NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

ELEMENTARY COURSE IN CRYPTANALYSIS

INDEX

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

RULES FOR STUDENTS

INTRODUCTION

1. You have been enrolled in the correspondence course in Elementary Cryptanalysis. Your request for enrollment is appreciated and it is the belief of this office that you will find the course interesting and useful.

SECRECY

2. DO NOT DISCUSS THIS COURSE WITH ANY ONE, EXCEPT MEMBERS OF THE NAVY OR NAVAL RESERVE WITH WHOM YOU HAVE BUSINESS IN CONNECTION WITH THIS TRAINING.

3. THE NUMBER OF PERSONS SKILLED IN CRYPTANALYSIS, THEIR IDENTITY, AND THEIR DEGREE OF PROFICIENCY MUST BE CAREFULLY GUARDED.

4. A KNOWLEDGE OF THE MERE EXISTENCE OF THIS COURSE OF TRAINING MUST BE RESTRICTED TO THOSE CONCERNED. DO NOT USE THE WORDS CRYPTANALYSIS, INTELLIGENCE OR SECURITY IN TELEGRAMS NOR IN ANY MANNER ACCESSIBLE TO UNAUTHORIZED PERSONS.

ROUTINE TO BE FOLLOWED

5. The course consists of twelve assignments. Each assignment consists of a set of instructions, followed by a number of problems to be solved.

6. The assignments should be done in order.

7. Receipt of the next assignment will constitute acknowledgement of the correctness of the preceding assignment.

8. No assistance will be given on the first three assignments of the course. When requesting assistance on assignments 4 to 12, please forward your work sheets. Outline your reasoning and indicate the basis for your assumptions. Such assistance as you may be furnished can only be temporary in effect.

9. Students are urged not to obtain any books on the subject from libraries or other sources. Years of experience in teaching cryptanalysis have demonstrated that a student's progress is retarded rather than advanced by so doing.

10. No definite time for completion is placed on any assignment, but students are expected to give as much time to the course as their regular duties and necessary recreation will permit.

11. The solutions when completed should be mailed to the Chief of Naval Operations, using only the official envelopes provided for that purpose. It is necessary that the student's full name and address appear on the first page of work sheets of each assignment.

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

MECHANICAL AIDS IN CIPHER SOLUTION

1. Mechanical aids in cryptanalysis will not by themselves solve any problem, but it has been found that by their use the student is able to concentrate on solution more deeply and is therefore successful in cases where he otherwise might have failed or at least been delayed. Some of these aids or "tricks of the trade" are given below.

2. First, the student should provide himself with cross-section paper, preferably ¼" x ¼" for use as work sheets. The cipher text should be copied in ink on the work sheet, leaving adequate spacing between lines for the insertion of plain text assumptions and of frequencies of individual letters when applicable. If the cipher text furnished is spaced into correct word lengths, the text on the work sheet should be similarly spaced. If the cipher text is spaced into groups of five letters, it should be copied solid on the work sheet without spacing between groups to eliminate the mental hazard of unconsciously trying to make word endings at the end of groups. Next, repetitions and peculiar letter distributions should be located and underlined in ink. From these repetitions and peculiarities an analysis of the problem is made in accordance with the methods explained in the various assignments of the Elementary Course in Cryptanalysis.

3. When the preliminary work is completed, the student should proceed to enter plain text assumptions in pencil under the inked text. After a complete trial, if the assumptions prove incorrect, they may be erased and new assumptions tried without destroying the inked cipher text, repetitions, symmetrical sequences and frequencies. Under these conditions, the student almost invariably makes assumptions of words or phrases more daringly and thereby greatly expedites solution.

4. In polyalphabet systems, after learning the length of the period, the cryptogram should be written in lines across the work sheet in such a manner that cipher letters enciphered in the same alphabets will line up vertically from line to line. Each period or cycle may then be blocked off by a vertical line, and after numbering each alphabet in the top line, the student knows at a glance in which cipher alphabet any letter belongs. Many students carry this segregation further by using colored inks or pencils, a different color for each alphabet.

5. In problems employing twenty-six secondary alphabets instead of laboriously writing out all the alphabets in the Vigenere table, considerable time may be saved by drawing diagonal lines from the first secondary downward in varied color crayons. "Running down" the diagonal to find the correct value is fast and easy on the eyes.

6. Neat, well arranged work sheets and short cuts are worth while but solution depends upon the student's ability to analyze the problem correctly to interpret the significance of repetitions, symmetry, and peculiar letter distributions, and finally, upon his skill in placing the right word in the right location.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 1

INTRODUCTION

1. The student should immediately grasp the idea that his success as a cryptanalyst will depend almost entirely upon his own initiative and industry. A complete mastery of the art of cryptanalysis can only come as the result of independent study and the solution of cryptograms themselves.

2. Although the principles to be dealt with in elementary cryptanalysis are widely known, a knowledge of the mere existence of this course must be restricted to members of the Naval Service. The number of persons skilled in cryptanalytics, their identity, and their degree of proficiency, must be carefully guarded. Do not discuss anything connected with this course with anyone outside the Navy or Naval Reserve.

HISTORICAL NOTES

3. Cryptography, in its simpler forms, would appear from the evidence available to be as old as the written language itself. In fact, it seems probable that it may have in some instances actually ante-dated the written language, for we find numerous indications of usage, in the most remote times, of arbitrary signs for conveying secret information. Certainly by the time of the Greek and Roman civilizations we find cryptography occupying an important place in practically all important military operations. Julius Caesar is reported to have used a system in which each letter was replaced by the letter in the alphabet in the third position from it, such as, D for A, etc., while Augustus used the letter preceding the desired letter. It is interesting to note that this system with variations is still in use by amateur correspondents today.

4. Throughout the Middle Ages the art and practice of cryptography continued to develop. Numerous scholars and philosophers attempted to construct a perfect cipher. Among these might be mentioned Francis Bacon and Blaise de Vigenere, both of whom contributed materially to the art without, however, achieving the ideal for which they sought.

5. In these early days the transmission of communications was ordinarily restricted to the use of couriers and other equally slow and uncertain means. Frequently, the use of trustworthy messengers achieved the result desired and the employment of cryptography was not always essential to secrecy. With the advent of telegraphy all this was changed. Communication became almost instantaneous, but the channels themselves could not be so thoroughly guarded. Wire tapping was nearly always possible with the ordinary telegraph or cable, but with the advent of radio, even this became unnecessary, for radio transmissions are always available to anyone with a sufficiently sensitive receiver. All this tended strongly to concentrate attention on cryptography as the only means available whereby a reasonable degree of secrecy could be attained, and led to a much more rapid advance of the art. It also served to crystallize development along those lines which were suitable to telegraphic transmission, eliminating to a large extent the importance of secret inks, as well as pictorial, and such other kindred methods with which we need not concern ourselves. A cryptogram to be transmitted by telegraphic means must, of necessity, consist primarily of letters or numerals whether alone or in combination.

6. While the history of the development of cryptography is none too complete, the history of cryptanalysis is even more fragmentary and one must resort even more to surmise. It is likely that cryptanalysis is as old as cryptography itself, for it seems to be an innate trait of human nature to attempt to read the secret of others. Fortunately for the peace of mind of the majority of us, this trait seems to have been most often deflected into the pursuit of the puzzles and riddles which have occupied mankind in all ages.

7. Despite the general lack of historical material numerous instances of the use of cryptanalysis do stand out. After the battle of Naseby, Cromwell employed the English mathematician, John Wallis, to decipher the secret papers of Charles I, proving conclusively that the King has been guilty of double dealing in his negotiations. Another early investigator, Francois Viete, successfully analyzed the cipher used by the Holy League, but the effort very nearly cost his life, for it was charged that only by the use of necromancy could he have obtained the key, and it was with great difficulty that he cleared himself. At a much later date, Edgar Allen Poe delighted the world with "The Gold Bug" and his treatises on cipher analysis. Also, much reference to cryptanalysis is to be found in modern detective literature, but, in general, history is strangely silent on this important subject. This is no doubt largely due to the high degree of secrecy with which such matters have of necessity always been clothed. Disclosures of any kind are highly inimical to the interests of the military or diplomatic cryptanalyst, as well as to the country which he serves, for such disclosures almost invariably close an important avenue of information. It should not be concluded from this, however, that cryptanalysis has failed to play an important part, both in peace and war. An instance of this may be noted in the affair of the Zimmerman note to Mexico during the World War. The details of that affair are so well known that they need not be rehearsed here, but we should note how the reading of a single enemy message so materially aided England in bringing the United States into the war. In the more restricted fields of military strategy and tactics, it is quite obvious that the commander who has full knowledge of the enemy's plans and intentions through the reading of his intercepted despatches is in a much better position for bringing the action to a successful conclusion than one who is denied this information. Thus the military importance of the successful cryptanalyst can be scarcely over emphasized.

8. The rise of modern communication methods, especially radio, have had two very profound effects on cryptanalysis. Due to the resultant improvement of cryptographic methods noted above, the skill and labor involved in the processes of analytical solution has been greatly increased. On the other hand, however, there has been placed in the hands of the cryptanalyst an almost infallible source of cryptographic material which in former times could scarcely be obtained except as the result of fortuitous chance. This has led to the development of cryptanalysis to the high status which it holds almost universally today. With this development, regrettably enough, the United States has scarcely kept pace. It is doubtful if the time will ever come when this country can and will maintain in times of peace a highly developed and well organized cipher bureau such as are reputedly maintained by other countries and for that reason the primary reliance in time of war must be placed on the skilled amateur cryptanalyst. It is in the hope of establishing such a body of trained amateurs that this course has been inaugurated.

DEFINITIONS

9. The definitions found in this course have been taken from the Army Extension Course in "Elementary Military Cryptography" through the courtesy of Major W. F. Friedman, Signal Reserve, U. S. Army.

10. Cryptology is that branch of knowledge which treats of all the means and methods of secret intercommunication.

11. Cryptography is that branch of cryptology which treats of the various means, methods, and devices for convering plain-text messages into cryptograms and reconverting the so-produced cryptograms into their plain-text form by a direct reversal of the steps or processes employed in the original conversion.

12. Plain text is writing which conveys an intelligible meaning in the language in which it is written.

13. Cryptographic text is writing which conveys no intelligible meaning in any language, or which apparently conveys an intelligible meaning that is not the real meaning intended to be conveyed.

14. A cryptogram is a communication written in secret language, which may be transmitted by any of the agencies of inter-communication. As mentioned before, we are concerned only with cryptograms which can be transmitted by radio or telegraph.

15. Cryptographing and decryptographing are accomplished by means collectively designated as codes and ciphers. In Cipher systems cryptograms are produced by applying the cryptographic treatment to individual letters of the plain text messages, whereas in code systems cryptograms are produced by applying the cryptographic treatment to entire words, phrases, and sentences of the plain-text messages. The code systems become, in the final analysis,a more or less highly specialized form of substitution.

16. Substitution and transposition are the only two distinctly different types of treatment which may be applied to plain text to convert it into secret text, yielding two different classes of cryptograms. In substitution the elements of the plain text retain their original positions or sequences, but are replaced by other elements with different values or meanings. In transposition the elements or units of the plain text, whether one is dealing with individual letters or groups of letters, retain their original identities but merely undergo some change in their relative positions or sequences so that the message becomes unintelligible.

17. It may be stated that, as a general rule, all or nearly all cryptographic systems suitable for practical use can be broken down, or solved, that is, properly prepared cryptograms can be "translated" or read without a knowledge or possession of a general cryptographic system and the specific key applying to the cryptograms.

18. That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptograms is called cryptanalytics.

19. The steps and operations performed in applying the principles of cryptanalytics constitute cryptanalysis. To cryptanalyze or to decrypt a cryptogram is to solve it by cryptanalysis.

20. The normal alphabet for any language is one in which the sequences of sounds or symbols have been definitely fixed by long usage or convention.

21. A cipher alphabet is one in which the elementary speech sounds are represented by characters other than those representing them in the normal alphabet.

22. When the plain text of a message is converted into secret text by the use of one or more cipher alphabets, the resultant cryptogram constitutes a substitution cipher.

23. It will be convenient to designate that component of a cipher alphabet constituting the sequences of speech-sounds, the plain component, and the component constituting the sequence of symbols, the cipher component.

