~~TOP SECRET~~

13 October 1950

BRUSA COMSEC CONFERENCE

FIRST REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various crypto systems falling under the following item headings:

a. Low Echelon (including Minor War Vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services.

b. Merchant Ship Telegraphic Systems.

c. Meteorological Security Systems, including Facsimile, Teleprinter and Telegraph.

d. Voice Security Systems for Tactical Purposes.

2. During the course of the discussion and demonstrations 33 crypto systems were considered. Technical descriptions of 29 of these are included in the appendices as follows:

	MACHINES	CIFAX	CIPHONY	HAND SYSTEMS
U.S.	a. AFSAM 7 b. AFSAM 9 c. 7 Rotor BCM d. "PCM" e. MCM	f. ASAX 2 g. NRL Cifax	h. ASAY 4 i. ASAY 6 j. ASAY 8 k. AN/TRA 16 l. TSS	m. ASAD 1 n. Running Key Cipher
U.K.	o. Mercury p. Concert q. Rollick r. Singlet s. Pendragon t. DUP 1	s. METFAX	v. Hallmark w. Sorcerer x. D 70	y. Playfex z. Linex aa. Cursex bb. Otmetco cc. Alametco

Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries. Brief mention was made of a modification of the M-209 which has been proposed by Hagelin. A description which he has submitted is included in the appendix. The appendix also includes some miscellaneous notes on general items.

3. None of these crypto systems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations during the interim between the close of this conference and the opening of the next.

~~TOP SECRET~~

4. Incidental to the discussions of the various crypto systems consideration was given to the problem of the number of different sizes of rotors which are contemplated for use in the mechanical crypto systems. The Sub-Committee feels that the 26-point rotor may have to be used for a long time to come but that some future agreement is necessary as to a selection among the 31, 32, and 36-point rotors. This agreement would limit the number of different types of rotors employed and thereby facilitate the interchangeability between U.K. and U.S. sources.

5. The Sub-Committee has the following observations and conclusions to report from its deliberation on the four items on its agenda:

A. Low Echelon (including Minor War Vessels) Telegraphic systems - including combined assault codes and tactical systems for all military Services.

1. We note that the Fleet Code and Combined Assault Codes are under discussion in the UK - US JCEC.

2. We note that there are no other Low Echelon systems yet under consideration for combined use.

3. We note that both US and UK have a number of new machine systems under development but that none of these is likely to be available for general combined use before 1954.

4. We conclude:

a. No machine system is likely to be available for general combined use before 1954.

b. If combined systems are required for any purpose in the interim period, possible systems are:

Strip
Linex
Cursex
Playfex
Running Key Cipher

c. To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months. Possible devices are:

DUP 1
AFSAM 7
"PCM"
AFSAM 9
MCM
Concert
Rollick

B. Merchant Ship Telegraphic Systems.

1. We note that Cursex is under consideration in the US-UK JCEC and is likely to be adopted as the interim solution for Allied Merchant Ships.

2. We recommend that a machine system of at least equivalent security but faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

"PCM"
DUP 1
AFSAM 7
MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.

1. We note the lack of any suitable combined crypto system for meteorological purposes.

2. We note that both the UK and US have under development new meteorological systems in the following categories:

Air-Ground
Telegraph
Teleprinter
Cifax

3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for general combined use before 1954.

4. We note that requirements and characteristics for combined plain text facsimile equipments have not yet been agreed upon.

5. We conclude:

a. No machine crypto system for meteorological purposes is likely to be available for general combined use before 1954.

b. If combined systems are required for meteorological purposes in the interim period, possible devices are:

(1) Air-Ground - ASAD 1
Otmetco
Alametco

(2) Telegraph - CCM (modified for weather encipherment)
Pencil and paper system for very low echelon purposes.

(3) Teleprinter - ASAM 2-1

(4) Facsimile - None available

c. To meet the long term requirements for encipherment of meteorological data selection should be made within the next 12 months. Possible devices are:

(1) Air-Ground - ASAD 1
Otmetco
Alametco
Any available ciphony system

(2) Telegraph - BCM 7 with provision for weather encipherment
AFSAM 7
"PCM"
Singlet
Pendragon
DUP 1 - designed for weather encipherment
Pencil and paper systems

(3) Teleprinter - AFSAM 9
ASAM 2-1
Concert
Rollick
Mercury

(4) Cifax - ASAX 2
NRL Cifax
METFAX

NOTE: Selection in category (4) may not be possible until an agreement is reached in the UK-US JCEC on the requirements and characteristics for plain text facsimile equipments and associated transmission systems for meteorological use.

D. Voice Security Systems for Tactical Purposes.

1. We note that there are no ciphony systems under consideration for combined use.

2. We note that both the UK and the US have a number of new systems under development but that none of these is likely to be available for general combined use before 1954.

