Record taken from WFF's home

# ARMY EXTENSION COURSES

## SUBCOURSE

## ELEMENTARY MILITARY CRYPTOGRAPHY

**1943**

**INTRODUCTION AND LESSON 1**

**Printed by**
**U. S. ARMY SIGNAL CORPS**
**WASHINGTON, D. C.**

WAR DEPARTMENT,
WASHINGTON, MAY 3, 1943.

The following Subcourse, Elementary Military Cryptography, Army Extension Courses, 1943, lessons 1 to 14, inclusive, and examination, is published for the information and guidance of all concerned.

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
*Chief of Staff.*

OFFICIAL:

J. A. ULIO,
*Major General,*
*The Adjutant General.*

# ARMY EXTENSION COURSES

## SUBCOURSE—ELEMENTARY MILITARY CRYPTOGRAPHY

## INTRODUCTION

**Purpose and scope.**

This subcourse is intended to familiarize the student with the means and methods of assuring secrecy in signal communication by the use of codes and ciphers. It is assumed that the student approaches the subject with little or no preliminary information.

The scope of this subcourse is: Codes and ciphers as adjuncts to military signaling; definitions; simple types of ciphers; enciphering and deciphering dispatches; simple code books, encoding and decoding; important precautions to be observed in handling codes, ciphers, and cryptographic paraphernalia.

**Number of lessons and approximate time required.**

This subcourse consists of 14 lessons and an examination and will probably require approximately 31 hours of work by the average student.

The time listed for the subcourse and for each lesson and the examination is only an estimate and should be considered merely as a guide. It does not in any way limit the time that may be devoted to the lesson, examination, or subcourse.

**Texts required.**

Special Text No. 165, Army Extension Courses, Elementary Military Cryptography, 1943.

**Materials required.**

None.

**Special instructions and information.**

This subcourse and the special text used therewith were prepared in the office of the Chief Signal Officer.

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 1 —Preliminary Definitions.
ESTIMATED TIME —1 hour.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Section I.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

12 1. Two messages have been prepared as follows:

*a.* The first message is contained in the following text and is read by considering only the second letter in each word:

STILL AWARD CONTRACT UNLESS MEMBERS SWEAR ABSOLUTE BANKRUPTCY STOP ATTORNEY'S ULTIMATUM SEEMS ACCEPTABLE PROVIDING NUMEROUS LIQUID ASSETS MENTIONED BRING ESTIMATED VALUATION STOP CHECK BANKRUPTCY CLAUSE FIVE IF CANCELLATION EXPECTED.

*b.* The second message is written with secret ink.

In the table below place check marks in appropriate columns opposite all descriptive terms at the left which are applicable.

| | First message | Second message |
|---|---|---|
| Cryptogram..... | | |
| Cryptographic text..... | | |
| Invisible writing..... | ✓ | |
| Secret writing..... | ✓ | |
| Visible writing..... | | |

*Weight*

15 2. Explain the difference between the two terms "decrypting" and "decryptographing."

3. Define the following terms:

5 *a.* General cryptographic system.

5 *b.* Specific key.

4. Captain *A*, who is the communications officer at regimental headquarters, is sending the following message to division headquarters at X:

CASUALTY REPORT FOR YESTERDAY TUESDAY ONE HUNDRED AND FIVE KILLED INCLUDING TWO OFFICERS COMMA THREE HUNDRED AND SEVENTY NINE WOUNDED INCLUDING SEVEN OFFICERS.

He turns it over to *B*, a clerk in the code room, who converts it into a secret message by using an Army code. The secret message is:

NABER ATIFO COPUZ EXIZY OVEKI MUBUC
RILYC YTURA IMOLE BABID ZOVAP RYTIL

The message is now sent by radio to X. At a point between regimental headquarters and division headquarters, *C*, a civilian, has a radio receiver tuned to the Army frequency and intercepts the message and forwards it to a hostile commander.

Meanwhile at the division headquarters at X, a clerk, *D*, reconverts the secret message to its original plain text, and hands it over to *E*, for whom the message was intended.

15 *a.* Name the various processes through which the message passed and the technical term applied to the text after each process.

20 *b.* Using the terminology of this subcourse, what name would you give each of the individuals, *A*, *B*, *C*, *D*, and *E*?

8 *c.* Judging from the above code message, what advantage can you see in the use of code over cipher?

10 5. Would you consider a message written in the ancient Vedic Sanskrit to be in secret language? Why?

6. Define the following terms:

2 *a.* Decipherment.

2 *b.* Encodement.

2 *c.* Enciphered code.

2 *d.* Cryptograph (noun).

2 *e.* Decryptograph.

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 2 —Practical Suggestions and Details.
ESTIMATED TIME —1 hour.
TEXT ASSIGNMENT —Attached Memorandum.
MATERIALS REQUIRED—Cross-section paper (3 sheets) herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

1. Copy the following cryptograms according to the manual system of printing referred to in the attached memorandum. Use the cross-section paper furnished with the lesson, and write each letter or figure as large as possible but completely within each small square. Write in lines containing five groups, leaving one square blank between each group of five letters, two rows of blank squares between successive lines of the same message, and three rows between those of successive messages.

| *Weight* | | |
|---|---|---|
| 10 | *a.* | UIJTV GZVDV AIPPF XYVKI OGRAL |
| | | EAWVM BRGCS HLYOX QEEAZ NFFVT |
| 10 | *b.* | AZRAG FOBRH DAJIX DCHMU HUGIV |
| | | GRIVU TQPBE EBTFZ AMDZY HVIIW |
| 10 | *c.* | FKNPF DKXIN AOANR AZEFB CMDRH |
| | | FMZKJ OUFMM JHFOD FUGEV KQPRI |
| 10 | *d.* | ILFHS JYMJI NOKLY OMTGR VMMPJ |
| | | LYEIZ MNYJA CVNWC GKCRS XQDYX |
| 10 | *e.* | 5Ø392 11861 4 327 761Ø8 55259 |
| | | 89991 427Ø4 662Ø4 37873 43568 |

