	Name of equipt.	Nat.	Function	Digit Speed or Bandwidth	Crypto Principle	Approx. Size	Approx. Wt.	Development or Production Status	Type of FAX	Estimated Cost	Ref.	Remarks
1.	AFSAX 500	U.S.	Fixed plant CIFAX.	1000 bauds	Special Electronic Keyer	Five 7' x 22" bays	5000 lbs	In production	Black/ White only.	$75,000	32	Equipment can be used to encypher Teletype multi-channel equipments AN/FGC-5 or AN/FGC-14.
2.	Mountebank	Br.	Fixed plant or shipborne CIFAX	1000 bauds	Double Tutte	Two 6' bays	600 lbs	Development models under test	Black/ White only	-	69	Final models will operate at 1750 bauds.
3.	AFSAX D503	U.S.	Variable Speed General purpose system for field use	500 to 12,000 bauds	59 stage Koken	20" x 30" x 60"	475 lbs	Lab. models on test	Black/ White only	-	33	Wire or VHF radio
4.	AFSAX D505	U.S.	Fixed Plant Broadcast	1000 bauds	37 stage Koken	Transmitter two 5' bays Receiver One 4' bay	Tx 600/700 lbs Rx 300 lbs	Engineering models in late 54	Black/ White only	-	34	Long range Wire or H.F. radio system. Receivers may be shipborne
5.	AFSAX D7308	U.S.	Half tone adaptor for AFSAX D503	-	-	3 drawers	100 lbs	Research only	Half tone	-	36	A 2⁸ level quantiser for Half tone pictures. Definition not yet determined.

~~TOP SECRET~~

OFF LINE LITERAL CRYPTO SYSTEMS

LCS(53)/N/R

	Equipt. Name	Nat.	Power	Speed	Input	Output	Crypto Principle	Size	Weight	Development or Production Status	Estimated Cost (see note)	Reference	Remarks
1	AFSAM D.17	U.S.	Manual (Pneumatic)	15/20 w.p.m.	Keyboard	Tape Printer	10 26 pt. permuting rotors	8"x8"x4"	10 lbs.	Final Eng. models by June '54	$150	Page 1	Total load 14 lbs.
2	Portex	Br.	45V Self contained battery	10 w.p.m.	Letter Setting disc	Tape Printer	8 26 pt. permuting rotors	12½"x6½"x7" ancillaries 9"x½"x4"	22 lbs.	Troop trial models available	£150/250	Page 46	Total load ¼ lbs.
3	AFSAM 36	U.S.	Manual	10/15 w.p.m.	Keyboard	Tape Printer	Double Hagelin	10"x10"x6"	18 lbs.	Production now starting on order for 1,500 machines	$360	Page 3	
4	AFSAM D.21	U.S.	Manual	10/15 w.p.m.	Letter Setting disc	Tape Printer	O.T. Key Tape	½"x5½"x½"	5½ lbs.	In service Test	$95	Page 2	
5	ROCKEX	Br.	230V A.C.	50 w.p.m.	5 unit Tape	5 unit Tape or Page	O.T. Key Tape	49"x23"x13"	150 lbs.	Production Completed		Page 52	
6	AFSAM 7	U.S.	28V D.C. 110/220 V with converter	60 w.p.m.	Keyboard	Tape Printer	8 36 pt. permuting rotors	12"x12"x6½"	18¼ lbs.	In production	$1,900	Page 4	ADONIS crypto system Total load 35 lbs.
7	AFSAM 47	U.S.	115V AC/DC or 28V D.C.	60 w.p.m.	Keyboard	Tape Printer	7 26 pt. permuting rotors	11"x10½"x9½"	43 lbs.	Production to start Apr. '54	$3,500	Page 5	
8	AFSAM 47B	U.S.	115V AC/DC	60 w.p.m.	Keyboard	Tape Printer	8 36 pt. permuting rotors	13"x10½"x9½"	50 lbs.	First Eng. model Feb. '54	$3,500	Page 6	ADONIS crypto system
9	SINGLET	Br.	A.C. Supply	60 w.p.m.	Keyboard	Tape Printer	10 36 pt. permuting rotors	2½ cu. ft.	75 lbs.	Dev. Model due Mar. '54	£ ?	Page 50	Check printer on keyboard input. Capable of ADONIS operation
10	PENDRAGON	Br.	A.C. Supply	60 w.p.m.	5 unit Tape	5 unit electrical	10 36 pt. permuting rotors	3 cu. ft.	100 lbs.	Eng. Model due June '54	£ ?	Page 51	Cryptographically Identical to SINGLET
11	TYPEX 2 TYPEX 22 TYPEX 23	Br.	A.C. 230V	45 w.p.m.	Keyboard	Tape Printer	5 26 pt. permuting rotors	3'x2'x15"	160 lbs.	Production Completed		Page 47) Page 48)	Typex 23 is adapted for CCM only
12	CSP 889	U.S.	115V AC/DC. 230V 50 C/S with adaptor	60 w.p.m.	Keyboard	Tape Printer	5+5 26 pt. permuting rotors and 5 10 pt. rotors	15"x19"x12"	97 lbs.	Production Completed	$2,500	Page 7	
13	AFSAM 25 B/C	U.S.	115V AC/DC	60 w.p.m.	Keyboard	Tape Printer	5 26 pt. permuting rotors	15"x19"x12"	97 lbs.	Production Completed	$2,500	Page 8	Also known as CSP 1700

Note: The figures entered in the column labelled Estimated Cost must be regarded as unreliable, as they are based on production runs of differing sizes.

TELETYPE 'ON LINE' CRYPTO SYSTEMS

LCS(53)/N/R

	Equipt. Name	Nat.	Synchronous or Non Synchronous	Electro Mechanical or Electronic	Speed	Input	Crypto Principle	Size	Weight	Development or Production Status	Estimated Cost	Reference	Remarks
1	AFSAM 9	U.S.	Non Synch.	Electro Mech. (E)	60/100 w.p.m.	Teletypewriter Signals	9 36 pt. permuting rotors	15"x16"x7½"	46 lbs. without carrying case	Production starts Sept. '54	$5,000	Page 10	
2	Non Synch. Mercury	Br.	Non Synch.	Electro Mech.	66 w.p.m.	Teletypewriter Signals	6+4 31 pt. double rotor permuting maze	2' x 2' x 3' Console	200 lbs.	Limited numbers only	£850	Page 55	
3	Circuit Mercury	Br.	Synch.	Electro Mech. (E)	66 w.p.m.	Teletypewriter Signals	6+4 31 pt. double rotor permuting maze	Two 2'x2'x3' consoles and 6' bay	500 lbs. total	In use and production	£2,500	Page 58	
4	Minster	Br.	Non Synch.	Electro Mech.	66 w.p.m.	Teletypewriter Signals	6 31 pt. double rotors (A)	28"x19"x16"	135 lbs.	Development complete. None in production.	£ ?	Page 53	
5	Metropole	Br.	Non Synch.	Electro Mech. (E)	66 w.p.m.	Teletypewriter Signals	6 31 pt. double rotor permuting	28"x19"x16"	135 lbs.	Under development	£ ?	Page 54	
6	(AFSAM 15) AFSAZ D.7315	U.S.	Synch.	Electro Mech. (E)	60 or 100 w.p.m.	Teletypewriter Signals Tape only	Uses AFSAM 9 unit with AFSAM 409	2 units 19"x20"x15½" 1 unit 14¼"x9½"x7"	221 lbs.	Service test models due June '54.	$7,500	Page 15	(T)
7	5 UCO	Br.	Synch.	Electro Mech. (E)	66 w.p.m.	Teletypewriter Signals	One time Key Tape (A)	6' bay	450 lbs.	In use and production	£2,500	Page 59	(T)
8	Artichoke	Br.	Synch.	Electronic	Two 66/100 w.p.m. Channels	Teletypewriter Signals	Double Tutte (A)	7' bay	700 lbs.	Engineering models on trial	£4,000	Page 60	(T)
9	Rollick I Philomel	Br.	Non Synch.	Electronic	66 w.p.m.	Teletypewriter Signals	Single Tutte (A)	54"x22"x12"	250 lbs.	Limited numbers in use. Production now switched to Philomel.	£1,200	Page 56	
10	AFSAM D.26	U.S.	Synch.	Electronic	60/100 w.p.m.	Teletypewriter Signals	53 Stage Koken (A)	6' bay	500 lbs.	First engineering models under way	$5,000	Page 20	Anti depth feature used (T)
11	AFSAM D.22	U.S.	Synch.	Electronic	Four 60 w.p.m. channels	AN/FGC.5	53 Stage Koken (A)	2 units each 48"x24"x24"	500 lbs.	Final development models first quarter 1954	$8,000	Page 19	(T)
12	Convertor No. 5	Br.	Synch. or Non Synch.	Electronic	60 w.p.m.	5 UCO. or Teletypewriter Signals	Double Tutte (A)	6' bay	500 lbs.	Development models due late 1953	£2,000	Page 57) Page 61)	
13	Incubator	Br.	Non Synch.	Electronic	66 w.p.m.	Teletypewriter Signals	Cypher Text Auto Key	Say 24" cube	Say 50 lbs.	Breadboard stage only	Say £300	Page 62	
14	(SSM.4) TT/160/FG	U.S.	Synch.	Electronic	60 w.p.m.	Teletypewriter Signals	None. Synchroniser and mixer	19"x18"x12"	130 lbs.	Production completed	$1,200	Page 18	
15	SSM.3	U.S.	Non Synch.	Electronic	60 w.p.m.	Teletypewriter Signals	None. Mixer only	8"x10"x15"	10 lbs. without power supply	Production dropped	$150	Page 17	
16	AFSAZ D.7305	U.S.	Synch.	Electronic	60/100 w.p.m.	Teletypewriter Signals Tape only	None. Message Synchroniser only	1 cu. ft.	20 lbs.	Engineering models April '54	$300	Page 16	
17	AFSAM 44/45	U.S.	Non Synch.	Electro Mech.	60 w.p.m.	44-Tape only 45-Keyboard or tape	One time Key Tape (A)	0.5 cu. ft.	20 lbs.	Development suspended	$500	Pages 13, 14	
18	AFSAM 2-1	U.S.	Non Synch.	Electro Mech.	60 w.p.m.	Teletypewriter Signals	5 26 pt. rotor Additive Key (A)	19"x14"x11"	73½ lbs.	Production completed	$2,000	Page 11	Requires ancillary combining equipment
19	AFSAM 4A (SIGNIN)	U.S.	Non Synch.	Electro Mech.	60 w.p.m.	Self-contained keyboard	8 26 pt. rotor Additive Key (A)	22½"x25½"x17"	252 lbs.	Production completed	$3,000	Page 12	

