Record taken from WFF's home

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 1 —Preliminary Definitions.

Weight		First message	Second message
12	1. Cryptogram	X	
	Cryptographic text	X	
	Invisible writing		X
	Secret writing	X	X
	Visible writing	X	

15 2. To decrypt is to reconvert the secret text of a cryptogram into its equivalent plain text by means of cryptanalysis.

To decryptograph is to reconvert the secret text of a cryptogram into its equivalent plain text by a direct reversal of the cryptographing process.

5 3. *a.* The general cryptographic system is the sum total of all the basic, invariable rules to be followed in cryptographing a message according to a given method, together with all the agreements, conventions, or private understandings drawn up between the correspondents or their authorized agents, or furnished them by higher authority.

5 *b.* The specific key is an element, usually variable and easily changeable, which controls or directs the details of the steps to be followed in cryptographing a message. It may consist of a single letter, a number, a word, a phrase, a sentence, a set of specially prepared tables, a special document, or it may even be a book.

Weight

15 4. *a.* *A* wrote the message in plain language; the text of the message is therefore plain text.

B encoded the message, after which he had an encodement of the plain text or a code message.

D decoded the code message, after which the message was again in plain language.

20 *b.* *A*—originator. *D*—decoder.
B—encoder. *E*—addressee.
C—enemy.

8 *c.* Codes are more economical since they tend to condense the message, that is, one code word may represent two or more plain text words.

10 5. No. The Vedic Sanskrit conveys an intelligible meaning in the ancient Hindu language.

2 6. *a.* Decipherment is the decryptographing process applicable to ciphers.

2 *b.* Encodement is the cryptographic process applicable to codes.

2 *c.* Enciphered code is the cryptogram resulting from the encipherment of a code message.

2 *d.* A cryptograph is a mechanical (usually hand-operated) device or instrument employed in cryptographing or decryptographing.

2 *e.* To decryptograph is to reconvert a cryptogram into the equivalent plain-text message by a direct reversal of the cryptographing process.

30 April 1959

Paul S. Willard
Colonel, AGC
Adjutant General

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 2 —Practical Suggestions and Details.

Weight	
50	1. Note whether each letter and figure is made carefully and accurately as prescribed and whether the grouping required has been followed. Grade also on the general neatness of the work, and on whether it precludes all possibility of ambiguity in any letter or figure.
2	2. *a.* SUGAR PETER OBOE BAKER WILLIAM
2	*b.* ITEM TARE VICTOR ABLE CHARLIE
2	*c.* DOG KING PETER ZEBRA LOVE
2	*d.* LOVE NAN ABLE CHARLIE HOW
2	*e.* FOX YOKE HOW ITEM ITEM
2	*f.* ABLE QUEEN JIG LOVE BAKER
2	*g.* KING NAN MIKE NAN MIKE
2	*h.* FOX EASY SUGAR BAKER BAKER
2	*i.* TARE UNCLE UNCLE VICTOR FOX
2	*j.* ROGER PETER EASY VICTOR LOVE
2	*k.* MIKE SUGAR NAN SUGAR ITEM
2	*l.* EASY FOX HOW OBOE ZEBRA
2	*m.* ABLE QUEEN X-RAY OBOE DOG
2	*n.* MIKE ROGER GEORGE QUEEN WILLIAM
2	*o.* TARE UNCLE TARE ZEBRA ABLE
2	*p.* NAN MIKE WILLIAM WILLIAM YOKE
2	*q.* CHARLIE DOG ITEM ITEM MIKE
2	*r.* ABLE GEQRGE QUEEN ROGER YOKE
2	*s.* KING X-RAY LOVE GEORGE JIG
2	*t.* SUGAR HOW UNCLE X-RAY JIG
2	*u.* KING LOVE OBOE YOKE ITEM
2	*v.* GEORGE NAN UNCLE HOW LOVE
2	*w.* QUEEN MIKE ZEBRA PETER ROGER
2	*x.* EASY ABLE SUGAR GEORGE DOG
2	*y.* GEORGE YOKE ZEBRA PETER SUGAR

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 3 —Related Information — The Two Classes of Cryptographic Systems.

Weight

2 1. *a.* The act of listening-in and copying or recording electrically transmitted communications by persons other than the correspondents or their authorized agents.

