

ARMY SECURITY AGENCY

WASHINGTON 25 D C

Ey Aut' only of the Commanding General

Lastiqle

Derin

Waa 4

WDGSS-14

4 December 1945

SUBJECT: Historical Report

TO:

Deputy Chief, MIS
Room 2E 800, The Pentagon
Washington 25, D. C.

In accordance with your telephonic request, herewith is a copy of a document entitled "Preliminary Historical Report on the Solution of the 'B' Machine," prepared by me on 14 October 1940, shortly after the "Purple" system was solved.

l Incl
Pre Hist Rpt on the
Solution of the "B"
Machine

WILLIAM F. FRIEDMAN Director of Communications Research

Declassified and approved for release by NSA on 09-05-2013, pursuant to E.O. 13526





PRELIMINARY HISTORICAL REPORT

ON THE

SOLUTION OF THE "B" MACHINE"

TO SCRET

William F. Friedman, Principal Criptanalyst. October 14, 1940.

After 23 bittover 1940 hus machine, was, for securing per for lessensited as the "Purple matim" w 3.3 3 3 2 25

Part I. - Technical

- 1. In the latter part of 1938, messages appeared in a special secret Japanese cipher giving the authorization for travel for a "Communications Expert" named Okamoto, in order that he might put into service certain or ptographic paraphenalia termed by the Japanese diplomatic offices as the Type "B" cipher machine. This machine was to replace the then currently used Type "A" machine for highly secret communications among the important Japanese embassies throughout the world and the Foreign Office in Tokyo. On February 19, 1939, a message bearing the date of origin as February 18, 1939, in superenciphered code (K-1 transposed and enciphered by special A-machine procedure) was intercepted and was found to give the effective date of the initiation of the B-machine as February 20, 1939. The A-machine was still to be used by all holders for certain classes of communication.
- 2. Among the first messages received after the effective date of the B-machine were three messages, originating in "arsaw, which had a new type of indicator instead of the normal "A" type indicator. Examination of these messages showed that they were definitely not "A" type messages, but due to the fact that six of the twenty-six letters appearing in the text of the messages were abnormally high (as they would have been had the A-machine been used for their encipherment) it was assumed that the messages were prepared by the B-machine and that it was a modification of the basic A-machine. Further intercepts tended to corroborate this theory.

 The charmens was continued in regular use at Heinking and Shanghai and very occasionally (apparently when the B-machine was cut of consistion) the A-machine continued to be employed at the places which had been provided with B-machines.
- 3. After a brief study it was confirmed that the division of the letters into two categories (one group of six letters and another group of twenty letters) which was the basis of the cryptographic treatment in the A-machine was retained in the B-machine but with a very important change. Whereas in the A-machine the 6 letters comprising the "6's" as well as the 20 comprising the "20's" were enciphered by means of what had been deduced as being a rotating commutator, whose stepping was controlled by a break wheel of 47 positions with certain skips in the cycle (the commutator could advance 1, 2 or 3 steps at a time), in the B-machine the "6's" were enciphered by means of a series of 2; hetergeneous and differently mixed alphabets which were constant in their nature and cyclic repetition. These 25 alphabets were merely a carefully selected set of 25 of the possible 720 permutations or transpositions of 6 elements taken 6 at a time, and a



Tashing Berlin, London, Paris, Moscow, Rome, Geneva, Brussels, Ankara, Languai, and Peking.

deciphering chart or "development" was constructed to correspond with these 25 permutations. This chart was revised and corrected from day to day until it became certain that all its elements were absolutely correct.

- 4. This having been accomplished (by April 10, 1939), it tecame possible, as a result of cryptanalytic technique elaborated for the purpose, to decipher the "6's" in practically every message of any considerable length in the B-machine. It was found that so far as the "6's" between two messages with unlike indicators were concerned, the only difference between one indicator and another was the starting point in the cycle of 25 alphabets. There were 120 different indicators but only 25 different starting points, so that four (in certain cases, five) different indicators represented the same starting point.
- 5. Then the "6's" in a given message vere deciphered, the plain text values of cipher letters scattered here and there throughout the text became available, so that the skeletons of vords and phrases offered themselves for completion by the insenuity and the imagination of the criptanalyst. For example, suppose that on a given day the 6 letters forming the "6's" were Z Q A D R H and the following text was at hand:

Cipher: ERAXEFQCEVQOOXHECFDLNEGRVQPPLCERP.. Plain: _HE_A_A_E_E___ER__E___REQ_E___HA_..