24. As regards the sequence of the letters forming its cipher component, cipher alphabets are of two kinds:

(a) Standard cipher alphabets, in which the sequence of letters in the cipher component is the same as the normal, but either shifted from its normal point of coincidence with the plain component or reversed in direction.

Example -

Direct Standard Cipher Alphabets

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

It is obvious that the cipher component can be applied to the plain component at any one of 26 points of coincidence (except the one which coincides exactly).

Reversed Standard Cipher Alphabet

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

Here the cipher component can be applied to the component at any one of 26 points of coincidence. This is also an example of a reciprocal alphabet, that is, the equivalents are reversible or reciprocal in pairs. (A plain is Q cipher, and Q plain is A cipher). Thus reciprocal alphabets may serve either as enciphering or deciphering alphabets.

(a) Mixed cipher alphabets, in which the sequence of letters or characters in the cipher component is no longer the same as the normal in its entirety.

Example -

Random Mixed Cipher Alphabets

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

Systematically Mixed Cipher Alphabets

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

Systematically-mixed cipher alphabets will be discussed in Assignment No. 2.

25. If a cipher alphabet is drawn up and a message enciphered by its means, letter-for-letter consistently throughout the message, it is said that the cryptogram has been enciphered by a single alphabet, and it is a single-alphabet substitution cipher. When only one alphabet is employed, the system is technically called monoalphabetic substitution, and when two or more cipher alphabets are employed, it is called poly-alphabetic substitution.

SOLUTION OF A MONO-ALPHABET SUBSTITUTION CIPHER

26. The following problem is an example of a mono-alphabet cipher of the simplest type, that is, one of which the plain language word lengths have been left intact, and not combined in 5-letter groups for telegraphic transmission, as is ordinarily done.

EIFIXQZS QXXQOJM PNZDM DCXILIMN PS IXQFIQD DQVQF

QWXJCZIXIMY XJQX KMZEQD YWPEQZIDMY JQN PMND CZNMZMN

XC KC IDXC EMNIXMZZQDMQD YMQ XC QXXQOG SJM XUC

XZQDYBCXY OQZZSIDK QEMZIOQD YCFNIMZY EQZYMIFFM QDN
XCWFCD BMZICN ZMAWMYX FCDNCD PM IDLCZEMN HQOGYCD

27. The basic principle of cipher solution is that underlying the cipher text is plain text and the peculiarities of the plain text language itself lead to the solution. Solution is thus based on language itself rather than on the frequency of occurrence of individual letters. To fix this principle firmly in the mind of the beginner, an illustration of solution of this problem is given.

28. First, the cipher text is examined for repetitions and peculiarities of letter distribution. Repetitions have been underlined, and they represent words or parts of words which are probably common in English, otherwise they would not be repeated in such a short message. Peculiar letter distributions are: doubled letters, repeated letters within a small number of letters, and reversed digraphs. Some of the peculiar distributions have been overlined in the cryptogram.

29. It should be remembered here that language cannot be written or spoken without using certain connective words, syllables, and phrases. The most common of these are: that, which, tion, ing, ence, the, been, have, had, has, and, to, of, but, not, in. Also, punctuation is often used so the words "period", "comma", and "stop" may be added to the list. Since these words appear so often in the English language, regardless of subject matter, one or more of them has an excellent chance of appearing as a repetition in the cipher text.

30. Having carefully scrutinized the text, the next step is to make assumption of plain language values. Andre Langie, a French author of works on Cryptanalysis, has said that the motto of the cryptanalyst should be: "Let's suppose". He has also said that the most important aid in cipher solution is a good eraser. In other words, make logical assumptions where possible; if they do not lead to solution, erase the assumptions which have been proved incorrect and make others.

31. In our problem the word XJQX immediately attracts attention. First, we know it to be a complete word. Even when the text is not spaced into proper word lengths, such a combination would invite attention because it fits the very common word "that". Therefore, tentatively substitute T,H,A,T (plain) for XJQX. To verify this assumption, substitute the assumed values throughout the cipher text wherever X,J,Q appear. (The student should follow through on this solution by actually performing each stop). The assumption is certainly now a good possibility because of the excellent combinations which it gives elsewhere in the message: XJM (cipher) = TH - (plain); *JQN(c) = HA - (pl); QXXQOG(c) = ATTA - - (p). If the initial assumption was correct, then the M of XJM must represent E(p) to make XJM(c) = THE. Also, in JQN(c) = HA - (p), N(c), probably represents either S(p) or D(p) to make HAS or HAD. Where XC(c) = T - (p), C(c) must represent O(p). Therefore, throughout the text substitute E(p) for M(c) and O(p) for C(c). This substitution gives some excellent combinations of plain letters and no combinations which are impossible. Look at IDXC(c) = --TO (p). Obviously ID(c) - IN(p). Again substitute throughout. Now, there can no longer be any doubt as to the correctness of our initial assumption. IXQFIQD(c) = ITA - IAN, so F(c) = L(p); KC(c) = GO(p); QDN(c) = AN - (p), So N(c) = D(p). Substitute the newly recovered values, and continue the process. The entire cipher message is solved very easily from this point on.

32. The complete translation is: MILITARY ATTACHE BERNE NOTIFIED BY ITALIAN NAVAL AUTHORITIES THAT GERMAN SUBMARINES HAD BEEN ORDERED TO GO INTO MEDITERRANEAN SEA TO ATTACK THE TWO TRANSPORTS CARRYING AMERICAN SOLDIERS MARSEILLE AND TOULON PERIOD REQUEST LONDON BE INFORMED JACKSON.

33. The problem was solved without paying any attention whatever to frequency tables, and without any knowledge whatever as to the nature of the text, except that it was in English. Only one assumption had to be made and then step by step it was only necessary to substitute obvious values after substituting the initial assumed values. Had the initial assumption been incorrect, it would have been erased and a new start made. There were other obvious breaks which

would be inevitable and soon be found by "trial and error" or, if you prefer, by hypothesis and test. The three words in sequence XC KC IDXC is an excellent starting point and would soon have been assumed to be TO GO INTO. Another was the two words QXXQOJM and QXXQOG. The latter would sooner or later have been assumed to be attack and this would make the first ATTACHE.

34. The problems given the student in Assignment No. 1 for solution are to be solved in the same manner, which is called "by inspection". No frequency tables are to be employed. After solution of these problems, the student will readily see that ciphers of this type prove to be a very inadequate form of camouflage.

35. The lesson to be learned from Assignment No. 1, which should never be forgotten in Cryptanalysis, is "The fundamental principle of cipher solution is based upon the peculiarities of the plain language itself".

---

* XJM (cipher) = TH (plain) will hereafter appear XJM(c) = TH - (p). (K) is also used to mean (key).

PROBLEMS TO ASSIGNMENT No. 1

Answer the Following questions:

1. What is the difference between cryptography and cryptanalysis?
2. What is the difference between a code and a cipher?
3. What is the difference between substitution and transposition ciphers?

Solve the following problems:

Problem No. 1 -- Non-Naval Text

F T U E E T A D F O D K B F A S D M Y U E S U H Q Z

M E M Z Q J Q D O U E Q U Z F T Q E A X G F U A Z

A R M O U B T Q D N K U Z E B Q O F U A Z

Problem No. 2 -- Non-Naval Text

D S V M Z H P V W Z Y L F G S R H K O Z M L U

X Z N K Z R T M T V M V I Z O H G L M V D Z O O

Q Z X P P L M I V K O R V W G L Z M R M J F R H R G R E

X S Z K O Z R M X Z M B L F P V V K Z H V X I V G

B V H G S V V Z T V I X O V I R X Z M H D V I V W

D V O O H L X Z M R H Z R W G S V T V M V I Z O

Problem No. 3 --Non-Naval Text

D C L C V S R U C T N S B U C G T O B S P P G R Y D

E S U U M T Y E G N Y S T Z G O D S T C E S T O Y D C P G

F V C N S K G P D E P C G N Y T A G F C N N C P

Y T N C P T G N Y S T G V M T D C P O N G T D Y T A

Problem No. 4 -- Non-Naval Text

X A E R K V Z Z B Z F B B Q W O L Z I B O

L K I K M Q I K C U F F W O H Q M K B X A

M I W H E Z V I Q Y O F X J K E R X O N U E

E Z B Q W L Z I B O Q I K I U A E Z V K E R K I

Q A B E R K E K T E X O B X S X B K B X A E Z

W I Z U H O Z C C X S K F K E E K I O E Z

X A O U I K Q M M U I Q M W X A E K F K V I Q H R X M

E I Q A O Y X O O X Z A

Problem No. 5 -- Naval Text

F E N F W E N D H A N D O X Z N E V W P W D

S N E H N B A U D U O X Z E N Z F R O M T B L N

D B J N T H O E D N N X W F E B R F N E B H Z I N

F E N F W E N Z T H E J W G B J O J M F N N Z

D V N X D P Y X H D M

Problem No. 6 -- Non-Naval Text

N I X T R Y I L T N O N O Y W N Z X C R F L A X

R A H W R T W N O O C W X K N O M X F R A

C W X N O Y W N Z X C N I X I X T R Y I L T N O

R A Y N R I F

Problem No. 7

D O I B W Y U T X B C G E S W B S S B V O W Y R B W

S T X T V T Y E V B X B E O B B E Z C D E M B Z Y G W V B

O Y O C W B B U T X B U Y G W

Note: The word "destroyer" is believed to be in the text of this message.

Problem No. 8

A L T D M V S R J B X T Y L I P R N A V J U

I S B D C F N W O S B Q R R V A K S V C C O T M

V D Y L P U M A Q R B P F I O J K N P W F D L D E O

T V Q H

Note: If solution is not achieved in 45 minutes, break the seal and read the next page.

Before you mail the solutions to this assignment please include your full name, rate, rank, or title, and latest address. Use only the official envelopes provided for mailing your work sheets.

Problem No. 8 cannot be solved. It is a meaningless jumble of letters written at random.

POSTMORTEM

Having solved problems No. 1 to 7, and having learned that No. 8 is really not a cryptogram but a hodgepodge of letters, the student should be impressed with the fact that problems Nos. 1 to 7 can be solved because language is hidden by the cipher and No. 8 cannot be solved because there is no language there. Furthermore, he has seen how simple this type of problem becomes when there is a "KNOWN" word as in Problem No. 7.

Note: There are no more dummy problems in the Elementary Course in Cryptanalysis. All problems can be solved by the student.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 2

MECHANICS OF THE ENGLISH LANGUAGE

1. The problems in Assignment No. 1 were solved by inspection, illustrating the fundamental principle that cipher solution is based on the peculiarities of the underlying plain text. Words were assumed instead of individual letters, which led to rapid solution of the cryptogram. Before proceeding to more complex types of ciphers, a brief description of the individual letter distribution is given.

The English language is written by means of 26 characters called letters, which, taken together and considered as a sequence of characters, constitute an alphabet. Nearly all written languages are similar, but there are a few exceptions, notably Chinese. The principles discussed herein concerning the characteristics of English apply to all modern languages of alphabetical construction.

If a tabulation of the occurrence of individual letters, called a frequency table, is made of a large volume of ordinary Naval text (nearly but not quite identical with English literary text) some interesting facts are disclosed. The Mechanics of English Table shows graphically the relative frequency of each individual letter to be expected in 200 letters of Naval text (based on an actual count of 20,000 letters of text). Note that the most frequent letters are E, T, O, N, A, I, R, and S, and the most infrequent are J, K, Q, X and Z.

Just as single letters have characteristic frequencies, pair of letters, called digraphs, and sets of three letters, called trigraphs, do also. These tables are also given under Mechanics of English.

2. Frequency tables should be used only as a check on assumptions. A very common fault among amateur cryptanalysts is the placing of too much weight on the frequencies of individual letters. For instance, "E" and "T" have the two highest average values in English text, but they are not necessarily the highest-frequency letters in a given cryptogram. Repetition and peculiar letter distributions are far more important than frequencies. As an example of the above principles, a 4-letter repetition is found in the text and there is strong evidence to show that these 4 letters are word endings. Since it is a repetition, it probably is a common word ending. If no previous correct assumptions had been made, the decision between the common endings - ENCE, MENT, TION, and ING must be made. Here the frequency table comes into play for the first time. All of the letters involved are high frequency letters excepting M, C and G. M occurs as the first letter of the repetition. C occurs as the third letter and G as the fourth. The frequency table usually is very helpful in choosing the correct possibility, but even in such a case it cannot be relied upon completely. With limited text, or text containing unusual language, frequency tables must be viewed with suspicion.