(E) - Also contains electronics.
(T) - Provides Traffic Flow Security.
(A) - Additive system.

NOTE:- The figures entered in the Column labelled Estimated Cost must be regarded as unreliable, as they are based on production runs of differing sizes.

	Equipt. Name	Nat.	Function	Digit Speed or Bandwidth	Crypto Principle	Approx. Size	Approx. Wt.	Development or Production Status	Estimated Cost	Radio or Wire Line	Ref. Page	Remarks
1	Bangle	Br.	Theatre to Theatre links Pt. to Pt.	5 kc/s	O.T. Key film	Fourteen 6' bays	-	Radio trials due to start Mar. 54	£25,000	both	63	Full duplex. Vocoder System
2	Sorcerer	Br.	Semi Mobile pt. to pt.	3.2 kc/s	double Tutte	Three 6' bays	-	Development not yet complete	-	both	64	Full duplex. ditto.
3	AFSAY D806	U.S.	Semi Mobile pt. to pt.	Nominal 3.0 kc/s	Geared Timing Mechanism	6 units each 26"x17"x33½"	2,300 lbs.	Service trials due to start Feb. 54	$100,000	both	22	Full duplex. ditto. 5 teletype or 1 FAX channel could be used in lieu of speech
4	AFSAY D809	U.S.	Ciphony for Std. Telephone circuits	Nominal 3.0 kc/s	59 stage Koken	2 drawer file cabinet	say 300 lbs.	Research stage only	-	Wire	24	Push to talk. ditto.
5	Trumpeter	Br.	Tactical ciphony	25 kc/s	Cipher text autokey	20" x 16" x 14"	-	Research stage only	-	VHF radio	66	Push to talk Simplex.
6	AFSAY D804	U.S.	Low echelon Jeep born	25 kc/s	Cipher text autokey	1 cu. ft.	35 lbs.	Engineering models due mid 54	$3,500	VHF radio	30	Push to talk Simplex.
7	AFSAY D808	U.S.	Airborne ciphony	24 kc/s	37 stage Koken	1 cu. ft.	52 lbs.	Engineering models demonstrated. Service test models due end 54	$5,000	VHF radio	26	Push to talk Simplex. Incorporates automatic indicator and set up feature.
8	Hallmark II	Br.	Low echelon Tactical ciphony	33 kc/s	Plain text autokey	3 units each 20" x 16" x 14"	300 lbs.	Engineering models now available	say £2,500	VHF radio or 5 miles of quad. cable	67	Push to talk or duplex with two keyers in tandem if required for extra security.
9	AFSAY D801	U.S.	Special network telephone	50 kc/s	Cipher text autokey	30" x 10" x 24"	300 lbs.	Early development	-	Special wire lines	29	Push to talk Simplex. Probable use short range due to line restrictions.
10	Pickwick	Br.	Special network telephone	15 kc/s	Plain text autokey	6' bay	400 lbs.	Development models on trial	-	U.K. Music circuits	68	Full duplex. Contains 4 level transmission systems reducing speed to 7,500 bauds.
11	AFSAY D810	U.S.	Medium echelon special wire lines	4-20 kc/s	Cipher text autokey	Equivalent of one 6' bay	250 lbs.	Research only. Lab. models.	-	both	27	Intended to fit into the 4-20 kc/s portion of the carrier spectrum.
12	AFSAY D830	U.S.	Airborne Privacy equipt.	5 kc/s	Repeating time permutation in frame of 18	21" x 11" x 8"	35 lbs.	Development to be concluded early 54	$8,000	VHF radio	31	Production not contemplated. Not considered secure.
13	D70	Br.	12 channel microwave radio relay	420 Kilobauds	Tutte	Two 6' bays	-	Two engineering models nearly complete	-	Microwave D70 radio	65	24 teletype channels can be substituted for one telephone channel.
14	AFSAY 816	U.S.	8 channel microwave radio relay	320 Kilobauds	Plain text autokey	Total equipt. incl: reserve keyers 9 bays	2,250 lbs.	In use	-	Microwave radio	28	No production contemplated.
15	AFSAY D807	U.S.	24 or 48 channel Microwave radio relay	2,304 Megabauds	Plain text autokey	7 bays	1,700 lbs.	Service test models due 1955	-	Microwave radio	25	

Copy no. 6.

~~TOP SECRET - SECURITY INFORMATION~~

SECTION A. U. S. COMMUNICATION SECURITY EQUIPMENTS

PART I. LITERAL CIPHER MACHINES

1. Machines Requiring No External Source of Power

a. AFSAM D17

A small keyboard-operated, tape-printing literal cipher machine designed for use where electrical power is not available. Operates pneumatically at approximately 15 to 20 words per minute, all power being supplied by the depression of the keyboard keys. Crypto-unit is a reciprocal permuting maze consisting of ten 26-point rotors and a reflector. Eight of the rotors step in a single interrupted "CCM" cascade. Two of the rotors and the reflector are settable, but do not step. All rotors are identically "wired" and their order in the maze is not changed. All rotors have rotatable alphabet rings and seven of the stepping rotors have settable pin-pattern rings for motion control.

Size and Weight: 8" x 8" x 4"; 10 lbs.

Development Status: The first engineering model developed by a commercial contractor has been completed and will be delivered to NSA by 1 Sept. 1953.

b. AFSAM D21

The AFSAM D21 is a manually operated, tape-printing, literal cipher device using a five level one-time key tape. It is intended to replace one-time pads in some limited applications. The case, printing mechanism, and the bar drum of the M-209 are used; the key wheels are replaced by a tape reader. Operating speed is the same as the M-209.

Size and Weight: $7\frac{1}{4}$" x $5\frac{1}{2}$" x $3\frac{1}{2}$"; $5\frac{1}{2}$ lbs.