It is not difficult to imagine that the missing letters are those shown below:

Cipher: BRAXEFQCEVQOOXHECFDLNEQRVQPPLCCRP... Plain: THEJAPANESEGOVERNAESATRECTESTSTUFF...

In this process of filling in the plain*text values of the "20's" the criptanalyst could be guized only by two things: (1) the positions and ite tities of the deciphered "6's" and (2) the context. For it speecily tecame apparent that any cryptographic relationship between the plain text and the constantly-shifting cipher text values in the case of the letters constituting the group of "20's" had been most carefully eliminated, disguised, or suppressed. This fact corroborated the conclusion drawn from all statistical and analytical tests made on the cipher texts of the various messages studied.

6. The process of filling in the plain text values of the "2C's" was therefore, as a rule, a very difficult matter, depending usually upon the particular assortment of letters constituting the "6's". If the text was in Japanese there was, in addition to the difficulty inherent in that language itself, the added perturbation occasioned by the fact that the Japanese Foreign Office had, on War 1, 1939, instituted a species of "Fhillips Code in connection with their use of the B-machine, with a long series of arbitrary letters and abbreviations standing for numbers, punctuation signs, and frequently used combinations of letters, syllables, words, and sometimes convolete phrases. For instance, the combination C F C represents periou; C C F represents paragraph; the single letter L (not normally used in Japanese)



represents the dighthong ai; X represents ei; P represents ni; V represents long U; C T (represents Frita (sai) itasai tashi; B K represents Beikoku (- United States); T K 1 represents Telkokuseifu (- Japanese Covernment): S K V represents Sukunakarazu, etc., etc. Ine difficulties introduced by this abbreviated or rather code writing alone were quite stagering as well as aggravating, for often the "text" even when finally reconstructed appeared more like code or a random assortment of letters than plain text. 2 For the reconstruction of such text, the services of the Japanese experts were absolutely essential, and the work went very slo ly not only because of its difficulty, but also because the services of these translators were available only a small part of the time that traffic for the daily "Bulletin" permitted, which was quite seldom. However, occasionally it was found, after the "6's" in a given ressare had been decaphered, that these letters and their distribution throughout the message gave good indications of the presence, in whole or in part in the messare. of normal inglish text. In such cases, the "guessing" process as likely to be considerably easier because of the absence of abbreviations (except for punctuation signs, in which case these were a help), because of the

A typical example of the sort of "text" usually found at the beginning of messages is the following:

Cipher: FGFXP IXUDB DGECZ LBLNU ZQO LH YNARÇ ARJO. Plain: XFCGJ %FOVD DNOBB FYXFO CFYEC CF SG T3J%.

DEILO AXPPP LIGDK ZFGRA ANIFI CGUAV FELBK WTLSI...

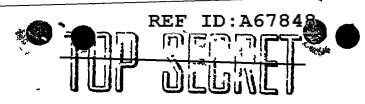
The correct grouping of letters and the interpretation of the foregoing "plain text" is as follows:

X F C = Da1 - go G J % = 15G T S = Getsu (month) F O V = Open parenthesis JVRK = Juroku (= 16th) DD H I = Japanese word for "dav" NC = "cf" (Jap.plain text F I C = Begin kana spelling GURV = Coru (= Gre;) particle possessive) 3 3 F E L = Close kana spelling r' Y X = Close parenthesis) E K W = Beikoku (= U. S.) F C C = Cokuhi (= Secret) F Y L = Wancho fugo atukai T L S I = Taishi (= Ampassador) C C F = Snin sho (= Paragraph)

In running language, the message begins as follows: "Number 15 (part 1 of 2 parts) Secret, to be kept within the Department paragraph on Laron low the American Ambassador, Grew", etc.



A CONTRACTOR OF THE PROPERTY O



er utanalyst's greater familiarity with the language, and because of the availability of the services of a larger number of workers. It happened that in several cases, after a fer words had thus been obtained by pure " "lessing", a clue as afforded as to the general nature of the reserge and this led to a frantic search for a complete document thich might be available either in our own files or in the files of other government agencies. One case was found in dich the B-macrine message contained a carachrased version of a message which had been transmitted in .- 1 code. Accountage as, of course, immediately taken of this circumstance but the ertire text of the B-machine message could never be reconstructed from the paraparased E-I version, possibly because of the excellent paraphrasing. cossibly because of the presence of abbreviations, possibly because of both. Cartain Inglish text messages, nowever, were reconstructed, some of them to the extent of 90-95,, because the documents being quoted in the messares were lortunately located and obtained, most often through the occoperation and good offices of G-2.

