~~TOP SECRET~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIC~~

[redacted] ~~No. 98~~

Date: 5th March 1955

Copy No.: 19

SECURITY OF AFSAM 4A

By [redacted]

SUMMARY

This paper briefly describes the AFSAM 4A and discusses its security. It is concluded that subject to certain qualifications about procedures for avoiding depth, the machine is secure for all classifications of traffic for at least the next three years.

Distribution

Standard.

EIDER

[redacted] No. 98

SECURITY OF AFSAM 4A

By [redacted]

1. Introduction

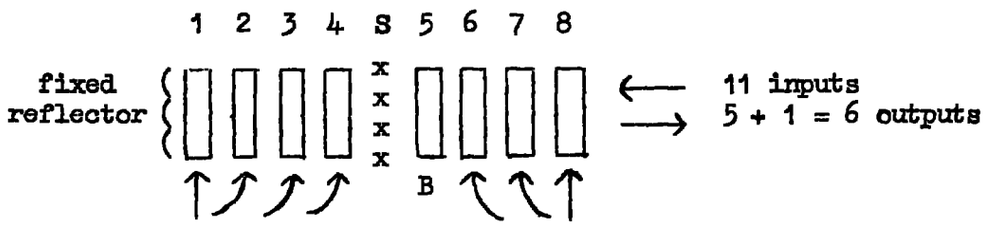
AFSAM 4A is an on- or off-line additive-producing twice-through rotor machine which has recently been introduced for use in U.S. D/F and administrative networks. It is a conversion from a once-through version call M-294 or SIGNIN (BALDER and PANDORA cryptosystems). The machine and the associated cryptosystems (CENTAUR and IXION) are described and assessed in detail in BRUSA C/S 306 dated October 19th, 1953. It is there concluded that the machine, when used with these procedures, is secure for all classifications of traffic for at least the next 5 years. This paper

(a) briefly describes the machine and the associated procedures,

(b) discusses its security.

2. Brief Description

(a) The machine



There are 8 26-point non-reversible rotors selected from a 10-rotor set. Each rotor has a fixed alphabet and an identical fixed 5-notch notchring. The rotors are pluggable but will not be replugged in the field. R1234 and R876 form cyclometric cascades with R1 and 8 the fast rotors. R5 is a bump rotor driven by one of the 6 outputs as in ASAM 2-1. S, between R4 and 5 is a permanent scramble-wired separator. The reflector is wired with 10 pairs and 2 triplets, as in ASAM 2-1, and the key-producing arrangements are likewise the same - 11 live inputs and 5 key outputs. The key is added level by level to 5-unit plain text, and is never transmitted in clear. The flatness of the key is discussed in Note A, where it is also shown that there is a slight correlation between the key and the stepping of the bump rotor.

(b) CENTAUR

(1) Each pad consists of 120 pages which are assigned in blocks to stations on a net. Each page contains: (A) 4 rotor arrangements each of which has 20 tetranome designators from a series which runs in order from 0001 to 9600 throughout the pad. (B) 176 random 4-letter groups, each designated by a digraph; the digraphs range from AA to GT on each page and are arranged alphabetically.

(ii) An indicator consists of a tetranome giving the roter arrangement, and 2 digraphs giving the alignment (as shown on the same page as the tetranome). Both tetranomes and digraphs are crossed off after use.

(iii) For off-line use any unused tetranome can be used as an indicator. Messages are limited to 6,000 characters. For on-line use a rotor arrangement can be used only once, but up to 20 necessary restarts throughout the 12-hour cryptoperiod may be made on the same arrangement. A restart may consist either of a new indicator or of a counter reset as in (iv) below.

(iv) Counter reset.

(A) Half duplex. A receive operator can cut off transmission if he is getting garble. The whole net goes over to plain. The send operator stops on a random number of positions, not less than 20, and transmits his character counter reading.

(B) Duplex. The receive operator who is getting garble sends BREAK on his send machine. He resets and sends his new counter reading on his send machine.

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

(v) There is no letter check procedure.

(c) IXION

IXION is like CENTAUR except that (i) there are about 200 pages to a pad and (ii) the tetranomes are replaced by trigraphs which are arranged alphabetically only within a single rotor arrangement.

(d) CENTAUR is the normal procedure. IXION will only be used when T/A considerations warrant it.