Development Status: Fifteen engineering models have been constructed. They are now undergoing service tests.

c. AFSAM 36

An interim keyboard operated, tape-printing, literal cipher machine for use where electrical power is not available. Operates mechanically at approximately 10 to 15 words per minute. Crypto-unit consists of twelve key-wheels and associated bar drum (Hagelin mechanism).

Size and Weight: 10" x 10" x 6"; 18lbs.

Production Status: 1500 models scheduled for delivery by end of December, 1953.

2. Power Driven Machines

a. AFSAM 7

A keyboard-operated, tape-printing cipher machine which encrypts literal text and numerals. Operates at speeds up to 60 words per minute. Crypto-unit consists of an eight-rotor non-reciprocal permuting maze. Rotors have 36 points and are provided with rotatable and interchangeable alphabet and notch rings. Ten points on one endplate are wired to ten points on the other. All major components are constructed as conveniently demountable sub-assemblies. Operates from 115/230 v AC or 28 v DC.

Size and Weight (Less carrying case and rotors): 12" x 12" x 6½"; 18¼ lbs.

Production Status: First models incorporating all major modifications required as a result of service test evaluations are scheduled for delivery from the production contractor in Sept. 1953. Development of an improved model of this equipment (AFSAM D7A) is underway. Major components which will be redesigned include the keyboard, base contacts, stepping unit, rotors and letters/figures shift circuit.

~~TOP SECRET - SECURITY INFORMATION~~

b. AFSAM 47

A keyboard-operated, tape-printing cipher machine which encrypts literal text, numerals and eight punctuation marks. Operates at speeds up to 60 words per minute. Crypto-unit consists of a seven-rotor non-reciprocal permuting maze and a set of adaptor plugs to provide the required rotor motion control circuits. Rotors are 26-point, with rotatable and interchangeable alphabet and notch rings. Has provision for semi-automatic tape reader operation from associated equipment. Operates from 115 v AC, 115 v DC, or 28 v DC with a change of the motor unit.

Size and Weight: 11" x 10½" x 9½"; 43 lbs.

Development Status: Development is essentially completed. Production models scheduled for delivery in April 1954.

c. AFSAM 47B

A modified version of the AFSAM 47 for ADONIS-POLLUX operation. Operates from 115 v AC and provides 280 volts through the rotor maze by means of a voltage doubler.

Size and Weight (approximate): 13" x 10½" x 9½"; 50/60 lbs.

Development Status: Breadboard model has been constructed by the contractor and is undergoing tests. First engineering model scheduled for completion by February 1954.

d. CSP 888/889

An electromechanical, keyboard-operated, tape-printing cipher machine used for off-line literal encipherment. The crypto-unit, for HERCULES operation, consists of three rotor mazes; 1. the alphabet maze, a 26-point five-rotor maze for encipherment; 2. the control maze, a 26-point five-rotor maze for motion control of the alphabet maze; and 3. the index maze, a 10-point five-rotor maze used to transpose the output of the control maze. With appropriate adapter may also be used for LUCIFER.

Size and Weight: 14 3/4" x 19" x 12¼"; 97 lbs.

Production Status: In use.

e. AFSAM 25B/C

An electromechanical, keyboard-operated, tape-printing cipher machine used for off-line literal encipherment. The crypto-unit consists of a 26-point five-rotor non-reciprocal permuting maze.

Size and Weight: 14 3/4" x 19" x 12¼"; 97 lbs.

Production Status: In use.

f. AFSAZ 7301

This special mechanism may be used with CSP 889, AFSAM 25B/C, or AFSAM 47. The principal function is automatic decipherment of cipher tapes. No modification of the cipher machines or operating instructions is required. May be used for enciphering, but only if very strict procedures are observed.

Size and Weight (packed for shipping):
20 3/8" x 14 1/8" x 15 3/4"; 59½ lbs.

Production Status: In use at major stations.

PART II. TELEPRINTER SECURITY EQUIPMENTS

3. Non-Synchronous with Electro-Mechanical Crypto-Components

a. AFSAM 9

A non-synchronous teletype security equipment designed for forward area use. Accepts 32 characters from remote teleprinters. Crypto-unit (AFSAM 109/209) is a non-reciprocal permuting maze with nine 36-point rotors. Uses 5-32-5 crystal diode translators. Rotors are identical with those used in the AFSAM 7. May also be used with AFSAM 309 tape reader in lieu of rotor maze for O.T. Key; provided with tape slitter and torn tape interlock.

Size and Weight: 15" x 16" x 7½"; 46 lbs.

Development Status: Released for production 1 April 1953. First production models expected by Sept. 1954. Development continuing on some modifications to prevent spurious plain-text radiations.

Radiation: In its present form equipment is inherently insecure due to spurious radiation of plain-text. Development is continuing on some modifications to prevent plain-text radiations.

b. ASAM 2-1

A modification of converter M-228 (SIGCUM). A five-rotor maze produces five levels of key which is added baud by baud to the plain text output of a teletypewriter or transmitter distributor. Eight different motion control plans, governed by multiswitches, provide eight different keys for each arrangement. Key is used on a one-time basis. Cryptoperiod is twelve hours. There is a variety of operating procedures including simplex use.

Size and Weight: 18 7/8" x 14 1/4" x 11 1/8"; 73½ lbs.

Production Status: In use.

Radiation: Equipment is inherently insecure due to radiation of plain text signals from associated equipment. If adapted for electronic keying it is considered that it would probably be secure.

c. AFSAM 4A (SIGNIN)

A combined teletypewriter and cipher machine. An eight-rotor maze produces five levels of key which are added baud by baud to the plaintext to accomplish encryption. May be operated on-line or off-line. Unit is mounted in a specially designed three-combination safe. For PANDORA operation, impulses travel through maze from left to right to produce five elements of key simultaneously. Rotor 1 is fast and controls Rotor 2; Rotor 2 controls Rotor 3; Rotor 3 controls Rotor 4; a mixed-wired stator is located between Rotors 4 and 5; Rotor 5 is fast; Rotor 6 is controlled by Rotor 7; Rotor 7 is controlled by Rotor 8; Rotor 8 is fast. For BALDER operation, impulses travel through maze from right to left and are reflected back to the right end-plate to produce the five levels of key. Rotors 1, 2, 3, 4, 6, 7, and 8 move as in PANDORA; Rotor 5 is a "bump" rotor, controlled from one of the end-plate contact positions; a mixed-wired stator is located between Rotors 4 and 5.

Size and Weight: $22\frac{1}{2}$" x 25 3/8" x 17"; 252 lbs.

Production Status: Approximately 450 machines have been produced.

Radiation: Extent of spurious radiations from this equipment has not been determined.

d. AFSAM 44

A one-time tape teletype security equipment designed to transmit on-line and receive off-line. Tape operated only. Has two sensing heads, one for the message tape and one for the key tape. Very rugged and compact. Operates from 115 volts A.C. or 28 volts D.C. power.

Size and Weight (approximate): 0.5 cu. ft.; 20 lbs.

Development Status: Final engineering model being redesigned by contractor to incorporate certain changes, including a Torn-tape interlock and Tape slitter, requested as a result of NSA and Service evaluation of a previous model. No production currently planned.

Radiation: No radiation inherent in the AFSAM 44; dependent on terminal equipment used.

e. AFSAM 45

A one-time tape teletype security equipment designed for use with a printer or transmitter - distributor. Has one sensing head (for key tape) and one selector mechanism; operates at speeds up to one-hundred words per minute. Very rugged and compact. Operates from 115 volts A.C. or 28 volts D.C. power.

Size and Weight (approximate): 0.5 cu. ft.; 20 lbs.

Development Status: Final engineering model being redesigned by contractor to incorporate certain changes, including a Torn-Tape interlock and tape slitter, requested as a result of NSA and Service evaluation of a previous model. No production currently planned.

Radiation: Same as AFSAM 44.

5. Synchronous With Electro-Mechanical Crypto-Components

a. AFSAZ D7315 (formerly AFSAM 15)

A single channel synchronous equipment designed for 24-hour operation at speeds of 60 - 100 words per minute. Traffic is accepted from a tape reader only (32 characters). Traffic flow security is provided by automatic insertion of random text between messages. This is supressed at the receiving terminal. Automatic message numbering is included in the equipment. Normal operation is the IRIS crypto principle i.e. with an AFSAM 9 and AFSAM 409 rotor stepping unit (minimum cycle 36^4). It may also be used on AENEAS crypto principle i.e. with AFSAM 9 and AFSAM 309 one time tape unit.