3. Another application of the frequency table is its use in identifying vowels and high-frequency consonants. With limited text, repetitions may not occur, or the cipher system may be sufficiently complex to conceal repetitions in the plain text. As a measure which is more or less a last resort, vowels are classified as such, not individually as A, E, etc., but as a class. Before attempting this, a study of the digraphic frequency table shows that in general vowels combine infrequent with vowels, but they do combine frequently with both high and low frequency consonants; that high frequency consonants combine most frequently with vowels and other high frequency consonants; and that low

frequency consonants combine most frequently with vowels. Vowel classification in a complicated system leads up to the point where "assumptions that fit" can be made. Even here the frequency table is only a guide, and sometimes an unreliable guide.

4. Recently (March, 1937) an author published a book of over 50,000 words in which the letter "E" does not appear at all. The book is readable and the sentences are not jerky or awkward. In normal English the six vowels A, E, I, O, U, Y represent 40% of the total text. Of these, the value of E alone is 13%. Yet in a book of large volume without a single "E", the percentage of vowels used still must closely approximate the same value, 40%. That is, the number of vowels as a class, can still be depended upon and if "E" does not appear, the other vowels will be used with greater than normal frequency to compensate for its omission.

5. In Naval text the sum of the thirteen highest frequencies will usually equal or exceed 80% of the total numbers of letters in the text. This characteristic may be used in the identification of mono-alphabetic substitutions and transpositions.

6. Just as vowels represent a definite percentage of the entire text, the low frequency consonants J, K, Q, X, Z, together represent a definite percentage of less than 2%. One or more of these letters may vary considerably from its normal frequency in a given amount of text, but the percentage of the group will remain less than 2%.

7. Another use of the frequency table involves the classification of both vowels and consonants. In vowel classification it is usually possible to classify as vowels the letters representing A, E, I, and O without difficulty, but U and Y are almost impossible to identify as vowels. Therefore, in connection with vowel classification, the classification of groups as high, intermediate, and low frequency is helpful. The eight high frequency letters E, T, O, A, N, I, R, S comprise 66½% of the text. Of this amount, the four vowels E, O, A and I are 36½% and the consonants T, N, R and S 30%. The other 18 letters, including the low frequency group J, K, Q, X and Z comprise the other 1/3 of the text. It is usually easy to pick the 8 high frequency letters of the cipher text with reasonable assurance that they represent at least 7 of the 8 high frequency letters of English because, as the frequency table shows, the values of the next highest frequency letters after S drop sharply. Of the 8 highest frequency letters, it is possible to classify 4 vowels, as explained previously, leaving the other 4 automatically classed as being in the T, N, R, S group. Thus with 4 vowels, 4 high frequency consonants, and 5 low frequency letters classified, the problem of making correct assumptions to fit the cipher text is simplified.

8. The foregoing discussion has been concerned only withe the English language. English is one of the most difficult of languages for the cryptanalyst. French and German, for example, both show E as outstandingly high, much more so than in English, and this letter can be spotted at once from the frequency table of the proper alphabet. Also, these languages have certain invariable high frequency combinations such as the German CH and the French or Spanish QU, which aid analysis to a great degree. Such language characteristics undoubtedly have led European authors of works on this subject to stress the value of individual letter frequencies far beyond the point where they can be depended upon.

9. In all but the simplest problems, a frequency table is constructed for use as a guide, as explained in the foregoing paragraphs. To construct a frequency table, the A's, B's, etc., of the cryptogram are counted. It is usually best to do this graphically, as shown in the Mechanics of English Table. The reason for this will become apparent in later assignments. It is also beneficial to make a Trigraphic Frequency Table. This is done by listing, for each letter of the Alphabet, A, for Example, the letter which precedes (prefix) and the letter which follows (suffix) for each appearance of A in the text. For the following cipher text - B A D V B C A Q R B A D L P R A S W B Q A, a

partial (for A and B only) trigraphic table is:

	B C B R Q	- V R W	The upper line of letters listed with A represents the prefix in their order of occurence, the lower line gives the corresponding suffixes. This table shows at a glance the digraphs, trigraphs, and repetitions in the message. It is the only sure way of locating all repetitions in a long cryptogram, and it is valuable in classifying vowels.
A		B	
	B Q D S -	A C A Q	

10. In the Mechanics of English table, the frequency of initial and final letters is also given. This should be used in the same manner as any other frequency table -- merely an aid and not a sign post.

MECHANICS OF ENGLISH TABLE (For Naval Text)

Frequency of Individual Letters to be expected in 200 letters of Naval Text. (Based on a count of 20,000 letters).

15	A	---------------
3	B	---
6	C	------
9	D	---------
26	E	--------------------------
5	F	-----
5	G	-----
5	H	-----
15	I	---------------
	J	
1	K	-
6	L	------
4	M	----
16	N	----------------
17	O	-----------------
5	P	-----
	Q	
15	R	---------------
11	S	-----------
18	T	------------------
6	U	------
3	V	---
3	W	---
1	X	-
3	Y	---
1	Z	-

Frequency of Digraphs and Trigraphs to be expected in 2,000 letters of Naval Text. (Based on a count of 20,000 letters).

Most Frequent Digraphs

ER-43	RO-24	OR-20
IN-42	ES-23	OU-20
ON-38	ST-23	RI-19
EN-34	TI-23	ET-18
RE-34	CO-22	PE-18
AT-31	ND-22	VE-17
AN-29	NE-22	AR-16
NT-27	NG-22	TA-16
TE-27	TO-22	DE-15
EE-25	IO-21	LE-15
ED-24	TH-21	SE-15

Most Frequent Trigraphs

ING-17	ERI-9	ATT-6
ENT-13	ION-9	DRE-6
ERO-11	PER-9	LAN-6
EEN-10	TEE-9	ONE-6
GHT-10	COU-8	RED-6
IGH-10	IVE-8	RIN-6
TIO-10	OUR-8	RIO-6
ZER-10	OUT-8	TER-6
AND-9	EST-7	TIN-6
	ATI-6	

FREQUENCY OF INITIAL AND FINAL LETTERS

Letters	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Initial	9	6	6	5	4	2	3	3	1	1	2	4	2	2	10	2	-	4	5	17	2	-	7	-	3	-
Final	-	-	1	-	17	10	6	4	2	-	-	1	6	1	9	4	1	-	8	9	11	1	-	1	-	8	-

ASSIGNMENT No. 2

DIGRAPHIC TABLE

First Letter
(Second letter appears in left column)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	4	7	10	9	2	4	6	2	-	1	14	11	10	3	4	-	14	8	16	4	3	4	-	3	-
B	4	-	-	2	3	-	-	-	1	-	1	1	1	3	-	-	2	2	2	1	3	-	-	-	1	-
C	9	-	1	2	8	1	1	-	6	-	1	1	-	8	3	-	-	6	8	4	1	-	-	1	2	-
D	5	1	-	2	24	-	1	-	2	-	-	-	-	22	11	-	-	9	1	3	2	-	-	-	1	-
E	-	8	10	15	25	2	8	7	2	-	3	15	5	22	4	18	-	34	15	27	3	17	10	-	2	10
F	2	-	-	3	7	1	1	1	5	-	1	1	-	5	9	-	-	2	2	4	-	-	-	1	3	-
G	3	-	2	1	1	-	1	-	11	-	-	-	-	22	2	-	-	3	-	1	1	-	-	-	-	-
H	1	-	5	1	2	-	11	-	-	-	-	-	-	2	-	1	-	-	4	21	-	-	1	1	-	-
I	8	1	1	12	7	13	2	6	-	-	2	8	4	6	6	1	-	19	13	23	4	4	5	4	1	-
J	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
K	3	*	4	-	1	-	-	-	-	-	-	-	-	2	1	-	-	1	-	-	-	-	-	-	-	-
L	7	6	-	2	6	5	2	-	8	-	1	6	1	2	4	5	-	1	2	3	2	-	-	1	3	-
M	2	2	-	2	6	1	-	1	2	-	-	-	2	2	9	-	-	3	1	1	2	-	-	-	2	-
N	29	-	-	-	34	-	1	-	42	-	1	-	-	3	38	-	-	3	1	2	9	-	-	-	-	-
O	-	4	22	4	6	12	2	3	21	2	-	7	4	10	2	7	-	24	5	22	-	1	6	-	2	-
P	4	-	1	3	10	1	1	1	2	-	-	2	2	2	8	3	-	2	6	3	1	-	-	-	2	-
Q	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-
R	16	-	4	8	43	2	2	7	10	-	-	1	-	2	20	8	-	2	1	10	1	-	1	-	1	-
S	11	-	1	6	23	1	2	1	10	-	-	2	1	9	9	3	-	8	6	8	4	-	-	-	2	-
T	31	-	4	6	18	5	6	11	11	-	-	1	-	27	7	2	-	10	23	8	10	-	-	2	2	-
U	1	1	-	2	1	1	3	6	-	-	-	1	-	3	20	1	3	4	6	4	-	-	-	-	-	-
V	3	-	-	1	7	-	-	-	9	-	-	2	-	-	1	-	-	-	-	-	-	-	-	-	-	1
W	-	-	-	1	2	-	-	1	-	-	-	-	-	1	4	-	-	1	3	12	-	-	-	-	1	-
X	1	-	-	-	4	-	-	-	5	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-
Y	5	2	-	3	1	1	-	-	-	-	-	2	3	-	1	-	-	-	-	8	-	-	-	-	-	-
Z	-	-	-	-	4	-	1	-	-	-	-	-	-	-	1	-	-	-	-	4	-	-	-	-	-	-

Digraphs to be expected in 2,000 letters of Naval Text. (Based on a count of 20,000 letters.)

SYSTEMATICALLY MIXED CIPHER ALPHABETS

1. The discussion contained in Part II is general in nature and contains information that is not necessarily exemplified in the following problems. In order to introduce certain ideas, and in order to present them completely, it was necessary to discuss these ideas beyond their possible application in this Assignment. The student is therefore warned to consider Part II as general information, introduced at this time to present cryptographic ideas which are applied in this and following assignments.

2. Any system which will permit the derivation of a sequence of letters from an easily memorized key, may be used to construct a systematically-mixed cipher alphabet. One of the most useful types is the keyword-mixed sequence. In this type the keyword or keyphrase is written down, repeated letters, if any, being omitted after their first occurrence; then the remaining letters of the alphabet are written in their normal order, omitting such letters as already occur in the key.

Example: Let the keyword be WASHINGTON. The corresponding mixed sequence becomes:

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

3. Although transposition methods have not yet been discussed, it will be necessary to demonstrate how these may be applied to keyword-Mixed Sequences to further disarrange the sequence.

Example: Three examples will be given using the keyword RENDEZVOUS. The keyword-mixed sequence may be written:

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

and the columns taken off so as to form the following sequence

(1) R A L E B M N C P D F Q Z G T V H W O I X U J Y S K

The alternate columns may be reversed to obtain this sequence:

(2) R A L M B E N C P Q F S Z G T W H V O I X Y J U S K

Also, a numerical key, derived from the keyword itself, may be applied to vary the order in which the columns are taken off:

5-2-3-1-9-8-4-7-6
R E N D Z V O U S
A B C F G H I J K
L M P Q T W X Y

The transposition-mixed sequence now becomes:

(3) D F Q N C P F B M O I X R A L S K U J Y V H W Z G T

4. Once aware of such systems of constructing cipher alphabets, it is comparatively easy to rebuild the generating figure. Note that, in example (1), W, X and Y are three letters apart with H, I and J to their left, respectively. This suggests that W, X and Y are on the bottom line of the generating figure, H, I and J on the next line above, and that V, O and U are in the keyword.

In example (2), the presence of LM, PQ and XY in their normally adjacent positions suggests that the alternate columns have been reversed, which is checked by the A and B on either side of LM, and the I and J on either side of XY.

In example (3), note again the HW, IX and JY combinations which suggest a columnar system and may be used to rebuild the original figure in much the same manner as in the case of the simple columnar transposition.

5. Another simple method of producing a systematically-mixed alphabet is called the decimation method. The basic sequence to be decimated is regarded as a circle, and the letters are counted off and written down in a separate list. When a letter has been used in the final sequence, it is eliminated from the basic sequence before the process continues.