3. We conclude:

a. No ciphony system is likely to be available for general combined use before 1954.

b. There are no possibilities for suitable devices in the interim period.

c. To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. Possible devices are:

(1) ASAY 4 (primarily designed as a low echelon ciphony attachment; can be used only over circuits of normal bandwidth)

(2) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)

(3) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)

(4) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)

(5) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)

(6) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)

6. The Sub-Committee has the following recommendations to make:

a. That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this exploratory conference. This should include technical visits.

b. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.

c. That security evaluations be made and exchanged on all items discussed.

d. That a copy of the final report of the conference be submitted to the U.S.-U.K. JCEC and that the U.S.-U.K. JCEC be requested to consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.

e. That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time.

a

AFSAM 7

OFF-LINE PERMUTING CYPHER MACHINE FOR TACTICAL USE

Size 12" wide by 12" high by 6" deep, approximately, less case.
14" wide by 14" high by 8" deep, approximately, in case.

Weight 15 lbs less case; 22 lbs in case.

Outline Description - A keyboard operated, tape-printing cypher machine 24 v D.C. operated (with adaptor for 115 v - 230 v AC operation). Encyphers letters and figures.

Technical Description

Cryptographic features: Eight 26-point rotors with independent alphabet and notch rings. 26 way input and output, 10 paths being re-entrant. Rotors 1-3, 5-8 turn. Motion is electrically controlled by sensing notch rings. Motion is "interlocked cascade," rotors 1 to 3 providing a dilated cyclometer giving a guaranteed minimum cycle. Machine is considered secure under all usual sorts of misuse. Read before step operation. Clear indicators are used.

Mechanical Features: A flying type wheel printer is used carrying a pulse generator on the same shaft. On depressing a key a circuit is set up through one stator coil in the pulse generator. At the appropriate time a pulse is generated in this coil which fires a thyratron operating the print magnet.

State of Progress - In an advanced state of development.

b

AFSAM 9

ON-LINE 32 WAY PERMUTING CIPHER MACHINE FOR TELEPRINTER USE

Size 16" x 12" x 6" less case
18" x 14" x 8" with case

Weight Approximately 27 lbs less case
Approximately 35 lbs with case

Outline Description - A tactical high security teleprinter cipher machine accepting teleprinter signals as an input and producing teleprinter signals as an output. Employs start-stop synchronization.

Employment - For use wherever teleprinter is employed in tactical echelons. (Tactical use of teleprinters is planned on a broad scale as low as regiment or battalion).

Technical Description - Accepts an input teletype signal, stores the five intelligence bauds, translates to one hot wire of 32, permuted in a rotor maze, the cipher signal translated to the five unit code for storage, and then transmitted in time sequence. Capable of operating at teleprinter speeds from 60 to 100 words per minute.

Cryptographic features - Employs nine 36-point rotors in the maze with 4 circuits recentried to reduce to a 32 character encipherment. Eight rotors move in an interlocked cascade with the center rotor not moving but fixed for the day. Three rotors automatically zeroized to a predetermined position before each message. Planned for use in a 5-letter clear text indicator with no restrictions as to use.

State of Progress - In advanced development. Prototype models expected Spring 1951.

7 ROTOR BCM (CSP 4800)

OFF-LINE 26-WAY PERMUTING MACHINE

Size 16" wide by 12" high by 12" deep, approximately

Weight 100 lbs approximately

Outline Description - 7 rotor mechanism using the carcase of CSP 1700 (CCM Mk II) with a single tape printer and a non-locking keyboard.

Technical Description -

Cryptographic Features: 7 rotor non-reciprocal maze. Planned to use removable notch rings and alphabet tyres. Rotors are reversible. Progression is notch controlled. Likely order of drive is 4 6 2 7 1 5 3, with 4 6 and 2 forming a cyclometer and the rest moving as in CCM. Rotors 2 and 6 always step backwards. Alteration of the direction of rotation of any rotor involves mechanical work. Maze is read before stepping. Backwards and forwards motion occur simultaneously.

Mechanical Features: Non-locking 4-bank keyboard with the numerals 1 to Ø on the top bank. Printer is magnet operated. 26-letter single case encypherment only. Printer has 26 letters, space and numerals 1 to Ø only. Facilities switch gives following conditions:

O - off

P - plain (in this condition all keys are effective)

D - decypher

E - encypher

R - reset (in this condition the rotors can be set by the figure keys 1 to 7)

Hand-drive facility of CSP 1700 has been abandoned, and the operation is by low voltage. An AC motor is fitted, and the printer, etc. is directly AC operated.

Another facility switch changes from CSP 4800 to CSP 1700. In the 1700 condition blank rotors are inserted in positions 2 and 6 (the backwards rotors) and these rotors will turn.

SECRET

2

7 ROTOR BCM (CSP 4800)

OFF-LINE 26-WAY PERMUTING MACHINE

Mechanical Features: (Continued)

A variant of this machine for weather operation (i.e. met) was also shown. The weather switch connects the figures 1 to Ø, space and X on encypherment to the maze, and on decypherment connects the appropriate maze outputs to the numerical functions of the printer.

