File - Hagelin

F. T. Leahy
AFSA-343
August 31, 1951

CRYPTANALYTIC SURVEY OF MODIFIED HAGELIN DEVICE

I. INTRODUCTION

A newly developed cipher machine has been examined to determine possible cryptanalytic procedures that should be followed in case this machine is employed by other countries. This machine is a modification of the M-209 (or equivalent) that is now widely used, commonly called the Hagelin.

II. DESCRIPTION

As the reader is undoubtedly familiar with the present Hagelin device, it will be simplest to state the differences and modifications incorporated into the new machine.

A. Relatively unimportant changes.

1. There are 30 slide bars instead of 27 (or 29).
2. The machine cannot be spun back to a previous window setting.
3. In the earlier machine, the rule: P (plain) + C (Cipher) = K (kick) + S (slide) has been replaced by: $P + C = (30-K)+S$.
4. The sizes of the wheels have been increased from 17, 19, 21, 23, 25, 26 to 29, 31, 33, 34, 35, 37, which in each case are relatively prime.

B. Important changes.

1. The wheels do not take exactly one step between encipherments, but may take (independently) any number from 0 to 5 steps.
2. Each bar is provided with five rather than two lugs. These lugs are raised from a fixed location rather than slid to

their proper spot as in the present machine. Any or all of the 5 lugs may be raised to an active position, but it is assumed that at least one lug will be used on every (or nearly every)bar.

The irregular stepping of the wheels is effected as follows: Five of the bars are assigned to each wheel, bars 1-5 to wheel 1, bars 6-10 to wheel 2, etc. Opposite the wheel to which the bar is assigned is a notch instead of what could have been a sixth lug. Of the five notches assigned to each wheel, each of four cause the wheel to step one if its bar is activated (slid to the left), and the fifth causes the wheel to step one if its bar is not activated. The bars are activated in the same manner as at present: an active lug opposite an active peg. (A new arrangement enables the active and inactive pegs at the start of the cycle to retain their initial status, even though the wheels are being stepped to new positions.)

III CYCLE LENGTHS AND RUTS

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

PL 86-36/50 USC 3605
EO 3.3(h)(2)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

PL 86-36/50 USC 3605
EO 3.3(h)(2)

FIG. I (cont.)

[redacted]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]