Example: Suppose the number agreed upon is 7, and the basic sequence to be decimated is a normal alphabet. The letters will be taken from the basic sequence, after counting off, in the following order:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
16	4	10	20	19	21	1	18	8	5	13	15	11	2	24	22	17	6	9	25	3	26	14	12	23	7

The Mixed-Sequence resulting is:

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

6. Almost any transposition method may be applied in the construction of systematically-mixed cipher alphabets. Practical considerations limit the complexities which may be introduced, and the greatest amount of mixing by systematic processes will give no more security than that resulting from a random selection.

7. During the process of solution of any cryptogram, much labor can often be avoided by a reconstruction of the system used, when only a portion of the simpler types have been recovered. In any case, the solution of a cryptogram should never be considered complete until the system used has been determined and reconstructed, insofar as the available material permits.

ASSIGNMENT No. 2

PRIMARY AND SECONDARY ALPHABETS

8. It is obvious that the cipher component of a cipher alphabet may be shifted or slid against the plain component at 26 points of coincidence so as to produce a series of different enciphering alphabets. The primary alphabet is the basic arrangement of the original sequences, and the derived alphabets are called secondary alphabets.

9. In producing the secondary alphabets the primary alphabet may be arranged as follows:

(a) The same sequence may be used as both the plain and cipher components, and slid against itself.

Example:

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

(b) The primary cipher component may be slid against the normal sequence.

Example:

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

(c) The primary plain and cipher components may be different mixed sequences.

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

10. When the plain component of a cipher alphabet is a normal sequence, as in paragraph 8(b) above, the original cipher sequence becomes evident as soon as the enciphering alphabet is reconstructed. However, when the enciphering alphabets of the type described in paragraph 8(a) and (c) are reconstructed with the plain components in normal order, the original sequences are not apparent.

11. The cipher alphabet in paragraph 8(a) would appear as follows when obtained after the solution of a cryptogram employing this alphabet:

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

Note the letters underlined, which indicate by their normally adjacent positions that these letters are adjacent in the primary cipher alphabet, which is reconstructed as follows:

Plain - EF JKL M PQR UV X YZ W A S H I N G T O B C D
Cipher - BC DEF J KLM PQ R UV X Y Z W A S H I N G T O

The letters not underlined are fitted in their proper locations, which are assumed from a knowledge of the possible constructions of the original sequence.

12. The cipher alphabet in paragraph 8(c) would appear as follows when the plain component is in normal order:

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

This alphabet may be rearranged in its original sequence in much the same manner as illustrated in the preceeding paragraph.

ASSIGNMENT No. 2

SOLUTION BY COMPLETING THE PLAIN COMPONENT

13. This is a very useful and rapid mechanical method of solving cryptograms when both the plain and cipher components are known sequences, but when their point or points of coincidence are unknown.

14. Consider the problem in which a direct standard cipher alphabet has been used. If we complete the normal alphabet sequence in a column under each letter, the result is the same as having tried the cipher component in each of the 25 possible points of coincidence with the plain component, and having applied the resulting deciphering alphabets to the cipher text.

15. If the first ten letters of the cipher text are F T U E E T A D F, the solution by completing the plain component will appear as follows:

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

An examination of the successive horizontal lines, called generatrices, (singular generatrix), discloses one and only one line of plain text: THIS SHORT. Instead of laboriously writing down the several columns, it is recommended that the student prepare a set of alphabet strips, each repeated so that every strip will contain 52 letters, and mount them upon some rigid material convenient to handle. Such a set of sliding alphabets will be found exceedingly valuable in all work of this kind.

16. Next consider the problem in which the cipher alphabet employed is any type other than a direct standard cipher alphabet.

17. In this case an additional step is necessary before completing the plain component sequence. In order to obtain the same result as having applied each of the 26 deciphering alphabets to the cipher text, the cipher letters must first be converted into their plain component equivalents. To find the plain component equivalents the cipher alphabet is written with both components in their original order, and placed at any point of coincidence.

18. Let us suppose the following random mixed cipher alphabet has been recovered from the solution of earlier cryptograms:

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

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

Also suppose another cryptogram, which begins F E N F W E N D H A, etc., is suspected of employing one of the secondary alphabets derived from this primary alphabet, that is, the same system has been used with a different key.

First convert the cipher letters into their plain component equivalents. Then use the normal alphabet sliding strips to complete the normal alphabet sequence beneath each plain component equivalent.

This example will demonstrate that although the whole series of values may be changed by merely shifting the cipher component to another point of coincidence, the solution of a cryptogram in a different key was obtained very easily, without any frequency table analysis.

Had the plain component been a mixed sequence also, the solution would proceed as in this example except that

ASSIGNMENT No. 2

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

the original plain component sequence would be used in completing the sequence beneath each plain component equivalent, instead of the normal alphabet strips.

PROBLEMS TO ASSIGNMENT No. 2

1. Define the word generatrix.

2. Answer the following questions:

   (a) What characteristics of a systematically-mixed keyword alphabet aid in the recovery of the keyword?

   (b) What is meant by converting the cipher text into its plain component equivalents?

   (c) What types of mono-alphabet substitution ciphers can be solved by the use of sliding strips alone?

3. Solve the following problems and reconstruct the system used:

Problem No. 1 Naval Text

K O D J W A S C H F W S F H C F X R F P W T R Q O F I T R D F B C X-
R B T R F W S I P R H F M R B O C T W B U C H H R T O B R S F R T
B R P W O H K O S O H O F X B R H T R Z K C J D F C P W G R
S C H F W S F W H T T R A O K R B S C M O R D W A A D R S B R F
W H T M J E A O S W F O C H D

Problem No. 2

Z N R D B U T D U W D G W M D H B Z X W X V K X W B W V W B N U
X P X W D R F U N S U E V Y B V X I L D X L Z V X D G L U L Y A M-
L K D W B U S M B I M G S L X X V K X W B W V W D G H N Z L
I N R R L D H N Z K I N R R L H H N Z I D W I B U M B X
I N Z Z D X A N U G D U I D

Problem No. 3

W U B G T B G G J K U P M B M V J M L Z J Z S U U M E X M P G U P
S E J N P B S U Z R G U J L M F U M R Z H B G G U N U M S S H R
D G J S J N E L X M D R B S N R M U Q B W B M U N U P U N S G R T U G
B S W W G U N U M S M R B W W G U E U M N J R M B F R M L
Z R G U J L M U G N I J S T C X J U S

ASSIGNMENT No. 2

Problem No. 4 Non-Naval Text

SIKED GKXRH VQNWH OKCIC UHGSC KEDSI RXNKS ADCOO WVCNE SGOWD
QDWWD RBHKE SGTDK EVRKE DGKXR DIKUD CWIGK VTCFD ESGVL ICICU
HGSGC IRSGI VKRDO DIRDI KVIWX UDGUD CWIDR QWVTK DZBKV VFG

Problem No. 5 Non-Naval Text

ZERKV CELKF UKTJN ACBTR KEFRE BFZBF BLAKA KTBTR KEFRE JERBI
TEREL ABKFZ EMKFK AEOBY TBFZV LKFRK VOETC BQEJE EFETA BJOKT
CEZYC KRCVE LABKF ANKAK AKTBO TNBFB LAJER BITEN MACEO BLUEV
BLAVO BPEZK FKAJP KWBUK FBAKN FTGKO OBFZE HVELK EFRE

Problem No. 6 Non-Naval Text

BQWDC IKVIF KQAAD OYCAQ JJACW CITOG CGJOJ JIOBJ QVGEV IVGCK
DVCSW CBJNI CNXAJ NOJVG BCKQJ DVXJA OPVIE VIJDC ICQNC YONJO
TVXGJ VEWXI CALIV XJQGC AOPVI QGJDC WICWO IOJQV GVEEI CHXCG
BLJOP ACNOG MVJDC IJDQG RNPCE VICJD CTCNN ORCPC RQGNJ VOWWC
OI

It is important that the Student's full name and present address appear on all work sheets and correspondence. Course material will be returned only in the penalty envelopes provided for that purpose.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 3

NUMERICAL CIPHER ALPHABETS

1. Cipher alphabets whose cipher components consist of numbers are practicable for telegraph or radio transmission. They may take forms corresponding with those employing letters.

(a) Standard numerical cipher alphabets are those in which the cipher component is a normal sequence of numbers, and the plain component is a normal sequence of letters.

Example:

Standard numerical cipher alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

Since there are but ten digits, it is obvious that, in order to represent a complete alphabet, combinations of at least two digits are necessary.

(b) Mixed numerical cipher alphabets are those in which the cipher component is not a normal sequence of numbers, used in conjunction with a normal sequence of letters in the plain component.

Examples: (1) Random mixed numerical cipher alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
76	88	1	67	4	80	66	99	96		2	69	90	77	5	87	60	89	79	3	78	68	98	86	70	97

This example will also illustrate a type of numerical cipher alphabet in which some of the digits may be employed singly and some in pairs to represent single plain-text letters, thus retarding the attempts of cryptanalysts to insolate the individual cipher equivalents of plain-text letters after they have been run together in the cryptogram.

(2) Systematically mixed numerical cipher alphabet

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

The pair of numbers which appear as row and column indicators are used as the cipher equivalent of the plain letter found at the intersection of the row and column. That is, A plain is 11 cipher, B plain is 12 cipher, etc.

Rectangles of various shapes and sizes may be used, having various key number arrangements, and including cells for proper names and places or blank cells. Also, the plain alphabet may be any type of mixed alphabet, and may be inscribed by following any prearranged route to fill the proper cells of the rectangle.

2. Numerical cipher values lend themselves to treatment by various mathematical processes to further complicate the cipher system in which they are used. These processes, usually addition or subtraction, may be applied to each cipher sequence individually, or to the complete numerical cipher message by considering it as one number.

52899

ASSIGNMENT No. 3

CIPHER ALPHABETS EMPLOYING VARIANTS

3. In order to disguise, suppress, or eliminate the characteristic frequencies of the plain-text letters, cipher alphabets may be made up with variant values in their cipher components.

4. An equal number of cipher values may be assigned each plain-text letter, usually by means of a systematic arrangement, or a set of values may be assigned each plain-text letter in accordance with its relative frequency in ordinary plain language.

5. A system which provides twelve variants of letter pairs for each plain letter may be constructed as follows:

Let the keywords be BALTIMORE and MARYLAND. The corresponding keyword sequences become:

(1) B A L T I M O R E C D F G H J K N P Q S U V W X Y Z, and

(2) M A R Y L N D B C E F G H I J K O P Q S T U V W X Z

The letters of the first keyword sequence are used as the row and column indicators of a 25 cell rectangle, and those of the second keyword sequence are inscribed within the cells of the rectangle according to a diagonal route.

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

In this example, A plain may be represented by any one of the following cipher equivalents:

BN, BV, MN, MV, DN, DV, NB, NM, ND, VB, VM, or VD.

6. There are not only numerous variations in the use of rectangles, but many types of lists and tables may be employed in the construction of miscellaneous types of cipher alphabets. The practical disadvantages in the use of most of these miscellaneous types in mono-alphabetic substitution are not compensated by any real gain in cryptographic security.

NOTES ON PREPARATION OF WORK SHEETS

7. Cross-section paper with one quarter inch squares makes the best work-sheet. A typewritten work-sheet is nearly as good, for it is the even spacing which is essential. Three spaces should be left between lines so as not to overcrowd the work-sheet. Use printed block capital letters. Colored pencils are helpful in marking off repetitions and peculiarities of letter distribution.

8. Over each cipher equivalent of a plain-text value write its frequency. Underscore all repetitions and reversible digraphs. Examine the text and overscore any peculiarities of letter distribution. Recording the frequencies on the work sheet is of the greatest importance when dealing with a minimum of text. It saves constant reference to the frequency tables, which interrupts the train of thought. It saves considerable time in the end, and might mean the difference between success and failure in a complex problem.

OUTLINE OF CIPHER SOLUTION

9. The solution of a substitution cipher generally progresses through the following stages:

ASSIGNMENT No. 3

(a) Analysis of the cryptogram(s)
   (1) Preparation of frequency table
   (2) Search for repetitions
   (3) Determination of the type of system used
   (4) Preparation of work sheet
   (5) Preparation of frequency tables for the individual cipher alphabets (if more than one).
   (6) Tabulation of long repetitions and peculiar letter distributions.