2. Print out in full, just as you would pronounce them to another operator, the letters in the following groups, using the phonetic alphabet prescribed. Follow this sample of spacing:

ZOPMN = ZEBRA OBOE PETER MIKE NAN

| *Weight* | | |
|---|---|---|
| 2 | *a.* | SPOBW |
| 2 | *b.* | ITVAC |
| 2 | *c.* | DKPZL |
| 2 | *d.* | LNACH |
| 2 | *e.* | FYHII |
| 2 | *f.* | AQJLB |
| 2 | *g.* | KNMNM |
| 2 | *h.* | FESBB |
| 2 | *i.* | TUUVF |
| 2 | *j.* | RPEVL |
| 2 | *k.* | MSNSI |
| 2 | *l.* | EFHOZ |
| 2 | *m.* | AQXOD |
| 2 | *n.* | MRGQW |
| 2 | *o.* | TUTZA |
| 2 | *p.* | NMWWY |
| 2 | *q.* | CDIIM |
| 2 | *r.* | AGQRY |
| 2 | *s.* | KXLGJ |
| 2 | *t.* | SHUXJ |
| 2 | *u.* | KLOYI |
| 2 | *v.* | GNUHL |
| 2 | *w.* | QMZPR |
| 2 | *x.* | EASGD |
| 2 | *y.* | GYZPS |

## ATTACHED MEMORANDUM

Standardization of the details of operation and procedure in cryptographic work is essential if confusion and its consequent loss of time and labor are to be avoided. If a definite method of procedure is adopted and followed consistently, after a time it becomes habitual, and skill and accuracy become second nature. The following suggestions and the exercise accompanying this lesson are for the purpose of pointing out certain details of procedure which will be helpful in all cryptographic work.

Cross-section paper of ¼-inch squares is almost indispensable for good work. Until the student has successfully completed the subcourse, all work sheets should be retained for reference.

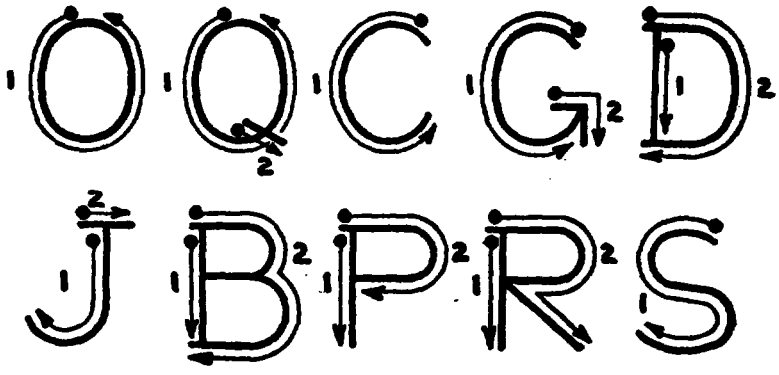
Do not crowd your work on paper. It goes almost without saying that your writing in cryptographic work must be clear and legible. In ordinary writing, if the identity of a letter is doubtful, or if it is actually in error, the correct letter may be supplied from the context; but in cryptograms there is no context to aid in such correction or resolving of doubts, and a single error or questionable letter may lead to serious consequences later on if a cryptogram cannot be decryptographed on account of the presence of errors. A soft lead pencil should be used in order to permit of easy erasure. It will be found that the eraser will be quite necessary. Often colored pencils will be useful to distinguish letters resulting from different stages in the cryptographing process; or a pencil of one color may be used for writing plain-text letters, another of a different color for writing cipher-text letters, and still another for key letters.

It is always advisable to indicate plainly on each work sheet, immediately before writing anything upon it, the problem, exercise, message, etc., to which it applies. This will often save much time that might otherwise be consumed in searching through work sheets many of which will present almost identical appearances.

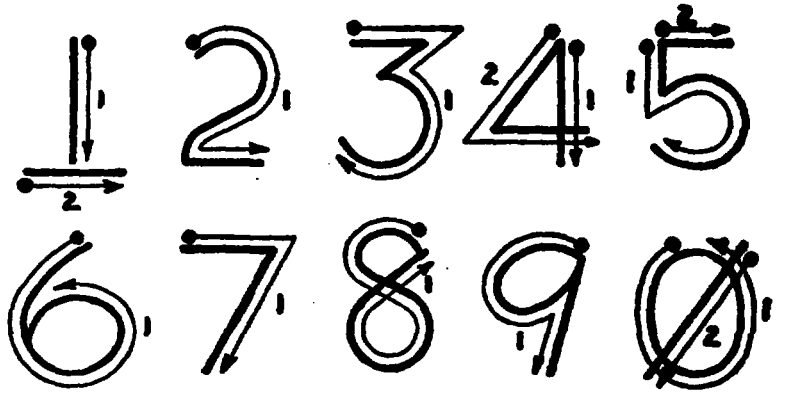
In order to secure legibility, such as in copying cryptograms and in other cases where a printed character better serves the purpose, the following system of manual printing is prescribed. The examples shown below indicate how letters and figures

should be formed and the sequence to be followed in making the various strokes:

The straight-line I is the foundation stroke. The letters Z, X, and K are made slightly smaller at the top. The letters H, E, and



F have the center horizontal strokes slightly above the middle. The letters X, Y, and K have the junction slightly above the middle.



The letters O, Q, C, and G are made in circular form. The letter B is slightly smaller at the top and has the center hori-

zontal part slightly above the middle. The letters R and S are slightly smaller at the top.

The bar under the numeral 1, the top of the 5 and 7, and the bottom of 2 are straight lines. The figure one (1) has a bar under it, slightly below the stem to distinguish it from the letter I, and the cipher (ø) has a bar diagonally through it to distinguish it from the letter O.

