MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

	NAME OR TITLE / ORGANIZATION AND LOCATION	INITIALS / DATE		
1	OO			CIRCULATE
				COORDINATION
2	OOA			FILE
	Do 12			INFORMATION
3	OOB			NECESSARY ACTION
			✓	NOTE AND RETURN
4	OOC			SEE ME
				SIGNATURE

REMARKS

Just received ltr from Hagelin enclosing info which Dub had reproduced as per attached. Copies to 02, 03, 04 also.

~~CONFIDENTIAL~~

FROM NAME OR TITLE	DATE
J	31 Jan 51
ORGANIZATION AND LOCATION: OOT	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used.

16—48497-4 GPO

Jan. 26, 1951.

Civilingenjör
Boris Hagelin

~~CONFIDENTIAL~~

Post-War development work on ciphering devices by Boris Hagelin.

During the first two or three years after the cessation of hostilities I mainly tried to take stock of the situation in the field of ciphering devices and their uses, and I returned to the actual work of developing new devices only very gradually in '47.

I was aware of the absolute security, offered by the proper use of the so-called one time blank system, and I also designed mechanisms for its application on the ciphering machines already manufactured on license by A.B.Cryptoteknik in Stockholm, Sweden. I did not however bring any of those designs on the market, as I felt that no practical solution as to the supply of the one time key tapes was available.
I did however construct a machine for the production of one time blanks, to be used for the ciphering of number codes; such machines are at present in use.

It was only in 1949, when work was started on devices for the direct ciphering and deciphering of teletype communications, that I began to devote a considerable part of my time for the construction of new ciphering devices. It was in this connection that a new displacing mechanism was invented, and it was subsequently found that this mechanism could be used for a number of different devices.

A short summary of the devices, now being designed and developed following my instructions at the A.B.Cryptoteknik is given below:

1/ A machine for the ciphering and deciphering of teletype communications. Apart from the new type of ciphering mechanism, using the displacing mechanism mentioned above, this machine features a construction, which produces undistorted cipher signals under all transmitting conditions.

2/ A small mechanical ciphering machine, similar in operation to the converter type M-209. This machine features freely exchangeable key wheels (of which there can be had about 12 different wheels), exchangeable drum bars, and exchangeable type wheels. The key wheels have an irregular advancing movement, the characteristics of which can be changed at will by the operator. The machine will be normally built to print on two tapes (clear text and cipher).

3/ A large mechanical ciphering machine, for correspondence with the small machine as per 2/ above. This machine is being designed for an operating speed of 4-5 signs per second. It can be equipped with a shifting mechanism, to allow the direct ciphering of both letters and figures, and will allow the use of any number of differently arranged alphabets.

4/ A large electrical ciphering machine, where the ciphering is obtained by electrical means, operating at a speed of ab. 7 signs per second. It is my intention to add a mechanism which would transform this machine into a ciphering teletype.

A mechanism, employing one time key tape, can be substituted for the key wheels in any one of the above four machine types, and a machine for the production of these tapes can also be supplied, if need arises.

(Signed) BORIS HAGELIN

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~