As an alternative to this scheme the same facilities may be provided by using special plugs and sockets connected into the snakes joining the scrambler to the machine base.

Socket connections for auto operation are provided.

SECRET

d

"PCM"

Size ½ cubic foot - 12" x12" x 6" approximately

Weight 15 pounds

Technical Description - This machine is cryptographically identical with the CSP 4800. The rotors, approximately 2½" in diameter will use removable notch rings and alphabet tires. Permits direct encryption of numerals.

State of Progress - Engineering model to be delivered about 15 November 1950.

~~SECRET~~

e

CSP-3600 (MCM)

OFF-LINE HAGELIN-TYPE CIPHER MACHINE

Size 10" wide by 10" high by 6" deep approximately.

Weight 12-16 lbs approximately.

Outline Description - Keyboard operated, tape-printing cipher machine intended for very low echelon use. Hand powered with provision for modification to motor drive.

Technical Description

Cryptographic Features: 12 M-209 pin wheels adding their combined effect to a common drum. Key is the result of two steps of the pin wheels. Pins and lugs are settable, with a maximum of 6 lugs to a bar.

State of Progress - In development with one preliminary engineering model available.

SECRET

f

ASAX 2

CIFAX TRASCEIVER FOR USE WITH BLACK-WHITE COPY, PRIMARILY FOR WEATHER MAPS

Size 1 Rack approximately 24" x 26" x 54"
1 Power supply approximately 14" x 24" x 10"

Including approximately 150 vacuum tubes of which 130 are dual triodes.

Weight 400 lbs.

Outline Description - Medium-high echelon, high security cifax, transmitting multitone cipher at effectively 1000 elements per second, produced by synchronous binary addition of 2-level quantized facsimile signal and 2-level key.

Technical Description

Cryptotechnique: Six basic sequences produced at 6000 elements per second are combined in a complex manner to produce a 2-level key at 1000 elements per second. The basic sequences are produced by six continually rotating relatively prime wheels (in the range 101 to 115).

Electronic Features: The ASAX 2 is designed to transmit over 300-2750 cps land-line or HF radio, either or both being included in a single circuit. Cipher at a 1 millisecond rate is read successively into four channels, each channel being amplitude modulation of an audio subcarrier. A fifth subcarrier is amplitude modulated by a 50 cps signal for automatic phase control. The composite signal is transmitted directly on land-line or modulates a conventional (double sideband AM) HF radio transmitter.

The receiver portions of the ASAX 2 are equipped for automatic starting, synchronization, continuous phase correction, and alarming, including indication of each function. A frequency standard is included for use when manual control is desired.

State of Progress - Two terminals, originally designed for engineering tests, have gone through limited service testing on land-line and on HF radio links up to 1000 miles. Technically, performance of the equipment was satisfactory over normal ranges of room temperature.

SECRET

NRL CIFAX

CIFAX TRANSCEIVER FOR BLACK-WHITE WEATHER COPY

Can be converted to full duplex by addition of a second key generator.

Size Transmission equipment 16" x 19" x 72" approximately.
Key generator 16" x 19" x 24" approximately.

Weight 500 lbs approximately.

Outline Description - High security, shipboard and base station cifax, transmitting multitone cipher at effectively 1000 elements per second, produced by synchronous binary addition of a 2-level quantized facsimile signal and 2-level key.

Technical Description

Cryptotechnique: Eight basic sequences are reproduced at 1000 elements per second from continuously rotating wheels that are relatively prime. Eight wheels are selected from a set of 28 in the range 101 to 199. Four sequences are binary added to produce X key, which is recorded as a continuously traveling magnetic tape having 10 reading heads. A four stage ring picks off X key from various preselected reading heads to produce Y key. X key and Y key are binary added to produce the final output key. Two of the unused basic sequences are added Boolian to determine when the four stage ring is reset. The remaining two basic sequences determine to which position the ring is reset when a reset is demanded.

Electronic Features: The NRL cifax equipment transmits AM sub-carriers in the range 2000-3750 cps, eight channels being transmitted over Class A telephone line or HF single sideband radio. The equipment incorporates precision frequency standards with provision for manual or automatic phase correction.

State of Progress - Two models have received engineering tests and operate satisfactorily. Four service test models are presently being completed by a contractor.

ASAY 4

TIME DELAY SCRAMBLE CIPHONY SYSTEM

Size 12" x 12" x 18", estimated.

Weight 15 pounds, estimated.

Outline Description - The individual elements within a group of 20 elements are delayed different amounts of time before transmission.

Technical Description - A 19 x 20 element matrix code box controls the delay of the specific elements of speech in each group of 20 elements. The same code is used for at least one conversation. The key code control is on a tape and is advanced one step to a new position. Whether change is to be on a message or time basis has not yet been established.

State of Progress - Engineering models are now under development.

SECRET

ASAY 6

Size Three bays approximately $5\frac{1}{2}$ x $2\frac{1}{2}$ x $1\frac{1}{2}$ feet.

Weight Approximately 250 pounds per bay plus spare parts and test equipment.