In order to insure accuracy in checking results, when two operators are working together and calling off letters or figures to each other, the following pronunciation is prescribed:

*Letters*

| Letter | Pronounced | Letter | Pronounced | Letter | Pronounced |
|---|---|---|---|---|---|
| A | Able | J | Jig | S | Sugar |
| B | Baker | K | King | T | Tare |
| C | Charlie | L | Love | U | Uncle |
| D | Dog | M | Mike | V | Victor |
| E | Easy | N | Nan | W | William |
| F | Fox | O | Oboe | X | X-Ray |
| G | George | P | Peter | Y | Yoke |
| H | How | Q | Queen | Z | Zebra |
| I | Item | R | Roger | | |

*Numerals*

| Numeral | Pronounced | Principal sounds |
|---|---|---|
| 0 | Ze-ro | Long O. |
| 1 | Wun | Strong W and N. |
| 2 | Too | Strong T and long OO. |
| 3 | Th-r-ee | Slightly rolling R and long EE. |
| 4 | Fo-wer | Long O, strong W and final R. |
| 5 | Fi-iv | I changing from long to short, and strong V. |
| 6 | Siks | Strong S and KS. |
| 7 | Sev-ven | Strong S and V, and well-sounded EN. |
| 8 | Ate | Long A and strong T. |
| 9 | Ni-yen | Strong N, long I and well sounded YEN. |

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 3 —Related Information — The Two Classes of Cryptographic Systems.
ESTIMATED TIME —1 hour.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections II and III.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

1. What is meant by the following terms:

2 *a.* Interception.

2 *b.* Radiogoniometry.

10 2. *a.* What are the essential differences between substitution and transposition?

10 *b.* Explain how it is possible to combine both substitution and transposition into a single system.

16 3. Differentiate between a code and a cipher system.

20 4. State briefly the four most important factors upon which the time required for cryptanalysis depends.

10 5. *a.* Give the reasons for the regular grouping of letters or figures in cryptograms.

5 *b.* What size of group is most commonly used?

10 6. As regards the degree of cryptographic security of a system for military use, what is the best that can be expected so far as present methods of cryptography are concerned?

7. An intercept station has been established in the combat zone. Shortly after the station commences operation, an enemy cipher message is obtained.

5 *a.* What arm or service is charged with the establishment of the intercept station?

5 *b.* What arm or service is charged with the solving of the intercepted message?

5 *c.* To what agency is the deciphered message forwarded?

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE — Elementary Military Cryptography.
LESSON 4 — Simple Monoliteral Transposition Methods.
ESTIMATED TIME — 2 hours.
TEXT ASSIGNMENT — Special Text No. 165 (1943), paragraphs 18 to 21, inclusive. Attached Memorandum.
MATERIALS REQUIRED — Cross-section paper (2 sheets) herewith.
MAXIMUM WEIGHT — 100.
SUGGESTIONS

The student should perform the operations involved in cryptographing and decryptographing the examples given in the text. Mere reading may give him an understanding of the methods, but it is essential that he gain experience and facility in the work by actually performing the steps required. *All work sheets employed in cryptographing and decryptographing messages forming part of this and future lessons are parts of the solutions to the exercises. They should be forwarded with the papers.*

EXERCISE

*Weight*

20 1. Encipher the following message according to the method of monoliteral route transposition, using the specific key indicated below. Forward all work sheets. Show the final cryptogram as ready for transmission.

Message:

OUR ADVANCE CONTINUING ALONG A FRONT 15 MILES IN WIDTH

Specific key: Width of rectangle: 10 columns.
Inscription: Route (E) (5) of figure 1 of text.
Transcription: Route (B) (1) of figure 1 of text.
(See attached memorandum for spelling numbers.)

*Weight*

20 2. Decipher the following cryptogram which has been enciphered according to the specific key given below. Show all work and the final plain-text message properly divided into words.

Cryptogram:

RELLI TRARU OYPOU NDEDE NERRU
SSENI LYMOU NDING THECG IEHMO
RFYTI HTSIN THEFO RTDNR AWFOT
SE

Specific key used in *encipherment:*

Width of rectangle: 7 columns.
Inscription: Route (B) (4) of figure 1 of text.
Transcription: Route (D) (2) of figure 1 of text.

20 3. In the specific key given below the route used for the inscription has been omitted. Determine it and decipher the cryptogram. Show all work and the final plain-text message as properly divided into words.

Cryptogram:

NEKCU RBRAS UREEN STRON GACTV
YHEEA STOFS ATJYL MEYBN OIAAE
IHTUO SSOLY SHERH GHTNI TT

Specific key used in *encipherment:*

Width of rectangle: 8 columns.
Transcription: Route (H) (2) of figure 1.

10 4. Is it possible for two different routes used in inscription and transcription to nullify each other, or, in other words, is it possible to read the plain text in normal manner of reading by using a route for transcription different from the one used in inscription? This does not refer to unusual or freak messages. Explain your answer.

20 5. In obtaining the following cryptogram, the route used for transcription was one of the cases listed under (F) of figure 1 of the text. Determine and state which route was used and decipher the cryptogram. Forward all work sheets and show the final plain-text message as properly divided into words.

*Weight*

Cryptogram:

MEARR NEEFO TCNTY VNIES REOSS
KUAEO CFPFB DESNR OACHY TTOET
HSNEC NTODR EURMP NOEGN CI

Specific key used in *encipherment:*

Width of rectangle: 9 columns.
Inscription: Route (A) (3) of figure 1.

