulses, except that it stops when it reaches a notched position and stores the remaining impulses to move until the next encipherment, at which time as many of the stored impulses will be discharged as possible without skipping a notch."

(References to Multiple Stepping)

Regarding the above device the following may be stated:

(A) If the N_i are chosen so that $K^w - N_1 N_2 \dots N_w$ is a prime, then the cycle length is $L = K^w - N_1 N_2 \dots N_w$. This is true no matter which subset of wheels are chosen to be governed by rule (a).

(B) If no wheels have consecutive notches only one motion impulse need be stored on any one wheel.

23 January 1947.-- A conference was held with Mr. Barlow of E. & E. Branch concerning principles to be employed in the 507 and 508. He was informed of new principles which might be considered such as multiple stepping. Ways and means of controlling stepping were discussed. Mr. Barlow stated that his branch preferred that multiple stepping not involve more than a choice of \emptyset , 1, or 2 steps. This, unfortunately, would weaken the principle so that it will not allow the number of rotors to be cut drastically.

20 February 1947 - 1. A paper has been written stating and proving several necessary conditions which must be satisfied in a device having w K-point wheels, with a cycle of K^w and with each setting having a unique successor. This theory was used to set up a multiple stepping device with a cycle of K^w .

2. Consideration was given to tabulating for the proposed Cipher Machine Generator the features most essential to the work of the unit.

26 March 1947 - Consideration is being given to a type of motion control organization called "planetary". In this type of organization one or more units of, say, two or three wheels, are each treated as single wheels in a larger device. Such units are permitted to step through their cycles only when they receive an impulse from other elements in the device.

For example, a three-wheel CCM unit of cycle length C might step through its cycle only when it received an impulse from one or more other wheels which move in any erratic manner (so long as they do not stop dead). These other wheels may have multiple stepping if desired; they could be controlled in whole or in part by the CCM unit, thus giving interlocking motion. The cycle of the complete device would not be definitely known but would be greater than C .

3 April 1947 - Investigation has proceeded on two further examples of devices whose "wheels" are units consisting of two or more actual rotors. (This type of motion control was referred to as a "planetary" in last week's report.) In one of the new examples one of the "wheels" is a CCM unit, which guarantees the cycle, even though the motion of the whole device is interlocking (a detailed embodiment of this is being forwarded for comment). In the other example the whole device may be regarded as CCM each of

(References to Multiple Stepping)

whose three "wheels" is a pair of mutually delayed rotors; notches can be placed on the six rotors so that for 88% of the wheel orders the cycles will all be greater than 13,000,000.

A study of C-41 cycles when the five incongruences imposed in TICOM/I - 72 are not all satisfied has shown that very short cycles are possible. By violating only one of the above conditions (equivalent to failure to activate one pin on one wheel) a cycle of 70 was obtained, as compared to a minimum of 95,220,000 under German usage.

$$[26^2 - (N_1, N_2)] \times [26^2 - (N_2, N_3)] \dots$$

WDGAS 76-C

23 April 1947

SUBJECT: Examples of Multiple Stepping

TO : CIC, Projects Section

1. Cyclic polymeric. On each motion phase, let all wheels move one step regularly, plus one step for a newly arrived notch on the wheel to the left (the last wheel on the right is considered as being to the left of the first wheel). However, if this would involve skipping a notch on C_{wi} , then C_{wi} moves only one step and stores the additional motion impulse until the next motion phase, at which time the impulse is discharged. Arranging notches non-consecutively will prevent having to store more than one impulse at a time.

It may be shown that the cycle for a device of w K -point wheels with this rule of motion is $K^w - N_1 N_2 \dots N_w$, provided this number is a prime. Moreover, the regular step may be omitted for any one or more wheels (but not all), without affecting the length of this cycle.

2. Modified CCM. In the standard CCM the middle wheel, C_{w1} , steps once on each motion phase. Suppose that C_{w2} moved as many steps as there were notches in two consecutive positions of C_{w1} , and C_{w3} moved as many steps as there were notches in two consecutive positions of C_{w2} . In other words, there are two effective positions on C_{w1} and C_{w2} , and the sum of the number of notches in those positions gives the number of steps of the next wheel. The following results have been obtained.

If K denotes the size of the wheels (26 in the standard CCM) and N_1 the number of notches on C_{w1} , the cycle of C_{w1} and C_{w2} is $\frac{K^2}{(K, 2N_1)}$. The cycle of C_{w1} -2-3 in general involves the pattern of notches on C_{w2} , not just the number of notches, and when $(K, 2N_1) = 3$ it is believed possible to choose patterns so that the cycle is $\frac{K^3}{3}$. When $(K, 2N_1) = 1$ or 2 the cycle is K^2 or $\frac{K^2}{2}$ respectively, regardless of the number or arrangement of notches on C_{w2} . Thus for 26-point wheels this type of motion would not be good, since $(26, 2N_1) = 2$ for all values of N_1 except 13.