Technical Description - Speech is converted into a 1500 baud per second on-off signal by means of a vocoder and PCM coder. To this signal is added a key sequence from an associated key generator. Transmission is accomplished by eight frequency multiplexed channels located in the standard voice frequency band. Six of these channels are for speech information, one is for synchronization and one is for station selection. The receiving end accomplishes the reverse operations of the transmitting end. Each terminal is full duplex.

Cryptographic Features - The key generator makes use of the geared timing mechanism to produce six basic sequences of 101, 103, 107, 109, 113, and 115 elements length. These sequences are combined by addition and multiplication in electronic circuits to produce output key at 1500 elements per second. The basic patterns are changeable as well as the individual starting points of each sequence.

State of Progress - Three models of the equipment are under construction by a contractor. These will be engineering and service tested to determine necessary modifications.

SECRET

~~SECRET~~

ASAY 8

SINGLE CHANNEL PCM CIPHONY SYSTEM

Size 2 cases each 12" x 12" x 18" estimated.

Weight 50 lbs., estimated.

General - The system is intended for general airborne tactical usage by VHF radio.

Outline Description - A single channel PCM system which employs "push to talk" transceiver element scrambling of a block of 32 pulses.

Technical Description

Cryptographic Features: The PCM coder output is "flattened" by means of "auto key techniques." The least weight baud of each speech sample (4 digit PCM) is delayed multiples of five elements. This causes it to be added to the 8 weight bauds of the next sample, to the 4 weight bauds of the next sample after that, and the 2 weight baud of the next sample after that. A code card or rotor system is used to determine a transposition in a block of 32 elements.

State of Development - Early development. 2nd Engineering model to be built by contractor. Air transmission test planned on lab model.

~~SECRET~~

AN/TRA-16

8 CHANNEL SPEECH SYSTEM FOR MICRO-WAVE RADIO

Size 7 4½' bays (counting 100% standby)

Weight About 1 ton (2000 lbs)

Outline Description - Enciphered PCM system transmitted by on-off pulses over micro-wave radio. The channels are in time division multiplex.

Technical Description

Cryptographic Features: The machine employs a key generator using four wheels of length 11, 13, 20, and 28. The motion of those wheels is controlled by plain text PCM elements and partially enciphered PCM elements.

State of Progress - Two terminals are nearing completion for use in a special experimental radio link. Several terminals without complete keyer circuits are available.

T.S.S.

Tactical speech encipherment system primarily for aircraft use.

Size and Weight - About 10" x 10" x 18" and weighs 39 pounds. (This is 18 element model.)

Outline Description - A TDS system of encipherment applied to PAM speech samples. Uses a fixed self-conversing code changeable by means of a switch matrix.

Technical Features - The set employs a rotory beam tube instead of a more conventional ring circuit to control the TDS operation. Two models of the system have been built, one employing a 12 element TDS the other an 18 element TDS. A 5 to 10 kc channel is required for transmission. The system synchronizes phase automatically.

State of Progress - Two models of each of the two types will soon be available for testing.

SECRET

m

ASAD 1

1. ASAD 1 is a small hand substitution device, designed for use in multiseater aircraft for the transmission of essential meteorological information.

2. It consists of a black box about 12" x 7¼" x 1¼" in dimension, containing a letter key-roll which can be rotated horizontally and overlaid by a stencil which can be rotated vertically. The stencil contains 13 lines each designated by the type of information involved (e.g. cloud ceiling, visibility, etc.) and containing up to 20 holes designated by numbers, directions, etc. Thus, at any position of the stencil or key-roll, there are 13 lines showing different types of information, and the exact detail can be designated by the letter appearing in the appropriate hole on the line.

3. The key-roll is produced so that a letter never repeats within a series of 20. The stencil is designed so that it covers every other line and column of the key; there are thus four independent keys on the roll. The roll can be set in 100 positions and the stencil in 26 positions. The setting numbers are substituted into random digraphs by means of an indicator table which fits into a slot above the window of the device.

4. The cryptographic principle is similar to that of the British UCO or ALAMETCO, and the system can be used for transmitting the same kind of information. A wider choice of key is available owing to the length of the key-roll and the principle of dual slide.

n

RUNNING KEY CYPHER

1. RKC is a literal hand substitution cypher, designed to give a high degree of security on strategical links where machine systems are not available.

2. The cypher comprises a book of random literal key-groups, and a book of random 26 x 26 letter substitution squares, one for each day of the month. For point-to-point working, the keybook would be used "once through" each day, commencing at a point chosen at random in the table; the system can also be employed for group working, choosing a random starting-point for each individual message. The encryption process consists of substituting each plain-text letter in turn against its associated key-letter, employing the substitution table valid for the day.

~~SECRET~~

MERCURY (LATE TYPEX Mk 10)

Synchronous on-line teleprinter cipher machine.

Size One 5'6" rack and four special tables.

Weight 450 lbs, very approximately

Outline Description - 31 way rotor permuting cipher machine using separate turnover control and ciphering mazes.

