MINUTES OF MEETING WITH NAVY
1 December 1947

8 December 1947

A conference of ASA and Navy representatives on the subject of CCM modification was held in Room 117 Hq., Arlington Hall Station at 1330 on Monday 1 December 1947. The following were present:

ASA

Mr. William F. Friedman, Chairman	AS-14
Mr. Mark Rhoads	AS-14
Lt. Col. Charles H. Hiser	AS-23
Major J. G. Moak	AS-23
Dr. S. Kullback	AS-70
Mr. Leo Rosen	AS-70
Dr. A. Sinkov	AS-80
Mr. F. C. Austin	AS-83
Mr. K. Kuhn	AS-85

NAVY

Capt. L. F. Safford	OP-20-D
Capt. M. R. Gerin	OP-20-Y
Capt. H. O. Hansen	OP-20-K
Capt. J. S. Harper	OP-20-N
Capt. L. W. Parke	State Dept.
Capt. A. M. Patterson	OP-20-R
Comdr. D. W. Seiler	NCSL
Lt. Comdr. J. C. Hargreaves	OP-20-Y
Mr. H. Campaigne	OP-20-N
Mr. R. H. Shaw	OP-20-K
Mr. L. D. Whitelock	BuShips

Mr. Friedman opened the meeting in the absence of Colonel Hayes who was out of town, and presented the ASA's viewpoint regarding the modification of the CCM (see Incl. 1). A general discussion followed regarding the difficulties involved in the CCM modification program as opposed to the difficulties of rewiring and distributing rotors more frequently.

Capt. Safford stated that in his opinion it would be advisable to postpone a final decision in regard to this whole matter for about one month inasmuch as some changes are to be expected in both Navy and Army high commands. For that reason he felt that no

commitments could be made at the moment. In the meantime the Army's proposals would be studied by Admiral Stone.

This suggestion by Capt. Safford met with the approval of all present.

Just before the close of the meeting, Captain Safford stated that Commander Seiler was working on a new CCM basket with improved contact-assembly that would give more positive functioning of the stepping-control contacts and hence more reliable operation of the CCM. The new contact-assembly would include back-contacts, and if shop tests indicated that the back-contacts were reliable, we could go to a more complex motion of the 5-rotor machine.

It was agreed then to adjourn the meeting, subject to call from the Navy.

William F. Friedman

WILLIAM F. FRIEDMAN
Chief, Communications Research
Chairman

1 Incl
ASA Statement on CCM

ARMY SECURITY AGENCY STATEMENT ON CCM

Conference with Navy on 1 December 1947

1. Background:

Almost one year has gone by since our last conference with the British on cryptographic equipment for use in Combined Communications. At that conference the principal subject was the possible improvement of the CCM to increase its cryptographic security. The Navy proposed at that conference certain modifications involving the use of rotatable and variable cam contours on the rotors for the CCM's. A certain amount of research and development was undertaken by the Navy, and after about 8 months it developed that the proposal was impracticable and could not be worked out so as to be satisfactory in application or usage. Thereupon other modifications were proposed both by the Army and the Navy, these involving changes in rotor motion so as to eliminate the short internal cycle and to make cryptanalytic solution more difficult in other respects. These proposals were thoroughly studied. The Army proposal was found objectionable by the Navy on mechanical grounds. This left the Navy proposal as the only one remaining.

2. Navy Proposal:

The Army Security Agency has carefully studied the Navy proposal for modifying the CCM and finds the following objections thereto:

a. Although the proposed changes would increase the cryptographic security of the machine, this increase would not be of sufficient degree to justify their adoption in view of the practical difficulties that would be encountered:

(1) ASA deems it doubtful that the proposed modifications could be incorporated in the British Typex machines. On this point the Navy has reported informally that the matter has been studied for about a year, purely on paper, and that the idea has not been worked out in a concrete model. The Navy thinks it is possible to make the changes in the Typex but admits that they would be major changes. In view of the British position, made quite clear at the conference last January, that they are going to discard the Typex, it is very doubtful if they would be willing to undertake a project involving the expenditure of a great deal of money, for which only minimal benefits would accrue to them in a machine soon to be discarded.

INCLOSURE 1

(2) Even if the foregoing point were found not to constitute a difficulty and the modifications were incorporated in the British machines as well as in the U.S. machines, or even if the U.S. services undertook to furnish the British enough machines for Combined purposes, it would take considerable time to test the modified machines in practical operation, to insure that there were no cryptographic, mechanical, or electrical defects arising from the changes. As the CCM machines now stand, we know that mechanically and electrically they are satisfactory and stand up well in operation; cryptographically we know where we stand, as a result of several years' study of the present arrangements. But we have not had any lengthy period to study the new proposals for motion and reversed stepping; it is impossible to forecast what unforeseen cryptographic weaknesses might be uncovered by further intensive study.

