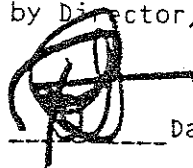


SRH- 216

ELEMENTARY COURSE IN CRYPTANALYSIS
OFFICE OF CHIEF OF NAVAL OPERATIONS
NAVY DEPARTMENT
CIRCA 1940

DECLASSIFIED per para. 3, E.O. 12356
by Director, NSA/Chief, CSS



Date 29 December 1982

REVIEWER'S NOTE:

The first review of this document was conducted by personnel of the U. S. Navy. The original classified versions were retained by them and have been placed in the NSG Repository, Crane, Indiana

N.B.:

This document is very similar to that which has been issued as SRH-214. There were enough differences, however, to warrant issuance under a separate number.

CONTENTS

ASSIGNMENT NO. 1. 001
ASSIGNMENT NO. 2. 012
ASSIGNMENT NO. 3. 024
ASSIGNMENT NO. 12 035
TRAINING PAMPHLET NO. 2 040
"THE USE OF WIRELESS TELEGRAPHY IN THE
WORLD WAR, MORE ESPECIALLY FROM THE
NAVAL STRATEGICAL POINT OF VIEW" by
N. Von KOCH. 048
LIST OF WORDS COMMON TO NAVAL TEXT. 070

RESTRICTEDELEMENTARY COURSE IN CRYPTANALYSISASSIGNMENT No. 1INTRODUCTION

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 Viète, 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 converting 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.

EI FIXQZS QXXQOJM PNZDM DCXILIMN PS IXQFIQD DQVQF
QWXJCZIXIMY XJQX KMZEQD YWPEQZIDMY JQN PMND CZNMZMN
XC KC IXC EMNIXZZQDMQD YMQ XC QXXCOG SJM XUC

XZQDYBCXY QQZZSIDK QEMZIOQD YCFNIMZY EQZYMIFFM QDN
XCWFCD BMZICH ZMAWYX FCDNCD PM IDLCZEMN HQGYCD

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 step). 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); QXXQOC(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

FTUE ETADF ODKBFASDMY UE SUHQZ
ME MZ QJQDOUEQ UZ FTQ EAXGFUAZ
AR M OUBTQD NK UZEBQOFUAZ

Problem No. 2 -- Non-Naval Text

DSVM ZHPVW ZYLFGR SRH KOZM LU
XZKNKZRTM TVMVIZO HGLMVDZOO
QZXPPLM IVKORVW GL ZM RMJFRHRGRE
XSZKOZRM XZM BLF PVVK Z HVXIVG
BVH GSV VZTVI XOVIRX ZMHDVIVW
DV00 HL XZM R HZRW GSV TVMVIZO

Problem No. 3 -- Non-Naval Text

DCLCVSRUCTN SB UCGTO BSP PGRYD
ESUUMTIYEGNYST ZGO DSTC ESTOYDCPG

FVC NSK GPD EPCGNYTA G FCNNCP
Y.TNCPTGNYSTGV MTDCPONGTDYTA

Problem No. 4 -- Non-Naval Text

XA ERK VZZB ZFB BQWO LZIBO
LKIK M QIKCUFFW OHQMKB XA
MIWHEZVIQYO FXJK ERXO NUE
EZBQW LZIBO QIK IUA EZVKERKI
QAB ERK EKTE XO BXSXBKB XAEZ
WIZUHO ZC CXSK FKEEKIO EZ
XAOUIK QMMUIQMW XA EKFKVIQHRXM
BIQAQYXOOXZA

Problem No. 5 -- Naval Text

FENFWEN DH AND OXZNEVWP WD
SNEH NBAUD UOXZENZ FROM TBLN
DBJN THOEDNNX WFEBR FNEBHZ IN
FENFWENZ THE JWGBJOJ MFNNZ
DVNXDP YXHDM

Problem No. 6 -- Non-Naval Text

N IXTRYILTNO NOYWNZXC RF LAX
RA HWRTW NOO CWX KNOMXF RA
CWX NOYWNZXC NIX IXTRYILTNO
RA YNRIF

Problem No. 7

DO IBWY UTXB CGESWBS SBVOWYRBW
STXTVTYE VBXBEOBBE ZCDEMB ZYGWVB
OY OCWBB UTXB UYGW

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

Problem No. 8

ALTDM VSRJBXTY LIPRN AVJU
ISBDC FNWOSBQRRV AK SV CCOTM
VDY LPUMA QRBPFIO JK NP WFDLDEO
TVQH

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.

GOUGE FOR ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 1

Problem No. 1

FTUE ETADF ODKBFASDMY UE SUHQZ ME MZ QJQDOUEQ UZ FTQ
THIS SHORT CRYPTOGRAM IS GIVEN AS AN EXERCISE IN THE

EAXGFUAZ AR M OUBTQD NK UZEBQOFUAZ
SOLUTION OF A CIPHER BY INSPECTION

System: Monoalphabet substitution. Direct standard alphabets,
A(plain) = M(cipher).

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

Problem No. 2

DSVM ZHPVW ZYLFG SRH KOZM LU XZNKZRTM TWMVIZO HGLMVDZOO
WHEN ASKED ABOUT HIS PLAN OF CAMPAIGN GENERAL STONEWALL

QZXPFLM IVKORVW GL ZM RMJFRHRGREV XSZKOZRM XZM BLF PVVK
JACKSON REPLIED TO AN INQUISITIVE CHAPLAIN CAN YOU KEEP

Z HVXIVG BVH GSV VZTVI XOVIRX ZHEDVIW DVOO HL XZM R
A SECRET YES THE EAGER CLERIC ANSWERED WELL SO CAN I

HZRW GSV TWMVIZO
SAID THE GENERAL

System: Monoalphabet substitution. Reversed standard alphabets,
A(plain) = Z(cipher).

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

Problem No. 3

DCLCVSRUCTN SB UCGTO BSP PGRYD ESUMTYEGNYST ZGO DSTC
DEVELOPMENT OF MEANS FOR RADIO COMMUNICATION HAS DONE

ESTOYDCPGEVC RSKGPD EPCGNYTA G FCNCP YENCPTGNYSTGV
CONSIDERABLE TOWARD CREATING A BETTER INTERNATIONAL

MTDCPONGTDYTA
UNDERSTANDING

System: Monoalphabet substitution. Reversed standard alphabets,
A(plain) = G(cipher).

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

Problem No. 4

XA ERK VZZB ZFB BQWO LZIBO LKIK MQIKCUFFW OHQMB XA
IN THE GOOD OLD DAYS WORDS WERE CAREFULLY SPACED IN

MIWHEZVIQYO FXJK ERXO NUE EZBQW LZIBO QIK TUA EZVKERKI
CRYPTOGRAMS LIKE THIS BUT TODAY WORDS ARE RUN TOGETHER

QAB ERK EKTE XO BXSXBKB XAEZ WIZUHO ZC GXSK FKEEKIO EZ
AND THE TEXT IS DIVIDED INTO GROUPS OF FIVE LETTERS TO

KAQUIK QLMUIQMW XA EKFKVIQHREM EIQAOYXOOXZA
INSURE ACCURACY IN TELEGRAPHIC TRANSMISSION

System: Monoalphabet substitution. Random mixed alphabets.

(p) - 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
(c) - Q M B K C V R X F Y A Z H I O E U S L T W

Problem No. 5

FENFWEN DH AND OXZNEVWP WD SNEH NBAUD UOXZENZ FROM TBLN
PREPARE TO GET UNDERWAY AT ZERO EIGHT HUNDRED PLUS FIVE

DBJN THOEDENX WFEBR FNEBHZ IN FENFWENZ THE JWGBJOJ MFNNZ
TIME FOURTEEN APRIL PERIOD BE PREPARED FOR MAXIMUM SPEED

DVNKDP YZLDM
TWENTY KNOTS

System: Monoalphabet substitution. Random mixed alphabets.

(p) - 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
(c) - W I Z N T A U B Y R J X H F E M D O L V G P S

Problem No. 6

N IXTRYILTNO NOYWNZXC RF LAX RA HWRTW NOO CWX KNOMXF RA
A RECIPROCAL ALPHABET IS ONE IN WHICH ALL THE VALUES IN

CWX NOYWNZXC NIX IXTRYILTNO RA YNRIF
THE ALPHABET ARE RECIPROCAL IN PAIRS

System: Monoalphabet substitution. Random reciprocal alphabets.

(p) - 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
(c) - N Z T K S W R V O U A L Y I F C M K H E P B

Problem No. 7

DO IBWY UTXB CGESWBS SBVOWYRBW STXTVTYE VBXBEOBBE ZCDEMB
AT ZERO FIVE HUNDRED DESTROYER DIVISION SEVENTEEN CHANGE

ZYGWVB OY OCWBB UTXB UYGW
COURSE TO THREE FIVE FOUR

System: Monoalphabet substitution. Random mixed alphabets.

(p) - 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
(c) - D Z S B U M C T E Y W V O G X R I

Problem No. 8

ALTDM VSRJBXTY LIPRN AVJU ISBDC FNWOSBQRRV AK SV CCOTM

VDY LPUMA QRBPFIQ JK NP WFDLDEO TVQH

System: Meaningless jumble.

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 infrequently 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

ASSIGNMENT No. 2

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 with 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

ASSIGNMENT No. 2

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
A	B	represents the prefix in their order of occurrence,
B Q D S -	A C A Q	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.

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	FE-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

INC-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

<u>Letters</u>	-	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
<u>Initial</u>	-	9	6	6	5	4	2	3	3	1	1	2	4	2	2	10	2	-	4	5	17	2	-	7	-	3	-
<u>Final</u>	-	-	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	5	-	1	1	-	5	9	-	-	2	2	4	-	-	-	-	1	3	-
G	3	-	2	1	1	-	1	-	11	-	-	-	-	22	2	-	-	3	-	1	1	-	-	3	-	-
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	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	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	29	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.

ASSIGNMENT No. 2

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

RENDEZVOUS
 ABCFGHIJK and the columns taken off so as to form the following sequence
 LMPQ TWXY

(1) RALEB MNQP 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) RALMB ENCP 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
 RENDEZVOUS
 ABCFGHIJK
 LMPQ TWXY

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:

C 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 O
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 preceding 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 FTUEETADF, the solution by completing the plain component will appear as follows:

```

FTUEETADF
GUVVFUBEC
HVWCGVCFH
IWXHHWDGI
JXYIIXEHJ
KYZJJYFIK
LZAKKZGJL
MABLLAHKM
NBCMMLBILN
OCDDNCKJMO
PDEOODKNP
QEFPPPELOQ
RFGQQQFMPR
SGERRGNQ S
THISSHORT
UIJT TIPSU
VJKU UJQTV
WKL VVKRUW
XLMW WLSVX
YMNK XMTWY
ZNOY YNUXZ
AOPZZOVYA
BPQA APWZB
CQRBBQIAC
DRSCCRYBD
ESTDDSZCE
    
```

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

```

FENFWENDHA - Cipher
JLYJULYNIA - Plain equivalents
KMZKVMZOJB
LNALWNA PKC
MOB MIOBQLD
NPCNYPCRME
CQDOZQDSNF
PREPARETOG
QSFQBSFUPH
RTGRCTGVQI
SUHSDUHWJRJ
TVITEVIXSK
UWJUFWJYTL
VXKVCXKZUM
WYLWEYLA VN
XZKXIZMBWO
YANYJANCPXP
ZBOZKBODYQ
ACPALCPEZR
BDQBMDQFAS
    
```

Also suppose another cryptogram, which begins FENFWENDHA, 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 P 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 X X I T X 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 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	VQNMH	OKCIC	UBGSG	KEDSI	RXNKS	ADCOO	WVCNE	SGOMD
QDWWD	RBHKE	SGTDK	EVRKE	DGKXR	DIKUD	CWIGK	VTCFD	ESGVL	ICICU
HGSGC	IRSGI	VKRDO	DIRDI	KVIWK	UDGUD	CWIDR	QWVIK	DZBKV	VFG

Problem No. 5 Non-Naval Text

ZERKV	CELKF	UKTJN	ACBTR	KEFRE	EFZBF	BLAKA	KTBTR	KEFRE	JERBI
TEREL	ABKYZ	EMKFK	ABOBY	TBFZV	LKFRK	VOETC	BQEJE	KFETA	BJOKT
CEZYC	KRCVE	LABKF	ANKAX	AKTBO	TNEFB	LAJER	BITEN	MACEO	BLUEV
BLAVO	BPEZK	FKAJP	KWBUK	FBAEN	FTGKO	ORFZE	HVELK	EFRE	

Problem No. 6 Non-Naval Text

BQWDC	IKVIF	XQAAD	OYCAQ	JJACW	CITOG	CGJOJ	JIOBJ	QVGEV	IVGCK
DVCSW	CBJNI	CNIAJ	NOJVG	BCKQJ	DVXJA	OPVIE	VIJDC	ICQNC	YONJO
TVXGJ	VEWMI	CALIV	XJQCC	AOPVI	QGJDC	WICWO	IOJQV	GVEKI	CHICG
BLJOP	ACNOG	MVJDC	IJDQG	BNPCE	VICJD	CTCNN	ORPCP	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.