6. Are the problems in this lesson termed monoliteral or polyliteral methods? Why?

## ATTACHED MEMORANDUM

In all exercises of this course involving the cryptographing or decryptographing of messages, the student is regarded as being a member of the cryptographic personnel of a message center. This being the case, he cannot be expected to know what ideas were intended to be conveyed by the originator of a message, or what impressions the addressee may obtain from the message; as a cryptographic clerk, he can only be expected to cryptograph every message exactly in the way in which it has been written by the originator and to indicate the plain text of a message exactly as it was decryptographed. The point is that responsibility for proper diction, orthography, and punctuation of a message filed for cryptographing and transmission rests upon the originator of the message and not upon the message center personnel. In actual practice, if a message is obviously ambiguous or in need of correction, the message-center chief can consult with the originator of the message with a view to its improvement; or, if it becomes necessary to modify the wording of a message to facilitate its cryptographing, the modified text can be submitted to the originator for approval before transmission. Similarly, in the case of a decryptographed message, the cryptographic clerk of a message center makes no additions, changes, transformations, or deletions to the decryptographed text; nor does he make any attempt whatever to punctuate the message; he merely gives the text as a simple succession of words, leaving the proper interpretation of the message up to the addressee.

Since in pursuing this course the student will not be in a position to consult with the message-center chief or with the originator or addressee of a message, the following rules are set down for his guidance:

A. In cryptographing—

(1) Cryptograph the plain text of every message to be cryptographed in connection with the exercises exactly as given.

(2) Only such signs of punctuation as appear in the text actually spelled out in words are to be cryptographed; otherwise, even if present as symbols, they are to be disregarded. No attempt should be made at punctuating any message.

(3) Abbreviations appearing in the plain text are to be cryptographed as abbreviations without periods. Examples: Am Tn would be cryptographed as AMTN; Sig Bn as SIGBN; Bn Hq as BNHQ.

(4) Cardinal or ordinal numbers when spelled out in words in the message to be cryptographed are to be cryptographed exactly as spelled.

(5) Cardinal or ordinal numbers when expressed in figures in the message to be cryptographed are to be spelled out in words *digit by digit* (except in cases where the cryptographic system permits of enciphering figures as figures).

Examples:

4=FOUR
10=ONEZERO (and *not* TEN)
40=FOURZERO (and *not* FORTY)
400=FOURZEROZERO (and *not* FOUR HUNDRED)
455=FOURFIVEFIVE
450.7–758.8=FOURFIVEZEROPOINTSEVEN DASHSEVENFIVEEIGHT POINTEIGHT
2005=TWOZEROZEROFIVE
12:01 a. m.=ONETWOZERONEAM
5:15 p. m.=FIVEONEFIVEPM

(6) Ordinal numbers above the ordinal number 10th, when expressed in figures followed by "d" or "th", are to be cryptographed merely as digits spelled out in words, but without adding the "d" or the "th." The omission of the "d" or "th" will cause no confusion or ambiguity. Examples: 3d Bn would be cryptographed as THIRDBN; 7th Pack Tn as SEVENTHPACKTN; 11th Regt. as ONEONEREGT; 403d Am Tn as FOURZEROTHREEAMTN.

B. In decryptographing—

(1) In giving the plain text of a decryptographed message, merely set down the text as a simple succession of words. Make no attempt to punctuate the message if no punctuation appears in the decryptographed text. If punctuation does appear, spelled out in words, let it stand as such; do not transform the words into the ordinary punctuation signs.

(2) If the text contains numbers spelled out in words, let the numbers stand as spelled out; do not transform them into their equivalent cardinal or ordinal forms. But if the text contains numbers expressed as figures (the cryptographic system being such as to make this possible), then the numbers are to be left as indicated in figures.

(3) If abbreviations appear in the text, let them stand as abbreviations; do not write them out in full.

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 5 —Key Words and Numerical Keys.
ESTIMATED TIME —1 hour.
TEXT ASSIGNMENT —Special Text No. 165 (1943), paragraphs 22 to 25, inclusive.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

10 1. The following cryptogram was obtained by first writing the plain-text message in groups of five letters and then reversing the order of letters within each group. Decipher it, showing the final plain-text message as properly divided into words.

Cryptogram: AIREA ITCAL WYTIV DERSA ODECU
OCCAN FOTNU EWDAB REHTA

15 2. The following cryptogram is a rail-fence cipher. Decipher it, showing all work.

GQEOT AROCW LOEAE NULII OWTOR
ADROS HRPRS IFREI LPRTI FLLAS
NIHUL NTOP

10 3. *a.* What is the purpose of using groups of regular length or false words in reversed writing? Which of the two methods is preferable and why?

5 *b.* Why should not such letters as J, K, Q, X, and Z be employed as "fillers" or nulls in cryptographing transposition ciphers?

*Weight*

4. Derive the numerical keys from the following literal keys, using the method illustrated in paragraph 25*b* of the text. If there are two or more words in the key phrase, treat them together as one unit. If necessary, key numbers may go as far up in regular sequence as is necessary in order to treat the last letter of the key phrase.

10 *a.* KENTUCKY DERBY
10 *b.* PHYSICAL QUALIFICATION
10 *c.* UNITED STATES PATENT OFFICE
10 *d.* CHRYSANTHEMUM

20 5. The combat zone is in the vicinity of Philadelphia, Pa. Select two of the following words and phrases suitable for serving as a basis for the cryptographic key:

| | |
|---|---|
| CIRCUMVOLUTION | PREFERENCES |
| EAT DRINK AND BE MERRY | QUAKER CITY |
| | MY WILD IRISH ROSE |
| FIFTEENTH DIVISION | SPRING FEVER |
| PANAMA CANAL | UNITED STATES MINT |

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 6 —Columnar Transposition Methods.
ESTIMATED TIME —2 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections V and VI.
MATERIALS REQUIRED—Cross-section paper herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

20 1. Cryptograph the message given below. Use the key word SCIENCE and the method described in paragraph 26*a* of the text. Add the minimum number of nulls to complete the design.

ENCOUNTERED RED INFANTRY ESTIMATED AT ONE REGIMENT

20 2. Decryptograph the cryptogram given below. It was cryptographed by the method described in paragraph 26*a* of the text with the key word EXPERIMENT. Show all work and the final plain-text message as properly divided into words.