[redacted]

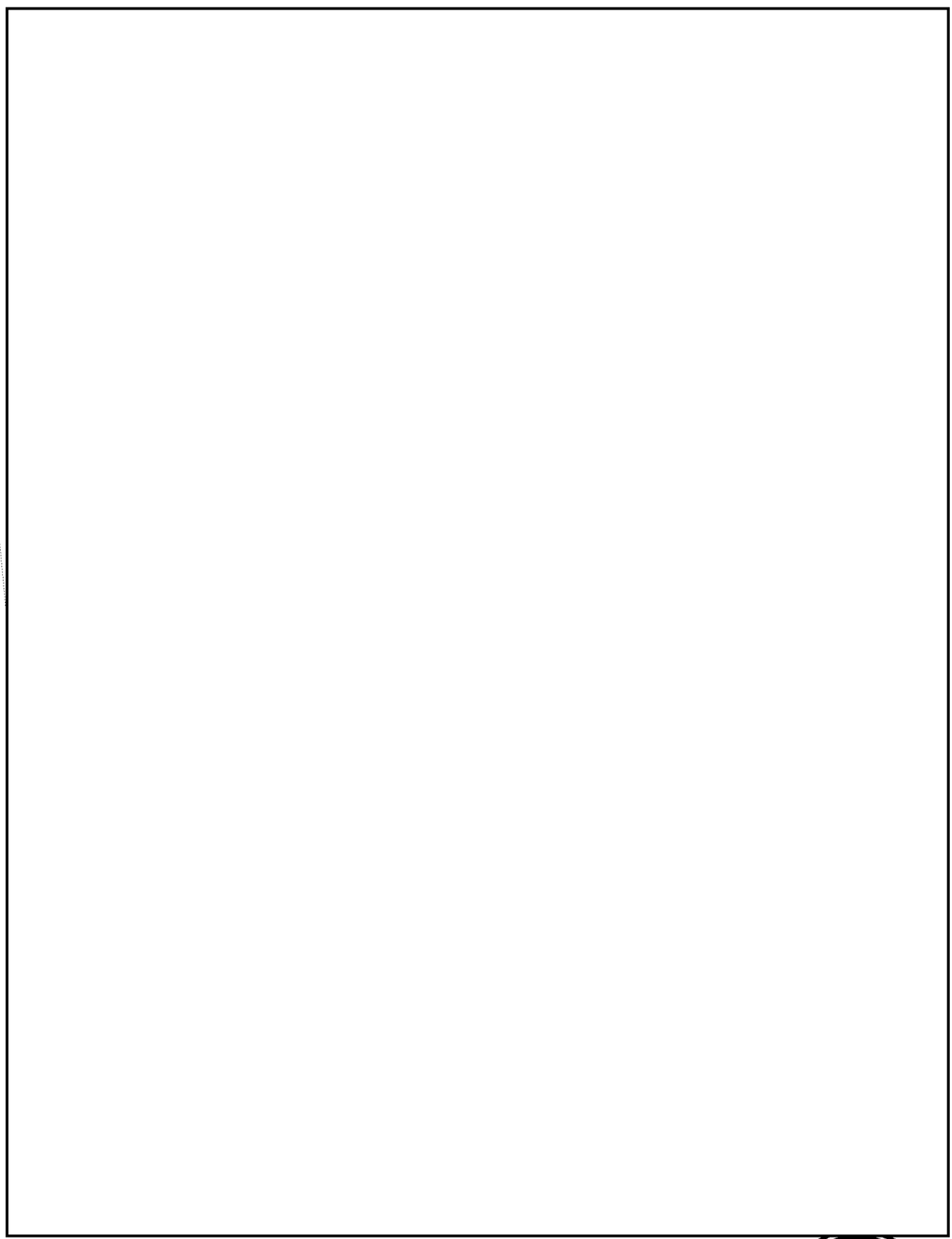
~~TOP SECRET~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIG~~

