28 April 1951

MEMORANDUM FOR MR. FRIEDMAN

The following comments on the two U.K. papers DGC/1640 and DGC/1643 are made at your request. From the standpoint of practicability it is difficult to judge how well the U.K. proposals would work, since we know so little about the present French practices, the temperament, ability, etc. of their code clerks, and the nature of their communications. Thus we can only consider how American code clerks would react to and would handle such ciphers were they forced on them. Some general security comments are also included.

1. DGC 1640 (non-dip)

Double encipherment on the M-209 or B211. From the higher level standpoint possibly satisfactory. Security-wise, addition of finnery and slippery would make this a good system. From the reliability and efficiency standpoint difficult, but probably to be preferred to super-encipherment of basic book. We find it much easier to repeat a process than to mix two together. Compared to what the U. S. Army uses at this level, double-Hagelin encipherment is murder, but would possibly work for the French. At the lower levels, double encipherment and recipherment, both appear hopeless.

2. DGC 1643 (dip)

The one-time pad proposals are OK, from the operator practicability viewpoint. One time pads are not difficult to use. The operational draw back is in quantity of pads required.to be held at each place. Security wise, and practicability wise-both, the reencryption proposal in paragraph 20, i.e. in an appropriate pad, is much to be preferred to the other suggestions.

Frank Austin