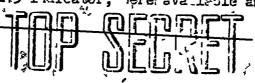
- In all, the plain texts for parts of sche 15 fairly lengthy messales were obtained by the methods indicated above, and these were subnected to most intensive and exhaustive criptanalytic studies. To the consternation of the cryptanalysts, it was found that not only was there a conflete and absolute absence of any causal repetitions within any single message, no matter how long, or between two messages with different indicators on the same day, but also that when repetitions of three, or occasichally four, cipher letters were found, these never represented the same plain text. In fact, a statistical calculation gave the astorishing result that the number of resetations actually present in these crimitograms as is than the number to be expected had the letters comprising them been in at random out of a hat! Apparently, the machine had inth malicious int -- but brilliantly -- bron construction to suppress all plain text rejetition. Hevertheless, the criptanalysts and a feeling that this very circumstance would, in the final analysis, prove to be the harmong of all Lite and mechanism. And so it turned out!
- In all the foregoing studies; several factors stood cut. First, the basic law underlying the 2-machine was of such character that the cipnering mechanisms seemed to start from certain initial settings and to progress absolutely methodically without cyclic repetition of any sort. strai at turough to the end of the messages, the longest of Thich for which plain text had been recovered com, rised over 1,500 letters. Secondly, two icentical plain-text, letters in sequence could never be represented by the identical cipher-text letters; nor could two identical plain text letters 26 letters apart be identically encuphered. This phenomenon which was tersed "suppression of duplicate encipherments at the 1st and 26th intervaks" formed the subject of long and archous study, fruitless experimentation and much discussion. Thirdly, two messages inth identical indicators endue same day appeared to be identically enciphered, and on direct superw.csition showed themselves to be monoalphabetic mithin columns, but fitte the monoalphabets constantly, irregularly and unpredictably shift-Iron column to column. Fourtaly, two messages anth identical indicators

on different days (different plugboard arrangements into the machine) were absolutely different. Fifthly, two messages with different indicators on the same day (same plugboard arrangement) were absolutely different and who med no cryptographic similarities whatsoever. Sixthly, in each line of 20-latters, the identical letters could be identically enciphered except at the 1st interval, that is, identical encipherents could, and often did, occur within a line of 25 letters at all intervals, except at the 1st interval, although this phenomenon was rare at the 2d, 3d, 4th and 5th intervals.

- 9. At the same time as the foregoing phenomena were being studied. intensive research as continued in an endeavor to establish primary or basic cipher sequences of the nature of those usually found in cryptographs with rotatane co mutators, rotors, and the like, such as in the Hebern and Laima v cryptographs, our w-134, etc. For it- as winconceivable that the machine enflored a multiplicity of non-repeating keys of lengths corresponding to the lengths of the messages and, moreover, theoretical considerations eliminated tre possibility that running keys were being used. Somewhere, somehow, the existence of cyclically repeating keys or sequences must be uncovered before. solution could be effected. But all efforts to disclose the presence of cyclically repeating sequences were fruitless. In one and only one case was there found ever the slightest 'iint of such sequences as were being sought. "In a certain English text message the letter i was found to be represented by 2, 26 letters a are another Z ras found to be represented by . 1. and again 20 letters away another E was found to be represented by V, _akin_ the sequence . IV; in the very same message the same trigraph Q i / was found to represent three D's similarly spaced. Attempts to and to this is A sequence were absolutely anavailing. In this long, exhaustive and tecious search for repeated sequences or partially repeated sequences much labor and energy was expended but it was realized that the difficultives trainal tue to the paucity of the text, restrict the number and learth of the individual messages available for study and for which the plain test and open reconstructed. It became a parent that that would be recommended & stien, b some ranner of other, several massages in the same in ucc or - .. ul ... sam .a . cr elor .c conort soural meserus tit. he take safor but on of ferent days to the same base, before even the existence of sic. crelic sequences could be detected.
- 10. In all the thousand or nore messages on hand there were but a mere caser's half dozen or so cases where there here two messages on the same tay and in the same indicator. Fore than two had never been found and this as its respected in a disternial 120 different indicators available for selection each day. In one case of this rare phenomenon the plain text for one of the two massages was available but very little could be done even then as regards the solution of the other member of this pair of messages. For each a rethod of attach at least 20-25 nessages all in the same indicator in the same day would be necessary and this as of course recognized as a perfectly hopeless expectation. There remained the possibility of consorting several messages with the same indicator but on different says to the same base and mile this net of of attack looked extremely difficult not appear hopeless.