2 *b.* The science which deals with the means and methods of locating a radio transmitting station by taking bearings on the waves emitted by the station.

10 2. *a.* In transposition the elements, or units of the plain text retain their original identities, merely undergoing a change in their relative positions; in substitution, the elements of the plain text retain their original positions but are replaced by other elements with different values or meanings.

10 *b.* First, cryptograph a message by a substitution method and then apply a transposition method to the substitution text, or vice versa.

16 3. Whenever in a single system the general system is such that the cryptographic treatment is as a general rule applied to textual units of regular length, usually single letters or pairs, and is only exceptionally applied to textual units of irregular length, the system is designated a cipher system. In a code system, the general method is such that the cryptographic treatment is as a general rule applied to textual units of irregular length, usually whole words, phrases, and sentences, and is only exceptionally applied to single letters, pairs, or groups of letters.

Weight

20 4. *a.* The degree of cryptographic security inherent in the system itself.

b. The amount or volume of text available for study.

c. The number, skill, and efficiency of organization and cooperation of the cryptanalytic personnel.

d. The amount and character of collateral intelligence available to the cryptanalysts.

10 5. *a.* (1) To promote accuracy in telegraphic transmission.

(2) To make cryptanalysis more difficult.

5 *b.* Five-character groups.

10 6. The best that can be expected is that the degree of security should be great enough to delay solution by the enemy for such a length of time that when the solution is finally accomplished the information thus obtained has lost its immediate value.

5 7. *a.* Signal Corps.

5 *b.* Signal Corps.

5 *c.* G–2 Division of the General Staff of the headquarters served by the intercept station and cryptanalytic section.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 4 —Simple Monoliteral Transposition Methods.

Weight

20 1. Design: ORVEIGGNFI
UDCTNNOEMI
ANNIORNESI
AOULFOVEWT
CNAATILNDH

Cryptogram:

OUAAC RDNON VCNUA ETILA INOFT
GNROI GONVL NEEEN FMSWD IIITH

20 2. Design: TRGCRER
DOIERNE
NFEHUEL
REHTSDL
AHMGSEI
WTONEDT
FNRINNR
OIFDIUA
TSYNLOR
STTUYPU
EHIOMYO

Plain-text message:

OUR ARTILLERY POUNDED ENEMY LINES SURROUNDING THE CITY FROM HEIGHTS IN THE FOREST OF WARNDT

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Weight

3. Design: RBRUCKEN
AASFOTSA
STSOUTHE
UJSTHGIE
RYONTHEH
ELLITRAY
EMYSHEAV
NEYBNOIT
STRONGAC

Inscription: Route (C) (3) of figure 1.
Plain-text message:
STRONG ACTION BY ENEMYS HEAVY ARTILLERY ON THE HEIGHTS JUST SOUTHEAST OF SAARBRUCKEN

4. No. In order for a transcription route to nullify an inscription route, the letters have to be inscribed and transcribed in the same order throughout the message, that is, the same route must be followed in inscription and transcription.

5. Design: INGRUSHED
CEMENTSBE
OPREENFOR
NDCORPSST
ONTOFSECO
TTACKINFR
YCOUNTERA
HEAVYENEM

Transcription: Route (F) (8) of figure 1.
Plain-text message:
HEAVY ENEMY COUNTERATTACK IN FRONT OF SECOND CORPS STOP REENFORCEMENTS BEING RUSHED

6. Monoliteral, as the transposition method deals with individual letters.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 5 —Key Words and Numerical Keys.

Weight

10 1. Plain-text message:
AERIAL ACTIVITY WAS REDUCED ON ACCOUNT OF BAD WEATHER

15 2. Plain-text message:
GHQ REPORTS AIR FORCE WILL OPERATE IN FULL LIAISON WITH OUR LAND TROOPS

10 3. *a.* Both have the same purpose of disguising the original word lengths. Groups of regular length have an additional purpose of promoting accuracy in transmission.

5 *b.* Because such letters are infrequent in plain English and, if found in a transposition cipher, offer clues to its solution.

