CCM (1943-1945)

A AP

SECRET ACC NO 4723 35914
LOCATION CBML 11

35696
(7)

SECRET

SECRET

MATERIAL IN THE C.C.M. FILE

The correspondence iN this folder pertains to the use of C.C.M.'s (modified ECMs) on the Dayton-Washington link and the GCCS (British) - NCA link. The correspondence pertains principally to:

(1) CCM Security

(2) Procurement and Servicing of CCMs for the above link.

SECRET

SECRET

13 April 1945

Reference: Secret dispatch from Eachus to Engstrom
10 April 1945.

Re CCM Mark II, need total of eighteen each bearing collar and support plate for off-on-encipher-decipher controller switch. These items wearing badly on four units, interfering with proper operation.

Receipt:

Received of Naval Code and Signal Laboratory this date:

4 ~~18~~ Part No. 100571 ~~Bearing collars~~ Cam Shaft.

4 ~~18~~ Part No. 10033Z Support plate

S. R. OREM, Jr.
Lt.(jg), USNR
Op-20-G-4-D

4/13/45 1¢3¢
Lt. Ballin
Parts Ofcr. - NCSL

U. S. NAVAL COMPUTING MACHINE LABORATORY
C/O NATIONAL CASH REGISTER COMPANY
DAYTON 9, OHIO

SECRET

23 March 1945.

MEMORANDUM TO COMMANDER H.T. ENGSTROM:

Subj: Paper tape for CCM - request for.

1. It is requested that one dozen rolls of subject tape be furnished this activity. The present supply is almost exhausted, therefore prompt attention to this matter would be greatly appreciated.

R. I. Meader
R.I. MEADER.

27 March 1945

Requested Stapleton to order tape from GQ and have it shipped to Comdr. Meader.

R.D.a

U. S. NAVAL COMPUTING MACHINE LABORATORY
C/O NATIONAL CASH REGISTER COMPANY
DAYTON 9, OHIO

SECRET

23 March 1945.

MEMORANDUM TO COMMANDER H.T. ENGSTROM:

Subj: Paper tape for CCM - request for.

1. It is requested that one dozen rolls of subject tape be furnished this activity. The present supply is almost exhausted, therefore prompt attention to this matter would be greatly appreciated.

R. I. Meader

R.I. MEADER.

File CCM

Comdr T. A. Smith has copies from Bu.

ARLINGTON HALL STATION

MESSAGE CENTER

INCOMING MESSAGE

FROM: GCCS LONDON ENGLAND

TO: SIGNAL SECURITY AGENCY

MSG. NO. GCCS 3293 101835Z MAR 45

SSA 535 CIT FRI FOR COLONEL ALLSOPP FROM SMALL ULTRA

STUDY BY BRITISH ON CCM. FAULTS HAVE BEEN DISCOVERED IN NOTCH PATTERNS OF ROTORS ON ARMY CCBP 0114 (CSP 1814) AND ON NAVAL NETS BRUSA (CSP 2513 AND CSP 2514) KADYQ (CSP 1580) AND CEMIZ (CSP 1581). ON CCBP 0114 ROTORS THERE IS POSSIBILITY OF LOBSTERS DUE TO NOTCHES OCCURRING AS RESULT OF FURTHER (WU) SIMULTANEOUSLY ON EACH SIDE OF ROTORS. THIS OCCURS 10 TIMES ON ROTOR NUMBER 40, 5 ON 41, 7 ON 42, 10 ON 43, 8 ON 44, 6 ON 45, 8 ON 46, 5 ON 47, 5 ON 48, 7 ON 49. ON BRUSA CIRCUIT TO BE IN FORCE AUGUST 1945 ROTORS NUMBERED 40 THROUGH 49 LOBSTERS OCCUR AS FOLLOWS 7-6-5-3-7-4-5-7-4-8. ON CURRECT BRUSA ROTORS 30 THROUGH 39 AS FOLLOWS 2-5-9-7-1-3-10-0-3-4. ON KADYQ 4-4-4-4-6-9-8-8-5-10 ON CEMIZ NUMBERED 10 THROUGH 19 5-5-5-5-5-7-7-3-7-8. ALSO 338 CYCLE OCCURS ON 4 OUT OF 5 WHEELS WHENEVER CEMIZ 10 IS IN POSITION 4 OR 10R IN 2 SEMICLN IN CURRENT BRUSA WHENEVER ROTOR 33R IS IN 4 OR 33 IN 2 SEMICLN ON AUGUST 1945 BRUSA WHENEVER ROTOR 43 IS IN 3 OR 43R IN 3 OR 47 IN 3 OR 43R IN 3. THESE LAST BRUSA ROTORS ARE IDENTICAL TO FAMOUS QUOTE ROTOR FOURTEEN END QUOTE IN THAT NUMBER OF NOTCHES AT ODD POSITIONS EQUALS NUMBER OF NOTCHES AT EVEN

POSITIONS. THE FACT THAT CERTAIN ROTORS IN POSITIONS 2 AND 4 GIVE RISE TO 338 CYCLE OF FOUR WHEELS IS DUE TO SUM OF E3ERY OTHER GROUP OF INTERVALS BETWEEN NOTCHES EQUALLING 13. THIS LAST WAS JUST DISCOVERED BY MAJOR BABBAGE HERE. ABOVE INFORMATION EXCEPT THAT PERTAINING TO CCBP 0114 IS NO DIRECT CONCERN OF ARMY BUT AM PASSING TO YOU FOR YOUR INFORMATION AND HAVE TOLD CAPTAIN LESHER. LESHER HERE AT GCCS TODAY. EQUIPMENT HE COURIERED DELIVERED TO BRITISH SERVICES

ARLINGTON HALL STATION

MESSAGE CENTER

INCOMING MESSAGE

FROM: GCCS, LONDON ENGLAND

TO: SIGNAL SECURITY AGENCY

MSG NR: GCCS 3420 111412Z MAR 45

SSA 544 CPT FRI ULTRA

IN GCCS 3293 I GAVE 2 REASONS FOR SHORT CYCLES TO OCCUR IN CCM. THESE REASONS WERE WRONGLY INTERCHANGED. FAMOUS ROTOR 14 HAD ALTERNATE INTERVALS BETWEEN NOTCHES SUMMING TO 13. OTHER ROTORS IN POSITIONS 2 AND 4 HAD NUMBER OF NOTCHES AT EVEN POSITIONS EQUAL TO ODD. BELIEVE BOTH THESE POSSIBILITIES KNOWN TO US LAST SUMMER WHEN WE STUDIED CCM. EACHUS REQUESTS COPY WIRE GCCS 3293 AND THIS WIRE BE GIVEN ENGSTROM AT JIP 20 G

S E C R E T

Op-20-G/mb

SECRET

29 December 1944.

MEMORANDUM

From: OP-20-G-4.
To: OP-20-3-GY-A.

Subj: Communication Change - Washington to Dayton.

1. Commander R. I. Meader has requested that a dispatch be sent to the Naval Computing Machine Laboratory immediately, before 1 January 1945, ordering the new C.C.M. set-ups into effect. This was requested to circumvent the confusion that occurred during the last change.

2. Will you please comply with this request.

H. T. ENGSTROM.

TOP SECRET
OP-20-GE

TOP SECRET

File

12 October 1944

TENTATIVE

Asked Lt. Clifford to pass the word by Lt. Levit. E 10/14

MEMORANDUM FOR OP-20-K

Subject: Possible Machine for Performing ~~Lt. Levit's~~ C.C.M. Tallying.

Enclosure: (A) Rough pencil sketch of subject machine.

1. ~~The subject~~ A machine ~~would~~ operate from four tape readers run synchronously, two for the (differenced) plain bigram and two for the cipher. One line-pattern could ~~be~~ run off in less than two minutes, hence all ten in twenty minutes plus time to change tapes. The fifteen patterns involving trigrams would be rather clumsy to handle along these lines, but the difficulty would undoubtedly be overcome under the pressure of necessity. ~~Please make allowances for the fact that we have not been able to put a great deal of time on this problem.~~

2. Picture Lt. Levit's catalogue as a 676 x 240 rectangle, the rows named by the 676 bigrams and the columns by the 20 x 12 combinations of wheel and displacement. A cell of the rectangle is marked if the corresponding entry occurs in the catalogue. In the machine, the rectangle would consist of 676 horizontal and 240 vertical wires connected at the marked cells. There are two such rectangles, one for the plain bigram and one for the cipher. The two impulses from the plain readers (taken to be E and N in Enclosure (A) as illustration) are converted by a 26 x 26 square matrix into a single impulse (for the bigram EN). This enters the plain catalogue board (at row EN) and emerges on the vertical wires connected to this row. The cipher bigram (JV) is treated likewise at the same instant.