GOUGE FOR ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 2

Problem No. 1

KODJWA SCHFWSE HCF XRF PWTR QOFI TRDFBCKRB TRFWSIPRHF
VISUAL CONTACT NOT YET MADE WITH DESTROYER DETACHMENT

MRBOCT WBUCHHR TOBRSPRT BRPWOH KOSOHOFX BRHTRZKCJD FC PWGR
PERIOD ARGONNE DIRECTED - REMAIN VICINITY RENDEZVOUS TO MAKE

SCHFWSE WHT TRAKRB SCMORD WAA DRBREF WHT SCHNOTRHFOWA
CONTACT AND DELIVER COPIES ALL SECRET AND CONFIDENTIAL

MJEAOSWFOCHD
PUBLICATIONS

System: Monoalphabet substitution. Keyword cipher component derived from WESTERN UNION TELEGRAPH COMPANY. A(plain) = W(cipher).

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

Problem No. 2

ZNRD BUTDUWDG WTD HBZAW YVKKWBWVWBU ZPKWDR FUNSU EVYBVX
ROME INVENTED THE FIRST SUBSTITUTION SYSTEM KNOWN JULIUS

IILXLZ VADG LU LYAMLKDW BU SMBIM G SLX XVKKWBWVWDG HNZ
CAESAR USED AN ALPHABET IN WHICH D WAS SUBSTITUTED FOR

L INRRL D HNZ K INRRL H HNZ I DWI BU MBX INZZDXANUGDUID
A COMMA E FOR B COMMA F FOR C ETC IN HIS CORRESPONDENCE

System: Monoalphabet substitution. Keyword cipher component derived from JANUARY FEBRUARY MARCH reversed. A(plain) = L(cipher).

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

Problem No. 3

WUBGT BGGJKUP HIRVJML ZJZSUUM EXMPGUP SEJN PBSU ZRGUJLM
PEARY ARRIVED NANKING FIFTEEN HUNDRED THIS DATE FOREIGN

FUM RZ HBG GUNUMS SHR DGJSJNE LMDRBSN PMU QBWBMUNU
MEN OF WAR RESENT TWO BRITISH GUNBOATS ONE JAPANESE

PUNSGRTUG BS WVGUNUMS MR BWVGUEUJNRM BFRML ZRGUJLMUGN
DESTROYER AT PRESENT NO APPREHENSION AMONG FOREIGNERS

IJST CXJUS
CITY QUIET

System: Monoalphabet substitution. Keyword cipher component derived from BLACK by vertical transposition. A(plain) = B(cipher).

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

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

Problem No. 4

SIKED	GKXRH	VQNVH	OKCIC	UHGSG	KEDSI	RXNKS	ADCOO	WVCNE
INTHE	STUDY	OFCRY	PTANA	LYSIS	THEIN	DUCTI	VEAPP	ROACH
SGOWD	QDWRD	RBHKE	SGTDK	EVRKE	DGKXR	DIKUD	CWICK	VTCFD
ISPRE	FERRE	DBYTH	ISMET	HODTH	ESTUD	ENTLE	ARNST	OMAKE
ESGVL	ICICU	HGSGC	IRSGI	VKRDO	DIRDI	KVTWX	UDGUD	CWIDR
HISOW	NANAL	YSISA	NDISN	OTDEP	ENDEN	TONRU	LESLA	ARNED
QWVTK	DZBKV	VFG						
FROMT	EXTBO	OKS						

System: Monoalphabet substitution. Keyword cipher component derived from CRYPTOGRAPHY by vertical transposition. A(plain) = C(cipher).

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

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

Problem No. 5

ZERKV	CELKF	UKTJN	ACBTR	KEFRE	BFZBF	BLAKA	KTBTR	KEFRE
DECIP	HERIN	GISBO	THASC	IENCE	ANDAN	ARTIF	ISASC	IENCE
JERBI	TEREL	ABKFZ	EMKFK	AEOBY	TEFZV	LMFRK	VOETC	BOEJE
BECAU	SEGER	TAIND	EFINI	TELAW	SANDP	RINCI	PLESH	AVEBE
EFETA	BJOKT	CEZYC	KRCVE	LABKF	ANKAK	AKFBO	TNEFB	LAJER
ENEST	ABLIS	HEDWH	ICHPE	RTAIN	TOITI	TISAL	SCANA	RTBEC
BITEN	MACEO	BLUEV	BLAVO	BPEZK	FKAJP	KWBUK	FBAKN	FTGKO
AUSEO	FTHEL	ARGEV	ARTPL	AYEDI	NITBY	IMAGI	NATIO	NSKIL
OBFZE	HVELK	EFRE						
LANDE	XPERI	ENCE						

System: Monoalphabet substitution. Cipher component is a standard alphabet transposed by columnar transposition in accordance with numerical key 7-1-3-6-2-5-4-8. A(plain) = B(cipher).

7-1-3-6-2-5-4-8
 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

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

Problem No. 6

BQWDC	IKVIF	KQAAD	OYCAQ	JJACW	CITOG	CGJOJ	JIOBJ	QVGEV
CIPHE	RWORK	WILLH	AVELI	TTLEP	ERMAN	ENTAT	TRACT	IONFO
IVGCK	DVCSW	CBJNI	CNXAJ	NOJVG	BCKQJ	DVXJA	ORVIE	VIJDC
RONEW	HOEXP	ECTSR	ESULT	SATON	CEWIT	HOUTL	ABORF	ORTHE
ICQNC	YONJO	TVXGJ	VEWXI	CALIV	XJQGC	AOPVI	QGJDC	WICWO
REISA	VASTA	MOUNT	OPPUR	ELYRO	UTINE	LABOR	INTHE	PREPA
IOJQV	GVEEI	CHXCG	BLJOP	ACNOG	MVJDC	IJDQG	RNPCE	VICJD
RATIO	NOFFR	EQUEN	CYTAB	LESAN	DOTHE	RTHIN	GSBEF	ORETH
CTCNN	ORCPC	RQGNJ	VOWWC	OI				
ELESS	AGEBE	GINST	OAPPE	AR				

System: Monoalphabet substitution. Keyword
 cipher component derived from
 OPERATIONS by alternate diagonal
 transposition. A(plain) = O(cipher).



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

RESTRICTEDELEMENTARY COURSE IN CRYPTANALYSISASSIGNMENT No. 3NUMERICAL 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			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.
1	:	A	B	C	D	E	:
2	:	F	G	H	I	X	:
3	:	L	M	N	O	P	:
4	:	Q	R	S	T	U	:
5	:	V	W	X	Y	Z	:

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.

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	A	Y	D	F
A	O	F	R	L	B
L	R	O	N	C	H
T	E	R	E	I	Q
I	C	J	K	S	V

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

EN, 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.

ASSIGNMENT No. 3

(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. "Y" 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:

LREKVEKVRNV	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

06021	00501	01051	52202	06082
32510	08040	22109	08040	82211
08041	71513	14222	10224	02012
20202	01081	90615	17080	11122
14020	11906	05100	20211	22140
62319	05150	12213	02050	61302
05011	00523	06210	22214	06020
22214	06020	22602	06052	11902
02112	20302	17240	21902	06150
51106	02190	50622	01050	50119
05211	52215	05012	20518	05060
60503				

Problem No. 2

53241	54532	24432	51243	24231
54445	45325	14344	14152	14115
43453	52123	35125	11421	53334
53244	23154	54524	43241	44432
12532	44344	24154	44524	43352
15333	13144	41545	44514	32515
23241	55224	43153	13313	31455
32413	45212	53352	24341	31245
44523	34433	22333	53345	21352
44444	45321	51315	52244	31531
24511	31424	44334	31522	35242
53521	33133	12312	13143	34533
12134	44124	43331	21432	24333
13245	12253	51253	23351	25114
44154	54143	24442	41345	15221
25145	12132	44532	12514	41513
14252	42445			

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 X
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 Y	D E V O L	A H J E G	U I K L A	P E I Q O
L A E Q I	O F A L H	A P E Z A	Q I E P O	R L O Z A
I Z O P E	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 E	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 E 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.

GOUGE FOR ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 3

Problem No. 1

06021 00501 01051 52202 06082 32510 08040 22109 08040 82211
 R E C O N N O I T E R A U X C A Y E S B A Y A T D

08041 71513 14222 10224 02012 20202 01081 90615 17080 11122
 A Y L I G H T S E V E N T E E N A P R I L A N D T

14020 11906 05100 20211 22140 62319 05150 12213 02050 61302
 H E N P R O C E E D T H R U P O I N T G E O R G E

05011 00523 06210 22214 06020 22214 06020 22602 06052 11902
 O N C O U R S E T H R E E T H R E E Z E R O S P E

02112 20302 17240 21902 06150 51106 02190 50622 01050 50119
 E D T W E L V E P E R I O D R E P O R T N O O N P

05211 52215 05012 20518 05060 60503
 O S I T I O N T O M O R R O W

System: Plain component is a keyword
 sequence derived from NEW YORK.
 Cipher component $\emptyset 1$ to 26.
 $N(\text{plain}) = \emptyset 1(\text{cipher})$.

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

Problem No. 2

53241 54532 24432 51243 24231 54445 45325 14344 14152 14115
 W E A T H E R F O R E C A S T T H U R S D A Y P A

43453 52123 34125 11421 53334 53244 23154 54524 43241 44432
 R T L Y C L O U D Y W I T H S C A T T E R E D S H

12532 44344 24154 44524 43352 15333 13144 41545 44514 32515
 O W E R S E A S T E R L Y W I N D S A T S U R F A

23241 55224 43153 13313 31455 32413 45212 53352 24341 31245
 C E A V E R A G I N G T W E N T Y F I V E K N O T

44523 34433 22333 53345 21352 44444 45321 51315 52244 31531
 S V I S I B I L I T Y L E S S T H A N A V E R A G

24511 31424 44334 31522 35242 53521 33133 12312 13143 34533
 E U N D E S I R A B L E F L Y I N G C O N D I T I

12134 44124 43331 21432 24333 13245 12253 51253 23351 25114
 O N S P E R I O D H E I G H T O F L O W C L O U D

44154 54143 24442 41345 15221 25145 12132 44532 12514 41513
 S A T P R E S E N T A B O U T O N E T H O U S A N

14252 42445
 D F E E T

System: Plain component is a keyword
sequence derived from MONDAY
and arranged in a 5 x 5 square.

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

Problem No. 3

AOU EI AIOIA UEEUE UAHIA IOIAU EEAAO UEUEA OEIIU EUEOE EEATA
 A T F I F T E E N F I F T Y A T T A C K E D B Y F

IOAUE UOAEU UOIOA IIEUE OIAII IEUAO AUEAE EOIOE EEIOA IIECO
 I V E L E X I N G T O N H E A V Y B O M B I N G P

OAAOA IEUAE AAAIE OEUUA AOAIU EIOAO IOUAE IUAAO IAUEI AIOUA
 L A N E S U N D E R A N T I A I R C R A F T F I R

EUUEI IUAEU EUOEI OAI AA UEEUA EOOOA AOATE UAEEE OIOEE EIOAI
 E T H R E E M I N U T E S P L A N E S B O M B I N

IEOOO IAETIO UEIOO IAIAO OAUEI OUEAA EOEUE IAIEU IAOLA AUAE
 G P O S I T I O N A L T I T U D E O N E F O U R T

IIOIA AAEAO AIEOI AEUEU UEAIO IEOAO OEAOI EEUUE OIAEA OUA AO
 H O U S A N D F E E T N O D A M A G E T O S A R A

UEOII EAO
 T O G A

System: Plain component is a keyword
sequence derived from US NAVY
and arranged in a 5 x 5 square.