10 4. *a.* K E N T U C K Y D E R B Y
6–4–8–10–11–2–7–12–3–5–9–1–13

10 *b.* P H Y S I C A L Q U A L I F I
16–7–21–18–8–4–1–12–17–20–2–13–9–6–10–
C A T I O N
5–3–19–11–15–14

10 *c.* U N I T E D S T A T E S P A T
24–13–11–19–5–4–17–20–1–21–6–18–16–2–22
E N T O F F I C E
7–14–23–15–9–10–12–3–8

10 *d.* C H R Y S A N T H E M U M
2–4–9–13–10–1–8–11–5–3–6–12–7

20 5. Any two of the following:
EAT DRINK AND BE MERRY
MY WILD IRISH ROSE
SPRING FEVER

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 6 —Columnar Transposition Methods.

Weight

20 1. Rectangle:

Key word: S C I E N C E
Derived numerical key: 7–1–5–3–6–2–4

E N C O U N T
E R E D R E D
I N F A N T R
Y E S T I M A
T E D A T O N
E R E G I M E
N T D N T R E

Note.—The underlined letters are nulls and may be any medium or high frequency letters, such as E T R I N O A S D L C H F U P M.

Cryptogram:

NRNEE RTNET MOMRO DATAG NTDRA
NEECE FSDED URNIT ITEEI YTEN

20 2. Rectangle:

Key word: E X P E R I M E N T
Derived numerical key: 1–10–7–2–8–4–5–3–6–9

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

Message:

FIRST BRIGADE HAS CONSOLIDATED POSITIONS IN ANTICIPATION OF ENEMY COUNTERATTACK

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Solutions
Elementary Military Cryptography, 6–p. 1
1943

Weight

30 3. Rectangle:

Key word: B A L T I M O R E
Derived numerical key: 2–1–5–9–4–6–7–8–3

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

Note.—R, L, and D are nulls.

Cryptogram:

ERYYA ETPAD RMRLW NLGEE EETIL
SIITR NVNVS SIABS HARIT CIRIE
EIREE LAGMD OLTNL GHAAU DPFRA
TAIEN

a. Three.

b. Before transcription.

4 4. *a.* Double transposition is the application of two transpositions in the cryptographing of a message. The cipher text produced by a first transposition is transposed as though it constituted plain text.

2 *b.* It is employed in order to increase the degree of cryptographic security.

4 5. *a.* Devices containing perforations in definite but irregular positions, used in enciphering messages on transposition principles.

6 *b.* (1) The necessity for carrying a device on the person.

(2) The many agreements and understandings necessary for their successful operation.

(3) The difficulties connected with their preparation and distribution.

2 6. *a.* Word transposition.

2 *b.* Not very great.

10 7. *a.* Advantages:

(1) Speed of operation.

(2) Simplicity of operation.

b. Disadvantages:

(1) Transposition systems are of such a nature as not to allow any latitude for the occurrence of errors in handling. Thus, telegraphic errors may often render messages impossible of solution.

(2) If two or more messages of identical length are available for study, no matter how complicated the method, the cryptograms may be solved and the key recovered and applied to other cryptograms of any length whatever in the same key.

(3) In the case of double transpositions, a poorly trained or careless clerk will fail to perform both steps correctly. This lays not only his own messages but also hundreds of others correctly prepared by other clerks open to easy solution.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 7 —Substitution Ciphers in General; Cipher Alphabets.

Weight

6 1. An enciphering alphabet is one in which the sequence of letters in the plain component coincides with the normal sequence, while a deciphering alphabet is one in which the sequence of letters in the cipher component coincides with the normal sequence.

12 2. Letter methods, syllable methods, and word methods.

8 3. The letter R of the plain text, or of the plain component of the cipher alphabet, is represented by the letter B of the cipher text, or of the cipher component of the cipher alphabet.

10 4. *a.* An alphabet in which the sequence of letters in the cipher component is the same as the normal, but (a) merely reversed in direction or (b) shifted from its normal point of coincidence with the plain component.

b. An alphabet in which the sequence of letters or characters in the cipher component is no longer the same as the normal in its entirety.

12 5. *a.* Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: TZLOBN KW MDIHUS QEYP C V

6 *b.* Mixed cipher alphabet.

10 *c.* Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: EWLS NM HCKFDUR PAOYI TB

6 *d.* Monoalphabetic substitution.