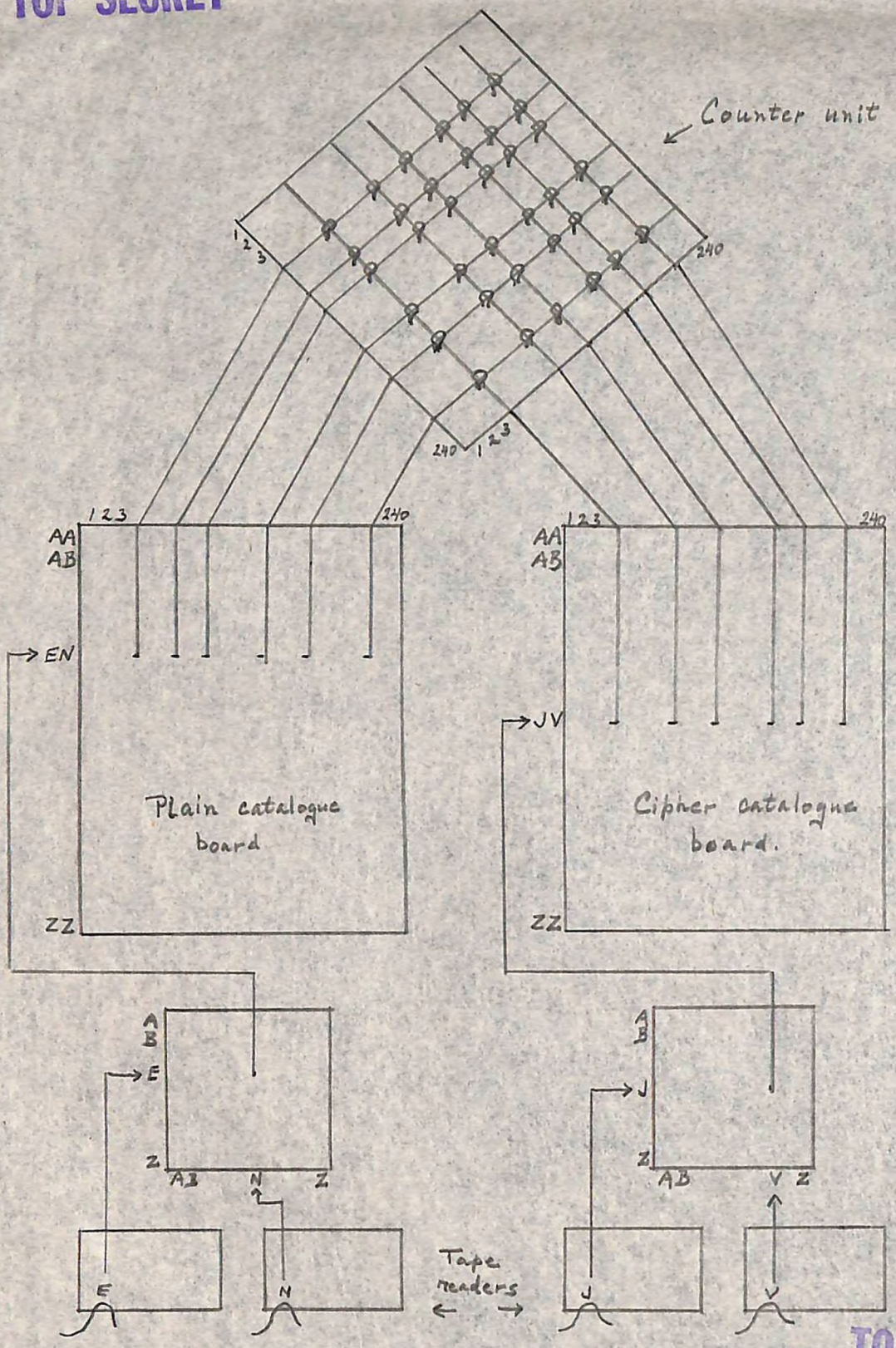
3. The 240 column wires of each of the two boards lead into a 240 x 240 square as shown in Enclosure (A). At each point of intersection (except possibly the "impossible" ones), there is a counter of some sort. 50,000 counters of the usual variety would probably not be feasible, but it would be possible to do the job photographically, using lamps costing only a few cents each.

G

G50
GE (originator) G.N. Clifford.

TOP SECRET

TOP SECRET



TOP SECRET

ENCL. (A). Rough sketch of machine for performing Lt. Levit's C.C.M. tallying.

A.H.C.

S E C R E T

SECRET

ACTIVITIES

File CCM
x Stat. Bombe
x Photo Radio
x Hagelin
x Viper
x Mamba
x NAJ
x IBM
x Wave Propagation
x Crypto [illegible] General

14 Sept. 1944

MODERNIZATION OF RADIO STATIONS.

I told Lt. Norris that you had agreed with Commander Cross that Ens. Ritchie and Lt. Anderson might be available part time on this work. As far as I know, nothing further has happened on this.

FRIEDEN CALCULATORS FOR LT. COMDR. MENZEL.

A request from Lt. Comdr. Menzel appeared for two Frieden calculators. This memo was addressed to GO via G-50 and G-20. The memo had previously been approved by G-20. I thought you would not like such tactics and called GE to get their opinion of Mr. Menzel's needs. They said that Mr. Menzel kept his present calculating equipment very busy and felt that he was warranted in asking for two more--particularly since GE might then be able to use them part time. Since G-20 had already approved the purchase, I approved the memo for you.

CALL FROM LT. P. R. WHITE.

Bob White called from Dayton to say that he was only working about two hours per day and was anxious to be reassigned, but that the matter could most certainly wait until you returned from leave.

BILL WRAY CLASSIFIED 1A.

Bill Wray said that he had just received notification that he was reclassified 1A. I took the matter up with Commander Foley who talked with someone in GR about the past history of this case. Commander Foley said that Bill Wray must have been classified as 1A for social purposes by friends on the local draft board. He says there is a rule by which it is not easy to ask for deferrment for civil service personnel on the grounds of indispensable work. He said that they could probably break this rule but that the memo might not be approved and might bring undesirable attention to Bill Wray's case. He wonders if the best bet is simply to let the matter ride on the basis that Wray will probably never be called for induction. He asked me to sound around to see what Bill Wray's feelings were in the matter and whether it was worth saving his pride. I believe that Wray feels rather on the defensive inasmuch as if his work here is not worth asking for a deferrment, he is not doing the job he should do. In view of your experience on this matter in the past, I thought I had just better let it ride until you return.

SECRET

S E C R E T

COMMITTEE MEETING.

The Joint Army-Navy Committee Meeting was postponed until Wednesday, 27 September.

CCM CONFERENCE.

Lt. Comdr. Linn and Lt. Levit were aboard Monday, 18 September for conference with Lt. Clifford regarding the CCM. The conference was held in Commander Ford's conference room.

DAYTON COMPLEMENT.

Commander Foley, Lt. Comdr. Latta, and various people in GR have been heckling us for exact information in regard to what is going on in the way of the assignment of the Wave complement in Dayton. Andy felt that the matter should be straightened out with a memo to all concerned and has a tentative draft prepared along this line for your approval.

ENSIGN NILES ABOARD.

A new engineering officer, Ensign Niles, reported aboard and was assigned to GJ. He has had no particular radio experience, but has worked on electronics and has evidently held some responsible jobs, including design of equipment for a power company and electronic demonstration equipment for his Alma Mater, Notre Dame.

STATISTICAL BOMBE.

Lt. Clifford's letter to Eachus last week included a rather complete write-up as to what we were trying to do in the way of a statistical bombe. I asked Commander Roeder about this in regard to whether it should be revealed in a more or less official channel at this time, and Commander Roeder said simply, "why not omit it this time and wait until Commander Engstrom returns". I told this to Lt. Clifford and he was very annoyed because Commander Roeder presumed to censor his letters to Joe. He said that if it kept up, he would write Joe directly. I believe that I calmed him down on this and told him that it was my fault that the item was omitted this time and explained that the policy top-side was very indefinite in regard to revealing new matters and therefore we had to be rather careful about it. He saw the point of this but I perhaps was a bit over-cautious in regard to this particular item.

PHOTO RADIO MOVE.

Lt. Norris received a chit from Commander Cross which stated that Commander Arps, evidently without consulting us, had instructed the Bureau of Ships to move the photo-radio set-up from Skaggs Island to San Francisco. Lt. Norris evidently feels the matter should wait until Commander Wenger returns.

SECRET

S E C R E T

STATISTICAL BOMBE.

We are still pushing ahead on means for obtaining a statistical bombe. Lt. (jg) Orem is drafting a letter to the GE representative here for someone's signature here which would declare our interest in Selsyn motors and would state what priority we intended to use to back such an item. Evidently the Army Signal Corps has about 9,000 sets being manufactured which would suit our needs to a tee. Perhaps we can hook onto one of these sets. We are also working strongly on a dudbuster application on Granddad. We are now in the process of weighting jackpot and random tries and Pete Deffert will sum and tabulate a series of these tries for us on I.B.M. equipment.

MOVE OF WARNER'S EQUIPMENT.

Equipment on the stage and in the room below are being moved today, Thursday, 21 September 1944. There was considerable feeling that Tetra "Tessie" should be moved at this time, not only to take advantage of the trucks available, but also to make room for a dark room for Wilson. I vetoed this suggestion, said I felt that moving of the photographic equipment should wait until we have more stable plans along this line. It may be quite difficult to move Tetra "Tessie" because at the time it was moved in there were no permanent bulkheads in the passageway in the old gymnasium leading into the school building.

YOUNG ENGINEERING OFFICERS.

Lt. Norris says that some of the officers that have been assigned to him have not exhibited any great degree of imagination in their work. He feels that they might be better fitted for maintenance. Perhaps they are just washouts. Blakely has quite a few officers on ice; perhaps now is the time to consider a shift around of these officers to more permanent duty. As I remember, Meader was supposed to get some of these officers; perhaps his needs should be considered also at this time. Meader feels that Palmer is way and above most of the other officers from a research standpoint. Perhaps Meader might be agreeable to have Palmer come here and take charge of the research and development and also the laboratory if Rowley goes on field work. This appeals to me very much as a solution to a number of our problems, particularly if the Navy is perhaps being squeezed out of the research work at the National Cash Register Co. I believe that Palmer would be able to hold his own on this job with respect to both Steinhardt and Blakely's group.

S E C R E T

SECRET

HAGELIN JOB FOR ARMY.

Captain Seaman brought over a 2700 character tape and asked if we could run six (6) stripping jobs on MIKE for the Army. We did this for him on one midwatch and the results (Hagelin) have been sent over. He said that the man in charge of this job was very interested in MIKE and that this was a test run to see how effective MIKE was on this type of work in comparison with I.B.M. methods which I understand takes several days to do.

VIPER BANKS FOR ARMY.

You will perhaps remember that you told Colonel Rowlett you would find out what we had available in the way of thirty (30) VIPER stepping switches that he might use in the construction of two (2) Purple machines. Perhaps you might want to take this up with Meader while he is here.

MAMBA.

Lt. Comdr. Meader reports that he became very annoyed with the slow progress on MAMBA at the Acme Pattern and Tool Company. He went over there a week ago and told them that they were laying down on the job since they had all detail drawings done, He wanted every part in the process of manufacture simultaneously in their place. He assigned Bateman for a half-day duty each day at Acme to expedite MAMBA. He feels that MAMBA will still not be available for from six to eight weeks. This is too bad in view of the feeling in GY-P that MAMBA should have been done long ago and their apparent strong desire to break into the type of JN-25 traffic that uses key additives in the indicator system.

CHINESE DIPLOMATIC TRAFFIC.

Commander Holdwick called me in to see who was working on Chinese diplomatic traffic. I found that you had given the job to Bill Wray and that Bill had only the original set of messages and under your instructions had more or less secured interest until further traffic occurred. Bill Wray and I went to see Commander Holdwick and Commander Wright and they were evidently interested in doing something about this. They are of the impression that a third large folder is available somewhere and I believe they are trying to track it down. Bill Wray can tell you more of the details in regard to this matter.

S E C R E T

SECRET

NATIONAL CASH REGISTER OFFICIALS ABOARD.

Mr. Allen and another official of the National Cash Register Company held a conference with Captain Kinney and Lt. Comdr. Meader on Thursday, 21 September 1944. The conference is going on as I write this so I don't know what is happening. I believe the subject under discussion is in regard to sending spare parts of Bombes here.

NAT BREAK.