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

Problem No. 4

IDUGE JFOIK IQPED IALUM WIECZ AGUHA QIVEC EIKUG KILAE PQIKI
 S I G H T E D S U B M A R I N E L A T I T U D E T

FOGUA ZIKOP EPIQE JAZQI QIDIK IBAIQ HAIKP OOLAH IQWU GAHAL
 H I R T Y D E G R E E S T W E N T Y O N E M I N U

KIQII DEVOL AHJEG UIKLA PEIQO LAHQI OFALH APEZA QIEPO RLOZA
 T E S L O N G I T U D E O N E H U N D R E D F O R

IKOPK IBALO EPQIJ EAZIQ QIDII DGUIN IKIQQ IHAWI UGHAL AKIQI
 T Y T W O D E G R E E S S I X T E E N M I N U T E

IDCEI KHAUG AHQII KQIIQ HAROO LZAKI OPORL OALAZ IKIQI QAHTW
 S A T N I N E T E E N F O R T Y F O U R T E E N M

CEAZN AOFQX QIZAG ULOPE XOO LI DIDUG MUVEQ IIKFO GUDI U GIDUM
 A R C H P E R I O D P O S S I B L E T H I S I S B

ECIDD IANLO MEQIZ AUGHA EJEJA ZQICE KINAG UZANA EVIQA ZOLLA
 A S S C O V E R I N G G R E A T C I R C L E R O U

KIIQK IOLDI CEAHO RZAEG HAANU GIDNA LO
 T E T O S A N F R A N C I S C O

System: Plain component is a keyword sequence derived from WASHINGTON and arranged in the following square:

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

Problem No. 5

MAPNC HMDUS YNLNN PUSHC YNFIN YIFFI PNFAR CLHFT PNCHO CSUMP
 D E S T R O Y E R S O F O F F E N S I V E S C R E
 NPFAY OHLMT TMIFE PPNIM MDYNO PNYSU USYNO YHCPE AFAML ELIUT
 E N W I L L F U E L T O M O R R O W S U N D A Y B
 PNYRH LAFAR LHFAR YELDM AMLEN LMTLH RYWSM DWIPN USLHY NMAHY
 E G I N N I N G A T D A Y L I G H T P E R I O D O
 HLTMN PSUCH DMLEC EPNCH DMLED MHLYN AFLEC HHCNY NYFAE LHCIW
 I L E R S T A K E S T A T I O N A S S O O N A S P
 SUELC ODM LH OCELU TTRNP ELAFM ACOYN POWIM TNPED PNELM TTFAR
 R A C T I C A B L E A N D C O M P L E T E A L L N
 PNCOP NHCCH LEUSL NELUS SULEA FYRNP OPPNF ADMCH
 E C E S S A R Y A R R A N G E M E N T S

System: High to medium frequency letters over medium to low frequency letters, digraphs reversible.

- (p) - 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
- (c) - E T O A N I R S H D E T O A N I R S H D E T O A N I
- (*) - L U C M P F Y W L U C M P F Y W L U C M P F Y W L U

CHAPTERS 4-11 NOT RELEASABLE

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.ELEMENTARY COURSE IN CRYPTANALYSISASSIGNMENT No. 12OPEN CODE

1. The type of problem dealt with in this assignment is called "Open Code", which is defined as a code or cipher that either appears to be innocent and harmless or else appears to be extremely vague and ambiguous. There are nearly as many systems of this nature as there are individuals using them. Open code has no place as a regular system in a military communication organization and is suitable only for use between individuals. Various types have long been favorites with those engaged in espionage and those trying to send information in censored mail. For such purposes, the more innocent appearing the cipher is, the better. Open Code is given in this assignment to familiarize the student with some of the more common types of cipher in this category. In many cases, problems can more accurately be considered puzzles rather than cryptograms.
2. A very common system is one in which frequently used words are substituted for other words which are closely associated with the subject matter that the correspondents expect to discuss. For example, "I have" might mean "New York", "I had" = "San Pedro", "of course" = "submarine". When cleverly used it is practically impossible to distinguish such a code message from other straight-forward communications which discuss the doings of genuine people in a natural way. Even if suspected, the system is hard to break and much more text is needed than is usually available. The futility of most "Open Codes" should be evident from the fact that paraphrasing by the censor completely destroys the hidden message.
3. Other common types are given with a brief word of explanation concerning them. One of the most common systems is one in which normal and innocent language is used and the hidden message is revealed by reading every Nth letter or every Nth word, or the first and last letters of words. The variations that have been employed are practically limitless. Another method is one in which the hidden letters or words are thickened slightly, as though the writer were having difficulties with a poor pen. Sometimes the hidden text is indicated by small dashes, misplaced commas, false punctuation, or breaks in a word. False punctuation may be employed to disguise short hand. The use of a grille is an old favorite, employing words instead of letters. In this type, the text doesn't make sense, and, of course, would not pass any censorship. Numeral ciphers are often employed disguised as legitimate business accounts or a jumble of figures on what had seemingly been used as a scratch pad.
4. The types mentioned are the most common of a large number of such systems. The problems given herein should offer no real difficulty to the student at this stage of training. In all cases, there is believed to be sufficient text and collateral information to permit solution.
5. There is one classic open code system invented by Sir Francis Bacon. By the various combinations of upper and lower case letters, taken by groups of five, he was able to disguise a hidden meaning to certain of his writings beneath what appeared to be poor typesetting. Still another system is one in which a few letters of the alphabet are used to encipher the hidden message and all other letters of the alphabet are used as nulls. The message is first enciphered using the effective cipher letters and the nulls are inserted where they fit to produce words and sentences. As in other types, paraphrasing obliterates the hidden text.

PROBLEM No. 1

The following letter might have escaped detection had not the addressee been under suspicion:

Dear John:

Yesterday I shot two ducks among a thousand I saw feeding. Tons of birds, plenty of time, lots of ammunition, but no luck!

I'm leaving here Sunday for New York. Please meet me at the Carleton about midnight that night or Monday morning at ten.

Sincerely,

PROBLEM No. 2

The following two messages were intercepted simultaneously on two different frequencies. The calls, headings, etc., were heard just previously on a third frequency:

Serial 1 - PRILY OFRER PRETR FETON TSAON NOEGT ETMSI NNNWQ

Serial 2 - ATALC NIMDE OTNIE LEGIG OEMRI GFIHE NHISO UKONP

PROBLEM No. 3

The following letter from a prisoner of war caught the censor's eye:

2 July 1917.

My dear Sally.

Last week's letters may not go through as they exceeded regulat io res. We are now out of quarantine and two other officers have joined us in the same house, making a party of five including Glatz-Brown and Stone - both old residents of the Camp and very good fellows. We are busy making ourselves as comfortable as possible. Anything except very primitive furniture is out of the question. Have met only a few of the other prisoners whose story of capture are most interesting and thrilling.

About that other matter we discussed you may think I have broken my word but if you read my letter right I am sure you will see it from this point of view. I don't want you and John feeling downhearted.

Write a line to Lieut. R.H. Root of H.M.S. Colossus telling him I received his letter of May twelfth but cannot reply till after a week's time. Inform Dorothy you have received this and to write me a line or two.

Love to all
Herbert.

PROBLEM No. 4

The following mass of figures appeared in a letter which otherwise seemed innocent. The numerals, however, did not seem to have any bearing on the rest of the letter, and were written carelessly on the back of one sheet, as though the sheet had been used previously as a scratch pad:

35	25	31	14	20	30	12	28	23
25	12	24	15	31	<u>25</u>	31	15	19
<u>31</u>	29	19	26	29	55	15	26	22
91	15	30	11	30		24	25	22
	28	15	28	19	23	25	28	15
11	32	<u>14</u>	30	13	15	29	<u>30</u>	<u>28</u>
28	11	133	23	<u>15</u>	34	136	152	129
<u>15</u>	30		15	157	19			
54	19	29	24		13	11	30	
	25	<u>30</u>	30	26	<u>25</u>	19	<u>25</u>	
31	<u>24</u>	11	216	28	129	28	55	
24	250	30		25		15		
14		15	25	13	30	<u>29</u>		
15	12	<u>29</u>	<u>16</u>	15	18	102		
28	<u>35</u>	144	41	15	15			
112	47			<u>14</u>	24			
				136	13			
					<u>15</u>			
					115			

PROBLEM No. 5

The following letter was found among the effects of a person suspected of being engaged in espionage:

BUILD NEW NO LEARN STOP UNABLE
SYSTEM DEFINITE WHICH NEWS WILL EXPLAIN
PRESENT PLANS USUAL REQUIRE FAILURE ABOUT
STOP SOURCES THINK AND TWO NO
LONGER NEW NEED CONTACTS FUNDS MUST
ABLE TO MONTHS TO BE MADE

PROBLEM No. 6

The following is one of the so-called Scotch telegrams (Scotch-o-grams) which appeared in Judge:

THOMAS INJURED ERASED AFFORD ERECTED ANALYSIS HURT TOO INFECTIOUS DEAD

PROBLEM No. 7

Dearest Mother:

Have you heard whether you will be allowed to travel this summer or have you made up your mind to wait until after the war? I hope that you have. It may be not at home but at least there you aren't running the risk of being torpedoed some dark night.

Speaking of heat, I am getting very tired of sitting at a desk in the office and I am very anxious to get a job at sea again. By the way, I saw Jack North last Sunday. He is home on leave looking very fit and refreshingly optimistic.

I'll let you know by Sunday when I can be home again for a few days. XX

With love,
Harry.

PROBLEM No. 8

The following telegrams were filed by the same originator to the same addressee on successive days:

SERIAL No. 1 - Money sent to New Haven in bank on Arts account He may have drawn all and gone home being so bored as always he needs a lot of cash yet is not able to do much with the money sent to pay his lab school bills.

SERIAL No. 2 - Sent forty dollars by check to Henry and Alice after they payed all Arts old debts stop I really want agreement with them and we must make Art stop charges and bills about town Send no more checks to him or cash to waste always for he spends it.

SERIAL No. 3 - Mother sends love and waits each letter as she always does so write as many as Tom and Elois do to her As always, Jerry.

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.

TRAINING PAMPHLET NO. 1 NOT RELEASABLE

RESTRICTEDNAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.ELEMENTARY COURSE IN CRYPTANALYSISTRAINING PAMPHLET No. 2GENERAL PRINCIPLES OF COMMUNICATION SECURITY

1. Communication security, as a subject, is at least 2,000 years old, for we find in the writings of the ancient Greeks and Romans, references to the ciphers used by them in their military campaigns. Throughout the ages, greater or lesser attention has been paid to the subject by virtually every nation which has engaged in warfare or diplomatic intrigue. But not until the Great War did it become a subject of sufficient importance to warrant more than a cursory interest on the part of any except those engaged in the inner circles of the work.
2. As a matter of fact, those experts who were most vitally concerned did everything within their power to keep the subject away from the glare of publicity. They felt, and justly so, that the smaller the group of persons who were cognizant of the security measures taken and the results of counter-espionage work, the less chance there would be of drying up the sources of information which careless enemies left open. Such a policy did very well as long as the number of messages which had to be enciphered remained small and within the capabilities of small groups of people. With the Great War, however, with its operations on an unprecedented scale and with the development of radio with its illimitable possibilities for the passing of information and orders, the handling of secret communications became absolutely impossible for the small, well-trained groups of people which had formerly been entrusted with it.
3. This was the time when the fallacy of the "ostrich policy" became not only apparent but disastrous. Poorly trained troops were rushed into the field with codes and ciphers which they did not understand and which they could not have been expected to handle properly. The result was an avalanche of misguided effort which enemy cryptanalysts were quick to seize upon and convert to valuable information.
4. With the ending of the war there was a marked change in policy with regard to communication security by all of the nations which had participated. Each one said in essence, "By keeping our methods of communication security so away from enemy eyes, we failed to let our own people in on the secrets. Thus, when called upon to function in the heat of battle they failed, and nothing else could have been expected. That will never happen again."
5. It may happen again, but the chances are very much against it. Since the war there have been innumerable books written in whole or in part concerning the role which communication security, and lack of it, had to play. Much of the literature has been for popular consumption and has proved extremely welcome. Much of it has been technical in nature, for the lessons of the war, and the developments of communications in general have both pointed to an even greater part for this element of military effort in any war to come, and the development of experts capable of dealing with it is essential. Some of it has been general and some of it has been most detailed in nature. But regardless of the general tenor, all of the literature and all of the experience gained points to the fact that only by education and indoctrination of all concerned, may communication security be successfully maintained.
6. The purpose of this pamphlet is merely to present in as readable form as possible, some of the lessons which have been learned and some of the measures that must be taken if we are to keep our vital secrets away from prying enemy ears.
7. "Communication Security" embraces the principles governing the safeguarding of information, conveyed by any means, (publications, letters, radio,

TRAINING PAMPHLET No. 2

visual, cable or landline telegraph, mail, messenger, and word of mouth) from falling into the hands of unauthorized persons, no matter how remote they may be from connection with potential enemy services. The conclusions reached herein pertain primarily to information transmitted by radio, but apply as well to other forms of communication. These conclusions are in no way based on hypothetical supposition, but, on the contrary, have been developed through actual experience, our own and that of other nations. Examples and authentic anecdotes are given in support of many of the ideas presented, but, in some cases, these are vague and lacking in detail for reasons which, it is thought, will be obvious.

