~~TOP SECRET~~

LCS/W3/R. Approved. Copy No: 13

U.K./U.S. COMMUNICATIONS SECURITY CONFERENCE 1951.

Replacement of the C.C.M. by BRUTUS and Improvements to the Existing C.C.M.

Report of Working Party 3
as approved by the Executive Committee.

A. Replacement of the C.C.M. by BRUTUS.

1. The BRUTUS MAZE.

The Working Party considered the security of the maze for the BRUTUS cryptographic system and made the following recommendations:-

(a) that the ROTOR MOVEMENT should be such that the rotors in positions two and six should step in opposite directions to the rest of the rotors: these latter step in the direction of the present CCM (AJAX);

(b) that the ROTOR STEPPING ORDER should be as follows:-

(i) Rotor 4 steps with each encypherment.
(ii) Rotor 6 steps if rotor 4 is in a notched position.
(iii) Rotor 2 steps if both rotors 4 and 6 are in notched positions.
(iv) Rotor 7 steps if rotor 2 is in a notched position.
(v) Rotor 1 steps if rotor 7 is in a notched position.
(vi) Rotor 5 steps if rotor 1 is in a notched position.
(vii) Rotor 3 steps if rotor 5 is in a notched position.

(c) that REMOVABLE CAM CONTOURS as recommended by the 1950 U.K./U.S. Communications Security Conference for use with the existing C.C.M. should be adopted for BRUTUS and that the U.K. and the U.S. technicians should exchange technical information and prototypes in order that the most suitable design should be adopted for common use by all Services. As, during operation, only one side of a rotor is used to effect the stepping motion each set of rotors should be provided with a set of removable cam contours with identity numbers but with no alphabet and a set of alphabet rings without contours. In use, therefore, each rotor would be fitted with one removable cam contour and one alphabet ring;

/(d)

(d) that the number of notches in the NOTCH PATTERN on any removable cam contour should not be other than 7, 9, 11, 15, 17 or 19. The questions of consecutive notch patterns, the possible provision of special high incidence notch cam contours for the centre rotor and the reversibility of the notch ring should be the subject of further study and an exchange of views between the U.S. and U.K. cryptographic security agencies;

(e) that a SET OF ROTORS should consist of ten rotors;

(f) that the WIRING of each rotor in a set should be different and that the wiring of each individual rotor should contain 18 distinct intervals (i.e. different wire lengths), the remaining intervals falling where they may.

In considering the rotors for the BRUTUS cryptosystem the Working Party took note of the fact that for the C.C.M. the U.K. and the U.S. Services were committed to rotors of different sizes and recommended that there should be no attempt at standardisation for existing equipments.

2. Other BRUTUS Security Factors.

The Working Party considered the other security factors relative to the BRUTUS cryptographic system.

(a) Compilation of Key Lists.

(i) The Working Party took note of a U.S. proposal to produce an equipment to speed up compilation of key lists and recommended that the U.K. cryptographic agency be provided with details as they become available.

(ii) The Working Party took note of the U.K. method of printing key lists with the first day of the period at the bottom of the sheet to facilitate early destruction of obsolete keys in hazardous areas and recommended that the application of this method to BRUTUS key lists should be examined.

(b) Indicator and Operating Procedures.

The Working Party took note that the prime user requirement was for the simplest procedure compatible with security. Subject to this general observation the Working Party recommended that the Indicator Procedure and the Operating Procedure for the BRUTUS cryptosystem should be the subject of further study and an exchange of views between the U.K. and the U.S. cryptographic security agencies.

/3.

3. Restriction on the Operational Use of BRUTUS.

The Working Party recommended that there should be no restriction on the level at which the BRUTUS cryptosystem could be used but that in accordance with the agreement between the U.S. and the U.K. Chiefs of Staff disclosure of the BRUTUS cryptosystem should be confined to the appropriate authorities in the U.S.A., U.K., Canada, Australia and New Zealand.

4. Requirement for Teleprinter Facilities in machines embodying BRUTUS.

(a) The Working Party considered the following draft recommendation made by representatives of the B.J.C.E.B. and the U.S. J.C.-E.C. at their joint meeting held in London in June 1951:-

"The B.J.C.E.B. and the U.S. J.C.-E.C. after considerable discussion agreed that it was desirable for Combined off-line cypher equipments, which would be designed in the future, to handle the full range of the Combined teleprinter alphabet and to operate from a standard teleprinter keyboard".

(b) The Working Party noted that the B.J.C.E.B. and the U.S. J.C.-E.C. were, at the time, discussing only off-line equipments. Had on-line equipments been under discussion the same recommendations would, no doubt, have been made.

(c) After considerable discussion the Working Party concluded that the present variation in designs of the keyboard on existing U.K. and U.S. off-line cypher equipments arose from a fundamental difference in message writing procedure adopted by the respective Service Staffs. Until this difference in staff practice was resolved it would be extremely difficult to resolve the cryptographic problem. Bearing in mind that the new series of A.C.P.'s might help to resolve the staff differences, the Working Party recommended that the provision of full teleprinter keyboard facilities on future off-line cypher machines should be the subject of further study and exchange of views and that this subject should be raised again at the next U.K./U.S. Communications Security Conference.

B. The Existing C.C.M.

5. Improvements to the Existing C.C.M.

(a) The Working Party reviewed the steps taken to improve the security of the existing C.C.M. in accordance with the recommendations of the 1950 U.K./U.S. Communications Security Conference and noted:-

(i) that additional rotors to increase the size of all sets used for U.K./U.S. traffic from 10 to 20 rotors per set were in course of production and that all U.K./U.S. C.C.M. cryptosystems should be based on sets of 20 rotors by 1st January, 1953;

/(11)

~~TOP SECRET~~

(ii) that the U.K. and the U.S. had solved the problem of fitting removable cam contours to their respective rotors but no exchange of such rotors for trials had yet taken place. As soon as this exchange shall have taken place and the final design had been agreed, production will be initiated and the system introduced as soon as possible;

(iii) that a new disguised indicator procedure had been worked out by the U.K. and U.S. cryptographic security agencies and this procedure was awaiting ratification by the U.K.-U.S. J.C.-E.Cs. with a view to its introduction on a Combined basis as soon as possible;

(b) The Working Party considered the operating procedures for C.C.M. at present in force and recommended:-

(i) that VARIABLE SPACING should be applied to all messages. The slight difference between existing U.K. and U.S. procedure has been reconciled and steps will be taken to introduce the agreed procedure as soon as possible;

(ii) the BISECTION PROCEDURE should be applied to all messages and in long messages should be applied once in each cryptographic part;

(iii) that SHORT MESSAGES should not be padded;

(iv) that the use of SIMPLEX SETTINGS should be considered with the present C.C.M. (AJAX) whenever overall long-term security is required at the higher levels irrespective of whether the other security refinements recommended had been introduced and, with this end in view, that a study should be made of the problems involved in the compilation, production and operational use of Simplex Settings with the C.C.M.;

(v) that C.C.M. PROCEDURE for use on NATO cryptonets should be the same as on combined nets.

11th July, 1951.