This document ~~may be~~ read only by those personnel officially indoctrinated in a~~ccordance w~~
munication intelligence security regulations and authorised to receive the information report~~ed~~
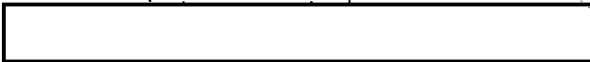
~~SECURITY INFORMATION~~

~~U. S. EYES ONLY~~

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

11 December 1952

SUBJECT: Report on

1. The date was inadvertently omitted on a recent NSA-202L publication,
Dr. Hugh F. Gingerich's report, subject:

2. It is requested that you date the copy or copies retained in your
Office: 8 December 1952.

A. W. FOLEY
Head, NSA-202L

Copies furnished:
  DDI
✓ CONS
  R/D
  C/SEC
  35B
  206
  23
  24
  202L
  DD/FI/CIA

~~U. S. EYES ONLY~~

REF. ID:A59040

~~TOP SECRET CANOE~~

This document ~~~~ be read only by those personnel officially indoctrinated in ac~~~~nce with com-
munication intelligence security regulations and authorized to receive the information reported herein.

~~SECURITY INFORMATION~~

~~U. S. EYES ONLY~~

SUBJECT:

    1. The attached report was prepared following my visit to the
workshop of the ⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜ This
visit took place during September – October 1952.

Hugh F. Gingerich
HUGH F. GINGERICH
NSA-35B

Published by NSA-202L

Copies furnished:
  DDI
  CONS ✓
  R/D
  C/SEC
  35B
  206
  23
  24
  202L
  DD/FI/CIA

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

TOP SECRET CANOE

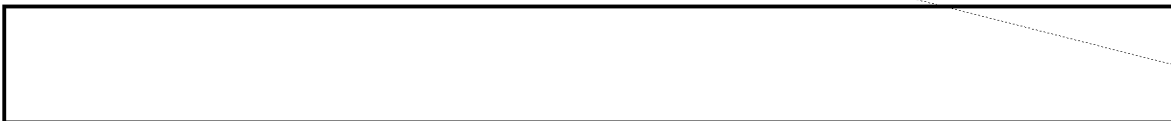This document to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

SECURITY INFORMATION

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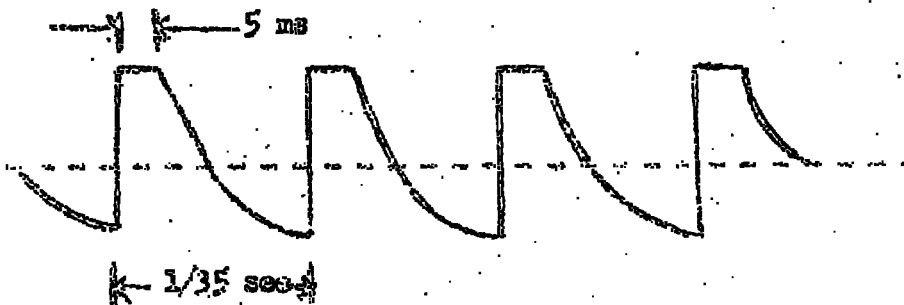PL 86-36/50 USC 3605

U. S. EYES ONLY

The one-time pads are printed by an electric typewriter at the rate of 7 characters (or spaces) per second. Up to 5 carbon copies can be produced at the same time.

The randomizing elements (of which there are two – one for tape production and one for pad production) produce a steady stream of random bauds at a rate of 35 bauds per second. The timing of the machine is determined by a multi-contact motor-driven jumping cam. The randomizing process is initiated by a five millisecond closure of one of the jumping cam contacts. Through this contact is applied the plate voltage of a relaxation oscillator gas-type tube. This voltage also is applied through a resistance to a condensor so that the plate voltage versus time curve, for the oscillator tube, is of this form:

The applied voltage is considerably greater than the minimum voltage (shown by dotted line) at which the oscillator oscillates.

The oscillator is tuned to approximately one hundred kilocycles per second; but this frequency varies somewhat with the plate voltage. The output of the oscillator is amplified (one stage, gas tube) and drives a flip-flop, producing one change of state of the flip-flop for each cycle of the oscillation.

When the plate voltage on the oscillator tube falls below the minimum, the oscillation stops, the flip-flop remains in whichever state it happens to fall until the plate voltage of the oscillator tube is reapplied by the next closure of the jumping cam.

U. S. EYES ONLY

REF ID:A59040

TOP SECRET CANOE

This document ~~... be read only by those personnel officially indoctrinated in a~~ ..lance with communication intelligence security regulations and authorized to receive the information reported herein.

~~SECURITY INFORMATION~~

~~U. S. EYES ONLY~~

During the time of non-oscillation a polarized relay is set up, according to the state of the flip-flop. The output of this relay determines whether the signal is to be "hole" or "no-hole". The parity of the number of cycles of oscillation determines the delta pattern of the baud stream. Since the mechanical and electrical operation of the plate voltage supply is subject to variations, the time during which the oscillations take place is variable, and the number of cycles per baud is determined only within a range of approximately one hundred cycles. Since the result depends only on the parity of the number of cycles, it seems evident that the sequence of bauds produced should be statistically random.

The output of one of the randomizing elements goes directly to a tape punch, the result being assembled five bauds to a frame. The output of the other is used to set up a "Christmas Tree", which, after five bauds, is probed and the result is either suppressed (in which case the typewriter does nothing) or is translated into five timed pulses representing the appropriate character. If the pad is to be alphabetic, 26 of the values produce characters, and the other 6 are suppressed. If the pad is to be digital, 30 of the 32 outputs of the "Christmas Tree" are grouped into 10 groups of 3 each, and a shot on any one of the three lines of a group, produces a 5 baud signal for the printing of the appropriate digit.