FDLIT ONSAA OINRI NPNIC ABCES
AMTRO DITYT GSOAO OCRHD ICEET
STNPE AAOSN NUKIE ITIFT

30 3. Cryptograph the message given below, using the method described in paragraph 27*a* of the text with the literal key BALTIMORE.

*Weight*

DESPITE TERRIFIC ENEMY ARTILLERY BARRAGE LAST NIGHT WE HAVE MAINTAINED ALL PREVIOUS GAINS

*a.* What is the minimum number of nulls required to make the final group of this message complete? Enter these nulls in the message.

*b.* When should the nulls be added?

4 4. *a.* What is meant by a double transposition cipher?

2 *b.* Why is it employed?

4 5. *a.* What are grilles as used in cryptography?

6 *b.* Why are they unsuitable for military usage?

2 6. *a.* What type of transposition cipher system was used by the Federal Army during the Civil War?

2 *b.* What degree of cryptographic security does such a system offer?

10 7. What are two advantages and three disadvantages of transposition ciphers?

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 7 —Substitution Ciphers in General; Cipher Alphabets.
ESTIMATED TIME —2 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections VII and VIII.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

6 1. State briefly the difference between an enciphering and a deciphering alphabet.

12 2. Classify substitution methods on the basis of the three different kinds of textual units that may be involved.

8 3. What is the significance of the expression: $R_p = B_c$?

10 4. Define the following terms:
*a.* Standard cipher alphabet.
*b.* Mixed cipher alphabet.

12 5. *a.* Reconstruct as much as possible of the *enciphering* alphabet upon which the following decipherment is based:

ENEMY PATRO LSATT EMPTE DRAID
BHBIV STYQU DETYY BISYB OQTWO
SNORT HEAST OFSAA RBRUC KENAN
EHUQY KBTEY UNETT QZQPL MBHTH
DWERE REPUL SED
OCBQB QBSPD EBO

6 *b.* What kind of cipher alphabet was used when the above message was enciphered?

10 *c.* Reconstruct the deciphering alphabet.

6 *d.* What type of substitution is this called?

*Weight*

30 6. Here are six cipher alphabets. Beside each one there is a plain-text word and its equivalent cipher, as produced by the alphabet.

| | | |
|---|---|---|
| *a.* | VETERAN | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | UIVIMHS | WHIQCUXAEMYBRDJKOLNSVTGFPZ |
| *b.* | DIVISION | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | NSFSCSYX | KLMNOPQRSTUVWXYZABCDEFGHIJ |
| *c.* | SATURDAY | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | BANQTKAZ | ASBZHMVCEODJPTIQUNWRGFKLXY |
| *d.* | ADMINISTRATION | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | EOBJYJTDCEDJPY | EIHONAVKJUFWBYPMRCTDLSXZGQ |
| *e.* | DISASTER | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | WRHZHGVI | ZYXWVUTSRQPONMLKJIHGFEDCBA |
| *f.* | SPECIALTY | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | PJOWBNFQX | NEWYORKABCDFGHIJLMPQSTUVXZ |

In the table below, place an X in each square if the descriptive term at the left of the line is applicable.

| | Alphabet | | | | | |
|---|---|---|---|---|---|---|
| | *a* | *b* | *c* | *d* | *e* | *f* |
| Reciprocal | | | | | | |
| Mixed | | | | | | |
| Normal | | | | | | |
| Enciphering | | | | | | |
| Deciphering | | | | | | |
| Reversed standard | | | | | | |
| Direct standard | | | | | | |
| Inverse with respect to itself | | | | | | |

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 8 —Mixed Alphabets; Primary Sequences and Secondary Alphabets.
ESTIMATED TIME —3 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Section IX.
MATERIALS REQUIRED—Cross-section paper (2 sheets) herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

6 1. Name three types of systematically mixed alphabets.

2 2. *a.* What is the chief advantage of random-mixed alphabets?

2 *b.* What is the chief disadvantage?

3 3. *a.* What is meant by "primary sequence"? By "secondary alphabet"?

3 *b.* How many different secondary alphabets may be produced by sliding a basic sequence of 20 elements against itself?

2 4. What is the chief disadvantage of figure ciphers?

2 5. Are cipher alphabets employing signs and symbols suitable for military usage? Why?

5 6. *a.* Derive the key-word mixed sequence based on the literal key:

CULTURE AND INDUSTRY

as explained in paragraph 45*a* of the text.

5 *b.* Show the deciphering alphabet based on the foregoing sequence with $A_p = H_c$.

*Weight*

7. Reconstruct the probable key word or key phrase upon which each of the following alphabets is based:

3 *a.* Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: KMPQUVWXZENGLISHFRCDTOAYBJ

3 *b.* Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: GHJKLQVWXZFIRESTONADUBCMPY

3 *c.* Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: BJICKLMNDOPQAGFRSTEUVWHXYZ

3 *d.* Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: TKROYWENZXVSQPMLJHGFDCAUBI

3 *e.* Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: QHRSNKTMUVJWOPIXYZALBCDEFG

10 8. *a.* Derive, by using the decimation interval 9 and the method described under paragraph 47 of the text, the sequence based upon the key RED SAILS IN THE SUNSET.

5 *b.* Write the mixed alphabet based upon the foregoing sequence, with $A_p=S_c$, arranging the alphabet in the form of an enciphering alphabet. Label each component of the alphabet.

5 *c.* Write the inverse of the cipher alphabet formed under *b* above, labeling the components.

9. Derive by simple columnar transposition the mixed sequences based upon the following words and phrases:

5 *a.* PINEAPPLE JUICE
5 *b.* GONE TO TOWN
5 *c.* DISASTER

10. *a.* Derive by numerical key columnar transposition the mixed sequences based upon the words and phrases:

5 (1) CINCINNATI OHIO
5 (2) OVER THE FENCE
5 (3) CUCKOO CLOCK

5 *b.* Write the mixed alphabets based upon the foregoing sequences arranging them as enciphering alphabets with $A_p=G_c$. Label each component of the alphabet.