Size and Weight: Two units each 19" x 20" x $15\frac{1}{2}$", one unit $14\frac{1}{4}$" x $9\frac{1}{2}$" x 7"; total weight 221 lbs.

Development Status: Development has been completed. Eighteen service test models are being constructed and are scheduled for delivery in June 1954.

Radiation: Same as AFSAM 9.

b. AFSAZ D7305

A short term message synchronizer for use with the AFSAM 9 and similar teletype security equipments. Will maintain synchrony during transmission fades up to 10 seconds duration. Designed for use at the receive terminal only and requires a constant speed transmitted signal.

Size and Weight (estimated): 1 cu. ft.; 20 lbs.

Development Status: First engineering model developed under contract scheduled for delivery by April 1954.

Radiation: Not applicable.

SSM 3

A non-synchronous teletypewriter mixer designed for operation on wire circuits for either on-line or off-line operation. For full duplex on-line operation two units are required at each end of a full duplex circuit. For half-duplex non-reversible on-line or off-line operation one terminal at each end of a half duplex circuit is needed. Operates from 115 volts A.C. A source of 110 V D.C. power is required for line current. Developed by the U.S. Air Force Security Service. Works with the ASAM 2-1, AFSAM-9 and One-time tape.

Size and Weight (estimated): 8" x 10" x 15"; 10 lbs.

Production Status: Production models in use; no further procurement planned by USAF in view of contracts let for the SSM-33, (two SSM-3's on one chassis).

Radiation: The equipment causes some radiation and at present it is assumed that security is compromised. Remedial measures are being taken to eliminate security hazards.

Addendum to page 17

~~TOP SECRET - SECURITY INFORMATION~~

SSM 33

A non-synchronous teletypewriter mixer designed for full duplex operation on wire circuits for either on-line or off-line operation. Essentially this equipment consists of two SSM-3's on one chassis with power supply.

Size and Weight (estimated): 9" x 20" x 13"; 30 lbs.

Production Status: Contract let for 500 units.

Radiation: Consideration has been given in specifications to reduce radiation. Tests will be performed on first production models when received approximately February 1954.

d. SSM 4 (SAMSON)

Full duplex synchronizing apparatus designed for use with the ASAM 2-1, AFSAM 9 and similar teletype security equipments. Uses a tuning fork as a frequency standard and will maintain synchrony during transmission fades up to approximately 30 minutes duration. Developed by U. S. Air Force Security Service.

Size and Weight (approximate): 19" x 18" x 12"; 130 lbs.

Production Status: Now in production and use.

Radiation: Same as SSM 3.

6. Synchronous with Electronic Crypto-Components

a. AFSAM D22

Electronic key generator designed for use with the AN/FGC-5 Electronic Multiplex Equipment. Enciphers the output of the AN/FGC-5, which accepts 32 characters from remote teleprinters. Capable of two, three or four channel operation. Provides traffic flow security. Crypto-unit, which has been recently changed, supplies an additive binary key derived from a 53-stage Koken and associated combining circuits. Crypto-period set-up will be made from a Remington Rand (or possibly IBM) card.

Size and Weight 2 units, each 4' x 2' x 2'; total weight 500 lbs.

Development Status: Development model has been completed and tested. An 18-month contract was awarded in May 1953, for the completion of a design approval model by February 1954, and pre-production model by November 1954.

Radiation: Extent of radiation has not been determined.

b. AFSAM D26

Single channel synchronous equipment; accepts 31 characters (excluding blanks) from remote teleprinter. Operates at 60 or 100 words per minute and provides traffic flow security. Crypto-component supplies an additive binary key derived from a 53 stage Koken and associated combining circuits and includes means to prevent the reading of messages in depth. Crypto-period set-up will be made from a Remington Rand (or possibly an IBM) card.

Size and Weight: One 6' x 19" rack.

Development Status: One engineering model of the transmit terminal is almost complete and construction of the receive terminal is underway locally.

Radiation: Extent of radiation has not been determined.

c. AFSAM D37

A proposed security equipment for broadcast teletype service which will include a crypto-component and synchronizing and transmission circuitry necessary for the output of any standard teletype device. A single transmitter will broadcast to a number of receive-only units. Means will be provided whereby receivers can be semi-automatically phased in to decipher the transmitted signals in case crypto-synchronism is lost or the receiver has started late. Crypto-components will be similar to the crypto-component of the AFSAM D26.

Size and Weight (estimated): Transmitter - one 6' x 19" rack. Receiver - one 4' x 19" rack.

Development Status: Project in the initial design stage; breadboard construction will start within a year.

Radiation: Unknown.

PART III. SPEECH SECURITY EQUIPMENTS

8. Vocoder Systems

a. AFSAY D806

Single channel full duplex speech security system for use over land line or long distance HF radio. Requires one 3 kc transmission channel. Alternatively it can provide five teletype channels or one facsimile channel. Uses a 9-channel vocoder (8 spectrum and 1 pitch); quantizes the speech into 8 levels and the pitch into 64 levels. 20 millisecond sampling in each channel. The 500 PAM pulses are time multiplexed and coded by an 8-level binary coder resulting in 1500 bauds per second. Crypto-component is the geared timing mechanism. A "Key Selector" (formerly "Station Selector") switch provides one of four different key streams for net operation. Tube complement approximately 650.

Size and Weight: 6 units, each 26" x 17" x 33½"; total weight, 2300 lbs.

Development Status: Three terminals from previous contractor on hand. First engineering model of the improved version was delivered in August 1953. Remaining six engineering models will be delivered by November 1953. Four of the engineering models will undergo wire line tests by the Services for six months starting January 1954. Two of the three models on hand from the previous contractor will be radio tested by a contractor on a link between Hawaii and Long Island.

~~TOP SECRET - SECURITY INFORMATION~~

b. AFSAZ D7300

One way regenerative repeater for the AFSAY D806.

Size and Weight: 2 units, each 26" x 17" x 33½"; total weight 760 lbs.

Development Status: Contract was awarded in April 1953, calling for the delivery of four engineering models by July 1954.

c. AFSAY D809

Single channel push-to-talk speech security system for general use over wire lines. Currently it is thought that a 16 channel vocoder (14 spectrum and 2 pitch) will be used. Baud rate: 1650 bits per second. Crypto-component will be a 59 stage Koken device with automatic indicator for each message. Tube complement: approximately 450 transistors and 1500 diodes drawing approximately 5 watts.

Size (estimated): Two-drawer file cabinet.

Development Status: An anticipated contract calls for 6 fully transistorized engineering models to be delivered in 2 years from the award date for testing.

9. Pulse Code Modulation Systems

a. AFSAY D807

Forty-eight channel, full duplex, microwave radio relay speech security equipment employing 8 kc sampling and 64 level PCM description. Total baud rate: 2.304 megacycles. Crypto-component is a keyer similar to that used in the AFSAY 816. A proposed modification would reduce the equipment to 24 secure voice channels, full duplex, giving 100% spare in the AN/TCC-15 (multiplex set) and 33% spare in the AN/TSA-5 (keyer) while providing 100% check on the key. Baud rate of the modification would be 1.15 mc.

Size and Weight (estimated): 7 bays; 1700 lbs.

Development Status: A contract for the AN/TSA-5 was awarded in November 1952. Two of the equipments will be delivered to NSA for tests. A contract was awarded in February 1953 for development models of the AN/TCC-15 to be delivered in June 1953.

b. AFSAY D808

A low echelon push-to-talk airborne speech security equipment employing 6 kc sampling and 16 level PCM description. Crypto-component is a 37-stage Koken keyer with automatic message indicator. Tube complement: 449 sub-miniature.

Size and Weight: PCM and crypto-unit 10½" x 8" x 23"; code changer 8" x 10" x 4"; control box 5¼" x 7" x 3 3/4"; Total weight 52.1 lbs.

Development Status: Four design approval models have been built and have undergone preliminary flight tests. Six additional units are to be delivered by December 1953. A new 18-month contract was awarded in June 1953 calling for the construction of 10 engineering models with emphasis placed on improving transmission reliability.