(b) Classification of vowels and consonants by a study of:

   (1) Frequencies
   (2) Spacing
   (3) Letter combinations
   (4) Repetitions

(c) Identification of letters

   (1) "Breaking in" process
   (2) Verification of assumptions
   (3) Filling in good values throughout messages
   (4) Recovery of new values to complete the solution.

(d) Reconstruction of system

   (1) Rebuilding of the enciphering table
   (2) Recovery of key(s) used in the operation of the system.
   (3) Recovery of the key or keyword(s) used to construct the alphabet sequences.

10. No outline can be made to suit all cipher solutions, because special conditions may call for short cuts or extra steps in solving a particular problem. Cipher solution is by no means an exact mechanical process, however the object of giving an outline is to show that success in cipher solution is the result of orderly reasoning.

11. Determination of the type of cipher system used in a given cryptogram is often the most difficult step in cryptanalysis. The student should notice the external characteristics of each new type studied, because a comparison of these characteristics is the basis for determining the type of system used in an unsolved cryptogram.

PRINCIPLES INVOLVED IN CIPHER SOLUTION

12. Whenever possible, classify the vowels and consonants before assuming values. The four considerations in distinguishing the vowels from the consonants are as follows:

(a) The low frequency values are almost invariably consonants of low or medium frequency. The intermediate frequency values are usually consonants but may be vowels. They cannot be classified except as they combine with letters already classified and are the most difficult to classify. The high frequency values are either the vowels "A, E, I, O" or consonants of high frequency.

(b) It is unusual to find over two or three consonants of low frequency in combination. Vowels usually stand alone - combinations of more than two vowels are extremely rare. A gap of six or eight letters between two known vowels indicates the need of one or more intermediate vowels.

(c) Consonants combine with vowels, most of which are of high frequency. Vowels combine with consonants, many of which are of low frequency. Letters associated with low frequency values are vowels. Letters associated with high frequency values are consonants.

(d) Of the 30 most frequent letter pairs, 22 are vowel-consonant or consonant-vowel, 5 are consonant-consonant, and 3 are vowel-vowel combinations. Repetitions in the cipher text indicate high frequency letter combinations. Therefore, the repetitions of a given letter combination creates the presumption that one of the letters is a vowel and the other a consonant.

"U" is of low frequency and can be classified only by "spacing" after A,E,I and O have been classified. The vowel of 5th highest frequency in an alphabet is almost invariably a "U". It is usually impossible to classify "Y" as a vowel partly on account of its very low frequency and partly because "Y" is sometimes a consonant.

Mark each vowel by a circle as soon as classified - both on the work sheet and the frequency table. Values identified as consonants should be marked by an overscore or some similar method.

13. The frequency table is only a guide in the identification of letters, and sometimes an unreliable guide. Repetitions are far more important than frequencies in the identification of letters. "E" is one of the poorest letters to identify first, as it combines with so many letters that it does not help in further identifications. "E" will always be discovered without special search. "N" is probably the most valuable letter to identify first, (and one of the easiest) on account of its frequent occurrence in "ING", "ENT", "AND", and "ION". Do not disregard the low frequency letters. A "G" may disclose an "N" or a "Q" show the "U" following it.

14. Do not force the solution by attempting to make a logical assumption prove correct when it cannot be verified. The attack should always follow the line of least resistance. Find a weak point in the cryptogram and then work on it until the cipher is broken. The beginning and end of a message are always weak, and there are usually several other good points of attack.

15. Do not give up an assumption too easily, but do not cling to it too long. Experience is the only teacher as to the time which should be spent on a given assumption. Consider what words would probably or even could possibly appear in the cryptogram, then try to fit them in. Check the letter values of the assumed words in a few places before filling in the assumed values throughout the cryptogram.

16. As far as possible, assume words or phrases with one or more letters repeated in them. Then fit them to the cipher text where the same peculiarities of letter distribution are found.

Example:

LVKKVKKVNNV	XNOAVJRJKOBDB	XFXHS
MISSISSIPPI	CRYPTANALYSIS	ENEMY

When repeated letters cannot be used to fit a word to the cipher text, the frequencies of the letters and the location of the vowels are nearly as good peculiarities of letter distribution on which to base an assumption.

17. In 1841, Edgar Allan Poe made the following significant statement which still remains of interest to present day students of cryptanalysis:

> "The basis of the whole art of cipher solution is found in the general principles of the formation of language itself, and is thus altogether independent of the particular laws which govern any cipher, or the construction of its keys".

18. Solve the following cryptograms. Naval telegraphic text has been used to give a certain degree of familiarity with naval language and to aid the student in making assumptions. The same general technique used in solving the problems of the first two assignments will also assure solution of these problems. Reconstruct the systems used in each problem.

ASSIGNMENT No. 3

Problem No. 1

0 6 0 2 1	0 0 5 0 1	0 1 0 5 1	5 2 2 0 2	0 6 0 8 2
3 2 5 1 0	0 8 0 4 0	2 2 1 0 9	0 8 0 4 0	8 2 2 1 1
0 8 0 4 1	7 1 5 1 3	1 4 2 2 2	1 0 2 2 4	0 2 0 1 2
2 0 2 0 2	0 1 0 8 1	9 0 6 1 5	1 7 0 8 0	1 1 1 2 2
1 4 0 2 0	1 1 9 0 6	0 5 1 0 0	2 0 2 1 1	2 2 1 4 0
6 2 3 1 9	0 5 1 5 0	1 2 2 1 3	0 2 0 5 0	6 1 3 0 2
0 5 0 1 1	0 0 5 2 3	0 6 2 1 0	2 2 2 1 4	0 6 0 2 0
2 2 2 1 4	0 6 0 2 0	2 2 6 0 2	0 6 0 5 2	1 1 9 0 2
0 2 1 1 2	2 0 3 0 2	1 7 2 4 0	2 1 9 0 2	0 6 1 5 0
5 1 1 0 6	0 2 1 9 0	5 0 6 2 2	0 1 0 5 0	5 0 1 1 9
0 5 2 1 1	5 2 2 1 5	0 5 0 1 2	2 0 5 1 8	0 5 0 6 0
6 0 5 0 3				

Problem No. 2

5 3 2 4 1	5 4 5 3 2	2 4 4 3 2	5 1 2 4 3	2 4 2 3 1
5 4 4 4 5	4 5 3 2 5	1 4 3 4 4	1 4 1 5 2	1 4 1 1 5
4 3 4 5 3	5 2 1 2 3	3 5 1 2 5	1 1 4 2 1	5 3 3 3 4
5 3 2 4 4	2 3 1 5 4	5 4 5 2 4	4 3 2 4 1	4 4 4 3 2
1 2 5 3 2	4 4 3 4 4	2 4 1 5 4	4 4 5 2 4	4 3 3 5 2
1 5 3 3 3	1 3 1 4 4	4 1 5 4 5	4 4 5 1 4	3 2 5 1 5
2 3 2 4 1	5 5 2 2 4	4 3 1 5 3	1 3 3 1 3	3 1 4 5 5
3 2 4 1 3	4 5 2 1 2	5 3 3 5 2	2 4 3 4 1	3 1 2 4 5
4 4 5 2 3	3 4 4 3 3	2 2 3 3 3	5 3 3 4 5	2 1 3 5 2
4 4 4 4 4	4 5 3 2 1	5 1 3 1 5	5 2 2 4 4	3 1 5 3 1
2 4 5 1 1	3 1 4 2 4	4 4 3 3 4	3 1 5 2 2	3 5 2 4 2
5 3 5 2 1	3 3 1 3 3	1 2 3 1 2	1 3 1 4 3	3 4 5 3 3
1 2 1 3 4	4 4 1 2 4	4 3 3 3 1	2 1 4 3 2	2 4 3 3 3
1 3 2 4 5	1 2 2 5 3	5 1 2 5 3	2 3 3 5 1	2 5 1 1 4
4 4 1 5 4	5 4 1 4 3	2 4 4 4 2	4 1 3 4 5	1 5 2 2 1
2 5 1 4 5	1 2 1 3 2	4 4 5 3 2	1 2 5 1 4	4 1 5 1 3
1 4 2 5 2	4 2 4 4 5			

ASSIGNMENT No. 3

Problem No. 3

A O U E I A I O I A U E E U E U A I I A I O I A U
E E A A O U E U E A O E I I U E U E O E E E A I A
I O A U E U O A E U U O I O A I I E U E O I A I I
I E U A O A U E A E E O I O E E E I O A I I E O O
O A A O A I E U A E A A A I E O E U U A A O A I U
E I O A O I O U A E I U A A O I A U E I A I O U A
E U U E I I U A E U E U O E I O A I A A U E E U A
E O O O A A O A I E U A E E E O I O E E E I O A I
I E O O O I A E I O U E I O O I A I A O O A U E I
O U E A A E O E U O I A I E U I A O I A A U A U E
I I O I A A A E A O A I E O I A E U E U U E A I O
I E O A O O E A O I E E U U E O I A E A O U A A O
U E O I I E A O

Problem No. 4

I D U G E J F O I K I Q P E D I A L U M W I E C Z
A G U H A Q I V E C E I K U G K I L A E P Q I K I
F O G U A Z I K O P E P I Q E J A Z Q I Q I D I K
I B A I Q H A I K P O O L A H I Q W I U G A H A L
K I Q I I D E V O L A H J E G U I K L A P E I Q O
L A H Q I O F A L H A P E Z A Q I E P O R L O Z A
I K O P K I B A L O E P Q I J E A Z I Q Q I D I I
D G U I N I K I Q Q I H A W I U G H A L A K I Q I
I D C E I K H A U G A H Q I I K Q I I Q H A R O O
L Z A K I O P O R L O A L A Z I K I Q I Q A H I W
C E A Z N A O F O X Q I Z A G U L O P E X O O L I
D I D U G M U V E Q I I K F O G U D I U G I D U M
E C I D Q I A N L O M E Q I Z A U G H A E J E J A
Z Q I C E K I N A G U Z A N A E V I Q A Z O L L A
K I I Q K I O L D I C E A H O R Z A E C H A A N U
G I D N A L O

ASSIGNMENT No. 3

Problem No. 5

M A P N C	H M D U S	Y N L N N	P U S H C	Y N F I N
Y I F F I	P N F A H	C L H F T	P N C H O	C S U N P
N P F A Y	O H L M T	T M I F E	P P N T M	M D Y N O
P N Y S U	U S Y N O	Y H C P E	A F A M L	E L N U T
P N Y R H	L A F A F	L H F A R	Y E L D M	A M L E N
L M T L H	R Y W S M	D W I P N	U S L H Y	N M A N Y
H L T M N	P S U C H	D M L E C	E P N C H	D M L E D
M H L Y N	A F L E C	H H C N Y	N Y F A E	L H C I W
S U E L C	O D M L H	O C E L U	T T M N P	E L A F M
A C O Y N	P O W I M	T N P M D	P N E L M	T T M F A
P N C O P	N H C C H	L E U S L	N E L U S	S U L E A
F Y R N P	O P P N F	A D M C H		

Before you mail the solutions to this assignment please include your full name, rate rank, or title, and latest address. Use only the official envelopes provided for mailing your work sheets.

B L A N K

Op-20-GR

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 4

POLYALPHABETIC SUBSTITUTION

1. A cipher system which employs two or more cipher alphabets and includes a method for designating which cipher alphabet is to be used for the encipherment of each plain-text letter, is called a polyalphabetic substitution system. Cipher systems employing variant values may appear to use more than one cipher alphabet, but they have the characteristics of mono-alphabetic substitution and are properly classified as such.

2. Polyalphabetic substitution systems consist of two general types; periodic and non-periodic.

(a) In the periodic type the text of a message is divided into definite, regular groups or cycles of letters which are enciphered with identical alphabets. The order of use of these alphabets is determined by a repeating key which may be either literal (a word or phrase) or a numerical sequence.

(1) Multiple alphabet ciphers in which any number of cipher alphabets are used in an order designated by a prearranged key.

(2) Progressive alphabet ciphers in which a primary cipher alphabet and its 25 secondary alphabets are used either in regular succession, sliding the components one letter at a time, or in irregular order according to a prearranged shift.

(b) In the non-periodic type there are no repetitions of the complete key and consequently no regularity, or periodicity, in the use of the alphabets.

