

To : OIG, Projects Section, Cryptologic Branch

Subject: Proposed System For Guaranteeing A Minimum Cycle Of Great Length In Any Irregular Motion Rotor System

A. It is proposed that any thoroughly irregular motion system whatsoever be used, including Sigaba type, or patterns of notches and GCM motion. This system shall be devised solely for erratic motion, with no sacrificing of unpredictability to insure a minimum cycle.

B. It is further proposed that a simple device be included as described below which shall have a definite known period. This device will in effect interrupt the erratic motion of the rotors, in an irregular manner according to its known cycle. Since this device has one function only and is to involve no contribution to security as a detail of erratic motion, its components, notches, etc. shall be fixed in the most expedient pattern.

I propose  $\frac{1}{8}$ " thick aluminum disks each attached to a stamped gear wheel of the type found in the M-209. Each gear shall be a number prime to each other and of such a number that the product of the  $F_{\text{disk}}$  will be a cycle long enough to permit 24 hour operation at maximum speed without resetting and without repetition of the cycle. Numbers such as 43, 45, 49, 51, fulfill these requirements.

These disks shall be on a common shaft and advanced 1/20th tooth for each step of the machine. They shall each register at a given point as in the M-209.

There shall be on the perimeters of these disks a sufficient number of notches so that at a given percentage of the time four notches will be simultaneously effective. Whenever this condition occurs the interrupter shall operate by:

- a. Denying stepping of one or more relatively fast rotors or control rotors.
- b. ~~Or~~ by stepping a relatively slow rotor.
- c. ~~Or~~ by reversing any 1 or 2 of the rotors, i.e., if rotor 2, for example, was by reason of the stepping system set to move, it would not, if it was not set to move, it would. This removes to the greatest degree predictability of the action of a rotor because of the known interrupter setting; a disadvantage of a. and b.

Irregular patterns are no object to the interrupter. Therefore on a given disk every fifth possible notch would not be effective. For example,

~~SECRET~~

Since ~~its~~ function is limited, the ~~interrupter~~ need add no complications to the setting of the machine either for each message, or daily. It could have a pin in each disk, so that at the end of each message a button could be pressed and have all disks automatically return to the same setting. *CP 11 R*

*9*  
*"D."* This device would permit greater flexibility of systems, since they could be used continuously on line without fear of ultimate depths for extended periods of time.

David Wagner  
1st. Lt., Signal Corps  
Cryptologic Branch