

AKTIEBOLAGET CRYPTOTEKNIK

STOCKHOLM 201

HAGELIN-CRYPTOS

DIREKTORINEN

Aug. 5, 1950.

Memo re new developments in ciphering devices, by Boris Hagelin, Zug.

1. An auxiliary ciphering machine, provisionally called Cryptex mod. CI, for the direct automatic ciphering of telewriter messages, exchanged over normal 5-impulse telewriter channels. The machine will work on either double current or single current circuits, or radio. The machine operates on the well known signal inversion principle, but, as the five cipher signal elements are set up separately, and transmitted independently of the incoming (from the telewriter) clear text signals, the line (cipher) signals will contain no telltale parasites.

The key (ciphering) impulses are obtained from four banks, each normally carrying the 32 different possible impulse combinations, which can be arranged and rearranged in any desired sequence. Four preselectors, which are set for each message in desired starting positions, are individually displaced from one position to another with the aid of a new-designed displacing mechanism. With the use of three selector relays, which are commanded from the same displacing mechanism, one of the four simultaneously preselected impulse combinations are connected to the ciphering relays.

The displacing mechanism has been specially designed for the operation of the selecting mechanism of this machine. It consists of a bar drum, carrying two sets of twelve bars each, a set of six key wheels, and an interacting mechanism between the drum and the key wheels. The construction of the drum and the key wheels resembles outwardly that of the converter M-209, the main difference is however that while in the M-209 the key wheels are displaced one step each time, with the aid of a separate driving device, here the drum bars and the key wheels interact with each other, and are both used for ciphering purposes. Through the interaction, the key wheels are advanced irregularly, with 64 different possibilities for each movement. This action is obtained in the following way; the drum bars are provided with special driving teeth, which mesh over intermediary pinions with the gears of each key wheel; and depending on the arrangement of the key wheel pins, of the lugs on the drum bars, and of the driving teeth (of the bars), different combinations of drum bars will on one hand be displaced, and different advancement combinations will on the other hand be given to the key wheels.

Two preselectors are placed at each end of the drum, with one at the front and one at the rear. For each displacing movement the drum revolves one half revolution, when the four preselectors will be subjected to four different irregular movements.

In front of the six key wheels, contacts are placed, which are acted by the pins (active pin - closed contact, inactive pin - open contact). Any three of these contacts can be connected to the operating magnet; the three selector relays, and these will act in an irregular manner; the key wheels are advanced irregularly.

While the diameter of the key wheels will be the same as for those of the converter M-209, they will have the following number of pins; 29, 31, 33, 34, 35 & 37. Another innovation is that they can be rearranged silly in any sequence desired (720 possibilities). key wheel pins & A suitable choice of driving teeth combinations and/lugs will result, easily changeable and to all practical purposes aperiodic key impulse combination series.

Dimensions; 12 1/2" x 10" x 6 1/2" . Price; depending on equipment,
Weight ; ab. 40 lbs. Standard; \$ 1200;- each, at
A drawing will be sent at an early date. Factory Stockholm

Inclosure 3 to AFSA Serial _____ dated _____.