(3) In executing the Army's SIGROD program, it has been necessary to use the SIGAMUG. These components were the ones originally used to convert the SIGABA's into CCM's. The SIGROD machines resulting from the conversion can still be used as CCM's, when CCM rotors are provided, so that the Army has not lost anything in regard to facilities for Combined Communications by virtue of its SIGROD program. But to incorporate the proposed Navy (or even the proposed Army) CCM changes into the SIGROD's would mean recalling all the SIGROD's which have already been issued and are now in service, thus putting the Army back to practically where it was over a year ago in the SIGROD program. Moreover, the Army has been endeavoring to complete the latter program so that it could commence on the very urgent program of rehabilitating all crypto-equipments being held in war reserve, a program which has already been delayed unduly.

b. The ASA believes that while at this moment the incorporation of either the Navy's or the Army's proposed changes in the CCM appear to offer the possibility of currently improving the CCM cryptographically, this improvement does not even now appear to be quite sufficient to eliminate all questions as to what the security of the so-improved CCM might be say five years from now. We know now that a theoretical solution of CCM messages would still be possible and we also agree that granting that there were a sufficient desire to make what is theoretically possible a practical reality, by use of many people and analytic machines, daily solution of CCM keys could be achieved. Thus, nothing substantial or of long-term benefit would be gained by modification of the CCM along the lines of the Navy's or the Army's proposals, which involve mere changes in rotor motion, with or without reversed stepping.

c. In connection with the last-mentioned item, reversed stepping, the Army would like to point out one thing and to query the Navy thereon. In embarking on its program to produce CSP-2900 machines, one of the motivating reasons therefor was to have one machine representing an improvement on the ECM, concerning which not even the British would have an idea as to its cryptographic nature. One of the principal features of CSP-2900 was the introduction of reversed stepping. The Navy proposal for CCM modification includes this very feature of reversed stepping. Is this not inconsistent with the basic reason for producing CSP-2900? Of what anticipated value would the CSP-2900 be if the same principal change were embodied in the CCM?

d. The ASA has recently considered various modifications of more radical nature than those proposed either by the Army or the Navy thus far, and finds that some of these more radical modifications appear to be feasible, on paper at least. But the practical embodiment of these modifications in an operative manner in the machines would involve a certain amount of research and development, and ASA cannot even suggest undertaking such research and development for the following reasons:

(1) The formal and broad directive of the Research and Development Division of the General Staff, Department of the Army, in respect to research and development is that no funds or effort be expended in trying to improve existing equipment by mere modifications therein.

(2) The commitments of the ASA and specifically of the Research Laboratories Division for research and development of equipment for the Army and for the Air Force are such that no further projects can be undertaken without jeopardizing the projects which have already been authorized and which have thus far been seriously delayed by causes not under ASA control. Very close scheduling has been necessary to keep these projects going in satisfactory manner and the position in this respect is rather precarious, there being little leeway for disruptions which might result from introducing any new projects, no matter how minor they may appear.

(3) The rehabilitation program assigned to the Security Division of ASA is at present far behind schedule. In fact, it is so far behind that an emergency at any early date would find the Army and the Air Force with an insufficient number of usable cipher machines to permit the use of any single one of the various types of equipments for general communication. The Security Division will shortly begin an intensive program of rehabilitation to remedy this situation and any delays introduced by modifications or changes in any of our machine would only cause further postponement of the whole program. It is for this reason that the Security Division cannot undertake any project of modifying Army CCM machines.

3. ASA Recommendations:

a. In view of the fact that the Army finds the Navy proposal for CCM modification impractical and that the Army is convinced that any proposals which would involve material physical changes in the CCM which cannot be made in the field are impractical and inadvisable, the Army believes that as an interim measure additional security in Combined Communications can more readily, more economically, and more practicably be achieved by more frequent changes in rotors. The ASA therefore proposes this as an interim solution to the problem. In connection with this, key lists should not be put out in advance for as long a period as is now the case, and we might even consider the possibility of a twice daily instead of a single daily change in settings. Also, it is possible the Navy might push to completion its program of developing the automatic rotor wiring machine. This would facilitate rewiring rotors and might simplify the problem of more frequent change of rotors for both Navy and Army.

b. The Army feels that should an emergency arise in the near future making voluminous Combined Communications a necessity, and should there at that time be any doubts about the security of those communications with the use of the CCM, the SIGABA-ECM could be issued to the British, provided no other suitable machine were available for the purpose at that time.

c. Finally, the Army feels that the Army and Navy should jointly inform the British of the foregoing and seek their opinion thereon.