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 9 —Monoalphabetic Substitution with Variants.
ESTIMATED TIME —3 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Section X.
MATERIALS REQUIRED—Cross-section paper (2 sheets) herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

15 1. *a.* Using the key word BUSY, construct four alphabets with numerical equivalents according to the method set forth in paragraph 52*b* of text. Consider I and J to be the same letter.

15 *b.* Decryptograph the following message, using the alphabets constructed in *a* above:

| | | | | |
|---|---|---|---|---|
| 5Ø994 | 56312 | Ø47Ø3 | ØØ588 | 23679 |
| Ø8433 | 91599 | 64995 | Ø7135 | 23545 |
| 2844Ø | 87125 | 79781 | 89642 | 82729 |
| 83675 | 5285Ø | 44491 | 16183 | 91782 |
| 2529Ø | | | | |

5 2. In a certain cryptographic system the following letters have the indicated number of variant values: E–5, O–4, P–1, R–3, T–4. In how many ways may the word REPORT be enciphered?

*Weight*

3. Decryptograph the following cryptogram by means of the cipher square shown:

```
CNEJD  NAESJ  HAOEI  WNWOC  EDSTO
WDJIJ  EWCDF  JNJFI  OJFAI  WTBNB
OOITC  TNOCW

       OBJECT
       INWARD

   FO  E5STA1
   AR  B2LI9H
   SC  8MNC3D
   TH  4F6G7J
   EI  ØKOPQR
   ND  UVWXYZ
```

4. Decryptograph the following cryptogram with the key indicated below it. Show all work.

```
4Ø963  28Ø55  16541  51844  81885
Ø1969  36588  98543  98148  84659
1Ø3Ø8  45192  5Ø363  48711  58189
Ø1415  176ØØ
```

Key: Construct a rectangle of 3 by 10 small squares as shown in figure 12 of text and as modified in paragraph 53*a*. Insert the key-word mixed sequence based upon the key phrase CENTRAL AMERICA. Column indicators: Numerical key based on the top line of the rectangle. (Represent 10th column by Ø.) Row indicators: 1–5–8 for first line, 3–4–9 for second line, and 2–6–7 for third line.

5. *a*. Decryptograph the following cryptogram by means of the cipher square shown:

```
GOGIG  IGODO  CIGUF  EFAFA  DOCAC
ECEGE  FIDOG  EGOGI  DEFEB  IGEGO
CEBEX

       UOIEA

   G   WATER
   F   SPNIL
   D   BCDFG
   C   HJKMO
   B   QUVXY-Z
```

*Weight*

5 *b.* What type of system is that used in 5*a*?

5 *c.* How could the simple monoalphabeticity of this system be disguised?

5 *d.* Which letters of the cipher square in *a* above are known as column indicators?

5 *e.* Which letters of the cipher square in *a* above are known as row indicators?

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 10 —Polyalphabetic Substitution Systems.
ESTIMATED TIME —3 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Section XI and paragraph 60.
MATERIALS REQUIRED—Cross-section paper (2 sheets) herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

25 1. Employing the repeating key method with the specific key given below, encipher the following message. Show all work, including the primary sequence, secondary enciphering alphabets, and the enciphering diagram. Show cryptogram in five-letter groups ready for transmission.

UNUSUAL NUMBER OF ENEMY RECONNAISSANCE AIRPLANES ACTIVE OVER OUR LINES APPARENTLY ON PHOTOGRAPHIC MISSIONS

Specific key:

Primary alphabet: Plain component—normal sequence.
Cipher component—key word sequence based upon the key phrase DEPARTMENT OF JUSTICE.

Key word for message: MANUSCRIPT.

5 2. What name is given to the type of substitution used in 1 above?

3. Write the equations which will express the following facts:

5 *a.* The letter M is produced by the encipherment of the plain-text letter C when the key letter used is R.

*Weight*

5 *b.* When the key letter B is used to encipher plain-text letter N, the cipher resultant is the same as when plain-text O is enciphered by the key letter V.

4. Consider the following system of encipherment:

A pair of sliding alphabets are used, their relative positions at the start being prearranged. Three letters are enciphered in the initial position and then the cipher component is moved one letter to the right. In this position three more letters are enciphered after which the cipher component is again moved one letter to the right, etc.

4 *a.* How many cipher alphabets will be produced by the encipherment of a message containing 80 or more letters?

4 *b.* What type of substitution does the above system exemplify?

4 *c.* How does this type of substitution differ from monoalphabetic substitution with variants?

3 5. In the repeating key method of polyalphabetic substitution, what determines the—

*a.* Number,

*b.* Identity, and

*c.* Sequence

of the cipher alphabets employed?

25 6. *a.* Employing the repeating key method described in paragraph 58 of the text and the key word CONTRACT, encipher the following message by means of the obsolete U. S. Army cipher disk (or equivalent sliding strips). Show the enciphering diagram and also the groups of the final text in proper form for transmission.

ENEMY PATROLS RUSHED OUR ADVANCED LINES IN QUEST OF PRISONERS BUT ALL WERE DRIVEN BACK

20 *b.* Decipher the following message by means of the obsolete U. S. Army cipher disk (or equivalent sliding strips), using the key word PENSION. Show the dediphering diagram and the plain-text in words:

YALKT XZNEC SRVFE TJBKO LWWZF
EOVWE APMKV WQIZB KVPEW RIWFC

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 11 —Sliding Alphabets and Square Tables; More Complicated Substitution Methods.
ESTIMATED TIME —3 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections XII and XIII.
MATERIALS REQUIRED—Cross-section paper (2 sheets) herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

4 1. *a.* What are cryptographs, and what is their purpose?
2 *b.* What cryptograph is normally used by the U. S. Army in the field?
6 2. *a.* Why are repeating key systems relatively easy for the cryptanalyst to solve?
6 *b.* What can be done to eliminate this weakness?
4 3. *a.* Define polygraphic substitution.
4 *b.* What is its object?
2 *c.* The Playfair cipher is an example of what type of substitution?
10 4. State five disadvantages common to practically all cipher systems employed for regular, voluminous traffic.
12 5. *a.* Construct the cipher square based on the key phrase GEORGE WASHINGTON UNIVERSITY (similar to figure 23 of text).

