SECRET

1. NAME: CSP 3300 - Teletypewriter Cryptographic Attachment Mark II.

2. STATUS: In use.

3. FUNCTION: Encipherment of Baudot text.

4. SECURITY: Category A.

5. CRYPTOGRAPHIC PRINCIPLES:

CSP 3300 is a cipher machine to be used off-line and semi-on-line for the encipherment of Baudot text. taken from a message tape and

The plain text of Baudot characters is stored in 5 input relays - 1 for each level of the tape. At the same time, a fixed 12 contacts on the right end plate of a 5 rotor maze are energized. The current passes through the maze and is reflected back to the right end plate. The energizing of a combination of 3 contacts on the left end plate and 7 contacts on the right end plate produces a transposition key which permutes the output of the 5 input relays according to the elements of the symetric group of degree 5. The energizing of a combination of 5 contacts on the right end plate produces an additive key, which is combined modulo 2 with the ouput of the transposition step, thus producing cipher text.

irregular ~~erratic~~ The stepping of the rotors of the maze is except that the center (# 3) rotor steps each time. (Rotors # 2 and # 4 step in reverse).

When contacts 7 and 25 on the right end plate are energized, the # 1 rotor steps. If the "back" contact on the # 4 rotor is closed at the same time the # 1 rotor steps, the # 4 rotor also steps. If the "make" contact on the # 1 rotor is also closed at the same time, the # 2 rotor steps. And if the "break" contact on the # 2 rotor is closed at the same time, then the # 5 rotor also steps. ~~Normally,~~ The contacts ~~on rotors # 1 and # 2 are closed unless hit~~ by a lug. ~~The contact on rotor # 4 is open unless hit by a lug, but when the lug on rotor # 4 actuates the back contact of that rotor, then rotors #1 and # 4 both step.~~

on the rotor, the same as in the ECM stepping maze

There is a manually operated switch which makes the change from decipher to encipher ... This switch is necessary because although the substitution (plain & reverse) ... reciprocal - the transp. is not - ...

SECRET

and
Caribbean

The transponders to be introduced at different points in the circuit for injecting + deciphering the engineering features are somewhat complicated + beyond the scope of this paper -

~~SECRET~~

6. INDICATOR SYSTEM:

Plain language transmission of ~~rotor alignment~~ message indicators.

7. COMPROMISE:

Transmission of 2 or more messages with the same indicator. A short crib is necessary in one of the two message. The result is that both messages can be read but it depends entirely on the ability to extend the crib.

8. ASSOCIATED DOCUMENTS:

None available.

6. KEY LIST AND INDICATOR SYSTEM:

Plain language transmission of message

indicators.

The rotors are set by hand to the message

indicator

1. Name: — CSP 3300 Teletypewriter Cryptographic Attachment Model II.
2. Status: — In use.
3. Function: — Encipherment of Baudot Text
4. Security: — Category A.
5. Cryptographic Principle: —

CSP 3300 is a cipher machine to be used off-line and semi-on-line for the encipherment of Baudot text.

The plain of Baudot characters is taken from a message tape and is stored in 5 input relays - 1 for each level of the tape. At the same time, 12 banded input contacts on the right end plate of a 5 rotor maze are energized. The current passes through the maze and is reflected back at the left end to the right end plate. The energizing of a combination of 3 contacts on the left end plate and 2 contacts on the right end plate produces a transposition key which permutes the output of the 5 input relays according to the elements of the symmetric group of degree 5. The energizing of a combination of 5 contacts on the right end plate produces an additive key, which is combined modulo 2 with the output of the transposition step, thus producing cipher text, which is locked up in 5 output "memory relays". The circuits through these relays and to a distributor put the proper signal on the line in sequential order, and also adds the necessary start and stop signals. All relays are actuated and locked during the start signal and released during the stop signal. Thus there is no chance for putting "pips" or momentary breaks on the line which would indicate the clear text signal, or of inducing feed-backs which would reveal the clear text signals. In deciphering a reverse process is followed. The cipher text of Baudot characters is taken from a message tape and stored in the 5 input relays. The transposition and substitution processes are reversed and the resulting plain text is stored in "memory" relays, from whence it pas-