Technical Description

Cryptographic Features: A 4 rotor cyclometric maze controlling a 6 rotor ciphering maze. Rotors consist of an outer annulus (carrying progression notches) with scrambled wiring and a separate inner rotor. The two parts can be assembled in 62 different ways. Current traverses through the outer rotor section, then through a scrambled turn around end plate and then returns through the inner rotor sections. Cryptographically therefore the mazes consist of 9 and 13 rotors respectively.

Mechanical Features: Mercury is a duplex on-line synchronous cipher system. In-coming teleprinter signals are tried out to 31 ways and fed onto alternate storage devices. Signals are fed synchronously to the maze and then reconverted to 5 unit code for transmission. The maze is stepped synchronously. In the no traffic condition the letters function is sent "en clair" to line.

State of Progress - One circuit on traffic experimentally.

~~SECRET~~

p

CONCERT

ON-LINE TELEPRINTER SYNCHRONOUS CIPHER MACHINE

Size 16" x 8" x 8" approximately.

Weight 40 lbs approximately.

Outline Description - A synchronous on-line subtractor teleprinter cipher machine for general tactical usage.

Usage - The device is planned for large scale tactical usage.

Technical Description

Cryptographic Features: Maze consists of 11 wired rotors periods 41, 43, 43, 45, 45, 46, 46, 47, 47, 49, 49. Rotors 1, 3, 5, 7, 9, 11 turn regularly one step per element. Rest stay still. 8 of the 49 paths through the maze "drop" off" at various points. 24 of 49 inputs are energized with battery through push-buttons and seven of the 41 outputs are tapped and fed into relays. The seven relays perform modulus 2 addition in series on the plain teleprinter element for encipherment. Rapid clearance of push-buttons is provided. Rotors not interchangeable; rotateable alphabet tyre. The device is capable of providing several streams of simultaneous key and will still be secure.

Mechanical Features: The maze turns, continuously driven, through a differential gear box for phasing purposes from a magnetic amplified controlled motor if high "Q" circuit is used for time control. Element storage is provided. Traffic is enciphered on an element by element basis including start and stop signals thereby giving traffic flow security.

State of Progress - Two lab models made from drawings are under test. Development of the time control features is incomplete.

~~SECRET~~

ROLLICK

ON-LINE TELEPRINTER CIPHER DEVICE

Size One 4'6" telegraph rack on castors

Weight 100 lbs approximately

Outline Description - An electronically operated half-duplex on-line teleprinter subtractor encipherment device.

Technical Description

Cryptographic Features: See notes on Cock-Robin. (Item ee). The cipher key is generated by cold cathode gas tubes. Provision is made for generating random indicators not under control of the operator and for automatically positioning the key generator to these indicators.

Mechanical Features: The whole equipment is electronic. Most circuits use cold cathode gas tubes.

General - The device is intended initially for use on GCHQ land line circuits. A basic concept has been the use of electronic techniques so as to permit ready mass production.

State of Progress - Two models now being built for user trials.

~~SECRET~~

SINGLET

General - Singlet is a keyboard operated motor-driven, tape-printing off-line permuting cipher machine. The keyboard corresponds exactly to a standard teleprinter keyboard except that there is one additional key called a "Bigram Key". The full range of teleprinter lower and upper case symbols are available but four letter keys and carriage-return and line-feed require the pre-operation of the bigram key.

The machine is designed to work from 100-125 volts or 200-250 volts 45-65 c/s single phase. It can be taken through the hatch of a submarine.

Details - The machine will have a 26-way maze with 7 or more rotors operating on BCM principles but can also be used as for CCM working. It will use American type rotors.

Use for Meteorological Traffic - The inclusion of full case-shift facilities enables the machine to be used for meteorological traffic. Since none of the bigrammed signals are used for this type of traffic the operation of the keyboard is exactly the same as that of a standard teleprinter. (Not a weather keyboard).

State of Progress - The machine is still under development. A development contract for prototype production models will probably be placed in the Summer of 1951.

PENDRAGON

General - Pendragon is an off-line cipher machine using a perforated tape input and producing a page-printed copy on a teleprinter and also, if required, a perforated tape on a printing reperforator.

The input tape can be prepared on a standard teleprinter perforator using the full range of teleprinter signals. Bigram signals are automatically inserted by the equipment which has a 26-way permuting maze exactly the same as that used in Singlet.

Pendragon will interwork with Singlet and can also be used for CCM or BCM working.

Details - The main unit will be identical with Singlet, except that the keyboard and printers will be replaced by a control unit for inserting carriage return and line-feed, etc.

State of Progress - Development is proceeding in parallel with the work on Singlet and it is expected that both Singlet and Pendragon will become available about the same time.

DUP 1

General - DUP 1 is an off-line hand operated tape-printing cipher machine with an electrical permuting maze, weighing about 18 lbs. Its dimensions are 12¼" x 6¼" x 5". On the model demonstrated, the input is controlled by a setting knob similar to that of M 209 but keyboard operation could be arranged. Electrical power is supplied by a self-contained 45 volt dry battery which gives 80,000 operations or more. For low temperature operation, an external source of power is necessary.

