PRELIMINARY HISTORICAL REPORT ON THE SOLUTION OF THE "B" MACHINE

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 cryptographic 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[1] 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

[1] Washington, Berlin, London, Paris, Moscow, Rome, Geneva, Brussels, Ankara, Shanghai, and Peking.

classes of communication.

2. Among the first messages received after the effective date of the B-machine were three messages, originating in Warsaw, 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 A-machine was continued in regular use at Hsinking and Shanghai and very occasionally (apparently when the B-machine was out of commission) 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 25 heterogeneous 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 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 became 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. When the "6's" in a given message were deciphered, the plain text values of cipher letters scattered here and there throughout the text became available, so that the skeletons of words and phrases offered themselves for completion by the ingenuity and the imagination of the cryptanalyst. For example, suppose that on a given day the 6 letters forming the "6's" were E Q A D R H and the following text was at hand:

Cipher: B R A X E F Q C E V Q O O X H E C F D L N H Q R V Q P P L C E R P . . .
Plain: _ H E _ A _ A _ E _ E _ _ _ E R _ _ E _ _ R E Q _ E _ _ _ _ H A _ . . .

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

Cipher: B R A X E F Q C E V Q O O X H E C F D L N H Q R V Q P P L C E R P . . .
Plain: T H E J A P A N E S E G O V E R N M E N T R E Q U E S T S T H A T . . .

In this process of filling in the plain text values of the "20's" the cryptanalyst could be guided only by two things: (1) the positions and identities of the deciphered "6's" and (2) the context. For it speedily became 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 "20'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 May 1, 1939, instituted a species of "Phillips 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 complete phrases. For instance, the combination C F C represents period; C C F represents paragraph; the single letter L (not normally used in Japanese) represents the diphthong ai; X represents ei; P represents ni; V represents long U; Q T Q represents Arita (shi) itashi tashi; B K W represents Beikoku (= United States); T K W represents Teikokuseifu (= Japanese Government); S N W represents Sukunakarazu, etc., etc. The difficulties introduced by this abbreviated or rather code writing alone were quite staggering 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 slowly not only because of its difficulty, but also because the services of these translators were available only a small part of the time when the traffic for the daily "Bulletin" permitted, which was quite seldom. However, occasionally it was found, after the "6's" in a given message had been deciphered, that these letters

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

Cipher: F G P X P I X U D B D G E C Z L B L N U Z Q O Q H Y N M R Q A R J O P
Plain: X F C G J W F O V D D N O B B F Y X F O C F Y L C C F M S G T S J V R

D E I L O A X P P P L I G D K Z P G R A
K H I F I C G U R V F E L B K W T L S I . . .

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

X F C = Dai - gō
G J W = 15
F O V = Open parenthesis
D D = 2
N O = "of" (Jap. plain text particle possessive)
B B = 1
F Y X = Close parenthesis
F O C = Gokuhi (= Secret)
F Y L = Kancho fugo atukai
C C F = Shin sho (= paragraph)
M S = 3
G T S = Getsu (month)
J V R K = Juroku (= 16th)
H I = Japanese word for "day"
F I C = Begin kana spelling
G U R V = Guru (= Grew)
F E L = Close kana spelling
B K W = Beikoku (= U. S.)
T L S I = Taishi (= Ambassador)

In running language, the message begins as follows: "Number 15 (part 1 of 2 parts) Secret, to be kept within the Department paragraph On March 16th the American Ambassador, Grew", etc.

and their distribution throughout the message gave good indications of the presence, in whole or in part in the message, of normal English text. In such cases, the "guessing" process was 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 cryptanalyst'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 few words had thus been obtained by pure "guessing", a clue was afforded as to the general nature of the message and this led to a frantic search for a complete document which might be available either in our own files or in the files of other government agencies. One case was found in which the B-machine message contained a paraphrased version of a message which had been transmitted in K-1 code. Advantage was, of course, immediately taken of this circumstance but the entire text of the B-machine message could never be reconstructed from the

paraphrased K-1 version, possibly because of the excellent paraphrasing, possibly because of the presence of abbreviations, possibly because of both. Certain English text messages, however, were reconstructed, some of them to the extent of 90-95%, because the documents being quoted in the messages were fortunately located and obtained, most often through the cooperation and good offices of G-2.