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Weight

30 6. Table should be as follows:

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

Solutions
Elementary Military Cryptography, 7–p. 2
1943

SC1035-G

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 8 —Mixed Alphabets; Primary Sequences and Secondary Alphabets.

Weight

6 1. Key-word mixed alphabets.
Transposition-mixed alphabets.
Alphabets produced by the decimation method.

2 2. *a.* Random-mixed alphabets give more cryptographic security than do the various less complicated types of systematically mixed alphabets because they afford no clues with regard to the positions of any letters, given the position of a few of them, as is the case with the latter type.

2 *b.* They must be reduced to writing since they cannot be easily remembered, nor can they be reproduced at will from an easily remembered word.

3 3. *a.* A primary sequence is a basic series of *n* different letters which, when juxtaposed and slid against a second primary sequence that may be the same as the first or different from it, can be used to produce a set of *n* derived alphabets, each giving different equivalents for the letters of the normal alphabet. Each of the alphabets so derived constitutes a secondary alphabet.

3 *b.* 20.

2 4. They require combinations of two or more digits in order to provide an equivalent for each letter of the plain component, thus making the cipher text at least twice as long as the plain text.

Weight

2 5. No. They can neither be telegraphed nor telephoned with any degree of accuracy, speed, or facility.

5 6. *a.* CULTREANDISYBFGHJKMOPQVWXZ

5 *b.* Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: RXLTQYZAUBCNDSEFGPVOMHIJWK

3 7. *a.* ENGLISH FRENCH DICTIONARY

3 *b.* FIRESTONE TIRE AND RUBBER COMPANY

3 *c.* MADISON WISCONSIN

3 *d.* NEW YORK TRIBUNE

3 *e.* BOOK OF THE MONTH

10 8. *a.* Key-word sequence:
REDSAILNTHUBCFGJKMOPQVWXYZ

Decimated alphabet:

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

Mixed sequence: TMRUQAJEFZGSPHDWOKVYNILXBC

5 *b.* Enciphering alphabet:
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: SPHDWOKVYNILXBCTMRUQAJEFZG

5 *c.* Deciphering alphabet:
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: UNODWXZCKVGLQJFBTRAPSHEMIY

5 9. *a.* PINEALJUC
BDFGHKMOQ
RSTVWXYZ

PBRIDSNFTEGVAHWLKXJMYUOZCQ

5 *b.* GONETW
ABCDFH
IJKLMP
QRSUVX
YZ

GAIQYOBJRZNCKSEDLUTFMVWHPX

5 *c.* DISATER
BCFGHJK
LMNOPQU
VWXYZ

DBLVICMWSFNXAGOYTHPZEJQRKU

Solutions
Elementary Military Cryptography, 8–p. 2
1943

Weight

10. *a.* (1) 2451763
CINATOH
BDEFGJK
LMPQRSU
VWXYZ

AFQYCBLVHKUIDMWNEPXOJSTGRZ

(2) 692784351
OVERTHFNC
ABDGIJKLM
PQSUWXYZ

CMEDSFKYHJXNLZOAPRGUTIWVBQ

(3) 15243
CUKOL
ABDEF
GHIJM
NPQRS
TVWXY
Z

CAGNTZKDIQWLFMSYOEJRXUBHPV

b. (1) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: GRZAFQYCBLVHKUIDMWNEPXOJST
(2) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: GUTIWVBQCMEDSFKYHJXNLZOAPR
(3) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: GNTZKDIQWLFMSYOEJRXUBHPVCA

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 9 —Monoalphabetic Substitution with Variants.