Details - The maze is 26-way and has 8 rotors of which 1 and 5 are fast turning, 2, 3 and 4 being driven cyclometrically by 1, and 6, 7 and 8 cyclometrically driven by 5.

The rotors have alphabet tyres rotatable with respect to turn-over patterns, and removable wiring inserts which can be fitted in any one of 26 positions. The turn-over pattern is the same on every rotor in a set and there are 16 wiring inserts to each set. Compromise of the machine and wirings is covered by the fact that adequate security is given in the daily setting.

Use for Meteorological Traffic - Proposals are under consideration for encipherment of numerals and the letter X by the use of a manually operated case shift.

State of Progress - One hand made model has been completed and six more are under construction. A development contract has been placed for the manufacture of 50 models engineered for large scale production and intended for Service trials. Delivery of these prototype production models is expected to commence during the Summer of 1951.

General - LET-FAX is a system for the enciphered transmission of black and white meteorological charts. It is intended to meet a requirement for the transmission of charts 20" x 16" in a time of not more than 30 minutes with a definition of 100 lines per inch, the transmission channel (line or H.F.) having a band-width of 300 to 3,400 C/S.

The enciphering equipment will consist of one rack 20" wide by 6' high employing about 200 valves. The deciphering equipment is of about the same size.

According to present proposals the intelligence will be enciphered in an 8-way electrical permuting mase working entirely electronically.

Details - The picture intelligence is quantized 4,500 times per second, that is at twice the nominal picture element rate so as to avoid degradation of definition. Groups of 3 quantized elements are converted to signals on one of eight wires having a recurrence rate of 1,500 per second. These signals are permuted and converted to signals having one of eight levels for transmission by F.M.

The permuter will have eight stages ("wheels") with pluggable turnover patterns and changeable wirings. The latter will consist of paxolin cards with metalized strip connections. The variables will be turnover pattern, order of progression and wiring. The deciphering equipment will be started automatically and its speed will be controlled by differentiation of the incoming signals.

Stage of Development - Back to back laboratory tests have been made using bread-board assemblies. Bread-board experiments of the transmission equipment are proceeding.

The electronic permuter may later be replaced by a Rollick key generator.

V

~~HALLMARK~~

PCM CIPHONY SYSTEM FOR TACTICAL USAGE

Size and Weight - Lab models consist of one 5'6" rack. Weight, 300 lbs approximately. Packaged equipment for vehicle use planned.

Outline Description - Duplex 32 level PCM subtractor encypherment ciphony system for point-to-point service.

Technical Description -

Cryptographic Features: Subtractor encypherment using binary key from a group of transition counters of moduli between 2 and 29. Counters are reset automatically by a maze at periodic intervals.

Technical Features: Duplex operation using a common key generator giving different key to go and return channels. Framing, synchronization, maze stepping, etc. is automatic.

State of Development - 6 copies of lab models being made for special GCHQ circuits. Development contract placed for engineered models for field use.

H

SORCERER

VOCODER SPEECH SECRECY SYSTEM FOR GENERAL USAGE

Size and Weight

(Planned) 2 double sided racks 5'6" high

600 lbs

Outline Description - PCM Vocoder analysis and synthesis system with subtractor encypherment for operation over circuits of normal bandwidth.

Technical Description

Cryptographic features: Encypherment will be by using the Cock-Robin principle.

Electrical features: One pitch and eight spectrum channels. Pitch channels are defined to 16 steps, the spectrum to 8 steps. Optional provision of two transmission systems, one for land line and VHF radio. Operating at 1800 bauds, and a multichannel V.F. system 170 cps spacing and a 100 baud speed on each channel. Provision can be made for a secure teleprinter channel for order wire purposes if required.

State of Development - Development contract placed with a contractor. First models for trial due in 18 months.

~~SECRET~~

X

D 70

MULTI-CHANNEL CENTIMETRIC RADIO RELAY EQUIPMENT

Size and Weight - Duplicate equipment consisting of 4 transmitters, 4 receivers, antenna masts, etc., carried in one vehicle. Duplicate PCM multiplex etc., carried in a second vehicle.

Outline Description - Centimetric radio relay system providing 12 top secret speech channels.

Technical Description

Cryptographic Features: Encypherment is carried out by the Cock-Robin principle (Item ee).

Electrical Features: The equipment is fully duplicated with automatic change-over facilities. The 12 PCM channels are carried by FM on a 6cm radio link. An engineering channel is also provided using the spectrum below 4 kc/s. PCM system is analogous to Hallmark.

SECRET

V

PLAYFEX (SMALL SHIPS CYPHER)

1. Playfex is a tactical hand system, designed to effect a very rapid change of code with a minimum of documentation and production. It is specifically intended for use in small ships, and could be employed for any traffic where short term security is required and where a quick encryption process on a basic book is operationally acceptable.