The British got into the NAT traffic this month by the "X" method. The break they got was on a wheel motion that astounded Alexander in view of their work on the traffic on another day. We do not know yet whether Alexanders figures were wrong or that the motion changes frequently. Alexander and Gleason will continue with the post-mortem trial on it. Icky ran their first problem with a fair degree of success, but without finding the jackpot -- possibly because the wrong motion was assumed. Alexander says his + Andy's figures had a 2½ sigma bulge on the wrong wheel motion.

SEMI-AUTOMATIC PROGRAM.

The Captain saw the Admiral on Wednesday and then called Lt. Norris in to say that the Admiral wanted a complete review of this situation together with comparison between teletype and letterwriter semi-automatics. At Norris' request, I put Lt. Rowley on this job with Lt.(jg) Patterson to help. Today Commander Wright called and requested the original program for semi-automatics. I took him a copy of the memo I wrote you setting up the next year's order on I.B.M.

JADE RIP.

Lt. Comdr. Raven finished his RIP on the JADE and I signed for it. It is in your file.

WRITE-UP ON ENGSTROM FANS.

Ten (10) copies of a write-up on Engstrom Fans are in your file.

CONFERENCE ON WAVE PROPAGATION.

The following was received from the Wave Propagation Committee on which you might wish to take action: Plans are being made for third conference to be held at 9:30 A.M., 16 and 17 November 1944, in Auditorium, National Academy of Sciences, 2101 Constitution Ave., Washington, D. C. This notification asks that information be supplied as to who would attend and who might submit reports, etc.

T O P S E C R E T
OP-20-GE/mb

File CCM
+ Sub. Comm. on research

TOP SECRET

24 July 1944

MEMORANDUM

From: OP-20-GE
To: OP-20-G50

Subject: C.C.M., termination of researches on at Arlington Hall.

1. The technical Sub-committee of the Committee to investigate the security of the C.C.M. met for the last time at Arlington Hall on 22 July. The first meeting was on 1 May. The projects completed during this period are outlined below. Lt. Levit (OP-20-K) is continuing with a project of his own, and I shall maintain contact with him and Lt. Cmdr. Linn. The Army contingent is, however, securing. A report will be made shortly to the Committee.

2. The Sub-committee will make the following suggestions to the Committee:

(a) Rigid enforcement of the "legal limit" of 200 groups to a message.

(b) Change the indicator system to one not exhibiting monoalphabetic characteristics. Thus, under the present system, two messages in the same day with indicators LJCAQ and XTCRQ have the same initial setting of the 3- and 5-wheels.

(c) When the 3-wheel has a stepping contour on both sides, all wheels will turn ("lobster") one time in four. This may be remedied by avoiding oppositely placed contours in making up the wheels. Actually, OP-20-N has already made a set of "anti-lobster" wheels.

(d) It is unwise to simply rewire a compromised set of wheels, without changing the cam contours. In destroying wheels to prevent capture the cam contours must be obliterated as well as the wiring.

3. The projects leading to the above suggestions follow. Except in (c), it is assumed the enemy is in possession of a C.C.M. and the appropriate set of wheels.

(a) The wheel-order and setting of a 1000-group message (actually sent), with matched plain and cipher text, were found by means of lobsters. The same was accomplished with a

TOP SECRET

day's file of 250 messages all within the legal limit of 200 groups; to do this the indicators were used to line up messages to be in depth on the 3-wheel.

(b) From the one set message in (a), the daily indicator setting was found by an IBM sort. Thus, with known wheel order, a five-letter crib is easily set.

(c) Using the long message in (a), and assuming the stepping pattern, which can be found from the lobsters, the wiring was recovered.

(d) Two 200-group messages were enciphered with all but the 5-wheel in depth, and having a 7-letter plain text coincidence between them. Using the cipher text only, the wheel order and settings were found, and the messages read. The technique used was statistical, and a machine similar to Hypo could handle it. Without the 7-letter coincidence, however, the number of trials would be about 2½ billion, and there is some doubt whether the right answer would stand out.

4. Lt. Levit's project is to find the wheel-order and setting of a single message of 300 groups, using the period of 338 on the center three wheels and the constant precession of the end wheels. (These were also used in project 3 (c) above). His method becomes unworkable at the legal limit of 200 groups, and consequently no recommendation is contemplated at the present time to avoid the center cycle of 338.

5. Needless to say, consideration of "bad" wheels, which produce a short cycle, was excluded.

6. I believe that the results of paragraph 3 show that, unless the suggestions of paragraph 2 are adopted, there is a small but non-negligible chance that the enemy (having captured a C.C.M. and wheels) might read an occasional day. The use of the C.C.M. for Ultra dispatches of the bean-spilling variety would then plainly be unwise. On the other hand, it is noteworthy that none of us thought of an operationally feasible method, whereby the enemy could read more than a scattered day here and there. The difficulties are:

(a) close to a million wheel-orders;
(b) erratic stepping of the end wheels, the one regularly stepping wheel being well buried;
(c) no discoverable test on whether a stretch of plain and cipher text is properly aligned (such as by crashing on enigma). Because of (a), bombing is out of the question, and because of (b) it is hard

to see how to strip off wheels one by one. I feel that the designers of the C.C.M. did a very good piece of work.

Respectfully submitted,

A. H. Clifford.

A. H. Clifford,
Lt. U.S.N.R.

OP-20-G/rh

TOP SECRET

17 July 1944

file GM
+ Letterwriter.
cc: CCM

MEMORANDUM

From: OP-20-GY-A
To: OP-20-GM
Via: OP-20-G-50

Subj: CCM, Installation of Page Printer in Circuit of.

1. Confirming telephone conversation of this morning, it is requested that there be inserted into the circuit of the CCM used in this Section for traffic with the British a page printer to permit outgoing and incoming traffic to be placed in final form immediately upon decryption.

R. B. ELY
LT. CDR., USNR

Conference - Ely, Chalaux and Howard - decided for the present to not try this because of technical difficulties - Chalaux was to find out if carbon paper rolls could be found for CCM.

~~XXXXX~~.
C.C.M.X

CROSS INDEX

Date: 24 June 1943

From: Prof. Bayly

To: Captain Stone

Subject: Modifying request of 5 Jan.
Request equipment for use with CCM Machine

Filed Under: BRITISH PROCUREMENT

S E C R E T
OP-20-GE/mb

File

17 May 1944

SECRET

MEMORANDUM

From : OP-20-GE
To : OP-20-G50

Subject : Cross-tie In C.C.M. from 1-Wheel To 4-Wheel.

Enclosure: (A) Secret Monograph entitled "Effect of Cross-tie on Period of C.C.M."

1. On 4 May 1944 a modified C.C.M. basket, with a cross-tie from the 1-wheel to the 4-wheel, was delivered to this office. This device causes the 4-wheel to step when an indent comes up either on the left side of the 1-wheel or on the right side of the 3-wheel. Enclosure (A) represents our analysis of the effect of this device upon the period of the 4-wheel, and hence upon that of the middle three wheels and the machine as a whole.

2. In the unmodified machine, the period of the 4-wheel is 338. With the cross-tie, and using normal wheels, this period is never 338, but is either 4394 or 57122, depending upon the choice of the 2- and 3-wheels, and is the larger of these for at least 90% of the wheel choices. The period of 338 of the middle three wheels is thus completely destroyed, and the period of 4394 of the whole machine is stepped up to 57122 at least 90% of the time, not considering the behavior of the 5-wheel. We feel, therefore, that the cross-tie admirably disposes of the weakness of the C.C.M. due to the period of 338 on the middle three wheels, when normal wheels are used.

3. If defective wheels are allowed, the 4-wheel may, for a given wheel order, have periods of 338, 676, 4394, or 8788, depending on the initial setting. Although the two larger values hold on the average for at least 90% of the settings, the fact remains that there is a chance of up to 10% that a long message will hit a short cycle. In this event the 5-wheel will at best precess a fixed amount every 338 steps, and this situation may be as bad as true depth. It is our opinion, therefore, that the use of the cross-tie with defective wheels will greatly reduce the risk, but that since it is not reduced to zero such use cannot be classed as "secure".

Respectfully submitted,

Alfred H. Clifford.

Alfred H. Clifford
Lt., U.S.N.R.

SECRET

S E C R E T
GM-E/mb

SECRET

EFFECT OF CROSS-TIE ON PERIOD OF C.C.M. 16 MAY 1944

1. Summary of Results

The device under consideration is a tie from the left side of the 1-wheel to the 4-wheel, so that the latter will step if there is an indent either on the right side of the 3-wheel (as usual) or on the left side of the 1-wheel. Its effect is considered with relation to the following three facts concerning the C.C.M. when all wheels have an even number of indents.

(1) The period of the middle three wheels is 338.
(2) The period of the whole machine is normally 4394.
(3) When "defective" wheels are used, the period of the whole machine may be only 338.

Thus the setting AAAAA will become say KAAAS after 338 steps, the two end wheels precessing a constant amount, always even (here 10 and 18 respectively), and thus returning to their initial positions after 13 x 338 = 4394 steps.

The cross-tie will evidently have no effect upon the 1-, 2-, and 3-wheels. We consider only its effect upon the 4-wheel. The behavior of the 5-wheel would require much deeper analysis.

If the cross-tie is used with normal wheels, it is found that the 4-wheel can never have a period of 338. It does, however, have what we might call a "statistical period" in the sense that there is a certain probability, ranging up to about one chance in fifteen, that it will have the same setting in any two particular machine positions 338 steps apart. Since this probability is so low, we are justified in saying that the cross-tie effectively breaks up the period of the middle three wheels. The same is true if the right side of the 3-wheel is defective, and consequently any short cycle on the 3-, 4-, and 5-wheels is destroyed.

The effect is somewhat different if the short cycle occurs on the 1-, 2-, and 3-wheels. In this case, for a given wheel order, certain initial settings may produce a short cycle even with the cross-tie in operation. The 26^3 settings of these three wheels fall into 52 distinct cycles of length 338. One expects three or four of these to be "bad", producing a cycle of 338 on the 4-wheel, and hence on all except possibly the 5-wheel. In a "good" cycle, the 4-wheel can <u>never</u> return to its initial setting after 338 steps.

Using the cross-tie with normal wheels, the 4-wheel precesses a certain even amount d after 4394 steps. This amount is zero if the left side of the 1-wheel has the even-odd defect, in which case there exists a period of 4394 on all except possibly the 5-wheel. If, however, the left side of the 1-wheel is normal, the question of whether or not d = o depends wholly on the 2- and 3-wheels. It would be practicable to find it out experimentally for the 20 x 18 = 360 possible choices for these two wheels, in a set of ten wheels, but no simple criterion is apparent. The proportion of "bad" choices appears to be the random 1 in 13. When d = o, the period of the first four wheels is 13 x 4394 = 57122.