8. Some of the means by which secret information may reach unauthorized persons are:

- (1) Careless conversation.
- (2) Careless handling of translations of encrypted despatches.
- (3) Careless censorship of material released to newspapers and periodicals.
- (4) Careless handling and safeguarding of secret publications.
- (5) Improper classification of matter and improper selection of systems of cryptography.
- (6) Careless radio operation.
- (7) Cryptanalytic solution of code and cipher systems.
- (8) Improper selection of communication facilities.
- (9) Espionage.

9. The order of tabulation does not indicate order of importance. Such indication would be impossible because it is dependent upon time, place, and existing conditions. Forgetfulness of any one weakness may bring about calamity.

CARELESS CONVERSATION

A wise old owl lived in an oak;
The more he heard, the less he spoke;
The less he spoke, the more he heard--
Why can't we be like that wise old bird?

10. Admiral Bacon, R. N., has said, "So long as plans are locked up in the minds of the admiral and his one or two chief assistants, secrecy is possible. As soon as parts have to be let out, secrecy is apt to vanish. Mind you, when a person has guessed a secret, he usually feels himself quite at liberty to talk about it even if it be against the interests of his country, simply because it has not been divulged to him under the bond of secrecy. It is gratifying to some to let others know how clever they have been in guessing a plausible solution." It is typical of the American character to dislike ostentatious secrecy and to abhor secretiveness in any form. Admirable as this trait may be, it is a dangerous one in officers who must, by reason of their profession, keep in their heads information, the disclosure of which would be inimical to the interests of the country. The officer who, in the midst of a conversation on professional topics, finds it necessary to say, "I would rather not talk any further on that", feels uncomfortably, and, perhaps justly, like a character in a melodramatic novel. There are other ways, and, after all, sudden silence after unrestrained volubility can be as revealing as the most open statement of fact. The officer in frequent contact with outsiders can adopt one of three poses with regard to talking shop; he may assume consistent silence, he may resort to consistent and mendacious garrulity, or he may consistently plead ignorance. The first and last are undoubtedly the safest. The second is a method for experts: the old-fashioned sailor who regaled visitors to his ship with "tall tales" about the vessel and its gear may not have been a model Christian, but he had his points.

11. In discussing professional subjects with persons in whom one has the utmost confidence--close friends or members of one's family--it is well to consider that, although they would never knowingly reveal information given them, still they may, in ignorance of its importance, inadvertently pass on some detail to a third person in casual conversation. Confidential information can be actually embarrassing to one who has no need of it, and is therefore much better kept locked behind the lips of those for whom it is of professional interest and who

TRAINING PAMPHLET No. 2

are capable of realizing all of its possibilities. Some of those who served out of San Diego in the autumn of 1929, just prior to the commencement of the decommissioning of certain destroyers, may remember that, although the question of decommissioning was given a confidential character by Commander Destroyer Squadrons, and personnel were warned not to discuss it outside of the service, yet all the developments as they appeared were common knowledge throughout the vicinity of the fleet base. As a remoter, although far more serious "horrible example", witness the embarrassment of high British officials after Jutland when they found that the "rocking-chair brigade" around the tea-tables of London was chatting freely about the secret (so carefully guarded at the Admiralty) that the loss of British ships in the engagement was due to improper design of ammunition supply from magazines! In this connection, it is not the purpose of this pamphlet to enter into a digression into the relative merits of the two sexes in the exercise of discretion, so that the following unauthenticated anecdote will have to stand without further discussion.

12. History tells of the strange report that went the rounds during the early part of the war to the effect that 250,000 Russian troops had landed on the French Channel coast via Scotland and England, for service on the Western Front. The report caused a certain amount of consternation in Berlin and was believed by many in Paris. It exercised such control over the imagination of one German agent in Scotland that he actually reported having seen them--"huge, bearded men with snow still clinging to their boots". It is said that this fantastic tale was started on its way by British Intelligence officers who carefully imparted it as a deadly secret to ladies of their acquaintance!

CARELESS HANDLING OF TRANSLATIONS OF ENCRYPTED DESPATCHES

13. If the unguarded tongue is a menace to security in general, then the wastebasket is a double menace to communication security. For translations of encrypted despatches which are carelessly tossed in innocent-looking wastebaskets are not only available to an alert enemy for the information which they themselves divulge, but are of inestimable help to enemy cryptanalysts in the solving and reconstruction of the cryptographic systems utilized.

14. It simply stands to reason that if an expert cryptanalyst can obtain a copy of the cipher text of the message (a comparatively easy procedure) and then obtain an exact translation of it (as from a wastebasket), then by a simple process of working backwards, the values can be deduced, the general method worked out and subsequent messages in the same system read with ease. It is just one such "break" that cryptanalysts dream and hope for.

15. A paraphrase of the exact translation is of but slightly less value to the cryptanalyst. In many cases all he needs to know in order to be able to break into a message is the general subject--whether it concerns "submarines" or "battleships" or whether or not a date mentioned is "November 21" or "December 31". This means that although translations should always be paraphrased for distribution, the paraphrased copies should be as zealously guarded as the exact translations--and more particularly, that nothing connected with encrypted messages should ever be consigned to the ordinary wastebasket.

16. It is a fact that during the Peace Conference in Paris after the World War, the paper from the wastebaskets of the delegates became an almost openly marketable commodity. Scarcely a piece of writing on the subject of international espionage is published without some mention of the services of charwomen in this respect. Whether such writings can be trusted or not is beside the point. They at least reveal the possibilities in this direction.

17. The moral is: All notes, work sheets, carbon paper, and other materials used in coding work must be destroyed by burning as soon as possible, and, all translations, exact and paraphrased, must be kept in carefully guarded places until their usefulness is at an end, when they too must be destroyed by burning.

TRAINING PAMPHLET No. 2

CARELESS CENSORSHIP OF MATERIAL RELEASED TO NEWSPAPERS

AND OTHER PERIODICALS

18. Closely allied with the revelations made in indiscreet conversations are those made as a result of careless censorship in releasing material to the press. It must always be remembered that the press of a nation may, in general, be considered as extremely loyal and as anxious to help win a particular war as any other body of the citizenry. On the other hand, it must likewise be remembered that the business of the press is to obtain and publish news. It is going to publish anything it can lay its hands on, unless it realizes the inherent dangers to the security of the country in the publishing of such news. This means that all news concerning a nation's military operations (and therefore coming under the cognizance of military censors), which it is desired to keep secret, must (1) be kept from the press, or (2) be given to the press with a frank statement as to its danger.

19. The second method is invariably the best, for the ability of "newshawks" to ferret out news, despite efforts to keep it hidden, is axiomatic. It is the newshawk's only reason for being. Some of the nations in the Great War realized this fact and made most of it.

20. For instance, when the British Admiralty, early in 1918, planned to block the Zeebrugge submarine base entrance with concrete-filled block ships, it was decided to commandeer two Mersey River ferries for the purpose. As these craft were sure to be missed by the people of Liverpool and vicinity, and undesirable publicity threatened, the entire press of Britain was taken into the secret and their cooperation requested. Never a sign or trace of the news leaked out, and the press loyally carried out the wishes of the Admiralty.

21. It is significant that this instance of taking the press into the confidence of the nation came after 3 long years of war. Some earlier experiences with the press had not been quite so satisfactory. Admiral Jellicoe, for instance, had been most zealous in keeping news of the fleet away from the press and had thereby incurred its violent dislike. This dislike showed itself after the Battle of Jutland when the press, with presumably the best of intentions, flayed the administration and the naval command at sea. Whether or not this attitude hurt the British and Allied cause in the long run is doubtful, but there can be no question but that it hurt the British morale at a time when the best of morale was needed.

22. Another point to be constantly borne in mind in dealings with the press is that even the most innocuous-looking items of news may carry information of vital importance. The relation of every piece of information to the broad general picture must always be allowed for.

23. Early in 1918, it was known that the Germans were preparing a great spring offensive on the Western Front. Where they would strike was not known. In Switzerland, an intelligence agent of the Allies, in glancing through a small Baden journal came across a letter to the editor from the proud mother of a young German aviator who had lost his life while flying over the area of the Fifth British Army. She quoted a letter of condolence and sympathy from the German Army Commander in that area. It was signed "Von Hutier." The provincial editor had evidently seen no harm in printing it.

24. Never before had Von Hutier, organizer of the victorious campaign at Riga and elsewhere on the Russian front, been located on the Western Front. His taking over part of the line was a secret, carefully guarded by the Germans. The learning of this secret was the entering wedge by which the British Intelligence, through further research, of course, determined where, when, and how the expected offensive would break. Von Hutier's character, his past record, his location, all pointed to the crossing of the River Oise as the opening move in an attack with Amiens as objective. The British line was ready at the proper time--and Von Hutier did not accomplish his mission. This incident is especially interesting in showing from what small acorns of information the complete oaks of connected intelligence may grow.

TRAINING PAMPHLET No. 2

CARELESS HANDLING OF REGISTERED PUBLICATIONS

25. The business of modern navies has become so complex and technical that each navy strives to keep from the others those bits of information which it has laboriously arrived at and which it thinks will give it an advantage over others, if and when they should clash in another Jutland or another Coronel.

26. These bits of information are multitudinous in number and can only be recorded in sets of books which go to make up the confidential libraries of each navy. Among such books are the codes and ciphers, the instructions and all the other paraphernalia connected with cryptographic systems. "Security" in general, is interested in the safeguarding of the entire library. "Communication Security" is interested in preserving our cryptographic paraphernalia from prying enemy eyes.

27. At the outbreak of the World War the British Navy set up a gigantic cryptanalytical organization in the Admiralty which later became the famous "Chamber 40." Little is known concerning the success or failure of this organization at strictly cryptanalytical work, but it is known that German code books recovered from the German cruiser MAGDEBERG, which ran aground and was wrecked off the coast of Russia, found their way to "Chamber 40", and it is fact that "Chamber 40" produced invaluable intelligence on which were based many of the British operations. It can be no secret that at least some of this intelligence came out of the code books recovered from the MAGDEBERG, and yet, as far as is known, these books were not superseded for 2 years.

28. The first undoubted and absolute principle of communication security is preservation of the physical security of codes and ciphers and all that pertain to them.

29. It is not enough that such material be preserved permanently, or until they are superseded or placed out of effect. It must be kept constantly under proper supervision and in carefully guarded places. The reason for this is that an enemy agent, intent upon obtaining the information contained in a code book, will seize and keep the book for a length of time only sufficient to have it photographed and then return it, hoping that its absence from its authorized place has not been noticed. It has been estimated that a reasonably large-sized code book may be photographed in 2 hours. Codes or ciphers left on wardroom transoms are a menace, not only to the officer who is "signed up" for them but to the entire naval service.

30. Furthermore, it is vital that proper precautions be taken to insure that unauthorized persons are not allowed access to secret files or spaces containing secret files, or knowledge of the contents of such files. Even within the service there is no reason why officers unconcerned with secret matters or communications should have any access whatever to secret stowage until it becomes necessary in the normal conduct of their duties. As in a previous paragraph, it is appropriate to remark that unnecessary secret information is a burden to him who holds it.

CARELESS RADIO OPERATION

31. The historically outstanding examples of good and poor radio discipline may be found in any account of the conduct of British and German naval operations during the World War. The German commander in chief made a practice of sending out numerous operation orders by radio before a sortie, with the result that the radio direction finders of the British enabled them to know in every case when the enemy fleet had left Wilhelmshaven for the outer anchorage in the Jade. On the other hand, the German attempts at radio direction finding never succeeded in obtaining information of value.

32. The World War and our own fleet problems and exercises of past years are rich in examples of the proper and the improper use of radio. The lessons learned show that attention must be given to many items--maintenance of radio silence, adherence to correct procedure, careful sending to reduce number of

TRAINING PAMPHLET No. 2

repetitions, elimination of unnecessary and unauthorized transmissions, use of correct call signs, and so on.

33. But more important than blind attention to detailed and explicit orders in the preservation of radio security is an active and vivid imagination which pries into the question of what the enemy might be able to deduce from some particular transmission. The most innocuous-looking messages are sometimes loaded with military dynamite. For instance, one could not possibly have objected to the broadcasting of weather reports from the shore station at Scapa Flow. There was no information in them alone which could have been of any possible value to the Germans. However, instead of sending them out every day, the British sent them out only when important units of the Grand Fleet were at sea. A German operator at Neuminster noted this and for some time was able to advise his Admiralty as to when the enemy was at sea. No amount of radio discipline within the Grand Fleet could offset the damaging effect of those apparently innocent weather reports.