3. Because such systems as multiple alphabet ciphers employing a large number of random mixed alphabets, irregular progressive alphabet ciphers, as well as all non-periodic types are beyond the scope of this elementary course, only the simplest periodic systems will be described.

4. The cipher alphabets employed in multiple alphabet substitution systems may be constructed by any of the methods previously described.

Example:

Plain -	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher (1)	R	T	U	V	W	X	Y	Z	P	E	N	C	I	L	S	A	B	D	F	G	H	J	K	M	O	Q
Cipher (2)	E	N	C	I	L	S	A	B	D	F	G	H	J	K	M	O	Q	R	T	U	V	W	X	Y	Z	P
Cipher (3)	D	F	G	H	J	K	M	O	Q	R	T	U	V	W	X	Y	Z	P	E	N	C	I	L	S	A	B

Here the plain component is a normal sequence, and the cipher components are identical keyword sequences. The same keyword sequence may be used in both the plain and cipher components, or different sequences may be used, in the same manner as demonstrated for single alphabets in paragraph 8 of assignment No. 2 (Part II).

The key which determines the setting of the cipher components against the plain component (RED, in example) may be any prearranged word or phrase, or each cipher alphabet, of any multiple alphabet system, may be assigned a number and the alphabets used in the order of a prearranged numerical key.

5. The process of enciphering a message with the multiple alphabet system above would appear as follows:

Alphabet Number -	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Plain	M	Y	C	O	U	R	S	E	Z	E	R	O	T	H	R	E	E	Z	E	R	O
Cipher	I	Z	G	S	V	P	F	L	B	W	R	X	G	B	P	W	L	B	W	R	X

Alphabet Number -	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Plain	A	T	T	H	I	R	T	E	E	N	T	H	I	R	T	Y	T	H	R	E	E
Cipher	R	U	N	Z	D	P	G	L	J	L	U	O	P	R	N	O	U	O	D	L	J

In order to reduce errors of encipherment by the wrong alphabet, the plain text is written so that letters to be enciphered by the same alphabet are placed in the same vertical column, or the encipherment key is written over the plain text.

Note that repetitions in the plain text which begin on the same alphabet produce repetitions in the cipher text. If they begin on any other alphabet no repetition is produced.

PRINCIPLES OF FACTORING

6. If there are several repetitions in the cipher text of an unknown system, and the intervals between the initial letters of these repetitions have a common factor, this factor represents an exact multiple of the length of the key, or, in other words, indicates the number of alphabets used in encipherment.

Example: Let the cryptogram be:

IZGSV PFLBW RXGBP WLBWR XRUNZ DPGLJ LUOPR NOUOD LJ

The factoring process appears as follows:

Repetition	Interval	Factors	Common factor
L B W R X	9	3.3.	3
L J	12	2.2.3.	3
U O	6	2.3.	3

The common factor is three, and the number of cipher alphabets employed is three (see Par. 5).

The repetitions of digraphs, and sometimes trigraphs may be the results of chance instead of plain text repetitions, therefore their resulting factors should be given less weight than those of the longer repetitions, when determining the key length.

7. When the factoring process yields more than one common factor there may be some doubt as to which one represents the exact key length. For example, suppose the key length were 12; the factoring process would produce the common factor s 2, 3, 4, and 6, as well as 12. The highest common factor should usually be selected if there are a number of long repetitions. In any case, frequency tables made on the basis of the various factors should indicate by their resemblance to the normal frequence table which factor represents the correct key length.

8. Only in the case of relatively short messages enciphered by a relatively long key does this process of factoring an unsolved cryptogram fail to lead to the correct determination of the number of cipher alphabets employed in a multiple alphabet cipher system. Conversely, it follows that if the factoring process fails to yield definite results, a periodic cipher system has not been used.

ASSIGNMENT No. 4

SOLUTION OF A MULTIPLE ALPHABET CIPHER

9. The solution to follow is a reprint of the Office of Chief of Naval Operations Pamphlet No. 7. The routine clerical operations have been performed, and the problem is given in the form of a "work-sheet" instead of a message. Lines and columns are numbered to facilitate referencing.

Solved by Analytical Method

FROM: AB (BLACK FORCE COMDR).
TO : CD, EF, GH, IJ (BLACK SHIPS).
TIME GROUPS: ØØ13-23ØØ (APRIL 193Ø).
REMARKS: CRUISER TRANSMITTER.

Alphabet Number -	1 2 3 4 5 6 7 8 9 Ø	1 2 3 4 5 6 7 8 9 Ø	1 2 3 4 5 6 7 8 9 Ø
Line Number 1 -	K P T X S L I C T M	I A M C B B N M S Z	M J K A Q J B F Z A
Line Number 2 -	J G M B S L N P H H	E E J Z W N C L O W	Z F S A A S Z D E P
Line Number 3 -	Z X C D J D D H A J	O D B K A H P L G H	A J M K T V A M K H
Line Number 4 -	M B C A A C N W S Z	Z D W I J K G M C Z	M V X X U N B W Z T
Line Number 5 -	I Y N C P O G H H W	L G T B W P L V T T	O B O X J L R M H Z
Line Number 6 -	M V H A W A D G G Z	Y F A R Q V K M M Q	K F M P S L G X A H
Line Number 7 -	E F W K G C B F T H	S V C B B U A H S S	K P K D E C G O H Z
Line Number 8 -	L V O D S C O C H A	G V W B Z C A M O Z	M J K A Q J B F J H
Line Number 9 -	X B H A A V A K O S	K P K G U L T J O Q	D F Q Q J K K M H Z
Line Number 10-	M V H A E P Z W Q R	O P L A U L B M O Z	M J K A Q J B F

The sequence of alphabets used was determined as ten letters long by the process of factoring.

Repetition	Interval	Factors
Z M J K A Q J B F	210	2.3.5.7.
Z M J K A Q J B F	270	2.3.3.5.
Z M J K A Q J B F	60	2.2.3.5.
M H Z M V H A	120	2.2.2.3.5.
Z M V	40	2.2.2.5.
Z M V	160	2.2.2.2.2.5.
K P K	50	2.5.5.

The highest common factor is 10 or (2 x 5); therefore, the sequence of alphabets, or key (the cycle of encipherment) repeats itself every ten letters.

10. "Lining up" is one of the basic operations in cipher solution. In this operation, write the text so that all characters which were derived from the same alphabet are in the same column (beneath each other). In a system involving a large number of alphabets this technique works very well, however, when the number of alphabets is relatively small this operation may promote an unweildy work sheet. It has been learned through practice that the most efficient method of lining up is to write the text in continuous lines of characters horizontally in exact multiples of the key length and then divide the resultant cipher text into encipherment cycles by colored lines. Thus all characters in any column are in the same alphabet. (Note the set up of problem in paragraph No. 9).

ASSIGNMENT No. 4

Collateral Information

11. The BLACK and BLUE FLEETS are engaged in war maneuvers in the Caribbean Sea. The fleets are not in contact. The location of the "Enemy" (BLACK FLEET) is not known. The message in question was intercepted on the BLUE flagship at 0015 on 14 April 1930. The operator had reason to believe (from the "note" and frequency) that the message was sent by a cruiser.

The composition of the BLACK FLEET is known to be as follows:

Battleships

WEST VIRGINIA (Flagship)
MARYLAND
TENNESSEE
NEW MEXICO
MISSISSIPPI
CALIFORNIA

Destroyers

LITCHFIELD (Flagship)
PREBLE
PRUITT
NOA
DECATUR
SICARD
HULBERT
WILLIAM B. PRESTON

Cruisers

TRENTON (Flagship)
MARBLEHEAD
RICHMOND
MEMPHIS

Air Force

SARATOGA (Flagship)
LANGLEY
CANNET

Submarine Force

ARGONNE (Flagship and Tender)
V-1
V-2
V-3

Frequency Tables

#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
A-1	A-1	A-1	A-9	A-4	A-1	A-4	A-	A-2	A-2
B-	B-3	B-1	B-4	B-2	B-1	B-6	B-	B-	B-
C-	C-	C-3	C-2	C-	C-5	C-1	C-2	C-1	C-
D-1	D-2	D-	D-3	D-	D-1	D-2	D-1	D-	D-
E-2	E-1	E-	E-	E-2	E-	E-	E-	E-1	E-
F-	F-5	F-	F-	F-	F-	F-	F-4	F-	F-
G-1	G-2	G-	G-1	G-1	G-	G-4	G-1	G-2	G-
H-	H-	H-3	H-	H-	H-1	H-	H-3	H-6	H-6
I-2	I-	I-	I-4	I-	I-	I-1	I-	I-	I-
J-1	J-4	J-1	J-	J-4	J-3	J-	J-1	J-1	J-1
K-	K-	K-5	K-1	K-	K-2	K-2	K-1	K-1	K-
L-2	L-	L-1	L-1	L-	L-6	L-1	L-2	L-	L-
M-7	M-	M-4	M-	M-	M-	M-	M-8	M-1	M-1
N-	N-	N-1	N-	N-	N-2	N-3	N-	N-	N-
O-3	O-	O-2	O-	O-	O-1	O-1	O-1	O-5	O-
P-	P-4	P-	P-1	P-1	P-2	P-1	P-1	P-	P-1
Q-	Q-	Q-1	Q-1	Q-4	Q-	Q-	Q-	Q-1	Q-2
R-	R-	R-	R-1	R-	R-	R-1	R-	R-	R-1
S-1	S-	S-1	S-	S-4	S-1	S-	S-	S-3	S-2
T-	T-	T-2	T-	T-1	T-	T-	T-	T-3	T 2
U-	U-	U-	U-	U-3	U-1	U-	U-	U-	U-
V-	V-6	V-	V-	V-	V-3	V-	V-1	V-	V-
W-	W-	W-3	W-	W-3	W-	W-	W-3	W-	W-2
X-1	X-1	X-1	X-1	X-	X-	X-	X-1	X-	X-
Y-1	Y-1	Y-	Y-	Y-	Y-	Y-	Y-	Y-	Y-
Z-3	Z-	Z-	Z-1	Z-1	Z-	Z-2	Z-	Z-2	Z-9
30	30	30	30	30	30	30	30	29	29

Hints for Solvers

(1) The cipher is comparatively simple and solution presents no more difficulties than previous problems.

(2) Watch for development of "system" in the deciphering tables, and take advantage of the system.

(3) Utilize the "collateral information" to the fullest extent.

(4) Frequency tables have been prepared for the assistance of the student. Do not depend too much on the frequency of any individual letter.

(5) Solution is possible without the use of the frequency tables.

(6) Repetitions in the cipher text are underscored.

(7) Knowledge of ciphers is not necessary for the solution of this problem. All the data necessary will be revealed during solution.

Solution by Probable Word

12. When ample collateral information is available, the probable word technique affords the easiest and quickest method of solution. From the given conditions, the message is presumably from the Commander of a cruiser division to his four cruisers, giving orders for scouting operations of the cruiser division.

The words most likely to appear in the cryptogram are as follows:

Probable Word List

SCOUTING	SCOUTING LINE	TRENTON	LATITUDE
COURSE	SCOUTING COURSE	MARBLEHEAD	LONGITUDE
SPEED	SCOUTING SPEED	RICHMOND	HUNDRED
DISTANCE	SCOUTING DISTANCE	MEMPHIS	NUMBERS
POSITION	COMMENCE SCOUTING	ENEMY	TIMES & DATES

Note: The solution is concerned with developing methods of solution and not with skill in assuming words.

13. The "probable word" technique may be applied in two ways:

(1) Start at some point in the cryptogram, usually a repetition, or other pecularity of pattern and try to match a "probable word" at this point. This may be called the "probable location method".

(2) Start with a "probable word" and find a place in the text where the frequencies or pattern of this word resemble the frequencies or pattern of cipher text will fit. This may be called the "probable word method".

Probable Location Method

14. The long repetitions are words or phrases, important to the subject of the message, and may be probable words. Therefore, they are excellent points of attack. The beginning of the message and the end of the message are also good points of attack.

The longest repetition in the problem is of such length that it cannot be any of the probable words. The next longest repetition is the right length for TRENTON, MEMPHIS, or HUNDRED; furthermore, it links in letters of the longest repetition.