When defective wheels are used, and a short cycle exists on the 1-, 2-, and 3-wheels, then in a "good" cycle the 4-wheel precesses a certain amount d, not zero and possibly odd, every 338 steps. Consequently the first four wheels will have a cycle of 4394 or 8788 or 676, depending on whether d is even, odd and not 13, or 13. The number of these various cases, including the number of "bad" cycles for which d = o, is easily found for a given wheel order. With say, four defective wheels in a set of ten, they could be tabulated for the 4 x 12 x 10 = 480 possible choices of the 1-, 2-, and 3-wheels. In the examples, fictitious indent patterns are used.

For convenience, we assume throughout that when a wheel steps forward, the letters indicating its setting increase alphabetically.

2. Effect of Cross-ties at Intervals of 338.

Without the cross-tie, the 4-wheel returns to its initial setting after 338 steps. With the cross-tie, the 4-wheel will receive a certain number of "extra boosts" from the 1-wheel when the right side of the 3-wheel is in an inactive position. To find the displacement of the 4-wheel after 338 steps, we need only count the number of these "extra boosts" that it has received.

In Figure 1, assumming the indent patterns for the left side of the 2- and 3-wheels as shown, 338 successive settings of the 1-, 2-, and 3-wheels are given, starting at AAA. Those of the 3-wheel are the normal alphabet, repeated for each column, and are omitted. The 339th position would be YAA, and the next 338 settings differ from those shown in Figure 1 only in that the 1-wheel is two steps behind (Y instead of A, Z instead of B, A instead of C, etc., throughout).

In Figure 2, indent patterns are assumed for the left side of the 1-wheel and the right side of the 3-wheel. The 3-wheel is in the inactive setting E just 13 times during this block of 338 steps, and reference to Figure 1 shows that the 1-wheel

is at these times in the settings

B O Z L C K U C Q I T D O

Of these, the settings D, L, O, Q, and T (underlined) are active positions of the 1-wheel, and the rest are inactive. Consequently the 4-wheel receives six extra boosts while the 3-wheel is in setting E. By adding up the boosts for all the inactive positions (E, F, I, J, N, Q, S, T, X, and Z) of the 3-wheel, we find the desired displacement of the 4-wheel after the 338 steps shown in Figure 1. For this purpose a frequency count is made of the 10 x 13 = 130 letters (settings of the 1-wheel) in these rows of Figure 1. The result given in Figure 2. One extracts from this count the active settings of the 1-wheel:

A	4
D	4
G	4
H	2
L	4
O	10
P	3
Q	3
T	7
X	3
	44

Since the total is 44, the 4-wheel has received 44 extra boosts in these 338 steps. If it starts at A it will end at A + 44 = A + 18 = S.

If we started at position ZAA-- instead of AAA-- in Figure 1, every letter giving a setting of the 1-wheel is diminished by one alphabetically. If we made a new frequency count for the rows in which the 3-wheel is inactive, we would find as many A's as formerly there were B's, as many D's as formerly there were E's, etc. Hence we can find the number of extra boosts as the sum of the original frequencies of B, D, H, I, etc. These are entered in Figure 2 in the column headed Z, and the total is 41.

Since, in the example, the 1-wheel moves from A to Y in 338 steps, then to W, etc., the position of the 4-wheel is found from the upper line of totals (44, 56, 44, 49, etc.) in Figure 2. The successive positions of the 4-wheel after each batch of 338 are therefore as follows:

A + 44 = A + 18 = S
S + 56 = S + 4 = W
W + 44 = W - 8 = O
O + 49 = O - 3 = L
L + 55 = L + 3 = O

0	+ 39 =	0	- 13 =	B
B	+ 55 =	B	+ 3 =	E
E	+ 52 =	E	+ 0 =	E
E	+ 51 =	E	- 1 =	D
D	+ 40 =	D	+ 14 =	R
R	+ 54 =	R	+ 2 =	T
T	+ 52 =	T	+ 0 =	T
T	+ 49 =	T	- 3 =	Q

Twice in the above 13 times the 4- wheel returned to its starting point (E and T respectively) but there is no evidence of a period. Figure 3 indicates the absence of a period a little better. Here the settings of all but the 5-wheel are given for the first 31 positions of successive batches of 338 steps. Active positions of the left side of the 1-wheel and the right side of the 3-wheel are indicated by arrows. Of the 62 comparisons made here, between a given position and that 338 steps later, just 4 have the middle three wheels in the same position (IUK, IVL, JWM, and JXN). These are all in a lump, comprising "Zone 8". A zone is a stretch of active positions of the 3-wheel. Within a zone, the displacement of the 4-wheel is the same. If one begins at CDF-- instead of AAA-- in Figure 1, the frequency count is altered only in that one Z is added and one B is removed. Beginning anywhere in Zone 2 (CDG, CDH, or CEI), one adds an A and removes a C, in addition to the above Z - B exchange. Proceeding thus from zone to zone, we get the frequency changes noted in Figure 2. Increases or decreases in the resulting totals are shown by +'s and -'s. Places where the total equals 52 are encircled. Considering the width of the zones, there are 44 such repetitions in 676 comparisons, as seen in the following tabulation:

ZONE	WIDTH	NO. 52's	TOTAL 52's
0	5	3	15
1	1	1	1
2	3	3	9
3	1	0	0
4	4	0	0
5	3	0	0
6	2	0	0
7	1	1	1
8	4	3	12
9	2	3	6
			44

From the manner in which the totals change it is clear that a true period of 338 could exist for the 4-wheel only in the absurdly trivial case in which the 1-wheel had an indent in every other position. The example chosen indicates 44 chances out of 676, or 1 chance in 15.4, of the 4-wheel being in the same setting at two positions 338 steps apart. Considering the selection of 10 letters of the frequency count as a random matter, the probability that the total thereof is 52 is

$$ {}_{130}C_{52} \left(\frac{10}{26}\right)^{52} \left(\frac{16}{26}\right)^{78} = \frac{1}{14.95} $$

or very close to 1 in 15. Here the mean sum is 5 x 10 = 50. With 12 inactive places on the 3-wheel, it would be 5 x 12 = 60, and the probability of hitting 52 (or 78) considerably less.

3. Effect of Cross-tie at Intervals of 4394.

To see what happens to the 4-wheel after the normal cycle of 4394 steps when the cross-tie is introduced, we observe that it will be advanced by an amount equal to the sum of every other column of Figure 2 (44 + 56 + 44 + 49 + .. or 41 + 67 + 44 + 44 + ..). In general terms, let k be the number of notches on the right side of the 3-wheel, so that 26 - k is the number of inactive places. Then the total of the frequency count (130 in Figure 2) is 13 (26 - k) = N, and N is divisible by 26 since k is even for the type of wheels we are considering. Let N_e and N_o be the totals of the even and odd terms; in the example

$$N_e = 7 + 4 + 2 + \ldots = 60$$
$$N_o = 4 + 11 + 3 + \ldots = 70$$

Let a be the number of indents on the left side of the 1- wheel in the even positions, and b the number in the odd positions. In the example

$$a = 6 \quad (D, H, L, P, T, X)$$
$$b = 4 \quad (A, G, O, Q)$$

Then the desired total is

$$aN_e + bN_o \equiv (a-b)N_e + bN \equiv (a-b)N_e \pmod{26}$$

In the example, $(a-b)N_e = 2 \times 60 = 120 \equiv 16 \pmod{26}$. Thus A will change to A + 16 = Q after 4394 steps, as already noted above. If one started at BAAA- instead, one would get the negative (mod.26) of this.

If the left side of the 1-wheel has the odd-even defect, namely a = b, then the 4-wheel will always return to its initial position after 4394 steps. In the contrary case, it depends on whether or not N_e is divisible by 26, or actually by 13, since a - b is even. This number N_e depends only on the indent patterns of the wheels, and not on the initial setting. For the 1-, 2-, and 3-wheels still have the period of 4394. Or, viewed otherwise, the successive changes in the frequency count consist always of adding one even letter and taking another away, or adding one odd letter and removing another odd letter. N_e could be found experimentally for each of the 360 = 20 x 18 choices of 2- and 3-wheels, in a set of 10 wheels, but no

a priori way of avoiding its being divisible by 13 is apparent.

If N_e is not divisible by 13, then the 3-wheel evidently precesses the amount $(a-b)N_e$ every 4394 steps, coming back to its original setting only after 13 x 4394 steps.

4. Effect of Cross-tie When Short Cycle Exists.

In Figure 4, one indent on the left face of the 2-wheel has been changed (Z to W) in order to produce a short cycle. In Figure 5, the appropriate frequency count and totals are shown. In this case, since the 1-wheel returns to its initial setting after 338 steps, there are no changes to be made in the frequency count as we progress along the same cycle. In other words, we find that the 4-wheel gets 47 boosts in the 338 steps starting with AAA--, so that AAAA- will become AAAV-, and we see that the 4-wheel also gets 47 boosts if we start at CDF--, or anywhere else in the same cycle.

The 263 initial settings of the 1-, 2-, and 3-wheels break up into 52 cycles of length 338. For each of these cycles, the 4-wheel precesses a constant amount d every 338 steps, and d may have any value at all from 0 to 25. For the cycle starting AAA, d = 47 = - 5. In Figure 5 the totals give the values of d for each of the 26 cycles starting at AAA, BAA, ..., ZAA. The values of d for the other 26 cycles starting at ABA, BBA, ..., ZBA can be found similarly.

The expected proportion of "bad" cycles, with d = o, seems no different than the theoretical 1 in 15 occurring above, but will of course fluctuate widely from wheel order to wheel order. In the example, not a single bad cycle exists, at least for half of the 52 cycles.

The period of the 4-wheel will thus be 338, 676, 4394, or 8788, depending on whether d is o, 13, even, or prime to 26. Note the occurrence of d = 65 = 13 for the cycle starting GAA in the example.