- 5 -

- II. A method for this conversion to the came base as developed and was termed "the identification of homologs." That is, an attempt has to be made to establish that a given letter on a certain day and another letter on a different day, ere treated in an absolutely identical or, homologous mann riby the hacking then set to the case indicator. This conversion process is too involved to explain in this report but suffice it to say that difficult though it is, it was successful in two cases. One of these fielded a set of 6 ressaies, all in indicator 59173, which could all be reduced to the same base. Those formed the rectal set of messages from the study of which success in solution of the machine was finally achieved.
- 12. Distribution tables of the letters constituting the text of these six nessages here made. It should be stated that in four of these six crucial messages only fragments of plain text had been reconstructed, here and there; the complete or nearly complete plann texts of only to of these six messages had been reconstructed. He never, enough data were accuralated from these to completely and the other partially reconstructed necsages to yield distribution tables lich, on careful examination, disclosed the presence of repeated sequences, here and there. This, on September 1), 1940, at about 2:00 P.M., was the very first indication that a successful attack might be possible. There was much excitement at this first glimmer of light upon's subject that had for so many months been shrouded in complete darkness and regarded occasionally inth some discouragement. The nature of the distribution tables, reserved to/is also too involved to emplain in this report, but suffice it to indicate that they shower certain symmetries between the successive cither equivalents of a given plain-test (letter and the successive appearances of that plain-text letter in the cryptogra nic text.
- 13. As soon as the existence of cyclic or symmetric se wences reor mortist, automotione made to uncover complete pasic sequences of the type theoretically predicted., But many conflicts and inconsistencies soon develored, due to the fact that the crait togra inc las underlying the slifting from sequence to sequence tere still un moun. Concurrently ath the work connected with straightening out and removing inconsistencies in these reconstructed basic sequences ran the .crk of uncovering the criptographic laws referred to, and very soon the general nature of the latter oscale quite clear. All efforts were concentrated upon the development of the specific, laws and specific basic sequences applicable to the indicator under study, viz. 59173, inth a view to uncovering all the cryptographic rerement in this case and then searching for analogous phenomena in the case of other indicators. Cortain qualified personnel from other sections mere brought in to assist, and a considerable amount of night fork vas found desirable in order to push this study to completion at the earliest possible coment.
- 14. By beptember 27, just one seek later, the early had procressed to a point here it became post le to and in two translations representing the very first "solution" to the D-mac one: Two messages of recent, dates, both in the 50173 indicator, were svalable and were solved by



SEXTER

applying the principles of solution by honologs, guided by the aid of the reconstructed basic sequences. It was all the more gratifying that this could be done on the very way that announcement was made of the signing of the Tripartite Agreement among Germany, Italy, and Japan.

15. Much work remained to be done, no ever, since only the data applicable to but one out of the whole set of 120 indicators were at hand. To solve the remaining 119 indicators appeared still to present quite a large problem. These solutions consist of finding the initial settings of three 20-layer rotary, electrical cryptograms are elements of 25 points ero, and finding the order in which these three elements are brought into play within each indicator system. With but little slackering of the pace sot by the personnel themselves, ork now progressed with vigor and at this moment solutions for over one-third of the 120 indicators are available.

16. As to the mechanics of the E-machine, naturally the basic principles of its construction and operation were deduced from the criptographic pnenomena ooservable in the messages, and immediately plans were initiated. for the construction of an equivalent machine for our purposes. Orders for the material for 2 fully automatic machines were placed and excedited. Thile awaiting the arrival of this materiel a hand-operated machine as desired by personnel of the J-B section, constructed by them, and is at this imiting being used to assist in the decipherment of messages. Basically, the B-lice na consists of 13 rotary, 6-level, 25-point, statenes of the type employed in automatic telephony. One of these 13 satches controls the encycherment of the "c's" and it goes through the same 25-point cycle over and over again as many times as is necessary to encipher the messages. It has 150 crossconnections, which, as stated above, had been established lon- ago. Is to i o "AC". ', i soo dhe chomandhided of Board of Dica is of A sinte as ween bank having 500 cross-connections, making a dotal of 1,500 sub-circuits, availthis for the encilarment of any given letter. The arremements for advancring these splitches is such that for a riven indicator, say 20045, bar, hunber 3 steps continuously, bank number 2 steps once for every 25 steps of pant number 3, and bank number 1 steps once for every 625 steps of bank number 3. This type of notion has been designated as a "C21" motion. For another incatar the order of this stepping may be different and in all there a place to be 6 different types of stepping: 1-2-3, 1-3-2, 2-1-3, 1-3-1, 3-1-2, and 3-2-1. Although there are 120 different indicators there are only 6 different types of rotion or stepring of the three ciphering satches, so that it appears that each type of motion is represented by 20 different indicators. what differentiates one indicator from another within such a set of 30 indicators are the relative starting points within the three ourks of sintenes. These starting points appear to have been very carefully selected so as to preclude or reduce the possibility of "overlaps," that is, the production of two massages ' ion in whole or in part have been enciphered by identical keying elements in identical sequence. Chice these factors concerning all inmicators have oeen established, and our machine is in operation, the reading of B-machine messages resolves itself into the establishment of the wally plugboard arrangement, that is, the order and identity of the wires leading From the keyboard into the cryptograph and thence out of the criptograph into the printing unit. Cryptanalytic procedures for this purpose have already open established and tested, so that this should not be a serious