2. In its present form it consists of a two-part (hatted) basic codebook, in which each vocabulary signification is given a two-letter group, omitting double letters and the letter J. The groups from the basic codebook are then encyphered by a double Playfair process, based on a pair of 5 x 5 squares changing every two hours. The keybook consists of 31 detachable pages, each containing 24 squares, divided into 12 pairs designated by the two-hour period for which they are valid. Each basic group is encrypted on the left hand square, and the resulting digraph encrypted on the right hand square. No indicator is required other than the date-time group of the message.

3. The keybook is designed so that squares valid for a period shorter than 24 hours can be issued for short front line operations. If a higher degree of security is required, the basic book can be changed monthly, the basic groups written out on a keylength, and the Playfair encryption applied to the vertical digraphs.

4. The small ships basic book and some editions of the keybook have been produced and are ready for issue if required. Field tests have proved satisfactory, but the system has not been used operationally.

LINEX

1. Linex is a literal hand substitution cypher, designed to give a high degree of security for forward-area strategical traffic, where machine systems are not available. It has been in use in the British Army forward of Brigade since 1944.

2. The cypher consists of a book of 25 pages of mixed alphabets, used in association with 10 cards known as cursors. Each cursor is designated by two or three letters, and contains a mixed alphabet along the top margin and a hole cut in one of ten positions on the right margin. The user selects one of the cursors and marks a letter in the mixed alphabet, as determined by the indicator. He finds the starting-point in the keybook, and places the marked letter under the first plain-text letter of the message; the cypher letter is read from the hole cut away on the right margin of the cursor. The cursor is then moved down one alphabet in the keybook and the process is repeated for the second plain-text letter; and so on, letter by letter through the message, using a new alphabet for each encryption.

3. The message indicator consists of a four-letter group selected from a page of random groups; the two pairs of letters are encrypted by a single Playfair process, to give the cursor and starting-point for the message.

SECRET

aa

CURSEX

1. Cursex is a literal hand substitution cypher, designed to give a high degree of security for strategical traffic where machine systems are not available. It is specifically intended for use as a combined merchant ships' cypher, and would be suitable for use on strategical links or as a general back-up to machine systems.

2. The cypher consists of a book of literal key, used in association with a frame containing a horizontal- and a vertical- sliding keysheet made up of a number of mixed alphabets. The plain text is written under the groups in the keybook, starting at a point determined by the indicator, and each of the keysheets is set up at one of 26 positions in the frame. Each letter of the text is then encrypted on the alphabet indicated by the associated key-letter. The key-letter is found in the alphabet on the horizontal keysheet, and the substitution alphabet is taken from the vertical keysheet, the process being facilitated by the use of a cursor sliding vertically over the frame.

3. Several specimen frames and keysheets have been produced, and field tests have proved satisfactory.

SECRET

bb

OTMETCO

1. Otmetco is a hand substitution cypher, designed for providing essential meteorological information to aircraft returning from operations. It can be used to transmit barometric pressure, followed by visibility and cloud-base if required. It is intended to place the *minimum* burden on the aircraft.

2. All ground-stations hold a book containing 1000 mixed alphabets, each designated by an indicator number. Aircraft are provided with a proforma card, containing an extract consisting of three alphabets from the book, a key barometric pressure and one or more letters indicating "plus" or "minus". The key pressure is obtained separately by each ground-station, by applying a daily-changing key-number to the actual barometric pressure observed at the station at a predetermined time.

3. When the aircraft returns to base, the ground-station transmits the barometric pressure as the deviation in millibars from the key pressure, in the form of a two-letter group; the first letter indicates "plus" or "minus", the second letter the deviation in millibars up to 25, as determined by the first alphabet on the card. If required, the cloud-base in hundreds of feet (up to 2500) is transmitted as the appropriate letter from the second alphabet, and the visibility in hundreds of yards (up to 2500) from the third alphabet.

4. In addition to the station key pressure, all aircraft in an area are given a daily-changing diversion key pressure. If an aircraft is diverted from base, it requests a report by transmitting its indicator number, and the ground-station bases its reply on the diversion key pressure.

5. Each indicator is allocated to one operation only, so that the key is virtually one-time, the only repetition being when a visibility or cloud-base alphabet on one operation may be used as a barometric alphabet on another.

6. The system is at present being given field tests, and preliminary indications are that it will prove satisfactory.

~~SECRET~~

CC

ALAMETCO

1. Alametco is a hand substitution cypher, designed for the transmission of meteorological information between ground-stations and aircraft. It has been in use in the R.A.F. since the latter part of the war.

2. Aircraft are provided with proforma cards, containing a number of lines devoted to various items of meteorological information, with blanks left for the insertion of letter keys (similar to the stencil on ASAD 1). Before an operation, the ground-station fills in the card with a number of mixed alphabets derived from a master key-book and changing daily. Any item can thus be expressed as the line-number in the proforma followed by the letter appearing in the appropriate space. Each aircraft normally carries more than one card, a different series being employed for area broadcasts.

