TOP SECRET

TOP SECRET

Joint paper 1/ 2

U. S. COMMENTS ON PROPOSED BRITISH RM26/32 CIPHER MACHINE

1. The U. S. finds it impossible to embark upon the development of a new CCM based upon the principles of RM26/32 for the following reasons:

(A) Engineering Aspects

1. Although the construction of such a machine could be easily accomplished it would be unwieldy in operation especially in the setting of twenty-four (24) rotors, its weight and size. It would, due to the use of twenty-four rotors, present engineering weaknesses and maintenance difficulties. The use of twenty-four (24) rotors each having twenty-six (26) contacts on each face of the rotor together with the necessary separator contacts involve the total use of two thousand eight hundred and eight (2808) contacts. The maintenance of all these contacts in a cipher machine would be impracticable. A single contact failure in this mass would require considerable time to locate. The contact resistance through the series of twenty-four (24) wheels is approximately forty-eight (48) ohms for clean contacts. Experience has indicated that frequent wheel cleaning and separator contact cleaning would be necessary. The life of a code wheel under average use is approximately six months at which time it is necessary to recondition or replace. The number of moving parts required to intermittently step twenty-four wheels is more than four times the amount of parts required for the same purpose in the average code machine.

2. The service and maintenance work involved in keeping such parts in perfect working order would naturally be four times as great. The total estimated weight of this machine would be approximately ninety-two (92) pounds for a hand-driven design. It would be approximately twenty-six (26) inches long, fourteen (14) inches wide and eleven (11) inches high. The power required due to accumulated resistance in a twenty-four wheel mass should be 220 volts AC or 150 volts DC for operation of stepping magnets and printer. Such power sources in the U. S. Army and Navy are not normally available.

3. Although it is appreciated that the proposed machine would present advantages in the elimination of code wheel supersession and multiplicity of wheel wiring it is considered that this machine is a step backwards in engineering progress, in that the U. S. has attacked this problem from the point of view of achieving simplicity and reliable performance by reduction of components and moving elements, at the same time achieving maximum security by increasing sophistication in the cryptographic principles employed.

Encl 1 - 25 Feb 43 Minutes

~~TOP SECRET~~

~~TOP SECRET~~

U. S. COMMENTS ON PROPOSED BRITISH
RM26/32 CIPHER MACHINE
(Continued)

(B) Cryptographic Aspects

1. In view of the short time the U. S. has had for cryptanalytical study a firm assessment of the cryptographic strength of RM26/32 is impossible. Although it is agreed that the principles involved in RM26/32 are probably sound the possible increase in security is not sufficiently great to warrant the undertaking of the development and production of this machine.