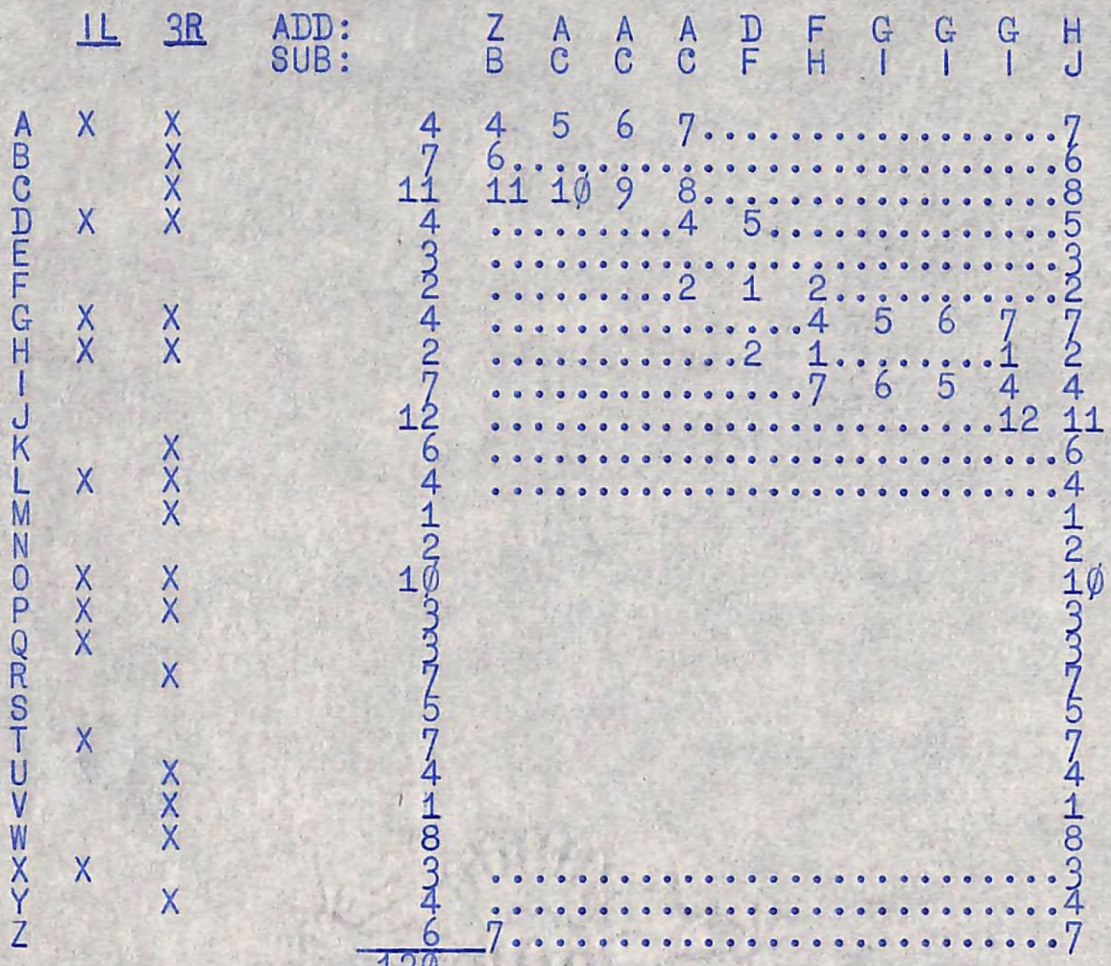
SECRET

FIG. 1 338 SUCCESSIVE POSITIONS OF 1- AND 2-WHEELS.

	2L	3L	12	12	12	12	12	12	12	12	12	12	12	12	12
A			AA	KK	VU	KE	ZO	JY	UI	BS	NC	FM	TW	CG	OQ
B	X		AA	LK	WU	KE	AO	JY	UI	BS	OC	GM	TW	CG	OQ
C	X	X	AA	MK	XU	KE	BO	JY	UI	BS	PC	HM	TW	CG	OQ
D		X	AB	NL	YV	KF	CP	JZ	UJ	BT	QD	IN	TX	CH	OR
E		X	BC	OM	ZW	LG	CQ	KA	UK	CU	QE	IO	TY	DI	OS
F	X		CD	PN	ZX	LH	CR	KB	VL	DV	QF	JP	TZ	DJ	OT
G			CD	PN	ZX	MH	CR	LB	WL	EV	RF	JP	UZ	DJ	PT
H	X	X	CD	PN	ZX	NH	CR	MB	XL	FV	SF	JP	VZ	DJ	QT
I			CE	PO	ZY	DI	CS	NC	YM	GW	TG	JQ	WA	DK	RU
J		X	CE	QO	ZY	OI	CS	OC	ZM	GW	TG	JQ	WA	EK	SU
K	X		CF	RP	ZZ	OJ	CT	PD	AN	GX	TH	JR	WB	FL	TV
L	X		DF	RP	AZ	OJ	DT	PD	AN	GX	UH	JR	XB	GL	UV
M	X	X	EF	RP	BZ	OJ	ET	PD	AN	GX	VH	JR	YB	HL	VV
N		X	FG	RQ	CA	OK	FU	PE	AO	GY	WI	JS	ZC	IM	WW
O	X		FH	RR	CB	PL	GV	PF	BP	GZ	WJ	JT	AD	JN	WX
P			GH	RR	DB	QL	HV	QF	BP	HZ	WJ	KT	AD	JN	WX
Q		X	HH	RR	EB	RL	IV	RF	BP	IZ	WJ	LT	AD	JN	WX
R			II	RS	FC	SM	JW	SG	BQ	JA	WK	MU	AE	JO	WY
S			II	RS	GC	TM	JW	SG	BQ	JA	XK	NU	AE	KO	WY
T	X		II	RS	HC	UM	JW	SG	BQ	JA	YK	OU	AE	LO	WY
U	X		II	RS	IC	VM	JW	SG	BQ	JA	ZK	PU	AE	MO	WY
V	X	X	II	RS	JC	WM	JW	SG	BQ	JA	AK	QU	AE	NO	WY
W			IJ	RT	KD	XN	JX	SH	BR	JB	BL	RV	AF	OP	WZ
X		X	IJ	ST	KD	XN	JX	TH	BR	KB	CL	SV	BF	OP	XZ
Y			IK	TU	KE	XO	JY	UI	BS	LC	DM	TW	CG	OQ	YA
Z	X		JK	UU	KE	YO	JY	UI	BS	MC	EM	TW	CG	OQ	YA

SECRET

FIG. 2 FREQUENCY & CHANGES



CONTINUED-

SECRET

FIG. 2 continued-

A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	
4	7	11	4	3	2	4	2	7	12	6	4	1	2	10	3	3	7	5	7	4	1	8	3	4	6	
4	3	2	4	2	7	12	6	4	1	2	10	3	3	7	5	7	4	1	8	3	4	6	4	7	11	
4	2	7	12	6	4	1	2	10	3	3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	
2	7	12	6	4	1	2	10	3	3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	4	
4	1	2	10	3	3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	4	2	7	12	6	
10	3	3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	4	2	7	12	6	4	1	2	
3	3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	4	2	7	12	6	4	1	2	10	
3	7	5	7	4	1	8	3	4	6	4	7	11	4	3	2	4	2	7	12	6	4	1	2	10	3	
7	4	1	8	3	4	6	4	7	11	4	3	2	4	2	7	12	6	4	4	2	10	3	3	7	5	
3	4	6	4	7	11	4	3	2	4	2	7	12	6	4	1	2	10	3	3	7	5	7	4	1	8	zone
44		56		44		49		55		39		55		(52)		51		40		54		(52)		49		) 0
	41		67		44		44		51		61		(52)		38		53		53		64		35		59	)
	-	+		-		+		-	⊕	+		-	-	+		-		+	+	-	-	+		-	+	1
+		-	+		-		+		-	+	+		-	⊖	+		⊖		+	+	-	⊖	+		-	2
+		-	+		-		+		-	+	+		-	-	+		-		+	+	-	-	+		-	3
+		-	+		-		+		-	+	+		-	-	+		-		+	+	-	-	+		-	4
+		-	+		-	+		-		+		-	+	+		-	-	+		-		+	+	-	-	5
-	-	+		-	+		-	+		-		+		-	+	+		-	-	+		-		+	+	6
+	-	-	+		-	⊕		-	+		-		+		-	+	+		-	-	+		-		+	+	7
+	-	⊖	+		-	+		⊖	+		-		+		-	⊕	+		-	-	+		-		+	+	8
+	-	-	+		-	+		-	⊕		-		⊕		-	+	⊕		-	-	+		-		+	+	9
+	+	-	-	+		-	+		-	+		-		+		⊖	+	+		⊖	-	+		-		) 10
51		50		43		53		51		44		53		51		52		42		52		58		47		)
	37		73		38		47		51		61		52		39		53		53		62		36		58	)

SECRET

FIG. 3

SECRET

FIG. 4

	2L	3L	12	12	12	12	12	12	12	12	12	12	12	12	12
A			AA	KK	VU	IE	XO	MY	WI	DS	OC	GM	WW	FG	RQ
B	X		AA	LK	WU	IE	YO	MY	WI	DS	PC	HM	XW	FG	RQ
C	X	X	AA	MK	XU	IE	ZO	MY	WI	DS	QC	IM	YW	FG	RQ
D		X	AB	NL	YV	IF	AP	MZ	WJ	DT	RD	JN	ZX	FH	RR
E		X	BC	OM	ZW	JG	AQ	MA	WK	EU	RE	JO	ZY	GI	RS
F	X		CD	PN	AX	JH	AR	MB	XL	FV	RF	KP	ZZ	GJ	RT
G			CD	PN	AX	KH	AR	NB	YL	GV	SF	KP	ZZ	GJ	ST
H	X	X	CD	PN	AX	LH	AR	OB	ZL	HV	TF	KP	ZZ	GJ	TT
I			CE	PO	AY	MI	AS	PC	AM	IW	UG	KQ	ZA	GK	UU
J		X	CE	QO	AY	MI	AS	QC	BM	JW	UG	KQ	ZA	HK	VU
K	X		CF	RP	AZ	MJ	AT	RD	CN	KX	UH	KR	ZB	IL	WV
L	X		DF	RP	AZ	MJ	BT	RD	CN	KX	VH	KR	AB	JL	XV
M	X	X	EF	RP	AZ	MJ	CT	RD	CN	KX	WH	KR	BB	KL	YV
N		X	FG	RQ	AA	MK	DU	RE	CO	KY	XI	KS	CC	LM	ZW
O	X		FH	RR	AB	NL	EV	RF	DP	KZ	XJ	KT	DD	MN	AX
P			GH	RR	BB	OL	FV	SF	DP	KZ	XJ	LT	DD	MN	AX
Q		X	HH	RR	CB	PL	GV	TF	DP	KZ	XJ	MT	DD	MN	AX
R			II	RS	DC	QM	HW	UG	DQ	KA	XK	NU	DE	MO	AY
S			II	RS	EC	RM	IW	UG	DQ	KA	YK	OU	DE	NO	AY
T	X		II	RS	FC	SM	JW	UG	DQ	KA	ZK	PU	DE	OO	AY
U	X		II	RS	GC	TM	KW	UG	DQ	KA	AK	QU	DE	PO	AY
V	X	X	II	RS	HC	UM	LW	UG	DQ	KA	BK	RU	DE	QO	AY
W	X		IJ	RT	ID	VN	MX	UH	DR	KB	CL	SV	DF	RP	AZ
X		X	IJ	ST	ID	VN	MX	VH	DR	LB	DL	TV	EF	RP	AZ
Y			IK	TU	IE	VO	MY	WI	DS	MC	EM	UW	FG	RQ	AA
Z			JK	UU	IE	WO	MY	WI	DS	NC	FM	VW	FG	RQ	AA