*Weight*

20 *b.* Encipher the following message by means of the foregoing table using the key BUCKWHEAT. Consider the top line of the square as containing the plain-text letters; the first column on the left, the key letters.

ENEMY MOTORIZED COLUMNS ADVANCED RAPIDLY AND PUSHING TOO FAR IN FRONT OF THEIR SUPPORTING INFANTRY WERE CUT OFF AND BADLY DEFEATED

10 *c.* Write and properly label the enciphering and deciphering alphabets corresponding to the key letter N, given by the cipher square constructed in *a* above.

20 *d.* Decipher the following cryptogram with the key phrase STOCK EXCHANGE, using the cipher square constructed in *a* above:

DFADL HNWPS CSJFW DFBCS XHIBI
FVVUL OOHDO JBIWQ JRNNS IINKR
ETALW AXBBD YCVOB HGQLO BRQTE
RATHD HXNSH LOGLN NDJWX ZFNTR

## ARMY EXTENSION COURSES

### LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 12 —Code Systems.
ESTIMATED TIME —2 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections XIV and XV.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

1. Two persons, *A* and *B*, knowing that they were soon to separate and live in different parts of the world, prepared two copies of a written document in which were listed about 2,000 common words, syllables, and phrases. Opposite each word the wrote a different four-letter combination. When they separated, *A* took one copy of the document and *B* took the other. One week after their separation, *B* sent the following message to *A*:

EDOG JYKO NYPO USRI MYEK ODGU IVZU FOFA
NONA IZEX ALNE

Using his copy of the previously prepared document, *A* converted the message to the plain text shown below:

| EDOG | JYKO | NYPO | USRI | MYEK | ODGU | IVZU | FOFA | NONA |
|---|---|---|---|---|---|---|---|---|
| LEAVING | SH | AN | GH | AI | FOR | K | 0 | BE |

| IZEX | ALNE |
|---|---|
| DECEMBER | TWENTY– |
| | FIFTH |

*Weight*

5 *a.* What process did *A* use to convert to plain text?

5 *b.* What name is commonly given to the document prepared by *A* and *B*?

5 *c.* How did *B* send words not previously decided upon?

5 *d.* What are the groups, EDOG, JYKO, NYPO, etc., called?

*Weight*

5 2. *a.* What are the primary and secondary purposes of code in commercial communications?

5 *b.* What are the primary and secondary purposes of code in military communications?

5 3. Code A has a vocabulary of 25,000 syllables, words, and phrases. Code B has a vocabulary of 6,000 syllables, words, and phrases. Which of these two codes has the greater condensing power?

6 4. In what three respects do code systems afford more economy than cipher systems?

20 5. In preparing the following six cryptograms, three different code books were employed. Indicate which messages were prepared by the same code book.

| | | | | | |
|---|---|---|---|---|---|
| *a.* | POLUE | NOKEC | HODED | GUIQA | PORIA |
| *b.* | NOKES | KUIQA | IRSLE | FIIKA | XEJCO |
| *c.* | POUVA | IRCLE | HODEC | GOJCO | XDOED |
| *d.* | MOECO | HOSED | POLIA | DIIKA | XDPCD |
| *e.* | PORVE | COPEC | IQDED | XVOED | GIIKA |
| *f.* | IEDEF | PORUE | MOJCO | XDOCD | HOIQA |

12 6. As regards the elements composing code groups, name four types of code groups.

4 7. *a.* What is a permutation table?

3 *b.* What feature is included in scientifically constructed permutation tables that greatly increases the reliability of code as a system of communication?

20 8. What type of two-letter difference do the following pairs of code groups show, identity or position?

| | | | |
|---|---|---|---|
| *a.* | BUEPZ | and | ZUEPB |
| *b.* | LEKZI | and | LKEZI |
| *c.* | RTOGU | and | CTONU |
| *d.* | EOTYA | and | EOTAY |
| *e.* | MOKBN | and | NBKOM |
| *f.* | LEMZI | and | LUMZJ |
| *g.* | PUDEM | and | PEDUM |
| *h.* | DOJZM | and | ODJZM |
| *i.* | MYPQL | and | MKPQR |
| *j.* | KAPOT | and | KAMOJ |

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 13 —One-Part and Two-Part Codes; Enciphered Code; Comparison of Code and Cipher Systems.
ESTIMATED TIME —2 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections XVI to XVIII, inclusive.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

4 1. *a.* What is the difference between a caption code and a strictly alphabetical code?

2 *b.* Give one advantage and one disadvantage of a caption code.

15 2. What two elements must every good cipher system combine? On which of them must the secrecy of a military cipher depend? Why?

14 3. The following are extracts from two different codes. In the table below place check marks in each square opposite all descriptive terms at the left which are applicable.

| Code A | | Code B | |
|---|---|---|---|
| Enemy | GAKAL | Division | NIHCO |
| Enemy airplane | GAKCA | Hostile division | EPYQE |
| Enemy artillery | GAKGE | Reinforcements for division | ATUDD |
| Enemy attack | GAKIG | Delay division attack | HYAGL |
| Enemy barrage | GAKKI | Reserve division | EPUEV |
| Enemy being reinforced | GAKOY | Division headquarters | ZAJDU |
| Enemy cavalry | GAKRO | Our division will | UQZFO |
| Enemy field artillery | GAKUR | Division command post | OYIFT |
| Enemy firing | GAKXU | Division attack | REBWU |
| Enemy ground station | GAKYV | Division has been sent | CULUB |
| Enemy has broken through | GALAK | Division reserves | BEFYW |
| Enemy heavy artillery | GALDA | Division casualties | JIWOR |
| Enemy infantry | GALFE | | |

| | Code A | Code B |
|---|---|---|
| Caption code | | |
| Decoding section | | |
| Encoding section | | |
| One-part code | | |
| Two-part code | | |
| Strictly alphabetical code | | |

*Weight*

10 4. *a.* Differentiate between the additive method of encipherment and the subtractive method of encipherment.