7. In all, the plain texts for parts of some 15 fairly lengthy messages were obtained by the methods indicated above, and these were subjected to most intensive and exhaustive cryptanalytic studies. To the consternation of the cryptanalysts, it was found that not only was there a complete 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 occasionally four, cipher letters were found, these never represented the same plain text. In fact, a statistical calculation gave the astonishing result that the number of repetitions actually present in these cryptograms was less than the number to be

expected had the letters comprising them been drawn at random out of a hat! Apparently, the machine had with malicious intent - but brilliantly - been constructed to suppress all plain text repetition. Nevertheless, the cryptanalysts had a feeling that this very circumstance would, in the final analysis, prove to be the "undoing" of the system and mechanism. And so it turned out!

8. In all the foregoing studies, several factors stood out. First, the basic law underlying the B-machine was of such character that the ciphering mechanisms seemed to start from certain initial settings and to progress absolutely methodically without cyclic repetition of any sort, straight through to the end of the messages, the longest of which for which plain text had been recovered comprised over 1,500 letters. Secondly, two identical plain-text letters in sequence could never be represented by two identical cipher-text letters; nor could two identical plain text letters 26 letters apart be identically enciphered. This phenomenon which was termed "suppression of duplicate encipherments at the 1st and 26th intervals"

formed the subject of long and arduous study, fruitless experimentation and much discussion. Thirdly, two messages with identical indicators on the same day appeared to be identically enciphered, and on direct superimposition showed themselves to be monoalphabetic within columns, but with the monoalphabets constantly, irregularly and unpredictably shifting from column to column. Fourthly, two messages with 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 showed no cryptographic similarities whatsoever. Sixthly, in each line of 26 letters, two identical letters could be identically enciphered except at the 1st interval, that is, identical encipherments could, and often did, occur within a line of 26 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 was continued in an endeavor to establish

primary or basic cipher sequences of the nature of those usually found in cryptographs with rotating commutators, rotors, and the like, such as in the Hebern and Enigma cryptographs, our M-134, etc. For it was inconceivable that the machine employed a multiplicity of non-repeating keys of lengths corresponding to the lengths of the messages and, moreover, theoretical considerations eliminated the 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 even the slightest hint of such sequences as were being sought. In a certain English text message the letter E was found to be represented by Q, 26 letters away another E was found to be represented by Y, and again 26 letters away another E was found to be represented by V, making the sequence QYV; in the very same message the same trigraph Q Y V was found to represent three E's similarly spaced. Attempts to add to this Q Y V

sequence were absolutely unavailing. In this long exhaustive and tedious search for repeated sequences or partially repeated sequences much labor and energy was expended but it was realized that the difficulty was probably due to the paucity of the text, despite the number and length of the individual messages available for study and for which the plain text had been reconstructed. It became apparent that what would be necessary was to obtain, by some manner or other, several messages in the same indicator and on the same day, or else to convert several messages with the same indicator but on different days to the same base, before even the existence of such cyclic sequences could be detected.

10. In all the thousand or more messages on hand there were but a mere baker's half dozen or so cases where there were two messages on the same day and in the same indicator. More than two had never been found and this was to be expected in a system with 120 different indicators available for selection each day. In one case of this rare phenomenon the plain text for one of the two

messages was available but very little could be done even then as regards the solution of the other member of this pair of messages. For such a method of attack at least 20-25 messages all in the same indicator and on the same day would be necessary and this was of course recognized as a perfectly hopeless expectation. There remained the possibility of converting several messages with the same indicator but on different days to the same base and while this method of attack looked extremely difficult it did not appear hopeless.