34. Nor was there anything particularly revealing in the fact that a "bier-abend" arranged for a group of destroyer officers at one of the German bases had been postponed. The British were supposedly not interested in how or when the Germans had their evenings of beer drinking. A radio message was therefore sent out to all the officers affected and likewise, to all intentional purposes, to the British Admiralty. But the British were interested in just such facts, particularly when linked up with other facts of a similar nature. In this specific case that message concerning the "bier-abend" served to justify completely the assumption that the Germans had a sortie on for that night--as indeed they did have. It resulted in the Battle of Dogger Bank.

35. Mighty events may well be outlined in tiny strings of innocent words.

CRYPTANALYTIC SOLUTION OF CODE AND CIPHER SYSTEMS

36. The failure of the great German offensive on the Western Front in 1918 may to a considerable extent be attributed to the work of one man, Captain Painvin of the French Intelligence Service. This officer, through decryption of German radio messages, was able to obtain vital information of the attack, prior to and during its progress. His "break" came as the result of an improper use of cipher on the part of perhaps no more than two German communication officers. Two days after the new German cipher had been put in effect (March 11, 1918), a German station transmitted in the old cipher a request for repetition of a message which had been sent out in the new. The originator obliged with the original message in the old cipher. The French now had the same message in the old, previously decrypted cipher, and in the new cipher upon which the Germans were depending for security of their plans. As a result the French were soon reading all German operation orders in the new system before the Germans themselves were quite accustomed to its use. This particular cryptographic error was enormously costly to the Germans.

37. That is an illustration of but one of the many coding errors which smooth the way for cryptanalysts. The instructions issued with each individual code or cipher must be followed carefully in order that the benefits of past experience may not be wasted through lack of knowledge. Experience is the best teacher, but the other man's experience is much less costly than one's own.

IMPROPER SELECTION OF COMMUNICATION FACILITIES

38. Undue radio activity in an area might serve to betray the location and movements of a fleet. It is also true that cessation of all radio signals will tend to indicate the imposing of radio silence and the probable imminence of a major operation. The German commander's great mistake at Wilhelmshaver lay in his use of radio where visual or mail boat would have served equally well with far greater security. Radio must never be used when telegraph, cable, courier service, guard mail, or visual can be made to serve the purpose.

TRAINING PAMPHLET No. 2

39. In time of war an officer courier service is usually established between important points. Secret communications are not normally transmitted through the mails, but are forwarded through this courier service. Secret matter will be carried on the person of the messenger or kept in his immediate vicinity. On prolonged voyages in merchant vessels under the registry of the nation involved, such matter is usually kept in the safes of the masters or pursers in sealed containers. Sometimes an armed naval guard is assigned to accompany the messenger.

40. Diplomatic officers in various parts of the world use diplomatic pouches for transmission of correspondence to and from their capitals. These pouches may usually be used for certain naval correspondence. Their inviolability is guaranteed by international agreement. But, so was the neutrality of Belgium.

IMPROPER CLASSIFICATION OF MATTER AND IMPROPER SELECTION OF SYSTEMS OF CRYPTOGRAPHY

41. Information once transmitted in a secret system must remain secret forever. The contents of a secret message must not be revealed to unauthorized persons in any way. Conversely, information which cannot be kept secret or is not actually secret must not be put into a secret code or cipher. It has happened on more than one occasion that a ship of the Navy has been ordered to undertake a certain movement, the instructions for the operation being encoded in a secret system. Such operations always become public, and it is obviously fatal to transmit in secret code anything whatsoever concerning them.

42. The considerations of (1) selection of communication facilities and (2) classification of matter are closely allied in their effects upon cryptographic security. Cryptographic security is maintained by the proper employment and use of code and cipher systems. The degree of security attained will depend directly upon (1) the purposes for which codes and ciphers are employed, (2) the technical perfection attained by the personnel connected with code and cipher work, and (3) the length of time codes and ciphers are continued in effect. The length of time a system is continued in effect depends upon (1) the amount of improper employment and use to which the system has been subjected and (2) the amount of proper employment and use to which the system has been subjected. The effective periods of cryptographic systems are determined and prescribed by high authority.

43. It is obvious that, in order that cryptographic systems may be continued effective for reasonable lengths of time, a careful supervision must be maintained over the employment and use of these systems. This supervision is carried on through the function of message censorship which is the immediate responsibility of the communication officer under the commanding officer. In time of war, certain major activities will establish a continuous watch of "message censors", who will function under the communication officer and, in some cases, directly under an "assistant to the communication officer for cryptographic security." The duties of these "message censors" is indicated in detail in confidential instructions. In commands where the limited officer complement does not permit of establishment of a continuous watch of "message censors", the function of message censorship devolves directly upon the communication officer and his assistants, in peace as well as in war.

ESPIONAGE

44. The most accurate and valuable information concerning important matters is to be found in secret documents. The principal governments of the world maintain extensive intelligence services whose missions are to obtain such secret information of other governments. The forms of espionage which have been used in the past and which are being used to obtain information are extremely effective. It has been quite possible for an agent to gain information through the confidence of an unsuspecting individual or to gain access to a secret document, photograph it and return it without the knowledge of the custodian.

TRAINING PAMPHLET NO. 40 NOT RELEASABLE

TRANSLATION FROM THE SWEDISH ORIGINAL BY

N. VON KOCH

OF AN ARTICLE APPEARING IN THE MARINE
RUNDSCHAU COVERING THE SERVICE OF RADIO
INTELLIGENCE AND RADIO SECURITY IN THE
BRITISH AND GERMAN NAVY DURING THE WORLD
WAR.

THE USE OF WIRELESS TELEGRAPHY IN THE
WORLD WAR, MORE ESPECIALLY FROM
THE NAVAL STRATEGICAL POINT OF VIEW

By N. von Koch

From Tidskrift i Sjöväsendet 1924 No. 8

----- Translated from the Swedish Original.

A wise old owl lived in an oak;

The more he heard, the less he spoke;

The less he spoke, the more he heard;

Why can't we be like that wise old bird? "

Lord Fisher, Admiral of the Fleet, and First Seaford for the greater part of the war, uses the above verse from an old English poem in his "memories" as a motto for a chapter on the British Admiralty Staff. That old verse absolutely hits the nail on the head, when it becomes a question of dealing with the question of the use of wireless telegraphy from the strategical point of view. Elsewhere in the same chapter Lord Fisher writes:

"The First Seaford and the Commander in Chief of the Fleet have to be Siamese twins. And when war comes, the Admiralty Staff at the Admiralty - by listening every moment to the wireless messages of the enemy (in so far as the latter dares to use them - puts the First Seaford in a position to let his twin brother at sea know exactly what is going on. He picks up the wireless messages, and not necessarily the Commander in Chief, as a wireless installation on shore has far more powerful receivers than an installation on board ship. When you look at that spider's web of wires on the roof of the Admiralty, then thank God, that England is more or less free, because that net of wires was rigged up by a crowd of bluejackets before anybody smelt a rat. A German naval letter intercepted at that time was a source of great personal joy to me, because it revealed the truth, that wireless telegraphy is the strong navy's weapon. For it is the development of wireless telegraphy that has rendered it possible to determine the direction from which somebody is telegraphing and to go straight for it. Consequently the German is afraid to open his mouth. If he does so nevertheless, the message is of course in cipher; that the Admiralty succeeded in

Deciphering that code is one of its most glorious achievements in the late war. During my time it never failed once in deciphering. Yes, wireless telegraphy is the strong man's weapon."

Thus far Lord Fisher. - But wireless telegraphy is a dangerous weapon; rightly used: dangerous for the enemy; but carelessly used much more dangerous for one's self. The English recognized that fact, but not so the Germans, even at the beginning of the war, and that is why their wireless organization became something entirely different from that of the Germans. It is with these facts forming the background that the whole question of the use of wireless telegraphy in the war should be reviewed.

I. THE ENGLISH WIRELESS SERVICE ORGANIZATION

A. Organization for listening-in to the enemy.

From the very beginning of the world war the listening-in to the wireless communications of the enemy, prepared in advance by the English, was in working order. In order that not a single message should be missed, no matter on what wave length, they had a large number of receivers, to each of which was assigned a certain wave section. Everything received was sent direct to the Admiralty, where a special de-coding office for the Allies had been established. Thanks to this arrangement of paying attention to everything received, an enormous and extensive mass of material became available, and before long the Associated Nations were masters of the German Code just as much as the Germans themselves. This knowledge was however for the greater part augmented by the chance discovery of German secret documents. Thus, for instance, the Russians, after the stranding of the small cruiser "Magdeburg" near Odensholm, are said, to have found an iron safe sunk near the cruiser, containing several German secret documents and books, including inter alia the key to the Code, signal books and charts. The collection was increased still further by mine-charts of the North Sea and the English coast, when about January 1915 the "U-31" was driven ashore at Yarmouth, undamaged but with the crew all dead.

B. DIRECTIONAL STATIONS

Apart from the listening-in stations already referred to, the English, as far back as the Fall of 1914 were getting good results from wireless "directional stations" established for the purpose of working hand in hand with the former. The "directional stations" were established at suitable points on the English coast line, and their duty was to get the bearings, the direction of every German sender. These bearings were then forwarded direct to the Admiralty, where they were collated, part of them with each other, by which means the position of the sender was located, and part of them with the message picked up by listening-in, whereby it was usually discovered who the sender was.

As to how the organization was worked in details, so that one could be sure that the bearings determined, notwithstanding the vast number of messages, referred to one and the same sender, and also as to how it was possible to fit the bearings to the right message, I have not been able to find any information. But it is hinted, that great skill and training on the part of the personnel were essential, and that especially during the first year of the war many mistakes were made. But, thanks to energetic work and far-sighted vision the information furnished by the directional stations gradually became absolutely reliable, and Jellicoe observes on this point, inter alia, that in consequence he was able to reduce considerably the scouting forces which the Grand Fleet was obliged to keep at sea. German warships or craft at sea almost invariably betrayed themselves by their wireless signals. All German attacks on a larger scale were preceded by a lively wireless conversation, as the Germans, never dreaming of anything wrong, generally issued their preparatory orders by wireless. Consequently, as a general rule, the British mostly knew in advance where the German warships were, and also what they had to expect!

In course of time the English operators at the listening- and directional stations became so familiar with the peculiar features of the various German ships with respect to sound, etc., that as a rule, as soon as they hear a German wireless message they were at once able to name the class of the sending vessels and frequently its name as well.

C. ORGANIZATION OF THE HOME WIRELESS SERVICE AND COMMUNICATIONS.

From the very beginning of the war the British had been cautious in their wireless communications, and the more they learnt to profit by the German system, the more clearly they saw the necessity of avoiding wireless telegraphy for the transmission of orders and intelligence.

1. Measures for elimination of wireless communications. -

In port or at anchor the senior commanders were always in connection with the telegraph system on shore. In Scapa Flow, for instance, a complete telegraph station was established on a ship, which remained at anchor permanently. This was in constant telegraphic communication by wire with all large ships, the ships of the Divisional Chiefs and those in superior command in port. Wireless signals were permitted from one ship only at Scapa, probably the stationary telegraph ship, and then these mostly related to flotillas of small vessels only, guard ships and the like who did not reply to them. Any discoveries made and important messages were of course communicated by the latter by wireless, picked up by the stationary telegraph ship and passed on. All orders from the Admiralty to the commanders in

051

in charge, as also those from Jellicoe to other divisions of the Grand Fleet posted elsewhere than at Scapa Flow were, so long as the ships remained in port, transmitted as coded telegrams by wire.

At sea it was more important still to maintain wireless silence than in port, a fact which was pointed out more than once by Jellicoe and by other commanders in chief.

To keep the Grand Fleet together and well in hand, without using wireless telegraphy, was no light task, however, especially in view of the ever extending guard duties, the constantly increasing distance of the scouting ships and the high speed which had to be kept up at all times on account of the submarine menace. To render this possible, every attention was devoted to optical signalling, using the heliograph in the daytime. For distances of 1 to 2 nautical miles as rule fixed semaphores were used, and the divisions within themselves frequently used signalling flags. For signalling at night the British used low-candle-power flash lights with beams of very small diameter and a radius of about 500 meters. As these could only be used for direct signalling between two vessels, it was at times necessary, especially during the first year of the war, to have recourse to wireless telegraphy in order to remain in touch with the rest of the ships. That was especially compulsory in the case of a sudden fog coming on. Gradually the Grand Fleet succeeded in preserving practically absolute wireless silence during its scouting expeditions in the North Sea, - even when conditions were unfavorable - namely by issuing in advance minutely exact and to a certain extent detailed general orders for every conceivable eventuality, and by giving orders, before darkness set in, with reference to all movement to be expected during the night, stating the exact time when the same were to be executed (changes of course, of speed, detachments, rendezvous, etc.).