~~TOP SECRET - SECURITY INFORMATION~~

c. AFSAY D810

Single channel speech security equipments. Transmission bandwidth requires a normal 4-channel wire and/or radio facility such as spiral-4 cables and/or AN/TRC-1, 8, 24, 31 and AN/GRC-10. Speech Sampling occurs at 3.5 kilocycle rate followed by 16-level Pulse coding. The 4-digit pulse code occurring at 14000 bits per second is converted to a 2-digit quaternary code occurring at 7000 pulses per second. These are used to modulate a 14 kilo cycle carrier with the output bandwidth limited to the range 4.20 kc. by a gaussian output filter. Crypto-component will be a delay line keyer similar to that used in the AFSAY D801.

Size and Weight (estimated): 1 standard 19" rack: 250 lbs.

Development Status: Coles Signal Laboratories has a bread-board model of the PCM and transmission circuitry. An anticipated contract (controlled by Signal Corps) calls for experimental models to be delivered one year after the award date. NSA will provide contract liaison on keyer portions of the equipment.

d. AFSAY 816

Eight channel full duplex microwave radio relay speech security equipment employing 8 kc sampling and 32 level PCM description. Total baud rate is 320 kc. The crypto-component using auto-key techniques supplies an additive binary key derived from irregularly stepping electronic rings. Tube complement approximately 600.

Size and Weight: 9 bays; 2,250 lbs, includes 100% standby equipment.

Development Status: Two terminals using laboratory models have been in operation 8 hours a day with 2% outage. Plans to construct two additional laboratory models have been dropped.

10. Delta Modulation Systems

a. AFSAY D801

Single channel self-synchronous push-to-talk speech security equipment for use as an intercommunication system over short wire links of excellent frequency response. Employs delta modulation coder operating at 50 kc. Low level noise is added to the speech input. Crypto-component is a cipher text auto-keyer using three shift registers in tandem.

Size and Weight: Purchase description requires that equipment be "of desk height (approximately thirty and one-half ($30\frac{1}{2}$ inches), no wider than ten (10) inches, and less than twenty-four (24) inches in depth"; "weight of the equipment shall be the minimum practicable, and in no event shall exceed three hundred (300) pounds".

Development Status: An 18-month contract was awarded in April 1953, calling for the delivery of a maximum of 8 final models in the latter part of 1954. No other construction is planned.

b. AFSAY D804

A low echelon, single channel, self-synchronous, push-to-talk speech security equipment. Speech is sampled at a 25 kc rate and converted to a binary signal by a delta modulation process. Crypto-component is a cipher text auto-keyer employing a 40 baud shift register. Tube complement: approximately 90 miniature.

Size and Weight: 1 cubic foot; 35 lbs.

Development Status: Two laboratory models of the AFSAY D804 (X-1), (40 baud delay line, no alarms) were constructed locally and shipped to the contractor who will construct a maximum of eight AFSAY D804 (X-3) models, (40 baud delay line, no alarms, 24 volt vehicular operation, 60 tubes). These will be delivered by June 1954. A contractor has delivered four models of the AFSAY D804 (X-2) (40 baud delay line with option of two random walk rings, no alarms). One laboratory model of the AFSAY D804 (X-4) has been constructed and shipped to the contractor. The (X-4) model has lumped constant delay lines, two random walk rings and alarms. The contractor will build six engineering models with delivery scheduled for November 1953. Future production plans will depend upon Service reception of the equipment.

11. Non-digital Systems

a. AFSAY 830

Single channel, push-to-talk airborne speech privacy equipment. The speech signal is limited to the 480-2200 cps band, amplitude sampled 5,040 times per second, stored and permuted within a frame of 12. A second model provides a permutation within a frame of 18.

Size and Weight (12-element model): 21" x 10½" x 8"; 35 lbs.

Development Status: Expected delivery date of the 18-element models has been changed to late 1953. NSA will receive two models for analysis.

PART IV. FACSIMILE SECURITY EQUIPMENTS

12.

a. AFSAJ 700 (formerly AFSAX 500)

An electronic key generator originally designed for the encryption of facsimile transmissions with AN/UXC-2 from fixed plant and shipboard installations. Alternatively the AFSAJ 700 may be used in conjunction with the ancillary equipment AN/FGC-5 to encipher up to four standard teletype channels or with the ancillary equipment AN/FGC-14 to encipher up to eight standard teletype channels. Operates at 1000 bauds per second. Crypto-component supplies an additive binary key derived from a key generator containing eight electronic keyer rings.

Size and Weight (estimated): 3 bays; total weight 2500 lbs.

Development Status: Eighteen models of the key generator have been completed. They will shortly undergo service tests on a Washington, D.C. - San Francisco link. A test terminal will require three key generators as follows: one keyer for transmission, one keyer to check the transmit keyer and one keyer for reception, on each of the three equipments AN/UXC-2, AN/FGC-5 and AN/FGC-14. Current contract provides for delivery of total of 102 equipments for US use by end of 1954 at rate of eight a month.

b. AFSAX D503

A facsimile security equipment designed for the encryption and transmission of black and white copy over land-line and VHF radio links. Together with ancillary transmission equipment, the AFSAX D503 will provide secure facsimile communications over HF radio. Operates at rates between 500 and 12,000 bauds per second. Crypto-component supplies an additive binary key from a 59 stage Koken equipped with automatic message indicator. The key failure alarm has been changed to increase its effectiveness. Check is made for failure of either partial key, A1 and B4 outputs (see Figure 1, BRUSA C/S 203), failure of special point deletion, B6, or failure of the final key addition, A2. Failure of partial key is checked by requiring at least two changes within a frame of 64 elements. Failure of special point deletion or final key addition or both is checked by circuits similar to the Cipher Failure alarm. Included also are an alarm and gate to insure that the output is removed in the event of an alarm.

Size and Weight: 20" x 30" x 60"; 475 lbs.

Development Status: Two laboratory models are currently in use by a non-Service organization. Two design approval models are ready for evaluation at the contractor's site. Six additional engineering models are expected by October 1953. Sub-miniature requirement has been deleted.

c. AFSAX D505

A facsimile security equipment designed for the encryption and transmission of black and white copy over long distance wire lines or HF radio. A single fixed plant cifax transmitter (AFSAX D505/1) will broadcast to a number of cifax receivers (AFSAX D505/2). The AFSAX D505/1 consists of three independent crypto-components with automatic alarms and three cipher combining circuits. Automatic switchout of defective contribution is accomplished without loss of transmission. The AFSAX D505/2 consists of one crypto-component and simple alarm circuitry. Baud rate is approximately 1000 bits per second. Crypto-component supplies an additive binary key from a 37 stage Koken device.

Size and Weight (estimated): AFSAX D505/1 - two 5 foot racks; AFSAX D505/2 - one 4 foot rack.

Development Status: Request for bids has been issued. Initial contract calls for one engineering model of the AFSAX D505/1 and two engineering models of the AFSAX D505/2. It is anticipated that a second contract will be awarded in 1955 calling for pre-production models which will undergo service tests.

~~TOP SECRET - SECURITY INFORMATION~~

d. AFSAZ D7306

Cifax wire transceiver equipment being developed to transmit 1650 bits per second over any toll line. Project is being engineered locally from Bell Telephone Laboratories' (Mr. A. C. Norwine) experimental circuitry. Engineering models being constructed have optional transmission rate of 1800 bits per second.

Size and Weight (estimated): 1 drawer; 35 lbs.

Development Status: Original schedule called for engineering models by 1 October 1953, but testing has been delayed because of the inability to obtain common carrier facilities.

e. AFSAZ D7308 - Halftone Cifax Adaptor

A 2^n level quantizer which converts half-tone copy into digital form, the information rate being dependent upon the facsimile speeds and the degree of coding necessary to sufficiently describe representative copy. Equipment will be used with the AFSAX D503 security equipment and the AFSAZ D7300 transmission equipment.

Size and Weight (estimated): 3 drawers: 100 lbs.

Development Status: Preliminary evaluation of applied research to determine the amount of information required to sufficiently describe representative copy is expected by 1 October 1953. Two laboratory models will be available for Service evaluation by 1 January 1954. After final evaluation of copy requirements and laboratory equipments, a contract will be awarded for prototype models.

14. One-time Tape Production Equipments

a. AFSAW 7200

This equipment consists of a random key generator, associated electronic circuits and five tape punches. Each punch unit punches 2 identical tapes. Each punch will operate randomly with respect to each of the other punches or 2 to 5 punches may punch identical tapes. Operating speed is 900 characters per minute.