11. A method for this conversion to the same base was developed and was termed "the identification of homologs." That is, an attempt was to be made to establish that a given letter on a certain day and another letter on a different day were treated in an absolutely identical or, more accurately speaking, homologous manner by the machine when set to the same 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 yielded a set of 6 messages, all in indicator 59173, which could all be reduced to the same base. These formed the crucial 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 messages were 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 plain texts of only two of these six messages had been reconstructed. However, enough data were accumulated from these two completely and and the other partially reconstructed messages to yield distribution tables which, on careful examination, disclosed the presence of repeated sequences, here and there. This, on September 20, 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 a subject that had for so many months been shrouded in complete darkness and regarded occasionally with some

discouragement. The nature of the distribution tables referred to is also too involved to explain in this report, but suffice it to indicate that they showed certain symmetries between the successive cipher equivalents of a given plain-text letter and the successive appearances of that plain-text letter in the cryptographic text.

13. As soon as the existence of cyclic or symmetric sequences became clear, attempts were made to uncover complete basic sequences of the type theoretically predicted. But many conflicts and inconsistencies soon developed, due to the fact that the cryptographic laws underlying the shifting from sequence to sequence was still unknown. Concurrently with the work connected with straightening out and removing inconsistencies in these reconstructed basic sequences ran the work of uncovering the cryptographic laws referred to, and very soon the general nature of the latter became 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, with a view to uncovering all the cryptographic phenomena

in this case and then searching for analogous phenomena in the case of other indicators. Certain qualified personnel from other sections were brought in to assist, and a considerable amount of night work was found desirable in order to push this study to completion at the earliest possible moment.

14. By September 27, just one week later, the work had progressed to a point where it became possible to hand in two translations representing the very first "solution" to the B-machine. Two messages of recent dates, both in the 59173 indicator, were available and were solved by applying the principles of solution by homologs, guided by the aid of the reconstructed basic sequences. It was all the more gratifying that this could be done on the very day that announcement was made of the signing of the Tripartite Agreement among Germany, Italy, and Japan.

15. Much work remained to be done, however, 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-level rotary, electrical cryptographic elements of 25 points each, and finding the order in which these three elements are brought into play within each indicator system. With but little slackening of the pace set by the personnel themselves, work has 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 B-machine, naturally the basic principles of its construction and operation were deduced from the cryptographic phenomena observable 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 expedited. While awaiting the arrival of this materiel a hand-operated machine was designed by personnel of the J-B section, constructed by them, and is at this writing being used to assist in the decipherment of messages. Basically, the B-machine consists of 13 rotary, 6-level, 25-point, switches

of the type employed in automatic telephony. One of these 13 switches controls the encipherment of the "6'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 cross-connections, which, as stated above, had been established long ago. As to the "20's", these are enciphered by means of 3 banks of 4 switches each, each bank having 500 cross-connections, making a total of 1,500 sub-circuits available for the encipherment of any given letter. The arrangements for advancing these switches is such that for a given indicator, say 20846, bank number 3 steps continuously, bank number 2 steps once for every 25 steps of bank number 3, and bank number 1 steps once for every 625 steps of bank number 3. This type of motion has been designated as a "321" motion. For another indicator the order of this stepping may be different and in all there appear to be 6 different types of stepping: 1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, and 3-2-1. Although there are 120 different indicators there are only 6 different types of motion or stepping of the three ciphering

switches, 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 20 indicators are the relative starting points within the three banks of switches. 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 messages which in whole or in part have been enciphered by identical keying elements in identical sequence. Once these factors concerning all indicators have been established, and our machine is in operation, the reading of B-machine messages resolves itself into the establishment of the daily plugboard arrangement, that is, the order and identity of the wires leading from the keyboard into the cryptograph and thence out of the cryptograph into the printing unit. Cryptanalytic procedures for this purpose have already been established and tested, so that this should not be a serious problem. Given a long message or several short ones of the same date, solution should be possible in an expeditious manner.