For the transmission of orders, intelligence, etc. from the shore to warships at sea, obviating the necessity of the latter having to betray themselves by replying at the beginning of the war, the officer in charge of wireless communications on the flagship, Lieutenant Nicholson, invented a first rate and simple plan, which as the years went by was elaborated and perfected more and more. I have not been able to gain any information on the details of its working, but broadly speaking, its main idea was, that the message was to be transmitted from one station to another on shore, with just sufficient power to enable the particular commander at sea, for whom it was intended, to pick it up. Immediately after the call, or sometimes at the beginning of the message itself, certain signals were given indicating the real recipient (usually his military designation signal). In his wireless log an entry would be made both of the transmitting and the receiving station, but at the head of the message there would be a note to the effect, for instance, "For C in C" if the message was intended for the Commander-in-Chief. Mes-

... messages direct from the Admiralty sender were broadcast, giving the name of the recipient.

In critically examining the extracts from the signalling and wireless logs of the Skagerrack battle in the Official Publication issued by the Admiralty ("Battle of Jutland, Official despatches") it is surprising how brilliantly optical signalling was handled in the fleet. All messages relating to mines sighted, merchant ships overhauled, etc., likewise all orders respecting change of course and speed, evolutions and the like, were transmitted optically, often with several repetitions. In this way, for example, optical messages were exchanged between the two cruisers on the extreme wings of the scouting line, at a distance of about 40 nautical miles, whereas the greatest direct distance for searchlight signals was probably not more than 10 nautical miles at the outside. In cases where optical communications could not be established, they rather sent a destroyer than run the risk of wireless telegraphy, in spite of the loss of time occasioned thereby. It is also specially noteworthy, that optical signalling appears to have been more reliable than wireless. Notwithstanding a minute search in the aforesaid extracts from the signalling and wireless logs of the Jutland, I have not been able to discover even a single signal which was incorrectly picked up or which did not reach the man it was intended for; and that is more than can be said for wireless messages. Even such an important signal as Beatty's message to Jellicoe, that the German battle fleet was in sight, is to all intents and purposes unrecognizable in the wireless log of the "Iron Duke", a fact which doubtless led Jellicoe astray at first.

2. THE USE OF WIRELESS TELEGRAPHY

We must not however assume that, because the British imposed great restraint upon their wireless service, they were not able to use it when it was necessary, and when "wireless silence" was no longer essential, i.e. when they were already in touch with the enemy. On the contrary, during the war great advances were made in the use of wireless telegraphy in tactical maneuvers of the battle fleet. Lieutenant Nicholson, already mentioned, in collaboration with several other wireless service officers of the Grand Fleet worked out a practically new plan for the wireless transmission of evolution signals and the like. Since then Jellicoe, according to his own statement, was in 1916 able to handle his fleet in evolutions by wireless with the same or even a greater degree of safety and accuracy as formerly by optical signalling. Jellicoe himself writes on the subject: At the beginning of the war it took 10 to 15 minutes, as a rule, before I could be certain that all ships had received a wireless maneuvering message addressed to the whole battle fleet. In

1916 the time required was seldom more than 2-3 minutes. This great improvement was due to the new method, and also to incessant practice when in port. Yes, the advance we made in the use of wireless telegraphy, was indeed very considerable

As a rule the British used a special low-power installation for sending messages within the confines of the several units of the fleet, the ordinary senders being used for long distances only. Every large ship was therefore, as a rule, provided with at least two complete wireless installations, and very frequently also with a reserve outfit, corresponding to our (i.e. the Swedish Translator) so-called battle wireless outfit. They also used different wave lengths for different purposes with different installations on board in the Grand Fleet, receivers tuned for the reception of messages for each particular purpose. Thus, for instance, the air scouts used one particular wave length, the scouting fleet another, and so on. By this means it was achieved, that the various sections on guard and scout duty never interfered each other in sending their signals and messages, a matter of great importance, especially when getting into touch with the enemy, information of whose approach was generally received from several directions simultaneously. These wireless messages were then passed on with all possible despatch by the recipients to the Commander in Chief by optical signalling.

In order to meet the ever increasing demand for wireless operators, and to keep those already trained in practice and up-to-date, a complete wireless telegraphy school was established at Scapa Flow,

As regards wireless communication with the Colonies and the rest of the world, England never had the slightest difficulty, adhering in this case also to the general principle of giving preference to coded cablegrams for military purposes.

II. THE GERMAN WIRELESS SERVICE ORGANIZATION

It has unfortunately been a very difficult matter for me to obtain a few authentic particulars relative to the organization of the German Wireless Service. This much however is certain, that the Germans in this respect were very much on the leeward side of their opponents, at any rate from the point of view of strategy. That is to be gathered as clearly as one could possibly desire from a remark by Admiral Scheer in his book: "Germany's High Seas Fleet in the world war", published in 1920. He writes there, having established the fact that the British in 1914 had received information in advance of a German advance on the East Coast of England: "The British had obtained this information through their "directional stations", which they had at their disposal even at that time, whereas we did not have

this organization until much later. These are wireless telegraph stations for taking bearings, which are able to designate the direction from which a wireless message picked up has been received, and which can consequently locate the position of the ship on which the sender is. If this is done simultaneously by several stations sufficiently far apart, the point of intersection of the lines of these bearings is the exact position of the ship which has sent the message. The extent of the English East Coast permits of the establishment in favorable positions of these "directional stations". In them the British possessed a considerable advantage in the conduct of the war, as by this means they were able to obtain absolutely exact information of the whereabouts of the enemy, whenever the latter sent out wireless signals of any kind. In the case of a big fleet, the divisions of which are separated from each other and dependent upon intercommunication with each other, absolute "wireless silence" is a very difficult thing to maintain. This statement is remarkable as a German confirmation of the great benefit of these directional stations, after the war many a time and often strongly emphasized by the British themselves.

A. LISTENING-IN TO THE ENEMY ETC.

At the beginning of the war the Germans had no organized listening-in service at all, but they gradually recognized the necessity of collecting at one center all messages picked up by every vessel and station. A decoding station of this kind had been established in Neumunster in 1916, but owing to the great caution of the British it was not of much use. Only by chance did I find out that it was able to give some information to the High Seas Fleet, namely before the Jutland Battle, but even then the message it sent was not particularly definite.

B. DIRECTIONAL STATIONS.

When finally and very late in the day the Germans got their directional stations into working order, they could only in very rare instances be used for taking the bearings of enemy forces or individual ships, thanks to the precautions of the British. Instead of that they were used to send orders for the movements of their own ships and especially airships. That however is a dangerous sport which, as far as we know, was never indulged in by the British. Owing to lack of training and practice on the part of the airships in taking exact observations, the British were nearly always warned in advance of their approach and impending attack, and were able to send up their fighting planes in time, and to prepare themselves in every possible way for the reception of the unbidden guests. In order to find out the position of the attacking airships they frequently did not even have to use their own directional stations, but merely required to

From this fact, and also from the great number of submarines reported off the English naval ports during the last few days it is concluded, that the Germans have some important scheme in view. The Admiralty therefore prepares for the sailing of the Grand Fleet, by notifying the various commanders by coded cablegrams, that the High Seas Fleet is preparing to put out to sea next morning, that is to say on May 31st.

Shortly after 5 Pm. however a wireless message was intercepted, to all intents and purposes an important one, addressed to all chiefs of divisions in the High Seas Fleet. As the signal was in a recently adopted code it could not be deciphered; but as everything pointed to its referring to an order respecting a plan of operation, the good old rule was adhered to: Better a little too soon than to let others steal a march on you.

At 5.40 Pm., that is to say, about half an hour later, Admiral Jellicoe received the following telegram from the Admiralty, which he immediately repeated (as a coded cablegram) to Viceadmiral Beatty: "Assemble eastward of Long Forties ready for all eventualities". Within five hours all divisions of the Grand Fleet were out at sea on the road to the above mentioned rendezvous, which almost coincided with the spot towards which the High Seas Fleet was steering at dawn the next morning (in actual fact the Grand Fleet was making for a meeting place just to the west of Skagerrack.) Wireless silence was ordered as usual and was maintained by both Fleets practically throughout. One of Beatty's wireless stations was to watch the wave length of the advanced scouts, another (together with the airplane mother ship) watched that of the aircraft, and so on.

Some of the ships, according to extracts from the signaling - and wireless logs appear to have been entrusted with the duty of trying to intercept German messages. Whenever anything suspicious was picked up, it was at once reported by optical means to the Commander in Chief, stating the wireless name of the sender and of the recipient, the wave length used and also the approximate strength. Should the scouts see the enemy, the report was to be sent with all the power available, in order to deceive the Germans as to the distance of the British main forces. For the same reason no reply was to be sent to a signal of this kind.

SAILING OF THE HIGH SEAS FLEET AND ORDER

RELATIVE TO WIRELESS.

The sailing of the High seas Fleet from the Jade at day-break on May 31st meant carrying into effect a long cherished plan, which had however to be postponed several times on account of unfavorable weather. As preparatory collaborators a great number of German submarines had been stationed outside British bases of the Fleet, partly for the purpose of being able to attack the Grand Fleet should it put out to sea, and partly so as to be able to report the sailing of the British forces to the German fleet. At 5.30 Am (Greenwich mean time) on May 31st "U 32 "

listen for the reply of the German stations, as soon as they had overheard the message asking for a bearing.

C. HOME ORGANIZATION OF THE WIRELESS
AND INTELLIGENCE SERVICE.

At the outbreak of the war wireless telegraphy was incomparably the most important military means of intelligence in Germany, not only as regards communication with the naval forces and between the latter themselves, but also in a very high degree for the transmission of orders etc. between the various naval authorities on shore. Then, when the Germans began to have a foreboding of the danger of wireless communications at sea, they certainly did try to reduce the practice as far as possible, at the same time using very low power installations for wireless communications when indispensable between the several units of the naval forces. They also appear to have used the closed aerial circuit for short distance signalling. The British listening-in stations on shore were however fitted with such extremely sensitive receivers, that they were apparently able to pick up even the buzzer signals of the Germans, that is to say, to pick up the messages of a few dry batteries at a distance of several hundred nautical miles, which to my mind is almost incredible.

These limitations to wireless intercourse were effected mainly for the purpose of not betraying the position of the ships to the British directional stations. That the British were even in possession of the German system of codes etc. appears to be a fact which the Germans did not grasp until a much later date, or about the beginning of 1916, and that is why wireless conversations in port and between the naval authorities continued quite unconcernedly for a long time.

The German submarines operating in the North Sea gradually learned the wisdom of maintaining almost complete "wireless silence", except of course for specially important messages. The submarines on the west coast of England, on the other hand, felt themselves much safer, and practically every night sent home more or less unnecessary messages, whereby they were many a time located to their own detriment. For the transmission of orders and information to submarines and other vessels, scattered about abroad, the Germans used the high power station at Naun. From there, at certain stated times and on certain wave lengths, known to all German vessels of war, and which they had to look out for as far as possible, such orders and information were sent out as might be necessary at the moment. No answers were to be given when a certain order was only intended for a certain ship.

Communication with the outer world, that is to say, in the early days of the war with the Colonies and the cruisers in foreign waters, likewise throughout the war with the Neutrals, also went by way of Nauen, which was regarded as indispensable by the German Admiralty Staff, above all probably for the submarine war against merchant shipping. It was the foresight of the Admiralty Staff that even provided for the dispatch by Nauen of press news twice in every 24 hours, work which the Germans themselves in view of their isolated blockaded position looked upon as most important, not only for the information of the Neutrals, but also to keep up the courage of the Colonies and ships cut off from home, as long as possible.

III.

EXAMPLES.

I now pass on to attempt, with a few specimen cases taken from different periods of the war, to illustrate what I have already said about the use of wireless telegraphy under various circumstances.

THE "GOEBEN" AND "BRESLAU" .