Size and Weight: 4' x 3' x $3\frac{1}{2}$'; 750 lbs.

Production Status: A number of these machines are currently in use producing one time key-tapes.

b. AFSAW D7224

This equipment consists of a random key generator and associated electronic circuits, a set of 5 punches and tape checking means. Each punch produces 2 identical tapes. Each punch may operate randomly with respect to each of the other punches or 2 to 5 punches may punch identical tapes. The equipment will operate at 3600 characters per minute. The equipment will be used to generate 100,000 character rolls of key tape.

Size and Weight: The size and weight have not been determined; however, they should compare favorably with the AFSAW 7200.

Development Status: Experimental work has been initiated. Development will be accomplished on contract.

15. One-time Key Tape Checking Equipment

a. AFSAW D7213 (DONNA)

A high speed electronic tape checking equipment consisting of three parts: (1) a photelectric tape reader, (2) an electronic decade counting unit and (3) a relay motor control unit. The photoelectric tape reader is designed to accomodate either 10,000 or 100,000 character tapes; three or four tape readers are supplied with each counter unit. The electronic counter discriminates, compares and counts the pulses from the tape reader and gives a visual indication of a good or bad tape together with the actual numerical count. The relay motor control unit selects an available tape reader and controls the speed, stopping and reversing of the motors during a run. Twenty different counts are made on each tape.

Size and Weight: Tape reader: 20" x 15" x 13"; approximately 60 lbs. Counter: two standard 19" cabinet racks 7' high and one 24" cabinet rack 7' high; approximately 1500 lbs.

Production Status: One machine completed and in operation. Five additional machines being constructed.

16. Letter Check Generating Equipment

a. AFSAW 7203 (LEECH)

A relay-operated machine for automatically generating 36-45 letter checks for POLLUX/ADONIS (AFSAM 7) and ATHENA/PYGMALION/IRIS (AFSAM 9/AFSAZ D7315) crypto-systems. In conjunction with associated IBM equipment, the AFSAW 7203 reads previously prepared IBM cards on which key list information, including rotor order, notch and alphabet ring alignments, has been punched; sets up the various crypto-components accordingly with the rotors aligned at "AAA...A", steps them 35 positions in accordance with the applicable rule of motion; and then punches in the original IBM card ten successive encipherments of the letter "L" for POLLUX/ADONIS (or ten successive decipherments of the "LETTERS" character for ATHENA/PYGMALION/IRIS) as the rotors step from position 36 through position 45. The IBM cards are then used for the preparation of printed key lists. Entire operation takes approximately four seconds.

Size (approximate): 150 cu. ft.

Production Status: One locally constructed equipment now in operation.

b. AFSAW D7221 (MOOSE)

A relay operated machine which generates letter check groups for MARS (AFSAM 36) and OLYMPUS (M-209) crypto-systems. The machine transposes the columns of lug settings on a previously prepared master card and punches the transposed columns onto a key list card (IBM type) containing previously prepared pin settings. The lug and pin settings from the key list card are used to generate a letter check which is printed on the same card.

Size and Weight: 7' x 4½' x 5'; approximate 2000 lbs.

Development Status: One locally constructed model is in final testing stage.

Security Status: Not applicable.

BRUSA C/S References:

U. S. Papers: None

U. K. Papers: None.

17. Automatic Rotor Wiring Equipment

a. AFSAW D7215

The automatic rotor wiring equipment consists of three machines related to each other in a manner to permit automatic transfer of the rotor bobbin from one machine to the other during processing. The first machine wires the bobbin in accordance with a particular system, seals the wires in the bobbin and cuts the wires to length. The second machine strips the insulation from the tips of the wires and tins them. The third machine inserts the bobbin in the rotor and solders the wires to the proper lugs.

Size and Weight (estimated): Wiring machine - 11' x 2' x 6'; 1300 lbs. Stripping and tinning machine - 5' x 3' x 4'; 800 lbs. Assembling and soldering machine - 4' x 2' x 4'; 500 lbs.

Development Status: The wiring machine is nearly completed. The stripping and tinning machine is being detailed. The assembling and soldering machine is in the design stage.

PART VI. SPECIAL PURPOSE CRYPTO-EQUIPMENTS

18.

a. AFSAM 499 (Authentication Device)

A small, manually operated, mechanical device for station and message authentication. Consists of two individually rotatable shafts, each carrying 13 mixed alphabet disks and two sleeves. The sleeves form a movable grill with slots for reading the letters on the disks beneath. Provides for a two-letter challenge and a two-letter reply.

Size and Weight: 5½" x 3½" x 1 3/4"; 2½ lbs.

Production Status: Tooling has been completed and most of the components for the initial production run of 2100 models, scheduled for delivery in September 1953, are ready for assembly.

b. AFSAM 498 (Authentication Device)

A small, manually operated, pneumatic device for station and message authentication. Consists of ten 15-point rotors with rotatable alphabet rings, a reversing rotor with points banded in five sets of three each, a single input bellows, and fourteen output bellows. These components are contained in a small metal case. Provides a five letter challenge (set-up on the rotors, which are movable in separate pairs) and a two-letter reply (displayed by the activation of two of the output bellows).

Size and Weight (approximate): $4\frac{1}{2}$" x 3 3/4" x 2"; $1\frac{1}{4}$ lbs.

Development Status: One development model has been constructed locally. Mechanical components and cases for five improved development models are being fabricated locally, and five sets of glass pneumatic rotors are to be supplied by a commercial contractor. After these models have been evaluated, a contract for further development of this device will be negotiated.

c. AFSAM D31 (Weather Cipher Device)

The AFSAM D31 is a manually operated, tape printing, cipher device using a five level one-time key tape, intended for use as a cipher device to encrypt digital weather information. The case and the bar drum of the M-209 are used. The key wheels are replaced by a tape reader. The printing mechanism is modified so that the plain text characters are the ten digits, "X", "/" and "Space". The cipher characters are the 26 letters of the alphabet. Operating speed is the same as the M-209.

Size and Weight: $7\frac{1}{4}$" x $5\frac{1}{2}$" x $3\frac{1}{2}$"; $5\frac{1}{2}$ lbs.

Development Status: One complete machine has been constructed. Two typewheel assemblies have been constructed for conversion of AFSAM D21 to AFSAM D31.

~~TOP SECRET~~

SECTION B. U.K. CRYPTOGRAPHIC EQUIPMENTS

PART I. LITERAL CYPHER MACHINES.

1. Machines requiring no external source of power.

(a) PORTEX.

A small hand operated off-line tape printing cypher machine with an electrical permuting maze designed for low echelon use. Electrical power to operate the maze is derived from a self-contained 45-volt dry battery good for over 100,000 operations. Speed 10 w.p.m. The cryptographic unit consists of an eight 26-point rotor maze with a crossover at the cypher end; the rotors step in two four-rotor cyclometric cascades. Each rotor consists of an insert and a housing; the insert is selected from a set of sixteen and can be fitted in the housing in any one of the twenty-six possible angular positions, the housing is fitted with a rotatable alphabet tyre.

Size of machine: $12\frac{1}{2}$" x $6\frac{1}{2}$" x 7", + accessories 9" x $7\frac{1}{2}$" x 4". Total weight 34 lbs.

Production State: No orders will be placed until after completion of user trials in September 1953. Production would start eighteen months after placing of firm order. Probable order is estimated at 2000 and the cost between £100 and £250 each.

Radiation: No detailed investigation has been made but it is considered to be secure particularly for the purpose in view.

2. Power driven Literal Cypher Machines.

(a) TYPEX 2.

A power driven keyboard operated tape printing cypher machine with a five 26-point rotor reciprocal permuting maze with a pluggable reflector. Rotors consist of a housing with a rotatable notch ring and alphabet tyre into which can be fitted reversible wired inserts selected from a set of fourteen. Only three rotors turn during the encryption of a message. The cryptogram is arranged in groups of five letters, a check printer is provided.

Size and Weight (in transit case): 3' x 2' x 1'3": 160 lbs.

Production State: No more of these machines will be manufactured.

(b) TYPEX 22.

The general purpose U.K. cypher machine; similar to the Typex 2 except that all rotors turn during the encryption of a message and a pluggable crossover is provided at the entry (and exit) to the maze.