SECRET

FIG. 5

		A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
A	14																											
B	2																											
C	6	14	2	6	10	3	5	4	2	7	6	8	2	9	2	3	5	2	12	2	2	6	4	3	3	1	7
D	10	10	3	5	4	2	7	6	8	2	9	2	3	5	2	12	2	2	6	4	3	3	1	7	14	2	6
E	3	4	2	7	6	8	2	9	2	3	5	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5
F	5	2	7	6	8	2	9	2	3	5	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5	4
G	4	2	9	2	3	5	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5	4	2	7	6	8
[redacted]	2	3	5	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5	4	2	7	6	8	2	9	2
I	7	5	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5	4	2	7	6	8	2	9	2	3
J	6	2	12	2	2	6	4	3	3	1	7	14	2	6	10	3	5	4	2	7	6	8	2	9	2	3	5
K	8	2	6	4	3	3	1	7	14	2	6	10	3	5	4	2	7	6	8	2	9	2	3	5	2	12	2
L	2	3	1	7	14	2	6	10	3	5	4	2	7	6	8	2	9	2	3	5	2	12	2	2	6	4	3
M	9	47		53		35		63		33		62		54		55		32		44		65		54		47	
N	2		49		64		44		44		49		55		43		62		50		55		38		58		45
O	3																										
P	5																										
Q	2																										
R	12																										
S	2																										
T	2																										
U	6																										
V	4																										
W	3																										
X	3																										
[redacted]	1																										
Z	7																										
	130																										

Op-20-G/jac

File

TOP SECRET

2 May 1944

TOP SECRET

MEMORANDUM FOR Op-20-K

Subj: C.C.M. - Security of.

Encls: (A) Secret memo entitled, "Analysis of C.C.M. Keys."
(B) Secret memo entitled, "The Period of the C.C.M.," dated 17 Apr 1944.

1. Informal experiments on the length of cycle of the C.C.M. were undertaken in the spring of 1943 at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio. It was observed that a cycle of 338 positions might occur. Because of this possibility, the length of messages between the Laboratory and this Division was restricted to 100 groups on 4 June 1943.

2. A systematic study of the period of the C.C.M. was undertaken by Op-20-GM on 16 January 1944. In addition to the short cycle of 338 already observed, a more frequent "partial" short cycle of 338 was noted in which four of the five wheels returned to their original setting after 338 steps. The key for each new day was tested for short cycle as part of the daily "25 to 30" test.

3. The existence of a short cycle depends only on the wheel order used, and not on the original setting of the wheels. It is therefore effective for a full day at a time, and every message on that day will begin to lap itself after 338 letters. Enclosure (A) lists the days between 12 February 1944 and 20 April 1944 on which the short cycle existed.

4. Early in February 1944, Mr. C. H. O'D. Alexander of the British G.C. & C.S., then a visitor at Op-20-G, was informed of the frequent occurrence of the short cycle. Mr. Alexander heads the section of G.C. & C.S. which is the principal user of the C.C.M. circuit between G.C. & C.S. and Op-20-G. Because of the high security value of this circuit, it was considered of paramount importance that he be informed. He immediately signalled his office to limit messages to 70 groups.

5. An interrupter procedure was agreed upon with G.C. & C.S. on 24 March 1944. A group of five (5) Q's sent in the clear is the signal to alter the setting according to a prearranged scheme. Since this was to be done not less often than every fifty (50) groups, it was considered safe to send messages up to 200 groups, and this limit was agreed upon by dispatch.

Op-20-G/jac

TOP SECRET

TOP SECRET

Subj: C.C.M. - Security of.

6. During the months of February, March, and April 1944, G.C. & C.S. has been kept informed by dispatch when the following day's keys produced a short cycle.

7. The mechanical cause of the difficulty was found and is described in enclosure (B). It is a simple matter to arrange the stepping contacts on the wheels so as to avoid the difficulty entirely. Pending mechanical alterations, it is also possible to avoid the short cycle by tabooing certain wheel orders. With these precautions taken, the cycle is always 4394 letters.

8. Mr. Alexander remarked that the "partial" short cycle can be just as risky as the "true" one. He took an actual message of about 1000 letters, which thus lapped itself in "quasi-depth" three times, together with the plain text, and showed that one could make a beginning on recovery of the wheel wiring.

9. No further work has been done on the C.C.M. at Op-20-G, and none is being done at the present time. Comdr. Reed has advised us that the contours in question were supplied by one of the British representatives at Op-20-G, working temporarily in the Cryptographic Security Section (Op-20-K-1.). Investigation has failed to reveal the identity of this individual.

J. N. Wenger
Commander, U.S.N.

TOP SECRET

ANALYSIS OF CCM KEYS

Case A: All wheels except right-hand wheel return to starting point after 338 steps. (Short cycle to left.)

Case B: All wheels except left-hand wheel return to starting point after 338 steps. (Short cycle on right.)

Case AB. All wheels return to starting point after 338 steps. (Short cycle.)

These cases occurred on the following dates:

Case A	Case B	Case AB
Feb. 13, 16, 19, 22, 26, 27.	Feb. 12, 17, 18, 19, 24, 28.	Feb. 19.
Mar. 3, 8, 10, 11, 15, 16, 21, 22, 24, 27, 29.	Mar. 1, 2, 7, 10, 12, 14, 19, 20, 24, 26, 30.	Mar. 10, 24.
Apr. 3, 4, 5, 8, 9, 13, 17, 20.	Apr. 2, 3, 4, 7, 9, 11, 12, 13, 18, 19.	Apr. 3, 4, 9, 13.

In case A, it will be seen from consultation of CSP 1842(B) that key gives either

81R, 88, 89 (List A 1)

in middle or

80, 82R, 83, 87, 88 (List A 2)

on left. In case B it will be seen that the key gives either

81, 88R, 89R (List B 1)

on middle or

80R, 82, 83R, 87R, 88R (List B 2)

on right. Each case under AB involves either an A2 on left with B1 in middle or B2 on right or else B2 on right with A1 in middle or A2 on left.

ENCLOSURE (A)

TOP SECRET

THE PERIOD OF THE CCM

The CCM has five wheels of which the center steps every time, and the others irregularly.

Designating the wheels by 1,2,3,4,5, in order, the 3 wheel steps continually, the 2 and 4 wheels stepping is under control of the 3 wheel, and the 1 and 5 wheels step under the the influence of the 2 and 4 wheels respectively.

Since the stepping of the 4 and 5 wheels is similar (differing only in the notches) to the stepping of the 2 and 1 wheels, we need only discuss the motion of the 3-4-5 system.

Let there be k notches on the 3 wheel which induce the motion of the 4 wheel.

CASE I. k is relatively prime to 26.
After the 3 wheel has revolved 26 times, each of the k notches has stepped the 4 wheel 26 times. Hence the 4 wheel has stepped 26k times or k complete revolutions.

When the 4 wheel comes to the A position under the influence of (say) the 1st notch of the 3 wheel it stays until the 2nd notch of the 3 wheel moves it on to B position. The time elapsed in the A position is the interval on the 3 wheel between the first and second notches. During the cycle the A position is attained under the action of each of the k notches, and the total time elapsed in the A position is the sum of the intervals on the 3 wheel between the first and second notches, the second and third notches, the (k-1)st and kth notches and the kth and 1st notches. This sum is clearly once around the wheel or 26.

By a similar argument each position of the 4 wheel is up 26 times during the cycle. Hence the 5 wheel has been kicked 26 times by each notch of the 4 wheel and hence has turned an integral number of times.

This shows that under the hypothesis k-relatively prime to 26, (where k is the number of notches on the center wheel) the period is 676.

CASE II. k is an even number, 2m.
After 13 revolutions of the 3 wheel, the 4 wheel has advanced 13 x 2m = 26m positions or m complete revolutions.

ENCLOSURE (B)

TOP SECRET

THE PERIOD OF THE CCM (Continued)

As before, if the A position of the 4 wheel is caused by the 1st notch of the 3 wheel, the A position remains for an interval equal to the interval between 1st and 2nd notches of the 3 wheel. During the 13 revolutions of the 3 wheel, the A position of the 4 wheel comes up m times under the influence (in some order) of the 1st, 3rd, 5th, (2m-1)st notches of the 3 wheel and the total time elapsed in the A position is the sum of the intervals on the 3 wheel between the 1st and 2nd notches, the 3rd and 4th notches, the 5th and 6th notches, ..., and the (2m-1)st and 2m th notches. Let this sum be q. The B position of the 4 wheel comes up from the 2nd, 4th, 2m th notches of the 3 wheel, and the total elapsed times the sum of the interval between the 2nd and 3rd notches, the 4th and 5th, ..., and the 2m th and 1st notches. This sum is 26-q. The C position comes up from notches 1, 3, 5, ... on the 3 wheel, and the total elapsed time is q. Thus the positions A,C,E, ..., Y have elapsed time q, and the positions B,D,F, ..., Z have elapsed time 26-q.

The total amount of kick received by the 5 wheel is

$$qr_1 + (26-q)r_2$$

where r_1 is the number of notches of the 4 wheel in positions A,C,E, ..., Y, and r_2 is the number of notches of the 4 wheel in positions B,D, ... Z.

The cycle of the whole 3-4-5 system depends on the factors common to $qr_1 + (26-q)\ r_2$ and 26.

The cycle is 338 if

$$qr_1 + (26-q)\ r_2 - o \pmod{26}$$

i.e.

$$q(r_1-r_2) = o \pmod{26}$$

Thus the cycle is short if

a) $r_1 = r_2$

b) $q = 13$ and $r_1 - r_2 = o \pmod 2$

Since all wheels have an even number of notches to prevent a short cycle occurring as in Case I, condition b) is simply $q = 13$.

Several wheels in the present set have been examined and several satisfy condition a). When such a wheel is in position 4 the cycle of the 3-4-5 system is 338. Similarly when such a wheel is in position 2 the cycle of the 3-2-1 system is 338 and the cycle of the whole machine is short.

If no wheels satisfy either a) or b) on either rim, then the minimum period would be 4394 letters.