EIDER

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

No.98

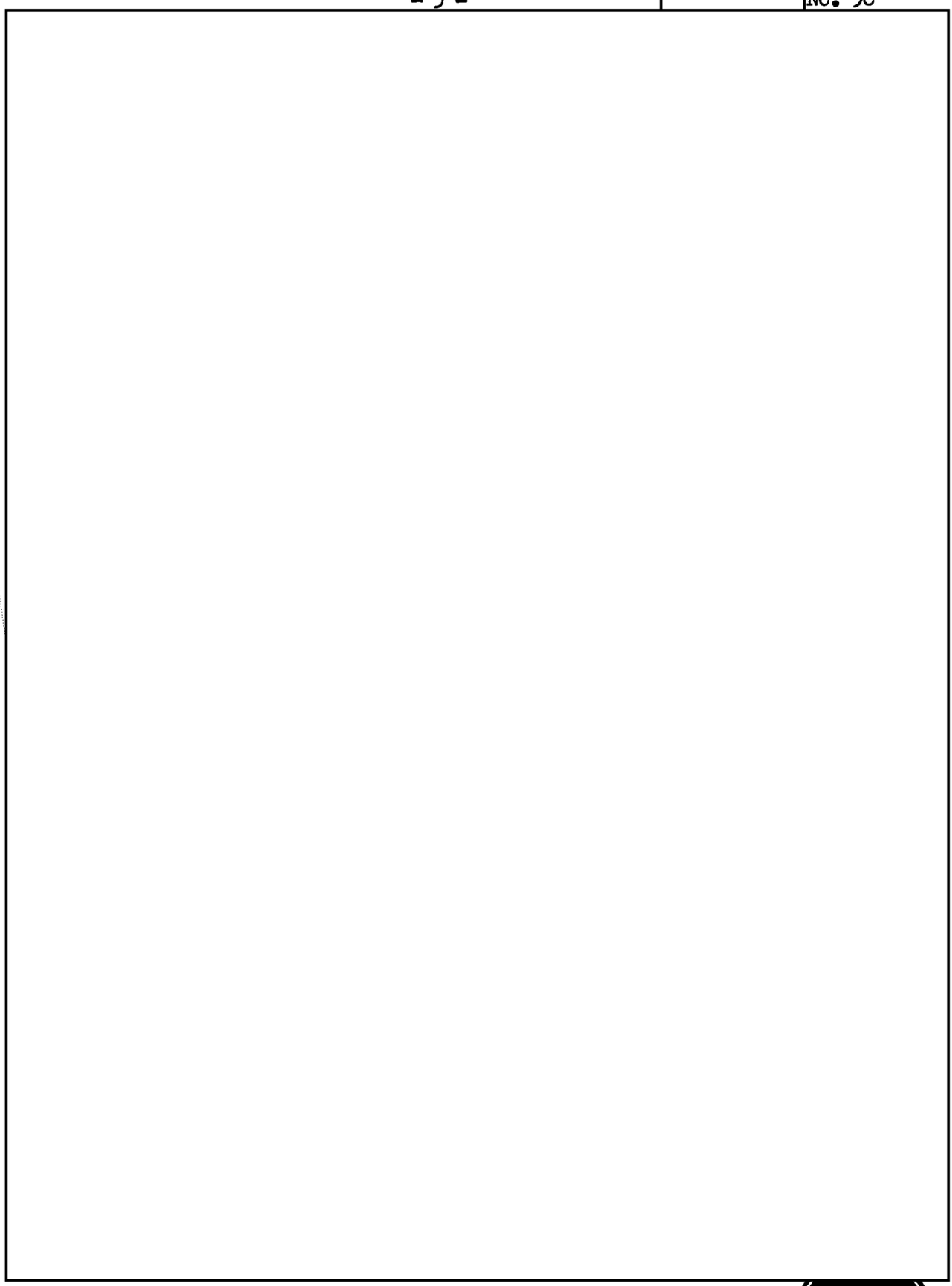


~~TOP SECRET~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIG~~

EIDER

[redacted] No. 98



~~TOP SECRET~~

EIDER

(b) CENTAUR and IXION are adequate for all classifications up to Secret. There is a very small chance of readable depth however (see para.3(c) (i), (ii) and (iii)); if CENTAUR and IXION are used for Top Secret traffic this risk must be accepted by the users.

(c) The procedure should be examined to ensure that there is no danger of depth as a result of 3(d)(v) (B) and (C) above.

NOTE A

Key properties

5. (a) In each stream the probability of cross is

$$\frac{20}{26} \cdot \frac{11}{25} + \frac{6}{26}\left(1 - \frac{14.13}{25.24}\right) = \frac{649}{1,300}$$

(b) Counted characterwise the key is a bit rougher than this, but not seriously so. The calculation is lengthy and only the results are quoted here.

Number of crosses in key character	Number of characters	Probability	$\frac{1}{\text{probability}}$	P.B.
0	1	.0324	30.84	.0378
1	5	.0315	31.75	.0080
2	10	.0311	32.14	-.0042
3	10	.0311	32.15	-.0043
4	5	.0313	31.93	.0022
5	1	.0314	31.85	.0043

(c) All-dot is thus the most popular character. However approximately 86,800 key characters are needed before it can be expected to exceed its expected frequency in random material by 2 standard deviations.

6. Bump rotor stepping

The probabilities have only been calculated for the two extreme cases:

Key	Probability that bump rotor steps
All dot	.490
All cross	.499

A correlation of this order of size has no effect upon the security of the machine. In the case of the other 30 key characters the correlation will be smaller still.

7. Key Sample

The results of a count of 20,000 characters of ASAM 2-1 key are attached. Although the figures are consistent with the theoretical ones the sample size is too small to give a significantly close correlation.

. . . . .	655	 x	632
x	639	x . . . x	640
. x . . .	562	. x . . x	652
x x . . .	668	x x . . x	630
. . x . .	629	. . x . x	590
x . x . .	625	x . x . x	686
. x x . .	636	. x x . x	636
x x x . .	618	x x x . x	614
. . . x .	616	. . . x x	582
x . . x .	607	x . . x x	599
. x . x .	592	. x . x x	604
x x . x .	643	x x . x x	684
. . x x .	622	. . x x x	600
x . x x .	598	x . x x x	640
. x x x .	577	. x x x x	685
x x x x .	590	x x x x x	649
			20,000

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