Radiation: No detailed investigation has been made but it is considered to be secure.

(c) TYPEX 23.

As for Typex 22 but adapted for C.C.M.

(c) PORTEX IIA.

A keyboard operated motor driven version of the PORTEX I. Operating speed 130 characters per minute.

Status: One development model constructed. Adoption of the machine depends upon policy for the adoption of PORTEX I.

Radiation: No detailed investigation has been made but it is considered to be secure particularly for the purpose in view.

(d) SINGLET

A keyboard operated motor driven tape printing cypher machine having a ten 36-point rotor non-reciprocal permuting maze using re-entry technique with a pluggable crossover at the cypher end. The keyboard will provide for the encryption of the full combined teleprinter alphabet as laid down in ACP 126 plus the punctuation marks, comma, colon, question mark, quote mark. In addition, the letters J and Z will be recovered in the upper case and facilities will be provided for encrypting carriage return and line feed. The cryptogram will consist of letters arranged in groups of five; a check printer will be provided. Inter-operation with AFSAM 7 and PENDRAGON will be possible.

Estimated size and weight: $2\frac{1}{2}$ cu.ft. 75 lbs.

Status: A model to comply with the latest specification (agreed in April 1953) due for demonstration March 1954.

Radiation: Has yet to be investigated.

(e) PENDRAGON

Higher echelon variant of SINGLET. Operates automatically from tape input and designed for use with both one-wire and five-wire page printers and other teleprinter ancillary equipments. Will interwork with SINGLET and AFSAM 7.

Estimated size and weight: 3 cu.ft. 100 lbs.

Status: A model to comply with latest specification (agreed in April 1953) due for demonstration June 1954.

Radiation: Has yet to be investigated.

(f) ROCKEX

An off-line teleprinter cyphering equipment using a six unit one-time key tape. Accepts 31 characters and by means of an electronic stunt suppression unit produces an all-letter cryptogram in five letter groups, ten groups to the line and five lines to a paragraph. A new unencyphered sequential indicator is used at the beginning of each paragraph. Operates at either Creed or Teletype speed. 5-wire and electronic versions have been produced for use where there is a danger of interception of radiated plain text signals.

Status: In use. Out of production.

Radiation: It is considered by the U.K. that the 5-wire (Rockex 4) and the electronic (Rockex 3) versions are secure.
Previous models are inherently insecure and security is compromised by radiation.

PART II. TELEPRINTER SECURITY EQUIPMENTS.

3. Non-Synchronous with Electro-mechanical Crypto-Components.

(a) MINSTER.

Interim equipment for on-line non-synchronous (start-stop) point to point usage over wire circuits. Half-duplex operation. Crypto-component is a rotor maze generating additive key using six 31-point double rotors. Maze steps at alternate encypherments.

Estimated Size and Weight: 2' x 2' x 3' 150 lbs.

Development Status: Development complete. Placing of contracts awaits clarification of user requirements.

Radiation: The equipment is inherently insecure and it must be assumed that security is compromised by radiation. Remedial measures would involve re-design.

(b) METROPOLE.

An on-line non-synchronous (start-stop) cypher machine. Intended for switched wire circuits on a half-duplex basis.

Differs from Minster in that the crypto system would be permuting, but the details have not yet been defined.

Estimated Size and Weight: Approx. same as Minster.

Development Status: 2 laboratory models using six 31 point rotors have been produced.

Radiation: The equipment is inherently insecure and it must be assumed that security is compromised by radiation. Remedial measures would involve re-design.

(c) MERCURY (Non-synchronous).

An on-line non-synchronous (start-stop) cypher machine. For use on switched wire or point-to-point land circuits on a half-duplex basis. Uses similar scrambler to synchronous MERCURY i.e. 31 point double rotors and a rotor controlled message maze motion.

Size and Weight: 2' x 2' x 3' approx 200 lbs.

Status: Used by Air Ministry on land line links between Europe and U.K.

Radiation: The equipment is inherently insecure and it must be assumed that security is compromised by radiation. Remedial measures would involve re-design.

4. Non-Synchronous with Electronic Crypto-Component.

(a) PHILOMEL (modified ROLLICK).

Non-synchronous equipment using subtractor (additive) key derived from an electronic key generator (single TUTTE) employing multi-cold-cathode tubes. Long term (maximum daily) cypher setting is changed by means of plugs and counter settings: a character counter device is fitted to enable operators to regain synchronism on the original key cycle following temporary loss due to line faults and operator errors between plug changes. This new method of resetting replaces the random generator setting. To limit the dangers of insecure radiation the equipment is arranged to be capable of control by electronic-keying methods. Philomel can be remotely controlled from the teleprinter position.

Size and Weight: 4' 6" x 19" x 12" 250 lbs.

Development Status: Contract for 115 equipments placed and due for completion May 1954. The first 50/60 will require retrospective action to incorporate the character counter and electronic keying modifications to change them from Rollick to Philomel.

Radiation: The equipment is inherently insecure in its normal form but can be readily adapted for electronic-keying in which case it is considered that it probably would be secure.

(b) CONVERTOR NO. 5 (See Page 61).

5. Synchronous Equipment with Electro-Mechanical Crypto-Component.

(a) CIRCUIT MERCURY.

Single channel duplex, synchronous equipment operating at rates of 45 or 50 bauds. Accepts 31 characters (excluding blanks) from remote teleprinters. Does not, but could, provide traffic flow security. Crypto-component consists of two rotor mazes, one with six 31-point double rotors for encypherment and the other with four 31-point double rotors for motion control. Uses relay 5/32 translators. Used by the Air Ministry over long-distance radio teleprinter circuits.

Size and Weight: Two 2' x 2' x 3' consoles and one 6' x 19" rack per duplex terminal. Wt. approx. 500 lbs.

Status: In use and in production.

Radiation: The equipment is inherently insecure and it must be assumed that security is compromised by radiation. Remedial measures would involve re-design.

~~TOP SECRET~~

(b) APPARATUS 5 UCO SINGLE CHANNEL NO. 1.

Single channel duplex synchronous equipment using random one-time five unit tape for cypher key. Accepts 31 characters (excluding blank). By using a magnet operated tape reader, facilities for the encryption of all 32 teleprinter characters can be provided. Designed to give traffic flow security but this facility has recently been found to be inadequate and a modification unit is being designed to rectify this deficiency. Equipment is used on long-distance telegraph circuits over radio and wire.

Size: One 6' x 19" double sided rack per duplex terminal. Weight 450 lbs.

Status: In use and in production at rate of six equipments per month. Existing orders will be completed early in 1954.

Radiation: The equipment is inherently insecure and it must be assumed that security is compromised by radiation. Remedial measures would involve re-design.

~~TOP SECRET~~

6. Synchronous Equipments with Electronic Crypto Component.

(a) ARTICHOKE.

Twin channel duplex synchronous system using subtractor (additive) key derived from an electronic key generator (double TUTTE) employing multi-cold-cathode tubes. Accepts 31 characters (excluding blanks) from remote start/stop teleprinter ancillaries or 32 characters from tape. In the twin channel condition each channel transmits at 35/53 bauds for 50/75 baud input. In the twin channel input single channel time division multiplex output condition the input speed per channel is 50/75 bauds and the transmission speed 70/106 bauds. Provides traffic flow security. Basic cypher setting of each key generator is achieved by means of 27 plugs chosen from a set of 80 according to a key list: interim re-sets are effected by a quasi-random setting of the counters and a 64 position cyclometer switch which is advanced one position for each reset. Plugs are changed completely after every 64 resets. To be employed on long distance radio and wire teleprinter circuits.

Size: One 7' x 19" double sided rack per twin channel duplex system. For vehicle installation the equipment can be mounted on one double-sided 5' 3" rack and one single sided 4' x 8" rack. Weight 700 lbs.

Status: Engineering ("A") model demonstrated in 1952. Service trials of manufacturers ("B") models due to commence in October 1953; production at 6 per month due to start July 1954.

Radiation: If adapted for electronic keying it is considered that it would probably be secure.

(b) CONVERTOR No. 5.