The power of the wireless messages sent by the German cruisers "GOEBEN" and "BRESLAU" betrayed to the scouting enemy forces the fact, that their prey was in Messina on Aug. 4, 1914, whereupon the Straits of Messina were promptly bottled up. As we know, the Germans nevertheless succeeded in making their escape, but after breaking through the blockade they were discovered by the small British cruiser Gloucester, which stuck to them like a shadow, and merely kept the pursuing forces informed by wireless of their position from time to time. The Germans did nothing to prevent that, and consequently the British ascertained that they were setting a course for the Adriatic and probably for Pola. - Suddenly they swung round to starboard towards the Aegean Sea and at the same time started sending out disturbing wireless waves at a terrific rate, which made it impossible for the Gloucester to signal the sudden change of course in good time. Here we have a concrete example of one of the rare opportunities where interruption of wireless can be of use, namely where it upsets the enemy without interfering with one's own wireless communications.

THE GERMAN EAST ASIATIC SQUADRON

AND OTHERS.

One of the first acts of the British after the outbreak of war was the destruction or seizure of all German telegraph cables and all telegraph stations, wireless included. For the first time we are confronted with absolute "wireless silence", and made to understand what it implies, during Admiral Jerran's expedition against the big German wireless station at Yap, which was of special importance for the maintenance of communications between the Germans and their cruisers in East Asiatic and Australian waters. During this expedition Admiral Jerran was repeatedly called up by wireless by another British Admiral in these waters, but he never replied, because "the undertaking called for absolute wireless silence".

During the first few weeks of the war the only indication that Admiral Count Spee had left Australian waters was the fact, that wireless messages picked up from him became more and more indistinct in Australia. The fact of the German squadron's cruise across towards the American side was in its turn likewise brought to the knowledge of the British solely by a few wireless messages picked up. One of these, picked up by the station at Suva on October 4th, was from the "Scharnhorst", and in all probability intended for one of her colliers. It was in the German secret commercial code, at that time already known to the British, and ran: "Scharnhorst on the road between Marquesas and Easter Island". The other, picked up by another station was in plain language and said: "Attention! Australia and all big English ships have left Rabaul on an easterly course. The Japanese squadron is in the vicinity. Today the British have established wireless connection with Rabaul. Attention!" - Owing to this information, which in view of all circumstances appeared to be quite genuine, the British cruisers made their way over towards the American side.

As a curiosity it should be mentioned that towards the end of November and the beginning of December 1914 the wireless station at La Plata in South America daily picked up calling signals intended for the German Battle cruisers "Seydlitz", "Moltke" and "von der Tann", which were sent out by the neutral wireless station at Montevideo. Rumours began to circulate; that the Germans intended sending out these battle cruisers, in order to strike a blow against enemy trade in the Atlantic, to supply Spee's squadron with fresh ammunition etc., and finally to help him to force a way home.

Although the English knew that the German battle cruisers were still in the North Sea, these rumours undoubtedly contribu-

ed towards their decision to send out their own battle cruisers against Count Spee. That led to the rapid destruction of Spee's squadron, for the sake of which Germany was planning a battle cruiser undertaking, which was bound to have a specially paralyzing effect upon British trade, and would have called for energetic British counter action, which in turn would have weakened the Grand Fleet considerably.

The German so-called pirate cruisers in general very soon learned the wisdom of "silence in the air", so as not to betray themselves by the power of their wireless signals, in the event of enemy craft being anywhere in the vicinity. That this plan was not always successful we have seen in the foregoing examples. In several published statements, both in German and English literature on the world war, one seems to gather the impression, that the British cruisers on the lookout for raiders on merchant shipping - and also some of the latter - were fitted with apparatus, enabling them to determine, at any rate approximately, the direction of a ship from which they were receiving wireless signals. We have an example, among others, during the chase after the "Goeben" and "Breslau" in August 1914, when an entire scouting line changed its course by 180° because "German colliers were distinctly heard sending wireless signals in a northerly direction". - Other examples of the same fact are found in the chase after the "Karlsruhe" and in the story of the "Emden", when she sent one of her colliers in a certain direction, because the signals of a British cruiser had been heard in another direction. As to the explanation, it is difficult to say anything, as these ships, especially the German, can hardly have been fitted with wireless direction finders of any kind.

THE NORTH SEA.

Meanwhile the real naval theater of war had been transferred to the North Sea, and here too it was that wireless telegraphy achieved its greatest triumphs, both from a strategical and tactical point of view. As I said before, the British generally knew beforehand when the German fleet was putting out to sea, partly owing to their well-organized wireless listening-in, but mostly owing to careless use of wireless telegraphy by the Germans.

THE BOMBARDMENT OF SCARBOROUGH AND OTHER PLACES

In the middle of December 1914 five German battle cruisers, accompanied by five small cruisers and three torpedo boat flotillas made an attack on the East Coast of England, and at daybreak on December 16th bombarded several small sea-side towns, including Scarborough. As support on the homeward journey the greater part of the High Seas Fleet put out to sea.

In the forenoon of the day preceding the bombardment Beatty received from the Commander-in-Chief a coded telegram worded as follows: "German squadron, consisting of four battle-cruisers (in reality there were 5 of them) five light cruisers, and 3 flotillas left the Jade this morning at day-break, returning Wednesday night" Then followed detailed orders for several divisions of the Grand Fleet, relative to times of sailing, course, speed, rendezvous etc. and some tactical instructions. A few hours later all were under way. During the night the two enemy fleets passed each other at short range, without either of them being aware of the fact. Absolute wireless silence had been ordered on the German side, and no doubt in the Grand Fleet also, although on this occasion I have not been able to trace any specific order to that effect. - In the wireless log of the small German cruiser "Stralsund" there is an entry under date December 15th. 2, 45 am: English Sander, distance 30 nautical miles.

Determination of distance of such exactitude on the basis of messages received from a transmitter is in reality hardly possible, but in this particular instance was probably correct. However that may be, at any rate the entry shows, that British wireless discipline still left much to be desired. But, in spite of the order forbidding wireless signals, the Germans were no better. Soon after 1 o'clock at night, and a particularly dark night, the German destroyer "S. 33" got out of touch with her companions and began sending wireless signals to the cruiser "Stralsund"; the latter however did not reply until the signal had been repeated four times, when the Commander lost his patience, and signalling with as low power as possible ordered the "S.33" to "shut up". --

On this episode we read in "North Sea" Volume III: "Through these wireless signals "S.33" might easily have endangered the safety of the entire expedition; because, as the chief point was to take the enemy by surprise, the maintenance of strict wireless discipline was of the utmost importance. To nothing but the fact that the enemy evidently was not keeping a sharp lookout do we owe it, that the repeated calls sent out by "S.33" were not noticed by him, and therefore did not draw his attention to the approach of German forces and so induce him to take counter measures in good time. -

A few hours before daybreak on the 16th there were several more or less casual skirmishes between the destroyers of both fleets, which fact was reported to the commanders in chief by wireless. At dawn the same morning German cruisers were discovered to the north-east of the British forces, so Beatty veers off in that direction and puts on more speed. Warrender with the II-battleship squadron followed at a slower gait. At the same time Admiral Ingenohl with the bulk of the High Seas Fleet makes from home, again without knowing the strength of the forces arrayed against him, but worried on account of repeated

reports from his destroyers and cruisers about encounters with enemy destroyer flotillas. The British also had not the faintest idea of the strength of the forces opposed to them, but thought themselves superior in strength, as of course they knew nothing about the German battle fleet being out, but only about the battle cruisers. Beatty had just taken up the chase of the German cruisers sighted, and as a matter of fact had practically the entire High Seas fleet in front of him, when both he and Admiral Warrender were suddenly taken by surprise by a most disquieting wireless message which had been picked up. It was sent by the "Patrol", the ship of the Commander of the Hartlepool flotilla, telling the guardship "Jupiter" on the Tyne, that she was being chased by two enemy battle cruisers. Admiral Warrender turned at once in order to cut off the retreat of the latter, but Beatty wavered. In the first place, the "Patrol" was about 150 nautical miles further westward, whereas he himself was quite close to the enemy, who was towards the East, and then after all it was only a stray message picked up. Within a few minutes, however, he receives a communication from the Admiralty about the bombardment of the Coast towns, and then he at once turns off westward. As we know, the British did not succeed this time in cutting off the retreat of the attacking forces, although they got in touch with their small cruisers and destroyers. That the battle cruisers were able to find their way home without being seen is probably due to the fact, that they noticed by the specially powerful and active British wireless messages, that strong British forces were in their vicinity. To avoid these the Commander of the "Derrflinger" suggested going home by the way of Skagen (as a matter of fact Admiral Hipper made the detour northwards on his own initiative; "Derrflinger's suggestion came much later and did not influence him in anyway. -Transl) It is true nothing came of it, but after all the German's course was laid much more northerly than the British expected.

The British forces learnt of their failure by wireless from the Admiralty at 2.43 pm. The message stated, that the German battle cruiser squadron and the small cruisers were stationed 12 n. miles outside the extreme edge of the British mine-field at 1.15 pm. on a course East by South and at a speed of 23 knots. This information was however not based upon any bearings taken by the directional stations, but solely upon a coded message from the "Seydlitz" to the commander in chief of the fleet, despatched at 1.20 pm., and which according to the wireless log of the German flag-ship, after decoding, ran as follows:

"Seydlitz 1.15 pm 008 B, additional number 5 East by South, 23 nautical miles I B. d. A." From the British communication we see as plainly as anybody could wish for, that the German method of coding and net of squares were not by any means secrets as far as the British were concerned.

About 3 pm. the Admiralty sent another message to the effect, that the German battle fleet was at sea; this information was based upon bearings taken by the directional stations, as also another message on the following day, stating that the German fleet had returned to its home ports again.

It is a noteworthy fact, that in studying the extracts from the wireless logs of the High Seas Fleet during this advance we find, that the order with respect to "Wireless silence" only applied

to the attacking forces themselves, and was not implicitly obeyed even by them. Besides the above-mentioned signals sent out by "G.33", several ship's reckonings were compared on the 15th at 5 pm, and again at 4.34 am, on the 16th. And in the High Seas Fleet there was plenty of lively signalling going on the whole time of the advance, (a mass of reports on drifting mines, fishing-boats overhauled etc.) As notwithstanding all this wireless activity no bearings were taken by the British directional stations, and the listening-in stations did not even notice that the German fleet was at sea until 2 pm on December 16th, we can understand, that their organization and reliability still left much to be desired. I have dealt at such length with this advance against the English Coast, partly because it gives a good insight into the way in which wireless was used in the early days of the war, and partly because, on account of favorable opportunity let slip by the Germans, it is discussed with a special wealth of detail both in English and in German writings.

THE CRUISER BATTLE ON THE DOGGER BANK

IN 1915

Events preceding the cruiser battle on the Dogger Bank on January 24, 1915 developed approximately on the same lines as in the advance on December 16th. This time however the Admiralty despatched the whole Grand Fleet, whereas the Germans kept the battle fleet at home. The preliminary order from the Admiralty to Jellicoe, Beatty and the Chief of the III Battle-ship squadron was a coded cablegram relative to intercepted German wireless messages, and read "Four German battle cruisers, six light cruisers and 22 destroyers will put to sea this evening, to reconnoiter in the direction of the Dogger Bank. Return probably tomorrow evening". Then followed a number of general orders to the various British forces. The order concluded: "After weighing anchor wireless may be used only when enemy in sight, or to reply to the Admiral". The British in fact succeeded very well in preserving "wireless silence". According to German wireless logs, however, the German ships picked up British wireless signals from the Grand Fleet, at first at 3 Am. and then again at 5 Am. on January 24th. The Grand Fleet however seemed to be a long way off, so that the Germans felt themselves secure in their advance, and that they would not meet the Grand Fleet this time.

Towards 6 o'clock in the morning, however, the wireless officer on the light cruiser "Graudenz" reported, that there must be a British destroyer wireless station quite close to the ship. At the same time a ray of light was espied, so that the "Graudenz" made for it at top speed and aimed its searchlight, only however to discover a steam trawler. Whether the wireless signals intercepted came from the latter was not clearly ascertained, but was thought to be quite possible, so that the ships moved ahead.

In the German wireless logs there are no entries of wireless messages between 6.37 Pm. on the 23rd and 5.45 Am. on the 24th of January, but the British assert, that here and there during the night they heard German wireless messages, indicating that

some serious business or other was going on. When the two forces got into touch with each other towards 8 O'clock in the morning, it was a complete surprise for the Germans, whereas the British had reckoned on a meeting precisely at that time.

As soon as the opposing forces sighted each other the wireless operators on both sides started to work with all their might. Reports flew from scouts to battle cruisers, and from the latter to the commanders in chief (in the German case at home port).