Original assumptions:

M H Z	M V H A	Lines 5-6
T R E	N T O N	TRE NTON is much the best assumption.
M E M	P H I S	
H U N	D R E D	

ASSIGNMENT NO. 4

Check:

M O Z	M J K A Q J B F	Lines 8-10	MOZ JKAQJBF could be
T E	N N	Excellent	TEE HUNDRED Excellent
M M	P S	Poor	THE E--N--- Poor
H N	D D		

Check the values of TEEN HUNDRED (plus TRENTON):

```
Column number - 1 2 3 4 5 6 7 8 9 Ø : 1 2 3 4 5 6 7 8 9 Ø
Line number 1 - K P T X S L I C T M :
                                    :
Line number 1 - I A M C B B N M S Z : M J K A Q J B F Z A
                              T   E : N H U N D R E D - -   (filled in)
Suggests ------               A T T E : N H U N D R E D - -   (excellent)
                                    :
Line number 8 - G V W B Z C A M O Z : M J K A Q J B F J H   (filled in)
                  T           T E E : N H U N D R E D - -
Suggests ------       T H I R       :
         ------       F O U R       :
         ------         F I F       :
         ------         S I X       :
         ------ A T S E V E N       :
         ------       E I G H       :
                                    :
Line number 10- O P L A U L B M O Z : M J K A Q J B F - -
                    N     E T E E : N H U N D R E D - -   (filled in)
Suggests ------       N I N E T E E : N H U N D R E D - -   (excellent)
```

It is possible that all the above assumptions are incorrect but they are too good to ignore. Therefore, enter the above values throughout the cryptogram to see if skeletion of words appear.

Possibilities are indicated below:

```
Column number - 1 2 3 4 5 6 7 8 9 Ø : 1 2 3 4 5 6 7 8 9 Ø
Line number 7 - E F W K G C B F T H : S V C B B U A H S S   The ED in line 7
                          E D     : .T             T     could be part of
                    S P E E D F I : F T E E N K N O T S   SPEED. Build up on
                              S I : X                    this and carry the
                                  :                      values.
Line Nos 7 & 8- K P K D E C G O H Z : L V O D S C O C H A  Other words can be
                  U         R E   :   T               R    built up also.
               C O U R S E T H R E : E T H R E E Z E R O
                                  :
Line number 4 - Z D W I J K G M C Z : M V X X U N B W Z T  TRENTON is the most
                          T   E   : N T           E        obvious break and
                          T W E   : N T Y M I L E S        was used by several
                      T           :       T H R E E        solvers.
                                  :       F I V E
```

We could have resorted to letter-combinations of frequencies to see which of the three words (TRENTON, MEMPHIS and HUNDRED) fitted best. This would have been necessary if the letters in question had not linked in to the longest repetition.

Check by letter combinations elsewhere in the cryptogram:

H Z = 1	Z M V = 1	Z M = 4	H A = 1	
R E	E N T	E N	O N	TRENTON is the only assumption
E M	M P H	M P	I S	justified.
U N	N D R	N D	E D	

Check by frequencies:

ASSIGNMENT No. 4

Frequency - 8 6 9 7 6 3 9		
Cipher ---- M H Z M V H A		
Frequency - X X X X X X X		X = High frequency.
Plain ----- T R E N T O N		
		- = Intermediate frequency.
Frequency - - X - - - X X		
Plain ----- M E M P H I S		0 = Low frequency.
Frequency - - - X - X X -		TRENTON is the only assumption justified.
Plain ----- H U N D R E D		

Probable Word Method

(a) Location by Frequency Pattern

15. One method of fixing the location of a probable word is by frequencies, provided the probable word has, one or more letters of very low frequency, or a distinctive pattern. The word should be fairly long to make this method practicable.

R E N D E Z V O U S is an excellent example.

M A R B L E H E A D is the only word in our list which fits this requirement.

First, enter the frequencies over each letter of the cryptogram. Then, write the "probable word" on a card (with spacing the same as on the work sheet) and indicate the low frequency letter(s) by an arrow. Slide the card along the cryptogram and match the arrow against each cipher letter of very low frequency. Check with the frequencies of the other letters, and by the short repetitions in the cipher text. Many possible locations will be found and the process of elimination is rather slow. This method is advised only as a last resort.

(b) Location by Repetitions

Of Identical Letters in Probable Word

16. The location of words by repetitions of identical letters or distinctive pattern is commonly employed in the analysis of many types of substitution ciphers, i.e., cipher text derived by a regular step-by-step (cycle) encipherment, from a given set of alphabets. With cipher text derived in a non-cyclic manner such repetitions or distinctive pattern depends very much on chance and cannot be relied upon. If the cipher alphabets are repeated within the length of cycle (or key), or we have a very short cycle, we can employ the repetitions or distinctive patterns in a limited form of symmetry, i.e., see illustration:

Cipher alphabets:	1 2 3 4 5 : 1 2
Cipher text:	K B L F O : M B
Plain text:	C R U I S : E R

The R----R in CRUISER is symmetrical with the B----B of the cipher text. The identical letters of plain text are represented by identical letters of cipher text and those identical letters are the same distance apart in both cases.

With a random selection of alphabets or a very long cycle this method cannot be employed. With a fairly short cycle this method can be employed, provided:

(1) We can assume a word or phrase longer than the cycle.

(2) This word or phrase happens to contain a letter repeated at an interval equal to the length of the cycle.

One of the known words fulfills these conditions:

S C O U T I N G D I S T A N C E (for a 10-letter key).

ive lines have common
dentical letters in the
e to find such a loca-

er text are 10 spaces
for SCOUTING DISTANCE.
iefly the letters C, G,
The remaining cases
togram. In this case,
s not appear in the text
other phrases.

familiar with Naval
nt justification for the

tions of the cruiser
in natural order, which

BLEHEAD

(4)
MEMPHIS

ows:

H E A D

N R I C

E M P H

, and can also be checked
ith two repeated letters
shown below and in no
binations in other por-

M C Z
I E
T W E

M V X
N T
N T Y

This is a sufficient check to justify entering these values throughout the cryptogram, and we may ignore the frequencies.

17. Table I gives a list of probable locations (cipher text letters repeated), and we may be able to find some word or phrase that will fit. The word COURSE appears in the text and must be followed by ZERO, ONE, TWO, or THREE, which in turn must be followed by two other numbers. Disregarding the third digit, we have five phrases (see Table II) to check through Table I, namely:

C O U R S E Z E R O F O U R	C O U R S E T H R E E Z E R O
C O U R S E O N E T W O	C O U R S E T H R E E O N E
C O U R S E T W O T W O	C O U R S E T H R E E T H R E E
C O U R S E Z E R O F O U R	Is the most promising, but it does not check.
C O U R S E T H R E E T H R E E	Is the next best. It fits reference No. 9 in Table I.

Assumption: Check:

Line 7 --- K P K D E C G O H Z — Line --- 9 --- S K P K G U L T
C O U C O U
S C O U T I N G

Line 8 --- L V O D S C O C H A
E T H R E E Z E R O Possible.
O N E Impossible.
T W O Impossible.
T H R E Impossible.
F O U R Impossible.
F I V E Impossible.
S I X Impossible.
S E V E N Impossible.
E I G H T Impossible.
N I N E Impossible.

Therefore, we can have COURSE THREE THREE ZERO and SCOUTING. These values should be entered in the cryptogram. If they should fail we can continue with the other possible courses. This is actually correct and gives an excellent break.

Discovery of the System

18. Study the values assumed in Table III.

Value	Alphabets	Value	Alphabets
C = E	#3, #6, #8.	H = O, O = H	#3, #6, #8.
O = H	#3, #8.	N = L, L = N	#3, #6, #8.
H = O	#3, #8.	K = U, U = K	#3, #6, #8.
B = E	#4, #7.	N = A, A = N	#4, #7.
A = N	#4, #7.	S = E, E = S	#5.

The common values indicate that alphabets #3, #6, and #8 are identical and that #4 and #7 are identical, and we should proceed on that basis.

Five reciprocal values are noted in three different alphabets. No values are noted which will not check as reciprocals. This indicates that all the alphabets are reciprocals, and if this is correct, we can add the reciprocal values to each alphabet. On the other hand, if this be incorrect, it will cause too

much confusion to a beginner. To play safe we will ignore this possibility; it will work out automatically if it is correct.

The system has thus revealed:

(1) (a) Alphabets #3, #6, and #8, are the same.

(b) Alphabets #4 and #7, are the same.

(c) Seven different alphabets are used.

(2) The alphabets are probably reciprocal alphabets.

If the seven alphabets are secondary alphabets (that is derived from the same cipher-component set against the same plain-component but in different alignments) a short cut solution is possible. In cipher solution, secondary alphabets are always assumed up to the point where they are definitely proved or disproved. Therefore, the next step is to combine the seven different alphabets into one system.

The principles involved in the reconstruction of a multiple alphabet system when secondary alphabets have been used, are explained in Assignment No. 5.

The solution may be completed as though unrelated cipher alphabets had been used, as shown by the text already filled in below:

	1	2	3	4	5	6	7	8	9	Ø	:	1	2	3	4	5	6	7	8	9	Ø	:	1	2	3	4	5	6	7	8	9	Ø
Alphabet number -											:											:										
Line number 1 -	K	P	T	X	S	L	I	C	T	M	:	I	A	M	C	B	B	N	M	S	Z	:	M	J	K	A	Q	J	B	F	Z	A
	C	O		M	E	N		E			:			T		N		A	T	T	E	:	N	H	U	N	D	R	E	D		
Line number 2 -	J	G	M	B	S	L	N	P	H	H	:	E	E	J	Z	W	N	C	L	O	W	:	Z	F	S	A	A	S	Z	D	E	P
			T	E	E	N	A		R	I	:			R			L		N	E		:				N						
Line number 3 -	Z	X	C	D	J	D	D	H	A	J	:	O	D	B	K	A	H	P	L	G	H	:	A	J	M	K	T	V	A	M	K	H
			E	R			R	O			:				S		O		H		I	:		H	T	S			N	T		I
Line number 4 -	M	B	C	A	A	C	N	W	S	Z	:	Z	D	W	I	J	K	G	M	C	Z	:	M	V	X	X	U	N	B	W	Z	T
	N		E	N		E	A	S	T	E	:			S			U	T	T	W	E	:	N	T	Y	M	I	L	E	S		
Line number 5 -	I	Y	N	C	P	O	G	H	H	W	:	L	G	T	B	W	P	L	V	T	T	:	O	B	O	X	J	L	R	M	H	Z
			I			H	T	C	R		:	E			E							:			H	M		N		T	R	E
Line number 6 -	M	V	H	A	W	A	D	G	G	Z	:	Y	F	A	R	Q	V	K	M	M	Q	:	K	F	M	P	S	L	G	X	A	H
	N	T	O	N			R			E	:					D		S	T			:	C		T		E	N	T	Y		I
Line number 7 -	E	F	W	K	G	C	B	F	T	H	:	S	V	C	B	B	U	A	H	S	S	:	K	P	K	D	E	C	G	O	H	Z
			S	S	P	E	E	D		I	:			T	E	E	N	K	N	O	T	S	:	C	O	U	R	S	E	T	H	R	E
Line number 8 -	L	V	O	D	S	C	O	C	H	A	:	G	V	W	B	Z	C	A	M	O	Z	:	M	J	K	A	Q	J	B	F	J	H
	E	T	H	R	E	E	Z	E	R	O	:	A	T	S	E	V	E	N	T	E	E	:	N	H	U	N	D	R	E	D		I
Line number 9 -	X	B	H	A	A	V	A	K	O	S	:	K	P	K	G	U	L	T	J	O	Q	:	D	F	Q	Q	J	K	K	M	H	Z
			O	N			N	U	E	S	:	C	O	U	T	I	N		R	E		:					U	S	T	R	E
Line number 10-	M	V	H	A	E	P	Z	W	Q	R	:	O	P	L	A	U	L	B	M	O	Z	:	M	J	K	A	Q	J	B	F		
	N	T	O	N	S			S			:		O	N	N	I	N	E	T	E	E	:	N	H	U	N	D	R	E	D		