| t t | | | | | | | | |

00000



roblem. Given a long message or several smort ones of the same date, solution should be possible in an expeditious manner.

considerable light upon the mechanism of the A-machine with the result that our present A-machine will be modified in the light of these discoveries and will be made more efficient. The whole situation with respect to the cipher machines em loyed by the Japanese Foreign Office now at pears to be integrated into a consistent scheme of development from its carliest and simplest beginnings, about 1930, to its present quite conflex form. Problems concerning the A-machine and questions for which logical and "reasonable" answers could not be found are now explainable on the cimple grounds of the type of cryptographic mechanism employed in the earlier machines, which seems to be the rotary switch used in automatic tele hony, rather than the revolving commutator employed in our present A-machine.

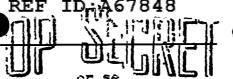
* * * * * * *

Part II. Credits

18. The successful solution of the B-machine is the culmination of 13 months of intensive study by a group of criptanalysts and assistants working as a harmonious, well-coordinated and cooperative team. Only by such cooperation and close collaboration of all concerned could the solution possibly have been reached, and the name of no one person can be selected as deserving of the major portion of credit for this achievement. The parts played by the individual members of the team may, however, be indicated.

19. The specific direction and coordination of all studies on this project was the joint work of Orgitabelyst Fra ' D.Porlett and issistant er prevalyst dobert 0. Ferner. Their indefatigable labors and brilliant analytical work testify and are a credit to their crimitanslytic shill, it is ing all experience. To their joint direction and efforts are due the evtresal; fruitful analysis of the criptographic mechanics underlying the operation of the B-macrine as a mucle, the theory of its operation, and the development and solution of the "6's" at any early date in these stud-Les. They were also extremely active in pushing the solution to a successful conclusion by organizing and nirecting the reconstruction of the cevelopments or rirings of the switches for the "20's". Junior Cryptanalysts Ichevieve L. Grotjan, Albert . Small, and Lamuel S. Snyder cid tost excellent work in recovering the "6's" during many months of apparently hogeless effort. In this work they were occasionally assisted by Oryptographic Specialists Cyrus C. Sturgis, Jr., Kenneth D. Liller, and Glenn 5. Landig. Of the latter two mentioned, it should also be stated that their very large output of work in one decoding of J code material, custsted part time by other memoers of the J-Section, lifted much of the heav, burden of this absolutely necessary current translation ork from the





mensele an ex ral short ones of the same date, inclosed on expression to the ditious manner.

of the B-ma, one has, as a concomitant, thrown the heart of the A-machine with the result in the wife be of the A-machine with the result in the light of these piscoverore off the The whole situation with respect to Lyad tent 'Tanese Foreign (ffice now appears conditation about the of development from its car
regulation | 1930, to its present quite complex

regulation | net | net | ne and questions for mich logical

regulation | cripy | found are now explainable | cripy | found are now explainable on the type of to be applied mechanism and transfer to be applied mechanism and transfer to be applied mechanism and transfer to be applied to t type of to be aphic mechanism employed in the country olver the rotary switch used in automatic the 14 /olv... commutator employed in our present

Part '.. Credits *

esseul polutic raive it dy by Los um lajo.

,t,*

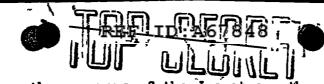
1-15.

of the B-machine is the culaination group of cryptanalysts and assistants mated and cooperative team. Only by close the fined. The and cooperative team. Only by en real late the name of no one person can be the individue ration of credit for this achievement.