Key Tape Eliminator for use with Apparatus 5 UCO. Consists of an electronic key generator (double TUTTE) similar to that used in ARTICHOKE. The setting of the key generator is identical to that in ARTICHOKE except that the quasi-random setting of the counters is replaced by counter setting according to key lists. Synchronous operation is derived from the Apparatus 5 UCO, traffic flow security is provided. The equipment can be converted at a moment's notice for use as a self-contained start/stop on-line teleprinter cypher device

Size: One single sided 6' rack. Wt. 500 lbs.

Status: Three Development models due in November 1953.

Radiation: If adapted for electronic keying it is considered that it would probably be secure.

7. Self-Synchronising (Auto-Key) Equipment.

(a) INCUBATOR (late CHEAPEX).

A start/stop cypher text auto key teleprinter cypher device for half-duplex working. The object of the device is to provide the maximum security at a minimum cost and to this end the error multiplication factor inherent in a self-synchronising system of this type is to be investigated - the delay line from which the cypher key is derived is forty elements long. The error multiplication factor limits the use of the equipment to good quality wire and radio circuits.

Size: Not yet determined.

Status: One breadboard model has been completed and tested on a line comprising 8 V.F. channels in tandem. Magnetic binary circuits are being employed for the delay line and hard valves with some magnetic binaries for the remainder of the equipment. Two models are to be produced for field trials to determine whether the error multiplication factor can be accepted in practice.

Radiation: If adapted for electronic keying it is considered that it would probably be secure.

PART III SPEECH SECURITY EQUIPMENTS.

8. Vocoder Systems.

(a) BANGLE.

Single channel duplex fixed plant speech security system for use over land line/or long distance HF radio. Requires one 5 Kc or two 3 Kc transmission channels. Uses a 12 channel vocoder (10 spectrum and 2 independent pitch channels each quantized into 9 levels). Crypto-component consists of 12 independent random keys furnished on 35 mm. film. Tube complement approximately 2000.

Size and Weight: 14 bays of equipment either fixed plant or in 3 special vehicles.

Status: Land-line trials carried out in U.K. over period March-July 1953. Radio trials scheduled for early 1954. Only four equipments to be completed; size, weight and administrative problems preclude general adoption of this equipment.

Radiation: Has not been investigated but is believed to be secure.

(b) SORCERER

Single channel full duplex/security equipment for use over land lines, short and long haul radio circuits. Uses nine channel vocoder (8 spectrum and 1 pitch). Crypto-component will be Convertor No. 5 supplying additive key.

Status: Two models for demonstration on a back-to-back basis, each consisting of four racks of equipment are due for completion in Autumn 1953. It is expected that the final model will be considerably smaller.

Radiation: Has not been investigated but believed to be secure.

9. Pulse code modulated Systems.

(a) D 70 (Crypto component Blue Boy)

Twelve channel full-duplex microwave relay speech security equipment. Twenty-four teleprinter channels may be furnished by time multiplexing in lieu of one telephone channel. Speech channels are quantized to 32 PCM levels. Each channel is sampled 7000 times per second, resulting in a total rate of 420 kilobauds. Employs an electronic key generator (TUTTE).

Status: Two repackaged development models of the key generator due for completion by end of 1953.

Radiation: Has not been investigated but believed to be secure.

(b) TRUMPETER.

A development project, the ultimate aim is to provide a low echelon airborne or ground push-to-talk speech security equipment. The crypto-component will consist of a cypher text auto-key device. The method of speech coding is not yet decided, but P.C.M. is under consideration.

Status: In the early development stage. A first development model of the key generator employing gas tubes due for completion October 1953.

Radiation: Should be secure.

10. Delta Modulation Systems.

(c) HALLMARK II.

Single channel, self-synchronous push-to-talk speech security equipment. Speech is sampled at 33.3 Kc. rate and is quantized by a delta modulation scheme. Noise is injected in parallel with the speech input. Encypherment is provided by three auto-key stages in cascade. The equipment is primarily designed for use over tactical line-of-sight radio circuits. Alternative methods of operation are possible as follows:-

(1) Line of sight radio: Push to talk with single key generator at each terminal.

(2) Special wire lines (4 wire): Full duplex with separate key generator at each terminal for send and receive.

(3) When additional security is required for line or radio: Full duplex or push to talk with two key generators in series at each terminal for each direction of transmission.

Size and Weight: Delta modulator 20" x 16" x 14". 80 lbs.
Each key generator unit 20" x 16" x 14". 107 lbs.

Production Status: Production prototype models under test. Production of sufficient models to permit full scale troop trials due to start 1955.

Radiation: Has not been investigated but believed to be secure.

(d) PICKWICK

A single channel duplex ciphony system for use on land lines of music (program) circuit quality. It is intended for use on a special switched network. Speech is Delta modulated at a sampling rate of 15,000 per second. Encypherment is by means of plain text auto-key consisting of four 32-point rings. Transmission system is 4 levels at 7,500 bauds.

Size: One cubicle 6' 6" x 20" x 20". Weight 400 lbs.

Production Status: Two development models have been produced and subjected to limited trials on a 170 mile music circuit.

Radiation: Has not been investigated, but believed to be secure.

PART IV. FACSIMILE SECURITY SYSTEM.

11. MOUNTEBANK (LATE METFAX).

A system for the encypherment of black and white meteorological charts and similar data. On the interim model the transmitted signal when used on a single channel basis is at the rate of approximately 1000 bauds. The final model will operate at 1750 bauds to provide for standard facsimile equipment transmitting charts 20" x 16" in a time of some 30 minutes. The crypto component is an electronic key generator operating on the Tutte-Tutte principle but incorporating also an 8 long random walk ring. The key output is added to the signal. The method of starting the key generators in step is a frame synchronising system similar to that used in AFSAY D 808.

Size: Transmit/Receive Terminal is 2 Racks each 6' x 20" plus one monitoring receiver.

Receive Terminal is 2 Racks each 6' x 20".

Radiation: Has yet to be investigated.

PART V. CRYPTOLOGIC EQUIPMENTS.

12. One-Time Pad Production Equipment.

(a) TRIMMER.

Represents the first effort towards utilising electronically generated random signals for the production of one-time pads. Source of signals is an electronic randomizer similar to that used in several other applications (e.g. 5 UCO key tape). Output is printed on wide carriage electromatic typewriters. Format programming is controlled by a unit using rotary line finder telephone switches.

Status: One multiple equipment operating five independent outputs has been constructed. Method of bringing it into operational use is being studied.

13. One-Time Tape Production Equipments.

(a) ROCKEX KEY GENERATOR.

Equipment for producing randomly perforated five-level tape. Source of random input signal is an unstable multi-vibrator requiring critical adjustment. A separate source is provided for each stream of holes in the tape. Paragraphing is punched into the tape and is accomplished by the para_raphing unit.

Status: Equipment currently in use and adequate supplies exist. No further production contemplated.

(b) 5 UCO KEY GENERATOR.

Equipment for producing randomly perforated five-level tape with same type of randomizer as used in TRIMMER. A pulse generator is used to time the random source from the reperforators which are free running with clutch locked out. Perforator operating speed is 400 characters per minute (same as rate of usage).

Status: 200 produced. No further production contemplated.

14. One-time Key Tape Checking Equipment.

High Speed Checker for 5 UCO key tape.

Electronic, high speed checker for 100,000 character spools of random tape used in the Apparatus 5 UCO No.1. Makes the following counts and prints out the results:-

(1) Plain stream (5 counts)

(2) Delta streams (5 counts)

(3) Combinations 1 and 2, 2 and 3, 3 and 4, 4 and 5, 1 and 3, 2 and 4, 3 and 5, 5 and 1 (eight counts).

(4) 15 consecutive dots in delta stream (5 counts)

(5) 3 consecutive strikes in delta characters (1 count)

Status: Three equipments built, fourth in course of construction.

PART VI. SPECIAL PURPOSE CRYPTO EQUIPMENT.

15. I.F.F. Mk. X. Code Changer for Mode I.

This is a small mechanical 26 point maze of 5 rotors. It is driven by a clockwork clock and the drums move at the code changing interval. It has not been finally decided whether this will be 5 mins. or 15 mins. The maze has a 5 wire output to produce the 5 unit binary codes required. It is used at ground radar I.F.F. interrogators and in airborne transponders.

Target size and weight: As small and light as possible. In practice it may be a cylinder 4"/6" Dia. and about 7"/9" long. Pressurised. Wt. under 10 lbs.

Development Status: First development models should be available early 1954, but clock may be later.