17. The solution of the B-machine has, as a concomitant, thrown 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 employed by the Japanese Foreign Office now appears to be integrated into a consistent scheme of development from its earliest and simplest beginnings, about 1930, to its present quite complex form. Problems concerning the A-machine and questions for which logical and "reasonable" answers could not be found are now explainable on the simple grounds of the type of cryptographic mechanism employed in the earlier machines, which seems to be the rotary switch used in automatic telephony, 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 18 months of intensive study by a group of cryptanalysts 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 Cryptanalyst Frank B. Rowlett and Assistant Cryptanalyst Robert O. Ferner. Their indefatigable labors and brilliant analytical work testify and are a credit to their cryptanalytic skill, training and experience. To their joint direction and efforts are due the extremely fruitful analysis of the cryptographic mechanics underlying the operation of the B-machine as a whole, the theory of its operation, and the development and solution of the "6's" at any early date in these studies. They were also extremely active in pushing the solution to a successful conclusion by organizing and directing the reconstruction of the developments or wirings of the switches for the "20's". Junior

Cryptanalysts Genevieve M. Grotjan, Albert W. Small, and Samuel S. Snyder did most excellent work in recovering the "6's" during many months of apparently hopeless effort. In this work they were occasionally assisted by Cryptographic Specialists Cyrus C. Sturgis, Jr., Kenneth D. Miller, and Glenn S. Laudig. Of the latter two mentioned, it should also be stated that their very large output of work in the decoding of J code material, assisted part time by other members of the J-Section, lifted much of the heavy burden of this absolutely necessary current translation work from the shoulders of the other members of the J-Section, thus giving the latter more time for research on the B-machine than would have otherwise been possible. For the original suggestion of the electrical telephone switching mechanism for duplicating the encipherment of the "6's", the design and construction, in collaboration with Mr. Rowlett, assisted by other members of the section, of the machine for deciphering the "6's" and for excellent work in the decipherment of the "6's" in current traffic over many months, Cryptographic Specialist (now

1st Lieutenant) Leo Rosen is to be mentioned. He also supervised and assisted in the construction of the hand-operated B-machine designed by the cryptanalytic staff of the J-Section; in this latter project Junior Cryptanalyst H. F. Bearce, Cryptographic Specialist Edward J. Hawkins, Sgts. Wilder and Roy also assisted. In this connection, it should also be mentioned that the shop facilities of the Radio Laboratory, Navy Yard, were kindly placed at our disposal and certain materiel furnished thereat, through the courtesy of Commander L. F. Safford of the Communications Security Group, Office of Naval Communications. This greatly facilitated the construction of the hand-operated B-machine. The excellent work of Tabulating Machine Supervisor Ulrich J. Kropfl and Cryptanalytic Aide Mary J. Dunning in performing countless tabulating machine operations deserves mention, as well as the painstaking work of the various card punch operators under their supervision. Miss Dronenburg performed and assisted in many clerical jobs of routine and special nature in connection with these studies. The

work of Research Analysts John B. Hurt 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 what little time could be spared from their regular and arduous duties as translators. The work 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 work in operating the "6's" deciphering machine was painstaking and accurate. To Cryptographic Clerk Mary Louise Prather credit should be given for the careful keeping of the records and index of all messages; it was also she who found the paraphrased K-1 message mentioned in paragraph 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 was great pressure to hurry the work 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 Sinkov, Assistant Cryptanalyst Lawrence Clark, Junior Cryptanalyst Delia Ann Taylor, Cryptographic Clerk Wilma 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 duties from which he had not been relieved. In addition to this general supervision he also directed and himself conducted special studies with a view to uncovering the cryptographic principles underlying the B-machine. He wishes to take this opportunity to indicate his gratification of the demonstration,

by his assistants, of their grasp of the cryptanalytic techniques taught them as a result of their participation in the training afforded by the Signal Intelligence School, as well as his pleasure at the manner in which the individual members of the team earnestly and wholeheartedly collaborated in this joint effort. 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 procurement of personnel, supplies, and special information when needed.

October 14, 1940

William F. Friedman,
Principal Cryptanalyst