TOP SECRET

Final paper as agreed upon at Combined Conference on 4 Mar 43.

U. S. and British Collaboration on
Combined Cypher Machine Development

The following memorandum sets out the British and U. S. representatives' understanding of the results of the talks and conferences which have taken place between them, on the subject of cypher machine development for combined purposes.

I. Preliminary Narrative

During the course of the discussions, the British representatives gave the U. S. representatives general details of their "double wired drums" which they stated were being incorporated in certain new British equipment, and described in detail the design of a new machine referred to as RM.26/32, which they submitted might form the basis for a new combined cypher machine. The U. S. representatives, on their part, gave details of their proposals for improving the security of the existing C.C.M. by altering the rotor stepping arrangement, in addition to the provision of "sets of rotatable and interchangeable cam contours". The U. S. representatives also stated that they were developing equipment for the automatic wiring of rotors, and added that they would make available to the British details of this equipment when it had been tried out.

II. For reasons as stated in a written Joint U. S. Memorandum, which was handed to the British representatives, the U. S. representatives stated they could not agree to collaborate in the development of the RM.26/32 principle for combined use. The British representatives, for their part, stated that, whilst agreeing that the U. S. proposals for the modification of the C.C.M. gave considerably improved security, they could not commit themselves to agreeing to these proposals without a very much more detailed study of them.

III. C.C.M. Interim Plan

It is agreed that the security of the existing combined cypher machine needs strengthening. It is further agreed that, from the cryptographic angle, the most satisfactory method of obtaining increased security, which is applicable to all Marks of C.C.M., is to alter the code wheels so that they are fitted with rotatable and interchangeable cam contours.

IV. It is agreed that the U. S. Navy will carry out field tests on the new type code wheels fitted with rotatable cam contours

Note: Copied from "official" carbon copy sent me by Capt. T. A. Smith.

TOP SECRET

COPY

(encl 14)

which they have developed, and that if these field tests are successful, they will submit, through the medium of the C.C.B., a plan for the modification of existing and reserve C.C.M. code wheels.

V. C.C.M. Long Term Plan

Having regard to the anticipated developments in cryptanalytical machinery during the next ten to twenty years, the British are not convinced that the existing combined cypher machine, even when fitted with rotatable and interchangeable cam contours, as agreed upon above, will provide adequate cryptographic security for a high grade combined cypher machine, and advocate most strongly that action should be taken which will result in the combined cypher machine to be used in the future being sufficiently secure cryptographically:-

(a) To allow re-encypherment from one crypto channel to another to be accepted without reservations.

(b) To allow encypherment of the message as written, i.e. no bisection procedure, no burying, no padding.

(c) To allow the P/L text to be distributed without paraphrasing.

(d) To avoid any change of code wheel alignment within a message; i.e. one message setting only for a message.

(e) For the machine to be immune from P/L cribs.

The British Staff requirements for a future combined cypher machine are, in fact, as follows:

Security

(i) Must provide top grade security for next fifteen to twenty years and therefore must be designed to withstand the anticipated developments in cryptanalytical machinery during the next fifteen to twenty years.

(ii) Must be completely immune to re-encypherment and to verbatim cribs.

(iii) Capture of the machine complete with variable elements must not endanger or lessen the security of crypto channels using the same machine but with other variable elements.

COPY

(iv) The crypto channel captured must be capable of being restored to complete security by the replacement of the minimum number of variable elements.

Facilities

(v) Standard Teletype keyboard.
(vi) Page print of P/L text and crypt.
(vii) Crypt to be in 5 letter groups.
(viii) Machine to cut a 5 unit tape in addition to (vi).
(ix) Machine to accept and decrypt automatically from a 5 unit tape.
(x) Number of variable elements requiring change by key list to be reduced to minimum.
(xi) Message indicator procedure (initial code wheel alignment) to be as simple as possible.

VI. The U. S. representatives, whilst admitting that the security requirements as set out in V (a) to (e) above are a desirable goal to aim at, are not completely convinced of the urgent need for improving the security of the C.C.M., beyond the proposed rotatable and interchangeable cam contours and modified stepping arrangement. Further they consider that:-

(a) Prior to the development, production and issue of any improved combined cypher machine, an assurance would have to be obtained from competent British authorities that uniform U. S. and British rules would be observed regarding the safeguarding, distribution and use of the new equipment.

(b) The question of the use of an improved machine very largely hinges upon the acceptance by the British of the proposed U. S. modifications to the C.C.M., and consequently no commitment can be made at this time that an improved machine will definitely be adopted.

VII. It is agreed, therefore, that the following action should te considered:

(a) To draw up a set of agreed rules for the safeguarding and extent and method of distribution of the improved equipment.

(b) The acceptance, by the British, of the U. S. proposed modifications to the C.C.M.

(c) To draw up an agreed set of encyphering rules applicable to the new machine, acceptable to both the U. S. and the British.

TOP SECRET

It is agreed that in addition to (b) above, the British authorities will consider the existing U. S. regulations with a view to submitting a draft set of rules to cover (a) above, and that the U. S. authorities will consider the British security requirements already set out in paragraph V (a) to (e) as a basis for (c) above.

VIII. It is further agreed that:

(a) In spite of the adverse U. S. comments, the British will continue with the engineering development of the RM.26/32 principle, and will make the result of such research available to the U. S. authorities, if, in the British view, it is likely to have any combined application.

(b) The U. S. authorities will continue engineering research on the U. S. proposed C.C.M. modifications, and will make the result of such research and development available to the British authorities.

IX. Collaboration on the Development of Combined Machine for Use by Lower Echelon

Although no agreement was reached, the British representatives urged that the U. S. representatives should seek and obtain the necessary approval from Higher Authority to collaborate with the British in the development of a Lower Echelon combined cypher machine.

X. Conclusion

It is mutually agreed that the series of talks and conferences has been of great assistance to both parties, and it is recommended that collaboration in this field should continue within the framework of the agreements set out in preceding paragraphs.

March 4, 1947

TOP SECRET

COPY