which is locked up in 5 "memory relays". output

The circuits thru these relays and to a distributor which puts the proper signal on the line in sequential order, and also adds the necessary start & ~~stop~~ signal. All relays are ~~actuated~~ & locked during the start signal & are released ~~thru the~~ during the stop signal. Thus ~~there~~ is no chance for putting "pips" or momentary breaks on the line which would indicate the clear text signal) or of inductive feed-backs which would reveal the clear text signal. For deciphering a reverse process is followed — The cipher text of Baudot characters is taken from a message tape & stored in the 5 input relays - ~~the~~ transposition & ~~[illegible]~~ substitution processes are reversed & the resulting plain text is stored in "memory relays" from where it passes in sequential order (thru the distributor) into the Teletype printer.

Stepping Cryptography the #3 rotor (center) is a constantly stepping rotor - rotors #1 #4 steps ~~[illegible]~~ approximately 1/3 times by 26 (on the average) but #4 drops behind ~~[illegible]~~ one step for every revolution of #1. ~~i.e. #4 is driven in inverse motor fashion from #1~~

#2 & #5 steps approximately every 35 letters (on the average) but #5 drops behind ~~one~~ ~~step~~ for every revolution of #2. The ~~average~~ cycle length is $4/3 \times 26^4 = 609,300$ ~~approx~~

At 60 wpm CSP 3800 can't run about 26 hours before the cycle repeats.

[illegible] [illegible] text computing cycle length

7. Comp.

It is believed that as we know more about the machine & its ~~solution~~ ~~we~~ method of attack, we can successfully block solutions or require far longer stretches of key to make solution within the realm of possibility by suitable modifications to the key - we are really scratching the surface of the possibilities of this machine -

~~Finally it must be recalled that this is a [illegible] machine only [illegible]~~

Correlation Machine
by able to capture -

For this purpose we should have a machine that when skillfully used will defy solution under service conditions at the same time permit solution by our own people if used by the enemy who will be presumed to used random key.

In this way a capture would boomerang against the enemy if he ever tried to use this machine.

The mechanism of the key board that CSP 3607 - ~~[illegible]~~ - comes nearer to fulfilling these "booby trap" requirements than any other cipher system known.

6. Indices

~~Rotors are set by hand~~ to the message indicator — control is set to the "setup" position and the start switch is thrown to the "ON" position. The machine steps a varying number of steps from 1 to ~~75~~ 75 (or more) & ~~an~~ averaging 15 steps and automatically stops due to combination of the settings of the 5 polarity reversal relays plus the additional "set-up" relay. ~~Starting~~ operate switch is thrown to off position, control switch is set to operate position, ~~then~~ the message tape is inserted in the sensing head — then the operate switch is thrown to ON position and the encipherment or decipherment proceeds from this point. Electrical interlocks prevent any error on the part of the operator. If desired, instructions can require the machine be stepped to a minimum of 5 or 10 steps by counter before starting; this is considered — which guarantees stepping the rotors & ~~probably~~ prevents mono alphabetic

unnecessary & is not contemplated at this time.

The exact action of the machine can best be understood by a careful study of the machine itself and its wiring diagram.

(7) A description of the ~~The~~ manner in which the typewheel is given its initial displacement from the keyboard is beyond the scope of this paper. It is sufficient to state that it is simple & reliable & an adaptation of standard adding machine technique developed by the Remington Rand Company for the Government. It accomplishes by depression of a key what is accomplished on the manual Hagelin machine by turning the Type Wheel Knob until the desired letter on the reproducing disc appears opposite the scribed reference line on the machine.

6. Key Lists

B. In order to get optimum security it is necessary that key lists be expertly prepared at a central point & that random setting of the machine (locally prepared keys) be absolutely prohibited. With carefully prepared key lists it is possible to assure that there be a minimum of bias.

(we can check all solutions with scientific accuracy)

It may be several years before perfect key lists can be prepared —

anyone [illegible] [illegible] have the same weaknesses & these Hagelin machines [illegible] correct be entirely [illegible]