The machine can also be set up so that the five bauds of one "throw" determine whether the next "throw" is to produce an alphabetic or digital character, with the choice of probabilities for a digital character of one half, one quarter, one eighth or one sixteenth.

There are switches on the machine to determine the number of spaces between characters, the number of characters per group, the number of groups per line, the number of line feeds between lines, the number of lines per page, and the number of line feeds between pages. Whenever a space, line feed or carriage return is executed by the typewriter the character for that "throw" is suppressed. Thus in computing the time for a job; spaces, line feeds, and carriage returns must be counted as well as characters. Maximum line length is 68 characters and/or spaces per line.

There is provision for suppressing "q" and "s" when they occur as results of a "throw" for the first character of an alphabetic or mixed group. Whenever a suppression of a character occurs the time of that "throw", i.e., one seventh of a second, is lost.

~~U. S. EYES ONLY~~

2

REF ID:A59040

TOP SECRET CANOE

This document ... be read only by those personnel officially indoctrinated in ac ...ance with communication intelligence security regulations and authorized to receive the information reported herein.

SECURITY INFORMATION

U. S. EYES ONLY

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

The machine may be set up so that if, in a given line, a character (digit or letter) has previously occurred it will be subsequently suppressed. The result is a randomly scrambled complete alphabet, or sequence of ten digits, for each line.

There are two sets of six counters each. One set is used normally with the tape producing die, one counter for a character count, and the other five for levelwise counting of "holes". The other set of counters is normally used with the pad producing die, one counter for a character count, and the other five for character category counts. The die for pad producing can alternatively be connected to the levelwise counters.

Stepping at both ends is controlled by the input keyboard or tape reader. Whenever the deciphering unit gets out of phase with the enciphering unit, a plain language signal is to be sent back requesting a new start at the next block. Blocks are probably to be fifty characters long, block numbers being printed on both tapes, which are to be produced similtaneously by a single punch, using specially prepared rolls of pairs of tape with carbon paper between.

TOP SECRET CANOE

This document ~~.~~ be read only by those personnel officially indoctrinated in a~~.~~ ~~.~~nce with communication intelligence security regulations and authorized to receive the information reported herein.

~~SECURITY INFORMATION~~

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

~~U. S. EYES ONLY~~

Standard procedure for checking material now being produced by the two machines already in operation is to run for perhaps half an hour with the counters on at the beginning and end of a run. If both tests show random values then the run is assumed to be all right.
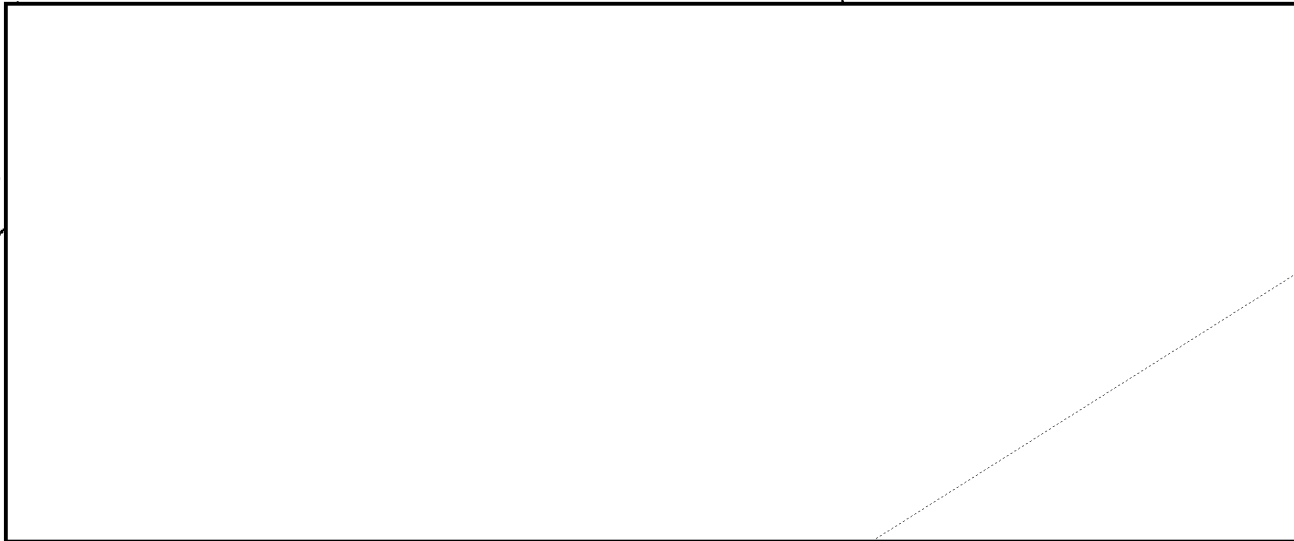
~~U. S. EYES ONLY~~

4

ARMED FORCES SECURITY AGENCY   Form 781-C10SC 1 Jul 52   ~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

This document ... be read only by those personnel officially indoctrinated in a... ...ance with communication intelligence security regulations and authorized to receive the information reported herein.

~~SECURITY INFORMATION~~

~~U. S. EYES ONLY~~

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

~~U. S. EYES ONLY~~

ARMED FORCES SECURITY AGENCY   Form 781-C10SC 1 Jul 52   ~~TOP SECRET CANOE~~