5 *b.* Can additive and subtractive methods be combined? How?

10 5. *a.* Name two types of code with reference to the arrangements of their contents and define briefly each type.

5 *b.* Compare the two types with regard to economy, secrecy, and accuracy.

15 6. Encipher the following code message upon the letter-transposition principle explained in paragraph 77*b* of the text, using the numerical key derived from the word BROWN:

QYLED TEAZL NGOKI XALDA BEPUX OXQAV

20 7. Name and briefly discuss the principal factors to be taken into consideration in comparing code and cipher methods as systems of secret communication.

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
LESSON 14 —Corrections of Errors; Fundamental Rules for Safeguarding Cryptograms.
ESTIMATED TIME —2 hours.
TEXT ASSIGNMENT —Special Text No. 165 (1943), Sections XIX and XX.
MATERIALS REQUIRED—None.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

10 1. The 1st Division has just issued a new code. The 1st Infantry message center cryptographs a message in the new code and has it transmitted by radio to the 4th Infantry (also 1st Division). Through some error, the 4th Infantry has not received copies of the new code and is unable to read the message received from the 1st Infantry. The message center, 1st Infantry, is notified by radio message in the old code. The message is important and must not be delayed. What action should the message center chief, 1st Infantry, take?

10 2. If the final group of a cryptogram is not a complete group, it is advisable to make it so by adding the necessary number of nulls. When should these nulls be added? Why?

10 3. *a.* What are the principal sources of error in cryptographic communications?

15 *b.* How can errors in cryptographic communication be reduced to a minimum?

*Weight*

30 4. In the following list there appear groups as they were received by radio and as they were corrected. Study the errors and indicate their probable sources, whether made in telegraphing, cryptographing, or copying. Place in parentheses a brief explanation of how you think the error occurred.

| | Group as received | Correct group |
|---|---|---|
| *a.* | ENABDE | ENABB |
| *b.* | UIKUK | FEKUK |
| *c.* | MESNY | MEHNY |
| *d.* | TRUCK | TRUAK |
| *e.* | FELT | INELT |
| *f.* | DYONC | DYOKR |
| *g.* | SOOTH | SODTH |
| *h.* | OCNES | OCMES |
| *i.* | GEFMI | GEMFI |
| *j.* | NEGRO | NEGEO |
| *k.* | MLARU | MALRU |
| *l.* | PWTOA | PAMOA |
| *m.* | EBROV | EBRVO |
| *n.* | OCUZW | OGUZW |
| *o.* | ITRAW | ITREY |

25 5. Summarize the fundamental rules for safeguarding cryptograms.

# ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE —Elementary Military Cryptography.
EXAMINATION
ESTIMATED TIME —3 hours.
TEXT ASSIGNMENT —Any text previously used.
MATERIALS REQUIRED—Cross-section paper herewith.
MAXIMUM WEIGHT —100.
SUGGESTIONS —None.
EXERCISE

*Weight*

10 1. Name and state the differences between the two principal classes of cipher systems.

9 2. Two cryptographic clerks, *A* and *B*, are encoding messages, but they are using different codes. In the code book *A* is using, the same portion of the code book is used for both the encoding and decoding processes. In the code book *B* is using, the encoding and decoding processes are performed in different portions of the book.

*a*. What type of code is *A* using?
*b*. What type of code is *B* using?
*c*. Which type of code has the greater security?

15 3. Employing the method given in paragraph 28, Special Text No. 165, and the key word CATFISH, cryptograph the following message prepared for transmission, showing all work.

ENEMY RAIDERS OVER NORTH SEA WILL BE MET BY FAST FIGHTING PLANES

4 4. Why should not such letters as J, K, Q, X, and Z be employed as nulls in cryptographing transposition ciphers?

*Weight*

12 5. State three different ways or methods of employing a key in polyalphabetic substitution so that periodicity or cyclic phenomena are not exhibited by the cryptograms.

20 6. *a.* Cryptograph the two messages given below, using the methods described in paragraphs 27*a* and 26*a*, Special Text No. 165, respectively. Use the key word WASHINGTON for both messages. Show all work.

(1) SLIGHT SKIRMISHES WITH ENEMY TODAY IN LORRAINE SECTOR BETWEEN MOSELLE AND SAAR RIVERS

(2) ANTIAIRCRAFT BATTERIES AT NANCY SHOT DOWN TWO ENEMY PLANES

5 *b.* Which of the two resulting cryptograms has the higher degree of cryptographic security?

3 7. What is a permutation table? What else is it sometimes called?

3 8. Define radiogoniometry.

4 9. What is the difference between an enciphering alphabet and a deciphering alphabet?

15 10. Decipher the following cryptogram with the key indicated below it. Show all work.

Key:

Construct a square 5 by 5 (25 cells). Insert the key word mixed sequence (I=J) based upon the key word VEGETABLE.

Column indicators: WHITE
Row indicators: BREAD

BHDIB TBHEE AEEHB WBHAT BHRIA WEEEE BEEHA
EAEBE EERIB HAEAW REBHE EBHET DTBEB HATAW
RTATA WETBH AEBTA WRTBE DTAEB TAWAH ETBEE
EDTAH EWAWB TAWBI ATBEA HEWAE BTBEE IBHEE