SECRET

dd

ROTORS

26-Point Rotors

It has been agreed on Sub-Committee A that rotors on both U.S. and British revisions of the 7-rotor BCM should be physically and cryptographically interchangeable. The size of rotor proposed (3½" diameter) is that now used on CSP 1700. It is also proposed that the physical design shall as and when possible take the form of a rotor with a soldered-in wiring bobbin, a removable turnover cam, and a removable alphabet tyre each of which are in effect capable of rotation. The rotors may be reversed by interchanging the position of the turnover cam and the alphabet tyre.

For lightweight machines it has been proposed that a rotor of similar design but having a diameter of 2½" (as used on PCM) should be employed.

31 Point Rotors (U.K.)

A 31 point rotor of special design is used in Mercury (British on-line teleprinter permuting system).

The rotor consists of an outer reversible scramble-wired annulus with a fixed turnover pattern and fixed alphabet tyre, in which is inserted a second scramble-wired disc. The insert may be fitted in any one of 31 positions and is reversible. The maze circuits first pass through the inserts and then return via the end plate through the annuli.

36 Point Rotors (U.S.)

The U.S. is developing a 36 point rotor for use in new cipher machine developments. The figure 36 was chosen to allow encipherment of the 32 character teletype alphabet, the 26 character literal alphabet, and various system wirings. Two physically identical types of rotors are being developed; one of whose wiring is capable of being "plugged" to any desired scramble, and a second whose scramble wiring is "printed" on a replaceable plastic insert.

Each rotor consists of 4 parts, a main body, a notch ring, an alphabet ring, and a lock ring. The main body contains 36 flush commutator contacts on one face and 36 plungers on the other face. The notch ring is interchangeable between rotors and, although it is not reversible, can be placed in 36 different positions with respect to the alphabet ring. The notch ring

dd - Rotors (continued)

provides stepping control for the maze. The alphabet ring is used as a drive ring and for message indicator settings and contains 10 blanks on its periphery. Opposite the letter "O" is a depression used to "zeroize" the rotor. The lock ring holds the assembly together. The daily set up will consist of assembling the alphabet ring in the proper juxtaposition to the main body's index mark, picking the proper notch ring and placing it in proper juxtaposition to the alphabet ring and locking the assembly by means of the lock ring.

The design goal was to produce a new rotor which would ease the rotor wiring problem and be capable of large scale production.

The dimensions are 3.7" OD, 0.42" thick, and a hub bore of 0.30". The expected normal life is over 200,000,000 operations.

SECRET

ee

COCK-ROBIN

1. Note: Cock-Robin is a basic cryptographic principle, and has many applications. It can be produced both electronically and mechanically. It is described here in one application as a key generator (Rollick) for on-line teleprinter encipherment but other applications are mentioned in descriptions of devices using it.

2. Components: The generator has 9 cold cathode decade counters divided into three sets A, B and C. Each set has one counter 10, one 9 and one 7. All three counters within a set are driven simultaneously by means of an on/off gate. Several of the cathodes in each set are tapped, strapped together, and led off to control the other two gates. Another selection, possibly overlapping, of the cathode is made to produce three streams of mark/space key X, Y & Z, which are added modulo 2 to produce the final key element.

3. Motion: The "motor" output of set A turns Gate B on if there is a voltage present, and turns Gate C on if there is no voltage present. Set B controls Gate C and A, and Set C controls A and B in the same way. A gate is therefore only off if there is no voltage from the preceding set and there is a voltage from the following set. When the number of tappings in the various sets satisfy a certain condition, the cycle is the guaranteed maximum of 10 X 9 X 7 cubed.

4. Key: Stream X is obtained by tappings from the 10 counters in Set A, the 9 in B and the 7 in C, these tappings being strapped to give Boolean addition. Y is obtained from the 10 in B, the 9 in C and the 7 in A, and Z from the 10 in C, the 9 in A and the 7 in B. X, Y and Z are then added modulo 2 for the final key element, which is added to the plain teleprinter element.

5. Settings: All the tappings of cathodes for key and motorization are completely pluggable, and obviously change of plugging, which will probably be daily, gives a change of machine. Message settings can generally be produced automatically (see description of Rollick).

ff

CIPHONY SCHEME FOR GROUP WORKING

Outline Description of Proposal

A scheme for quantising speech into say 8 levels and permuting these levels in both electronic and mechanical (maze) permuters. Synchronization of the electronic circuits can be acheived on a push-to-talk basis, the mechanical parts by a clock mechanism. In this manner the advantages of permutation can be used in mitigation of loss of security due to transmission in depth.

TOP SECRET

BRUSA COMSEC CONFERENCE

FIRST REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

The meetings of Sub-Committee B began on 27 September 1950 and continued intermittently through 10 October.

The final report of the Sub-Committee is attached hereto. The minutes that were kept of the meetings give only a summary of the highlights of the various subjects discussed. They are on file with the recorder.

TOP SECRET

TOP SECRET