From this battle of the signals Hipper gathered, that the whole of the Grand Fleet was out, and therefore he asked by wireless for the High Seas Fleet to put out to sea, and also endeavored to draw the coming inevitable battle as much as possible over into the German bay. His first message to the High Seas Fleet was 2047 (-8.47 Am. according to German regulations), and reported the presence of the British battle cruisers. His next (9.05) ran: "Judging by wireless signals II British squadron in the vicinity". At 10.55 he states his position:

"Urgently require assistance," to which the reply is received 8 minutes later: Main body and flotillas coming as soon as possible.

This information which appears to have been sent in plain language, was picked up by the British battle cruisers, and no doubt greatly contributed towards their abandonment of the pursuit so soon. The British never stopped to think, that "as soon as possible" meant, amongst other things, at least two hours to get up steam. However, that High Seas Fleet did not turn up. The result was, as we know, the sinking of the "Blucher". Nothing else happened of any consequence as regards the subject of wireless, which we are discussing.

THE JUTLAND BATTLE

The next time the two fleets met in conflict was at the Jutland Battle on May 31st and June 1st 1916. As this action has not yet been dealt with in the volumes hitherto published by the Naval Archive, I have had to rest content mainly with British descriptions. These, however, are exceptionally comprehensive for our present purpose, and show as plainly as anyone could desire, that during the long interval great advances had been made on both sides in the handling of wireless telegraphy. The organization of the British wireless service, however, continues to be most distinctly superior to the German.

SAILING OF THE GRAND FLEET WITH ORDERS RELATIVE TO WIRELESS

On the morning of May 30th, thanks to their directional stations, the British noticed that the High Seas Fleet had run out of Wilhelmshaven in the Jade, which shows how sensitive the instruments at the directional stations were by that time.

reported 2 big ships, 2 cruisers and several torpedo-boat destroyers about 70 nautical miles east of the Firth of Forth on a south-easterly course, and an hour later Scheer received a wireless message from the decoding station at Neumunster, that - judging by British wireless activity - two big ships or units with destroyers complete had left Scapa Flow. Shortly afterwards, or at 6.48 Am., (Greenwich mean time) a third report was handed in, this time from "U 66", which had sighted eight enemy battle ships with light cruisers and destroyers on a north-easterly course, 60 nautical miles east of Kinnaird Head.

These messages however as yet supplied no information about the intentions of the enemy. The peculiar combination and the course of the enemy forces spreading in all directions neither indicated cooperation on their part nor intentions against the German Bay. Scheer therefore was of the opinion that the British naval forces reported could not in any way be connected with the German advance. He did not change his plans, but hoped under certain conditions to be able to force some part or other of the enemy fleet into a battle at long odds against them.

When the High Seas Fleet weighed anchor, the wireless name or indicating sign of the flagship was taken over by the Wilhelmshaven station, and that is why the British took this station for the main body of the Fleet? The consequence was, that the British thought the battle fleet was still in the Jade, but clear, ready to sail in support of the battle cruisers.

FIRST FEELING WITH THE ENEMY

As already stated, practically absolute wireless silence was observed in both fleets, so that neither side knew much about the position of the enemy, before the scouting ships in advance got into touch with each other at 2.20 Pm on May 31st. The surprise in all probability was greatest on the German side, as of course the British had set out with the express purpose of dealing with a possible German advance. The first report with reference to the enemy was made to the British Commander in Chief by the light cruiser "Galatea" at 2.20 Pm, followed by several other reports. At 3.10 Pm a communication was received from the Admiralty giving particulars of the positions of a light German cruiser and a destroyer, whose bearings had been taken by the directional stations at 2.30 Pm, that is to say, probably about the time they were reporting to their Commander in Chief, that the enemy was in sight. The fact that this was the first bearing by wireless which the British had been able to take since the High Seas Fleet had put out to sea, demonstrates better than anything else, how well, at that time, the Germans had learnt to preserve wireless silence.

Feeling with the enemy having been established, Beatty sent up an airplane in order to obtain an exact idea of the situation. The wireless messages of the latter (on its own special wave length) at 3.31 and 3.45 Pm. were passed on to the airplane mother-ship, and read by Beatty at the same time, but were not repeated to Jellicoe, who does not appear to have had any installation for the wave

length of the air scouts. On this occasion that was surely of little importance, but later on was the cause of a change.

COMING INTO ACTION OF THE BATTLE FLEET.

For a long time after the battle cruiser fight had started in real earnest the British believed, that the German advance which they had stopped was an ordinary battle cruiser advance, without any real support from the German battle fleet. At 4.38 Pm. however a wireless message was sent by the British light cruiser "Southampton" which, worded as follows, came as a complete surprise for Jellicoe: "Urgent. Precedence. Have sighted enemy battle fleet bearing approximating S E; enemy course N. My position 56° 34' N. Latitude 6° 20' E. Longitude " about five minutes later this signal, (not absolutely verbatim) was repeated by Beatty via "Princess Royal" (Lions wireless apparatus had broken down and was useless), but then got through to the Commander in Chief practically unrecognizable, which at first made Jellicoe hesitate a little. (What "Iron Duke" had picked up was as follows: " 26 -30 battle ships, probably enemy, direction S.S.E. steering S.E.) not more than five minutes later, however, Jellicoe, relying on the first message, sent his first communication to the Admiralty. It was overpowering in its simplicity and read: "Urgent. Battle of the fleet impending." This was sent about 2 hours before the commencement of the main action; it was followed barely ten minutes later - 5 PM - by a communication from the Admiralty giving the position of the German battle fleet, which it had obtained at 4.09 from the directional stations. Even course and speed was stated. In a later similar message at 5.45 corresponding particulars were given for 4.30. One fault in using the bearings taken by the directional stations was, that the bearings of the British were not also taken, consequently the German position given was inexact in relation to the British own ships reckoning, which had been affected by tide and currents after practically 24 hours constant zig-zag sailing. That was probably the real reason why, when the battle fleet came into action, Jellicoe did not find the enemy exactly where he had expected him, and consequently was unable to employ his entire striking force at once, a point which has so often been debated since then, both in and outside professional journals.

It is interesting to note, how the Admiralty, after receiving Jellicoe's first message, immediately made all preparations by cablegram, with reference to previously issued instructions, for the reception of the Grand Fleet after the battle, so that it may be

ready for further fighting as quickly as possible. (Docks, towing, steam tugs, coaling orders etc. are made ready all along the East Coast.)

THE NIGHT AFTER THE MAIN ACTION.

As soon as the forces got in touch with the enemy, wireless telegraphy was released, and during the battle, but especially during the night following, wireless operations were enormous.

men it was a question for both fleets to collect their more or less separated units, mainly by wireless, to gather particulars as to damage sustained, fuel supplies, and so on, and all this had to be done while light forces on both sides were from time to time reporting the enemy in sight, and were making more or less successful torpedo boat attacks. During the dark hours of the night flash-light signalling was practically banned, to prevent the ships giving themselves away.

That in this busy wireless time some of the messages were picked up incorrectly, or even did not reach their addresses at all, is more or less a matter of course, but in certain cases in all probability was of paramount importance in deciding the issue of the action. This, for example, happened in the case of three consecutive messages from "Captain D 12 (Chief of the 12th Destroyer flotilla) who at 1.56 Am on June 1st signalled by wireless to the Commander in Chief: "Urgent. Precedence. Enemy battle ships in sight. My position 10 nautical miles to the rear of I battleship squadron". At 2.08 he signalled: "Urgent. Am attacking" and five minutes later: "Urgent. Enemy course S.S.W." There is not a word about these messages in the wireless log of the "Iron Duke"; on the other hand, portions are to be found in the logs of others which had picked them up.

It is most interesting to note how perfectly, by listening-in and taking bearings through the directional stations, the Admiralty was able to follow up the enemy fleet on its homeward run, and to report its position on other matters to the Grand Fleet. For this reason I append a few extracts from the "Iron Dukes" wireless log, giving messages sent by the Admiralty to the Commander in Chief during the night from May 31st to June 1st.

9.58 Pm. At 9. Pm rear ship of enemy battle forces in $56^{\circ} 33' N.$ Lat. and $5^{\circ} 30' E.$ Longitude on a southerly course.

9.55 Pm on May 31: "Three destroyers/flotillas have received orders to attack you overnight.

10.41 Pm. At 10.41 the Admiralty informed the Commander in Chief, that it was believed the enemy was returning to his base, as his course was S. SE $3/4$ E. and speed 16 knots.

1.48 AM. The Admiralty informed the Commander in Chief, that the enemy submarines were apparently leaving German ports, and that a damaged enemy ship, probably #Lutzow, at midnight was in $56^{\circ} 26' N.$ Latitude and $5^{\circ} 41' E.$ Longitude.

3.12 Am: German light cruiser in $55^{\circ} 45' N.$ Lat. $6^{\circ} 25' E.$ Long damaged. Crew taken off, destroyer standing by 5 Am.

3.20 Am: A communication to the effect, that relief ships are being sent to relieve light cruisers and destroyers who are short of fuel.

3.29 Am. #Urgent. At 2.30 German main body in $55^{\circ} 35' N.$ Latitude $6^{\circ} 50' E.$ Longitude. Course SE by S. 16 knots.

5.30 AM. "Elbing at 3.47 still afloat, without crew. Position at 3 AM. Etc/Etc.

GERMAN ADVANCE ON THE NORWEGIAN
COAST ON APRIL 23/24 .1918.

The advance towards the north upon the Norwegian coast, made by the High Seas Fleet in April 1918, was its last big undertaking before being handed over to the Allies on the conclusion of peace. The object of the advance was an attack upon the British convoys which sailed across the northern part of the North Sea from Stavanger and thereabouts. A necessary condition for its success therefore was, that the British should not have the faintest idea of what was intended, and consequently specially strict orders respecting wireless silence were issued to all Commanders. At 6 AM. on April 23rd the whole High Seas Fleet put out to sea, the battle cruisers, accompanied by some of the light cruisers and torpedo boat destroyers well in advance of the main body, as usual. On the following morning, April 24th, the predetermined turning point on the Norwegian Coast was reached, without any enemy craft having been seen, and everything appeared to be going well, when at 8 AM. the following wireless message from the battle cruiser "Moltke" was received by the Commander in Chief of the High Seas Fleet: "Serious breakdown. Speed is four nautical miles. Position about 40 nautical miles W.S.W. from Stavanger". Two hours previously the "Moltke" had been detached from the battle cruisers for the purpose of joining the battle fleet, as she could not do more than 14 knots. Her wireless to the C. in C. of the High Seas Fleet had not been heard by the battle cruisers, presumably because it was sent from a low power sender. Towards 9 AM. however Vice Admiral Von Hipper on the battle cruisers received another message from the "Moltke", saying that the ship would not answer the helm, and that the C. in C. had received no report on the matter, (the latter statement was based on a misunderstanding). Von Hipper thereupon decided to go himself to the aid of the "Moltke", and reported the fact to the main body, without knowing, that the latter had already been underway for nearly an hour for the purpose of assisting the broken down ship, and that by this time was probably already in sight of her. Von Hipper was therefore ordered to cruise again across the track usually taken by the convoys, but this expedition was just as abortive as the first.

Meanwhile the "Moltke" had been taken in tow by the battleship "Oldenburg", whereupon the whole battle fleet steered for home at a speed of 10 knots. At 6.30 Pm a German submarine sent a message to the effect, that eleven enemy cruisers and battle cruisers were about 80 miles behind the High Seas Fleet and standing on the same course as the latter. These were however in all probability not enemy but Von Hipper's forces on the way home after his last advance, but nobody dared to attempt to establish wireless communication with them, in view of the risk of drawing the attention of the British. Towards 7 O'clock in the

evening of April 25th, that is to say after about 36 hours of towing, the Moltke was able to continue the voyage under her own engine power at 15 knots, but nevertheless about an hour later, 10 miles north of Heligoland, whilst crossing the English submarine lines, was hit by a torpedo which fact, however, did not prevent her making port under her own steam. The German advance had not achieved its object, but it is most remarkable, that the British, although after so much wireless activity they must have heard that the High Seas Fleet was at sea, did not succeed in taking any counter measures, or perhaps, as far as my researches go, they never even tried.

Another noteworthy fact is, that this was probably the sole German expedition of any magnitude of which the British were not signisant in advance.

LIST OF WORDS COMMON TO NAVAL TEXT

Numerals - one, two, three, etc.	Submarine
Speed	Aircraft
Course	Carrier
Latitude	Operation Order
Longitude	At
North	Rendezvous
East	Division
South	Squadron
West	Request
Bearing	Join
Degree	Rejoin
Period	Disposition
Stop	Screen
Aircraft	Flight
Launch	Crash
Attack	Proceed
Bomb	Light
Landing	Heavy
Plane	Report
Battleship	Formation
Destroyer	Contact
Cruiser	