PAR MORE "- 31. vertier. IN THE STATE OF ST. 211373 //rus , the letter in the state of 15 2/7/

c: difection of coordination of all studies or this ralyst Frank B.Rowlett and Assistant ore indefatigable labors and brilliant it/ " 'r jo- "dit to their criptanalytic skill, ... the __rection and efforts are due the e _roction and efforts are due the e-Type and of e, the theory of its operation, and of s, the theory of its operation, and colin elv a "o's" at any early date in these studely a "o's" at any early date in these studthe same secting the reconstruction of the an, # : les for the "20's". Junior Cryptot . Small, and Samuel S. Snyder and
to se "6's" during good and they were occasionally assisted by turgis, Jr., Kenneth D. Aller, and mentioned, it should also be stated in the decoding of J code material, in the decoding of J code material, if the section, lifted much of the essary current translation work from the





shoulders of the other members of the J-section, thus giving the latter more time for research on the 3-machine than could have other use been possible. For the original suggestion of the electrical telephone sitching mechanism for duplicating the encipherment of the "6's", the design and construction, in collaboration ath ir. Rollett, assisted by other members of the section, of the martine for deciphering the "6's' and for excellent fork in the accipharaent of the "6's" in current traffic over many menths, Cryptographic Specialist (now 1st Lieutenant) Leo Rosen is to be mentioned. Fe also supervised and assisted in the construction of the hand-operated E-machine designed by the cryptanalytic staff of the J-section; in this latter project Junior Cryptanalyst H. F. Dearce, Cryptographic Specialist idward J. Hawkins, Sgts. Ilder and Boy also assisted. In this connection, it should also be mentioned that the shop facilities of the Radio Laboratory, Pavy Yard, .ere kindly placed at our disposal and certain material furnished therest, through the courtesy of Counander L.F. Safford of the Communications Security Group, Office of Naval Communications. This greatly facilitated the construction of the hand-operated E-machine. The excellent work of Tabulating Lachine Supervisor Ulrich J. Kropfl and Cryptanalytic lide Mary J. Dunning in performing countless tabulating machine operations deserves mention, as well as the painstaking nork of the various card punch operators under their supervision. "liss Bronenburg performed and assisted in many clerical jobs of routine and special nature in connection inth these studies. The work of Research Analysts John B. durt and Paul S. Cate must be mentioned in connection with our efforts to reconstruct the texts of messages in Japanese. This difficult work had to be done in that little time could be spared from their regular and arduous duties as translators. The .ork of Cryptographic Clerk Frances M. Jerome in maintaining the files of the intercept traffic necessary to these studies proved to be extremely helpful; her everyday ork in operating the "6's" deciphering machine was painstaking and accurate. To Cryptographic Clark Mary Louise Frather credit should be given for the calcilli keeping of the records and index of all messages; it vas also she who found the paraghrased K-1 message mentioned in Par. 6, and which played an important part in the final break into the system. After the initial solution of the "20's" had been made there is great pressure to hurry the ork along as fast as possible. In addition to considerable overtime work by members of the J-section, certain personnel from other sections of the S.I.S. were brought in to assist. Some of them performed this work only as voluntary overtime. In this special assistance the names of the following persons are to be mentioned: Associate Cryptanalyst Abraham Sinrov, Assistant Cryptanalyst Lawrence Clark, Junior Cryptanalyst Delia Ann Taylor, Cryptographic Clerk Tilma Z. Berryman, and Cryptographic Specialist Edward E. Christopher, Jr.

The vigilance and excellent work done by our various monitor stations in intercepting and copying the necessary traffic also deserves special mention. The assistance rendered by G-2 in obtaining certain data has already been mentioned.

The undersigned was directed to participate in the "B" machine studies in August 1939, and from that time on these studies were under his general supervision, at the same time that he carried on some of the cuties from wich he had not been relieved. In addition to this general supervision



he also directed and numself conducted special studies with a wiew to uncovering the criptographic principles underlying the B-machine. He wishes we to take this opportunity to indicate his gratification of the demonstration, by his assistants, of their grasp of the criptanalytic techniques taught them as a result of their participation in the training afforded by the Signal Intelligence Scrool, as well as his pleasure at the manner in which the individual members of the team earnestly and wholeheartedly collaborated in this joint affort. He also wishes to express his appreciation of the important assistance rendered by the Officer in Charge of the Signal Intelligence Service, and his commissioned assistants, in expediting the precurement of personnel, supplies, and special information when needed.

October 14, 1940

Fillian F. Friedman, Principal Cryptanalyst.