T E N T A T I V E

S E C R E T

Op-20-G/ev (1 May 1944)

MEMORANDUM FOR Op-20-K:

Subj: C.C.M. - Security of.

Encls: (A) Secret Memo entitled, "Analysis of C.C.M. Keys".

(B) Secret Memo entitled, "The Period of the C.C.M.", dated 17 April 1944.

1. Informal experiments on the length of cycle of the C.C.M. were undertaken in the Spring of 1943 at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio. It was observed that a cycle of 338 positions might occur. Because of this possibility, the length of messages between the Laboratory and this Division were restricted to 100 groups on 4 June 1943.

2. A systematic study of the period of the C.C.M. was undertaken by Op-20-GM on 16 January 1944. In addition to the short cycle of 338 already observed, a more frequent "partial" short cycle of 338 was noted in which four of the five wheels returned to their original setting after 338 steps. The key for each new day was tested for short cycle as part of the daily "25 to 30" test.

3. The existence of a short cycle depends only on the wheel order used, and not on the original setting of the wheels. It is therefore effective for a full day at a time, and every message on that day will begin to lap itself after 338 letters. Enclosure (A) lists the days between 12 February 1944 and 20 April 1944 on which the short cycle existed.

4. Early in February 1944, Mr. C. H. O'D. Alexander of the British G.C.&C.S., then a visitor at Op-20-G, was informed of the frequent occurrence of the short cycle. Mr. Alexander heads the Section of G.C.&C.S. which is the principal user of the C.C.M. circuit between G.C.&C.S. and Op-20-G. Because of the high security value of this circuit, it was considered of paramount importance that he be informed. He immediately signalled his office to limit messages to 70 groups.

5. An interrupter procedure was agreed upon with G.C.&C.S. on 24 March 1944. A group of five (5) Q's sent in the clear is the signal to alter the setting according to a prearranged scheme. Since this was to be done not less often than every fifty (50) groups, it was considered safe to send messages up to 200 groups, and this limit was agreed upon by dispatch.

6. During the months of February, March and April 1944, G.C.&C.S. has been kept informed by dispatch when the following day's keys produced a short cycle.

7. The mechanical cause of the difficulty was found, and is described in Enclosure (B). It is a simple matter to arrange the stepping contacts on the wheels so as to avoid the difficulty entirely. Pending mechanical alterations, it is also possible to avoid the short cycle by tabooing certain wheel orders. With these precautions taken, the cycle is always 4394 letters.

8. Mr. Alexander remarked that the "partial" short cycle can be just as risky as the "true" one. He took an actual message of about 1000 letters, which thus lapped itself in "quasi-depth" three times, together with the plain text, and showed that one could make a beginning on recovery of the wheel wiring.

9. No further work has been done on the C.C.M. at Op-20-G, and none is being done at the present time.

MEMORANDUM FOR CAPTAIN KINNEY:

Captain Harper telephoned the following information:

Lieut. Clifford is to report on Monday morning, 1 May 1944, at 0800, or as near thereafter as practicable, to:

Captain J. G. MOAT, USA

Room 3 C 340 Arlington Hall

GLEBE 4300 -.Ext. 242.

Captain Harper says there is no direct bus service from the Navy Department to Arlington Hall. However, the Arnold buses (public transportation) run along "K" Street NW, and the one marked "Buckingham" will take him right by Arlington Hall.

MH

4-25-44
1115

Also report we were going to furnish Kaiser.

NAVY DEPARTMENT

OFFICE OF DIRECTOR NAVAL COMMUNICATIONS

GPO 4—5769

27 April, 1944

Memorandum for files:

Informed Capt. Kinney that report on C. C. M will be forthcoming in a fortnight. Capt. Harper already has the preliminary report from Lt. Gleason

Engstrom

STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO :

FROM : G-1

SUBJECT:

DATE: 27 April

Harper Bros has not received report we furnished him in connection light trucks

OP-20-G/rh

SECRET

21 April 1944

MEMORANDUM

From: GY-A-1
To: G-40

Via: GY-A

Subject: CCM, Properties of.

Enclosure: Analysis of CCM keys.

1. Enclosed analysis of CCM keys is forwarded in response to verbal request of 20 April. It is based on data collected between 12 February and 20 April while running routine daily tests on CCM key for following day.

W. R. Church
Lieut., USNR

CC - G-50

SECRET

ANALYSIS OF CCM KEYS

Case A: All wheels except right hand wheel return to starting point after 338 steps. (Short cycle to left)

Case B: All wheels except left hand wheel return to starting point after 338 steps. (Short cycle on right)

Case AB: All wheels return to starting point after 338 steps. (Short cycle)

These cases occurred on the following dates:

Case A	Case B	Case AB
Feb. 13, 16, 19, 22, 26, 27.	Feb. 12, 17, 18, 19, 24, 28	Feb. 19
Mar. 3, 8, 10, 11, 15, 16, 21, 22, 24, 27, 29.	Mar. 1, 2, 7, 10, 12, 14, 19, 20, 24, 26, 30.	Mar. 10, 24.
Apr. 3, 4, 5, 8, 9, 13, 17, 20.	Apr. 2, 3, 4, 7, 9, 11, 12, 13, 18, 19.	Apr. 3, 4, 9, 13.

In case A, it will be seen from consultation of CSP 1842(B) that key gives either

81R, 88, 89 (List A 1)

in middle or

80, 82R, 83, 87, 88 (List A 2)

on left. In case B it will be seen that the key gives either

81, 88R, 89R (List B 1)

on middle or

80R, 82, 83R, 87R, 88R (List B 2)

on right. Each case under AB involves either an A2 on left with B1 in middle or B2 on right or else B2 on right with A1 in middle or A2 on left.

CCM

CROSS INDEX

Date: 19 April 1944

From: Engstrom

To: Eachus (Station X)

Subject: Re process for running 2 CCM's in tandem

Filed Under: DESPATCHES

SECRET

SECRET

File C.C.M

17 April 1944

MEMORANDUM

From : Committee on CCM Research.
To : OP-20-G50.

Subject : Short Cycles in CCM.

Enclosure: A. Memorandum Entitled "The Period of the CCM." (3 copies).

1. In enclosure A two causes are found for the short cycle on the CCM. These causes can both be eliminated by simple precautions in making the wheel notches.

2. It is requested that this memorandum be brought to the attention of OP-20-S as soon as possible.

Respectfully submitted,

A Gleason

A. Gleason
Lt.(j.g.) U.S.N.R.

SECRET

SECRET

17 April 1944

File CCM

THE PERIOD OF THE CCM

The CCM has five wheels of which the center steps every time, and the others irregularly.

Designating the wheels by 1,2,3,4,5, in order, the 3 wheel steps continually, the 2 and 4 wheels stepping is under control of the 3 wheel, and the 1 and 5 wheels step under the influence of the 2 and 4 wheels respectively.

Since the stepping of the 4 and 5 wheels is similar (differing only in the notches) to the stepping of the 2 and 1 wheels, we need only discuss the motion of the 3-4-5 system.

Let there be k notches on the 3 wheel which induce the motion of the 4 wheel.

CASE I. k is relatively prime to 26.
After the 3 wheel has revolved 26 times, each of the k notches has stepped the 4 wheel 26 times. Hence the 4 wheel has stepped 26k times or k complete revolutions.

When the 4 wheel comes to the A position under the influence of (say) the 1st notch of the 3 wheel it stays until the 2nd notch of the 3 wheel moves it on to B position. The time elapsed in the A position is the interval on the 3 wheel between the first and second notches. During the cycle the A position is attained under the action of <u>each</u> of the k notches, and the total time elapsed in the A position is the sum of the intervals on the 3 wheel between the first and second notches, the second and third notches, the (k-1)st and kth notches and the kth and 1st notches. This sum is clearly once around the wheel or 26.

By a similar argument each position of the 4 wheel is up 26 times during the cycle. Hence the 5 wheel has been kicked 26 times by each notch of the 4 wheel and hence has turned an integral number of times.

This shows that under the hypothesis k-relatively prime to 26, (where k is the number of notches on the center wheel) the period is 676.

CASE II. k is an even number, 2m.
After 13 revolutions of the 3 wheel, the 4 wheel has advanced

13 x 2m = 26m positions or m complete revolutions.

As before, if the A position of the 4 wheel is caused by the 1st notch of the 3 wheel, the A position remains for an interval equal to the interval between 1st and 2nd notches of the 3 wheel. During the 13 revolutions of the 3 wheel, the A position of the 4 wheel comes up m times under the influence (in some order) of the 1st, 3rd, 5th, (2m-1)st notches of the 3 wheel and the total time elapsed in the A position is the sum of the intervals on the 3 wheel between the 1st and 2nd notches, the 3rd and 4th notches, the 5th and 6th notches, ..., and the (2m-1)st and 2m th notches. Let this sum be q. The B position of the 4 wheel comes up from the 2nd, 4th, 2m th notches of the 3 wheel, and the total elapsed times the sum of the interval between the 2nd and 3rd notches, the 4th and 5th, ..., and the 2m th and 1st notches. This sum is 26-q. The C position comes up from notches 1, 3, 5,... on the 3 wheel, and the total elapsed time is q. Thus the positions A,C,E,....,Y have elapsed time q, and the positions B,D,F,...,Z have elapsed time 26-q.

The total amount of kick received by the 5 wheel is

$$qr_1 + (26-q)r_2$$

where r_1 is the number of notches of the 4 wheel in positions A,C,E,....,Y, and r_2 is the number of notches of the 4 wheel in positions B,D,...Z.

The cycle of the whole 3-4-5 system depends on the factors common to $qr_1 + (26-q)\ r_2$ and 26.

The cycle is 338 if

$$qr_1 + (26-q)\ r_2 - o \pmod{26}$$

i.e.

$$q(r_1-r_2) = o \pmod{26}$$

Thus the cycle is short if

a) $r_1 = r_2$

b) $q = 13$ and $r_1-r_2 = o \pmod 2$

Since all wheels have an even number of notches to prevent a short cycle occurring as in Case I, condition b) is simply $q = 13$.

Several wheels in the present set have been examined and several satisfy condition a). When such a wheel is in position 4 the cycle of the 3-4-5 system is 338. Similarly when such a wheel is in position 2 the cycle of the 3-2-1 system is 338 and the cycle of the whole machine is short.

If no wheels satisfy either a) or b) on either rim, then the minimum period would be 4394 letters.

TOP SECRET
Op-20-G/ev

CCM

TOP SECRET

28 March 1944.

MEMORANDUM

Subj: Security of the C.C.M. - Project for Investigation of.