19. This discussion will be concluded in Assignment No. 5.

ASSIGNMENT No. 4

TABLE I

Line Number	(S C O U T I N G D I S T A N C E)	Reference Number
2	Z F S A A S Z D E P Z X C D J D	(1)
3	K A H P L G H A J M K T V A M K	(2)
3	H A J M K T V A M K H M B C A A	(3)
4	Z Z D W I J K G M C Z M V X X U	(4)
5	Z M V H A W A D G G Z Y F A R Q	(5)
6	F A R Q V K M M Q K F M P S L G	(6)
6	F M P S L G X A H E F W K G C B	(7)
6	H E F W K G C B F T H S V C B B	(8)
7	D E C G O H Z L V O D S C O C H	**(9)
7	C G O H Z L V O D S C O C H A G	**(10)
7	H Z L V O D S C O C H A G V W B	**(11)
8	V O D S C O C H A G V W B Z C A	**(12)
8	C O C H A G V W B Z C A M O Z M	(13)
8	A Q J B F J H X B H A A V A K O	(14)
9	O S K P K G U L T J O Q D F Q Q	(15)
10	A E P Z W Q R O P L A U L B M O	(16)
10	A U L B M O Z M J K A Q J B F	**(17)

**Impossible for SCOUTING DISTANCE due to other repeated letters.

TABLE II

1234567890	1234567890	1234567890	1234567890
COURSEZERO	COURSETHRE	COURSEONE	COURSETWO
ZERO	EZERO	ERO Z	ERO Z
ONE	ONE	NE O	NE O
TWO	TWO	WO T	WO T
THREE	THREE	HREE T	HREE T
FOUR	FOUR	OUR F	OUR F
FIVE	FIVE	IVE F	IVE F
SIX	SIX	IX S	IX S
SEVEN	SEVEN	EVEN S	EVEN S
EIGHT	EIGHT	IGHT E	IGHT E
NINE	NINE	INE N	INE N
COURSEZERO	COURSETHRE	COURSEONET	COURSETWOT
FOUR	EZER	WO	WO
	EONE		
	ETHREE		

TABLE III - DECIPHERING TABLE

Plain --	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher -																										
1 -							G		K		L					M						V				
2 -										J						P										
3 -					C					O						H		J	W		K			X		
4 -					B									X	A			D	K							
5 -				Q	S			U							B		G		E			Z				
6 -					C						U	N			L											
7 -			N		B										A					G					O	
8 -				F	C			O								H			W	M						
9 -					O													H		S		C				
10 -					Z				H							A			S							

ASSIGNMENT No. 4

TABLE IV - ENCIPHERING TABLE

Plain --	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher -																										
1 -	G		K		L								M													
2 -										J						P						V				
3-6-8 -				F	C					O		U	N		L	H			J	W	M	K			X	
4-7 -	N				B									X	A				D	K	G					O
5 -				Q	S				U						B		G			E			Z			
9 -					O														H		S			C		
10 -					Z				H							A				S						

FREQUENCY ANALYSIS

20. In previous assignments of the Elementary Course, students have been warned against placing reliance on frequencies of individual letters. Frequency tables are useful in preliminary analysis, as an aid in determining the type of cipher alphabets employed, and in making tentative classification of letters. For more definite identification, individual letter frequencies cannot be trusted unless one is dealing with a fairly large amount of text. The table and explanation appearing in this pamphlet are intended to demonstrate mathematically the relative weights which can be attached to frequency counts with various amounts of text and with various values of observed frequencies.

Although with small amounts of text the frequency tables are disappointing for determination of absolute plain values, yet it is interesting that these tables follow exact mathematical formulae. In computing the attached table, mathematical functions were used which were slightly in error due to the fact that the actual mathematical formulae were too complicated to handle. However, in spite of the small inaccuracies introduced, the important fact remains that this table indicates what may be expected in various lengths of text.

The "Mechanics of English" Table in Assignment No. 2, of the Elementary Course gives the average occurrence (or frequency) of each letter in 200 letters of text.

The following (Table V) gives:

(a) The expected percentage of actual occurrences of the 8 high frequency letters (E T O N A I R S) in 100, 50, and 20 letters of text.

(b) The average occurrence of each of these letters is 100, 50, and 20 letters of text based on a count of 200 letters.

Example: E, with an average frequency of 13 in 100 letters, may be expected to occur that often only 11% of the time. We also note that 1% of the time we may expect to find as high as 22 E's in 100 letters of plain text.

The table shows that if the highest frequency of a letter in a distribution of 100 letters is 18 or more, there is practically no doubt that it represents E. However, if the highest frequency in such a distribution is, for example, 10 or 11, the chances are almost equal that it may represent any one of the eight high frequency letters.

With fewer letters per alphabet, the unreliability of frequencies is at once apparent. For example, with a distribution of 50 letters, the expectancy that E will occur with its average frequency (roughly 6 times in 50 letters) is very little better than the expectancy that T will occur this same number of times (in the ratio of 16 to 13). For 100 letters, the expectancy that E will occur

with its average frequency of 13 bears the ratio of 11 to 5 to the expectancy that T will occur with this frequency. For a distribution of 20 letters, it is seen that all eight letters may be expected to occur, say twice, approximately the same number of times.

When the number of observed occurrences of a cipher letter is exactly equal to the average number of E's to be expected in that much text, the chances that the letter in question represents E (rather than any other one of the eight letters) are approximately as follows:

No. of letters in alphabet	Chances of letter of E's frequency actually being E.	
	From table	Rough "rule of thumb"
200	8/22 = .667	2/3
100	11/29 = .380	3/8
50	31/135 = .230	1/4
20	47/319 = .150	1/7

ASSIGNMENT No. 4

TABLE V

EXPECTED PERCENTAGE OF TIMES A GIVEN NUMBER OF OCCURRENCES OF A GIVEN LETTER WILL BE FOUND IN ALPHABETS OF:

Number of Occurrences	E	T	O	N	A	I	R	S
100 letters per alphabet								
1								2
2			1	1	2	2	2	6
3		1	2	3	4	4	4	11
4		3	4	6	7	7	7	16
5	1	6	8	9	11	11	11	17
6	2	9	11	12	14	14	14	16
7	3	12	13	14	15	15	15	12
8	5	13	14	14	14	14	14	8
9	7	13	13	12	11	11	11	5
10	9	12	11	10	9	9	9	3
11	10	10	9	7	6	6	6	1
12	11	7	6	5	4	4	4	1
13	11	5	4	3	2	2	2	
14	10	3	2	2	1	1	1	
15	9	2	1	1	1	1	1	
16	7	1	1					
17	6	1						
18	4							
19	3							
20	2							
21	1							
22	1							
Average	13	9	8.5	8	7.5	7.5	7.5	5.5
50 letters per alphabet								
0		1	1	2	2	2	2	6
1	1	5	6	7	9	9	9	18
2	3	11	13	15	17	17	17	24
3	7	17	18	20	21	21	21	22
4	11	19	19	20	19	19	19	15
5	15	17	16	16	15	15	15	8
6	16	13	10	9	9	9	9	4
7	15	8	7	6	5	5	5	2
8	12	5	4	3	2	2	2	1
9	9	2	2	1	1	1	1	
10	6	1	1	1				
11	3							
12	2							
13	1							
Average	6.5	4.5	4.25	4	3.75	3.75	3.75	2.75
20 letters per alphabet								
0	7	17	18	20	22	22	22	33
1	19	30	31	32	33	33	33	37
2	25	27	26	26	25	25	25	20
3	22	16	15	14	13	13	13	7
4	14	7	6	6	5	5	5	2
5	7	3	2	2	1	1	1	
6	3	1	1					
Average	2.6	1.8	1.7	1.6	1.5	1.5	1.5	1.1

Page -14-

ASSIGNMENT No. 4

Problem No. 1 Naval Text

MMVEU JCFYT IEVWX GHKOJ ZSWNV QHAHW ZAAZN WLKUF XLQGH UIMNK QANZN
OYFNQ NOITI EVKIF YZOFX JYVMA RLYWH HIMHV MWUUB SNLBA LLYWH XIJNQ
NZLWY GHTYS LAHYN OIKYN YFZAP WXAML UFWWZ GLLSX CNYEC DYKZJ IEZDY
WNYOA XWJWL AIVMM VEUJC FYKOT GWLYY VZGLX CNYEC FOLYK UXNWL SNLUU
EHYJC GXGHJ YLOJH LIKOJ ZSWWJ DUFYK WGHLC FOWXS NLUUE OCLBE UUBAH
WAMHK

Problem No. 2 Naval Text

MTUCF XIXJA FODQY DONVO GRJFH KBICU FAEFA QREUD QEGPV DTYYL ETJKK
QOWDB AYVFJ TAEPL XFIQT ZOIVO QREDB AYJVV BOZPA MFZTT BEIKV PQLCP
XAEFA MNRIL DTRML ETRVP ANRVL ZTICU OESWV KPFKU FAWKY YPVTP ADBKU
SFZUO QRIGT MIECA MNTJV DAEFK QTREO QDWTV YMZPL EWVGW UNXFL FATJT
QNKVV DEGQY FTFEV YMRPK QRRKY ORRHA BEIKV PQYKW BOFTD ULCTL BOIVA
ACFOT MNUGY FEEFL DDVVH OHDGU FUGQU OODRS QTZQU AFGCA DOC

Problem No. 3 Naval Text

RJUEE LUZRL FVTEE FMHRV RRIAT MQRRF BWROL MURTE LRTYV LFIEW DCBOE
WMCNG GWPRR MAKNE HBXNX MAROH PFTDV TOLBM KIGPV KUSQL DVITF ZMHNF
DKTDK PQRGR IMKEG XDGRG WPTXZ GSXBG WLXRK RQMTA WTTRT XZXCX UMDDL
IFSCK HWTNK UAQOX GSCEY XMZLT QHDNV EUKUM FVJIJ XDHRV DXJRW BDIQL
LBIOI IQHBX VEILZ ZTXPK XMHEI MAVCX GSELR GQWNM WERKV WARRA HEKYT
KGMFX UTTNE LKPIT QMPFZ KQPFZ RRTLZ ZTXPK XMHEI MIIAM BQXNL MQWCX
UMDDF YRIAL LZTST KQIAG RADPV KMXVG JZXCZ GUXLX QIBYT KGMFX UGDNT
XZXET WMDNT HYQNE HBXNX MARAH WWXGY MQHGH GENPV KUSQH QITNV FKGEN
LWTRI XBSEM HHCIE XFCZB OIHTF XMWGP DVSOW HGVAH RREOJ BFMBG

Problem No. 4 Naval Text

HTRYN BXTIF HFGIG OASET MIASQ FNYWJ RTFOR KREMF JSXSA SXNOY XFZFP
TJSQK VNYRA QXGPT HNIYJ RHOTO QZNNJ MNYMH SOHNN SNRJU XYATM AXQAF
TFUYA HONQF NUFOH FEOQP FTWOR FMORH SOHNN SNRJU XYATM MAQFY XNAYX
THBJE PZXNU TJSXN OYXFM EPKHH MOPPH FQZPF QEGKH HQFNY WJNNM OYQAH
ONKFP KJDXS XRYYN DATRY NSQRA ZQKJS OFNYM THGJY RIJSX JSSMY XDDKF
TWIWQ XZNNQ FTFHN XFHJS SMYXD HTEFN YASCT ENNKH FM

ASSIGNMENT No. 4

Problem No. 5 Naval Text

BJLQO IUYPN BSFJL ITNYU QAECC STGGR ZIGUY ZQZCL BQGVX ITSYY VUWCX

ZKKIH QEFWN TJLZU QUILA XNNSW BKSCC TVGVI SQACC QWMAY XSGEL BQGVX

LTXPC SPLYF ZUJCF ZUYJA QVQOS PJIHG SQSCX SUYPS AFQSY QTMNT TBOAA

LPARC HJCBS XFOCF Y

Frequency Table

Cipher -----	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alphabet No. 1 -	1	5						1	3		1	2				1	6	3	5	3		1			1	5
Alphabet No. 2 -	1	1			1	2			1	4	2			1		2	5		2	5	6	2	1			
Alphabet No. 3 -	2		1			2	6		2	1		3	2	2	2		2		3				1	1	3	2
Alphabet No. 4 -	2	1	8				1	1	1	2		1		1	1	3	1	1	2		1	3	1	1	3	1
Alphabet No. 5 -	3		5			3	1	1	1			3		2	1			1	3	1	2		1	4	4	

It is necessary that the Student's full name and present address appear on all work sheets and correspondence. Course material will be returned only in the penalty envelopes provided for that purpose.

B L A N K