3. Pyramidal motion. A device of w K -point wheels, with multiple stepping permitted on all but one wheel, can be made to have a cycle of K^w by building up the cycle so that the first i wheels have a cycle of K^i . One way to do this is as follows. Let C_{w1} step once on each motion phase. Then at each setting C_{w1} either has a notch (+) or no-notch (-). At each of these two

(Examples of Multiple Stepping)

kinds of notch situation CW2 is caused to move a certain number of steps, 0, 1, 2, etc., in such a way that after a revolution of CW1 the number of steps of CW2 is prime to K. If CW1 has N_1 notches, with CW2 moving x steps for a CW1 notch and y steps for a CW2 no-notch, then for each CW1 revolution, CW2 moves $M_2 = xN_1 + y(K - N_1)$ steps. For example, if $x = 1$ and $y = 0$, as in ordinary polymetric motion, $M_2 = N_1$ and the cycle of CW1 and CW2 is K^2 if N_1 is prime to K. If $x = 2$ and $y = 1$, we get $M_2 = 2N_1 + K - N_1 = K + N_1 \equiv N_1 \pmod{K}$, and the cycle is the same as for $x = 1, y = 0$. During a cycle of CW1-2, there are four possible notch situations on the two wheels, namely ++, +-, -+, --. At each of these CW3 is caused to move 0, 1, 2, etc., steps. Since the cycle of CW1-2 is K^2 , every possible setting of CW1 and CW2 occurs exactly once, so that the number of notch situations of each type is calculable. The assignment of 0, 1, 2, etc., is made to each notch situation so that the resulting "offset" of CW3, after a CW1-2 cycle, may be made prime to K, thus obtaining a cycle of K^3 . By continuing in a similar manner, the cycle of any number of wheels, say w, may be made K^w .

4. C-41. Let N_i denote the number of active pins on W_i . Then we have

	Size of Wheel	Number of Active Pins
W_1	25	N_1
W_2	25	N_2
W_3	23	N_3
W_4	23	N_4
W_5	24	N_5
W_6	24	N_6

If N_1, N_2, N_3, N_4, N_5 are known, then for any setting it is determined how much each wheel shall step at the next motion phase. Thus the settings produced by successive motion phases can be written down until the first setting recurs, completing what we call a motion period. Since there are one or two motion phases between successive encipherments, the cycle (of enciphering positions) will be at least half of, but not greater than, the motion period. The exact cycle will depend on the pin pattern of W_6 .

The following conditions on N_i are necessary and sufficient to obtain the maximum motion period: $25^2 \cdot 23^2 \cdot 24^2 = 190,440,000$.

N_1 not divisible by 5.

N_2 not 21.

~~SECRET~~

(Examples of Multiple Stepping)

N_3 not 0 or 23.

N_4 not leaving a remainder of 1 when divided by 2 or 3.

N_5 not divisible by 2 or 3.

The cycle in this case is at least 95,220,000.

By using $N_1 = 10$ but obeying the remaining four conditions, a period of 125, with an associated cycle of 70, was obtained.

5. Polymetric cascade. In a five-wheel device let CW1 move one step on each motion phase, CW2 move one step as a notch departs the effective position of CW1, and CW3 move as many steps as there are departing notches on CW1 and CW2. By proper choice of the notch numbers on CW1 and CW2, the cycle may be made K^3 . The remaining two wheels can be given multiple stepping by rules which prevent lobsters and prevent the stepping of a single wheel.

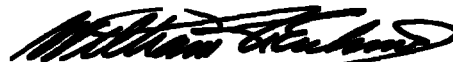
* * * * *

In addition to the specific rules of motion discussed above, there are two general statements as to how multiple stepping may be accomplished without interfering with the computation of cycle lengths.

1. Any device with a guaranteed cycle can have multiple stepping introduced on any or all wheels that are not involved in the cycle guarantee.

2. In any device in which half the minimum cycle is deemed adequate for security, multiple stepping can be achieved, in effect, by having two motion phases between successive encipherments. (This would not alter a cycle of odd length but would halve one of even length.) Or there could sometimes be one motion phase and sometimes two between encipherments, depending on the notch situation on one or more wheels.

In practically all the new rules of motion which are currently being devised the possibility of adjustments to permit multiple stepping is considered.



WILLIAM H. ERSKINE
Cryptologic Research
Subsection

~~SECRET~~