1. It is proposed to assign Lieutenant Commander F. A. Raven and Lieutenant (jg) A. M. Gleason to the problem of the investigation of the security of the C.C.M. These officers are to devote as much time as is consistent with their other duties to this investigation.

2. The investigation will take the following form:

(a) An investigation of the harm that may be done by the occurrence of anyone of the following circumstances:

(1) The availability of a long reencodement.

(2) The obtaining of a series of messages in depth.

(3) The knowledge of the existence of a highly frequent known crib.

(4) Any other cryptanalytic attack which may arise

3. It is requested that authority be granted for obtaining a C.C.M. machine for use on this project. Materials and personnel will be assigned to the project as necessary.

4. Reports on this project will be submitted via Op-20-GM.

H. T. ENGSTROM,
Op-20-GM.

STANDARD FORM NO.

File C&M

Office Memorandum · UNITED STATES GOVERNMENT

DATE: 15 March 1944

TO : GM

FROM : GM-F

SUBJECT: JORUT MACHINE AT DAYTON.

1. The special cipher machine at the Dayton end of the JORUT channel has not been serviced for maintenance since September, and is beginning to behave badly. At request of Lt. Cdr. Meader, I attempted to fix it during my last trip, but feel that it would be best to send out someone more familiar with the gear to look it over.

2. Especially bad are the E/D switch and the printing head which produces very indistinct letters.

Steinhardt

Lt. Alexander has requested two CCDs for Dayton, one to replace the old one and one to be used as a spare. HE 3/16

CCM

CROSS INDEX

Date: 23 March to 21 April 1944

From:

To: From Alexander To Church and vice-versa

Subject: No. of despatches re the security of the CCM

Filed Under: SECRET DESPATCHES

C.C.M.

CROSS INDEX

Date: 13 Mar 1944

From: Administrative Data

To:

Subject: re the discussion as to the question raised at conference with British concerning the desirability of placing a stecker on C.C.M.

Filed Under: ADMINISTRATIVE DATA

CCM

CROSS INDEX

Date: 19 Nov 1943

From: Lieut. Skinner

To: Lieut. Clifford Station X

Subject: Arrangements have been made to supply the terminal equipment for the varioplex line so that the semi-automatic CCM equipment can be effective

Filed Under: BRITISH PROCUREMENT

CCM WHEELS: STEPPING OF

WHEEL POSITIONS FROM LEFT TO RIGHT WILL BE REFERRED TO AS: 1 2 3 4 5

POSITION 3

WHEEL IN POSITION 3 STEPS ONE INTERVAL EACH TIME THEREBY RETURNING TO ITS ORIGINAL POSITION AFTER 26 TURNS. IT GOVERNS THE STEPPING OF WHEELS 2 & 4.

POSITIONS 2&4

WHEELS IN POSITIONS 2 & 4 STEP AN EVEN NUMBER OF INTERVALS IN DIRECT PROPORTION TO THE STEPPING IN WHEEL IN POSITION 3 (SAMPLE RATIO: 12:26:14), THEREBY RETURNING TO THEIR ORIGINAL POSITIONS AFTER 338, 676 ETC. TURNS (I.E. 13X26 26X26 ETC.). THESE WHEELS GOVERN THE STEPPING OF WHEELS 1 & 5, RESPECTIVELY.

POSITIONS 3&5

WHEELS IN POSITIONS 3&5 STEP AN ARBITRARY NUMBER OF INTERVALS, EACH IN DIRECT PROPORTION

TO THE STEPPING OF THE WHEEL NEXT TO IT (I.E. WHEEL 1 IS GOVERNED BY WHEEL 2 AND WHEEL 5 IS GOVERNED BY WHEEL 4). THE IRREGULAR CYCLE OF TURNS THROUGH WHICH WHEELS 1 & 5 PASS IS REPEATED AFTER 338 TURNS (OR WHEN THE 3RD WHEEL HAS MADE 13 CYCLES OF 26 TURNS). THE STEPPING OF WHEELS 1 & 2 HAS NO BEARING ON THAT OF WHEELS 4 & 5 AND VICE VERSA.

GENERAL CONCLUSIONS

1. AFTER 338, 676, ETC. TURNS WHEELS 2,3,&4 WILL HAVE RETURNED TO THEIR ORIGINAL POSITIONS
2. AFTER 338, ETC., WHEELS 1 & 5 MAY HAVE RETURNED TO THEIR ORIGINAL POSITIONS, ALTHOUGH THIS IS NOT NECESSARILY THE CASE.
3. THERE ARE, THEREFORE, THREE POSSIBLE TYPES OF SETTINGS AT 338, ETC: THOSE WITH ONLY WHEELS 2,3&4 IN THE ORIGINAL POSITION.

THOSE WITH WHEELS 1,2,3,&4 OR 2,3,4,&5 IN ORIGINAL POSITION.

THOSE WITH ALL FIVE WHEELS IN ORIGINAL POSITION.

4. THE ATTACHED SHEETS SHOW ACTUAL SETTINGS RUN THROUGH 676 LETTERS FOR A SERIES OF FIFTEEN DAYS. THE RESULTS INDICATE THAT COMPLETE REPITITION OF THE ORIGINAL SETTING IS COMPARATIVELY RARE.

ON 5 DAYS WHEELS 1,2,3&4 RETURNED TO ORIGINAL POSITIONS.

ON 4 DAYS WHEELS 2,3,4&5 RETURNED.

ON 6 DAYS, ONLY WHEELS 2,3&4 RETURNED.

17 JANUARY 1944

W.O. 86R 89R 83 87R 84R

D H G S K

STEPPED TO: D H F T K

338TH: X H F T K

676TH: R H F T K

16 JANUARY 1944

W.O. 86R 89 87R 82 8Ø

N B V C S

STEPPED TO: O B W B R

338TH LETTER: M B W B R

676TH: " K B W B R

C D E P P

STEPPED TO: C D F O P

338TH: E D F O P

676TH: G D F O P

18 JANUARY 1944

W.O. 82R 86 89 8ø 85R

E A D H C STEPPED TO: E A C H D

338TH: E A C H X

676TH: E A C H R

U W E N C STEPPED TO: U V D N D

338TH: U V D N X

676TH: U V D N R

19 JANUARY 1944

W.O. 87 83 88 81 84R

T T V X S STEPPED TO: T S U X S

338TH: T S U X A

676TH: T S U X I

Q C Y R F STEPPED TO: P C X R G

338TH: P C X R O

676TH: P C X R W

20 JANUARY 1944

W.O. 89R 87 82 83 88

P L N D B STEPPED TO: P L M C A

338TH: P L M C U

676TH: P L M C O

Y T D J H STEPPED TO: Y T C J G

338TH: Y T C J A

676TH: Y T C J U

21 JANUARY 1944

W.O. 8ø 83R 85R 86R 81R

R Q L D V	STEPPED TO:	Q Q M E V
	338TH:	S Q M E R
	676TH:	U Q M E N

S P W R N	STEPPED TO:	S P X R O
	338TH:	U P X R S
	676TH:	W P X R W

24 JANUARY 1944

W.O. 81R 83 87 82R 86

E C Y U V STEPPED TO: F B X V V V

338TH: F B X V T

676TH: F B X V R

M E S G I STEPPED TO: M D R G H

338TH: M D R G F

676TH: M D R G D

24

23 JANUARY 1944

W.O. 87 82 84R 81 8ØR

N R G J T STEPPED TO: M R H I T

338TH: S R H I L

676TH: Y R H I D

F N F M D STEPPED TO: F N G L D

338TH: L N G L V

676TH: R N G L N

22 JANUARY 1944

W.O. 89R 83 8Ø 86 88R

H S B Y T STEPPED TO: H R A X T

338TH: H R A X H

676TH: H R A X V

S V D Q E STEPPED TO: T V C Q F

338TH: T V C Q T

676TH: T V C Q H

14

14

27 JANUARY 1944

W.O. 8ø 89 85R 81 86R

H N L P Q STEPPED TO: H N M O Q

338TH: F N M O S

676TH: D N M O U

U L T B H STEPPED TO: T L U A H

338TH: V L U A F

676TH: X L U A D

2 3 2
2 2 3

26 JANUARY 1944

W.O. 81R 84 83R 88 87R

H F J F D STEPPED TO: I F K E D

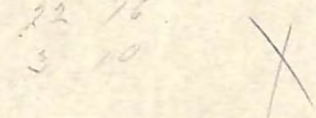
338TH: E F K E T

676TH: A F K E J

F W J G A STEPPED TO: F W K F B

338TH: J W K F L

676TH: N W K F V



25 JANUARY 1944

W.O. 82 83R 84 88R 86

W B Q G L STEPPED TO: V C P G L

338TH: N C P G L

676TH: F C P G L

I C E W G STEPPED TO: I C D X G

338TH: A C D X G

676TH: S C D X G

29 JANUARY 1944

W.O. 84R 89 81 83 85

L X M K N STEPPED TO: L X L K M

338TH: D X L K M

676TH: V X L K M

F U S N Y STEPPED TO: F U R N Y

338TH: N U R N Y

676TH: V U R N Y

X

18

8

28 JANUARY 19

W.O. 88R 89 86 8ø 83

L T B N K STEPPED TO: M S A N J

338TH: Q S A N N

676TH: U S A N Q

I D U M G STEPPED TO: I C T M G

338TH: M C T M C

676TH: Q C T M Y

X

4 4

4.2 2

30 JANUARY 1944

W.O. 86R 88R 83 89 82R

G R V D T	STEPPED TO:	H S U D T
	338TH:	X S U D B
	676TH:	N S U D J

V S Q Q D	STEPPED TO:	V S P P E
	338TH:	S S P P M
	676TH:	B S P P U

C.C.M.

CROSS INDEX

Date: 30 August 1943

From: Prof. B. de F. Bayly

To: Captain J. V. Murphy

Subject: M-228 development of the CCM Machine

Filed Under: British Army Procurement

MEMORANDUM

June 25, 1943

From: GM-C
To: GM

Subject: Semi-Automatic Operation of CCM's.

1. In order that the CCM's in the section may be converted to semi-automatic operation in very short order at any time, it is recommended that GM-4 be ordered to make at once the minor wiring changes necessary.

2. In order that the devices in the section and those being built for it may be coordinated in all respects, it is further recommended that no changes other than those mentioned herein be allowed in any of the machines presently aboard. It can easily be understood that what is alleged to be an improvement may, in fact, throw a whole set of plans askew.

J.A. Skinner

J.A.Skinner, GM-C

CCM

CROSS INDEX

Date: 21 June 1943

From: VCNO

To: CBS

Subject: Requesting equipment from IBM for operating two CCM's automatically for communication with GC&CS

Filed Under: IBM EQUIPMENT