Weight						
15	1. *a.*	A—25	32	59	78
		B—01	33	60	79
		C—02	34	61	80
		D—03	35	62	81
		E—04	36	63	82
		F—05	37	64	83
		G—06	38	65	84
		H—07	39	66	85
		I–J—08	40	67	86
		K—09	41	68	87
		L—10	42	69	88
		M—11	43	70	89
		N—12	44	71	90
		O—13	45	72	91
		P—14	46	73	92
		Q—15	47	74	93
		R—16	48	75	94
		S—17	49	51	95
		T—18	50	52	96
		U—19	26	53	97
		V—20	27	54	98
		W—21	28	55	99
		X—22	29	56	00
		Y—23	30	57	76
		Z—24	31	58	77

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Weight

b. Decipherment:

50	99	45	63	12	04	70	30	05	88	23	67	90
T	W	0	E	N	E	M	Y	F	L	Y	I	N
84	33	91	59	96	49	95	07	13	52	35	45	28
G	B	0	A	T	S	S	H	0	T	D	0	W
44	08	71	25	79	78	18	96	42	82	72	98	36
N	I	N	A	B	A	T	T	L	E	0	V	E
75	52	85	04	44	91	16	18	39	17	82	25	29
R	T	H	E	N	0	R	T	H	S	E	A	X

Plain-text message:

TWO ENEMY FLYING BOATS SHOT DOWN IN A BATTLE OVER THE NORTH SEA

2. 720.

3. Decipherment:

CN	EJ	DN	AE	SJ	HA	OE	IW	NW	OC	ED	ST	OW
M	0	V	I	N	G	T	0	W	A	R	D	S
DJ	IJ	EW	CD	FJ	NJ	FI	OJ	FA	IW	TB		
W	0	0	D	S	W	E	S	T	0	F		
NB	00	IT	CT	NO	CW							
V	E	R	D	U	N							

Plain-text message:

MOVING TOWARDS WOODS WEST OF VERDUN

4. Alphabet square:

	3–4–8–Ø–9–1–6–7–5–2
1–5–8	C E N T R A L M I B
3–4–9	D F G H J K 0 P Q S
2–6–7	U V W X Y Z

Decipherment:

4Ø	96	32	8Ø	55	16	54	15	18	44	81	88	5Ø
H	0	S	T	I	L	E	I	N	F	A	N	T
19	69	36	58	89	85	43	98	14	88	46	59	1Ø
R	Y	0	N	R	I	D	G	E	N	0	R	T
3Ø	84	51	92	5Ø	36	34	87	11	58	18	9Ø	14
H	E	A	S	T	0	F	M	A	N	N	H	E
15	17	6Ø	Ø									
I	M	X										

Solutions
Elementary Military Cryptography, 9–p. 2
1943

Weight

Plain-text message:

HOSTILE INFANTRY ON RIDGE NORTHEAST OF MANNHEIM

5. *a.* Decipherment:

GO GI GI GO DO CI GU FE FA FA DO CA CE
A T T A C K W I L L C O M
CE GE FI DO GE GO GI DE FE BI GE GO CE
M E N C E A T F I V E A M
BE X
X

Plain-text message:

ATTACK WILL COMMENCE AT FIVE A M

5 *b.* False code, or pseudo-code system.

5 *c.* By use of variants.

5 *d.* U, O, I, E, and A.

5 *e.* G, F, D, C, and B.

Solutions
Elementary Military Cryptography, 9–p. 3
1943

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 10 —Polyalphabetic Substitution Systems.

Weight

25 1. Primary sequence:

DEPARTMNOFJUSICBGHKLQVWXYZ

Secondary enciphering alphabets:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
(1) MNOFJUSICBGHKLQVWXYZDEPART
(2) ARTMNOFJUSICBGHKLQVWXYZDEP
(3) NOFJUSICBGHKLQVWXYZDEPARTM
(4) USICBGHKLQVWXYZDEPARTMNOFJ
(5) SICBGHKLQVWXYZDEPARTMNOFJU
(6) CBGHKLQVWXYZDEPARTMNOFJUSI
(7) RTMNOFJUSICBGHKLQVWXYZDEPA
(8) ICBGHKLQVWXYZDEPARTMNOFJUS
(9) PARTMNOFJUSICBGHKLQVWXYZDE
(10) TMNOFJUSICBGHKLQVWXYZDEPAR

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Enciphering diagram:

Key word: MANUSCRIPT

```
Plain:    UNUSUALNUM
Cipher:   DGEAMCBDWH
          BEROFENEMY
          NNYZHKHHCA
          RECONNAISS
          XNFZZERVQX
          ANCEAIRPLA
          MGFBSWVPIT
          NESACTIVEO
          LNZUCNSOML
          VEROURLINE
          ENYZMTBVBF
          SAPPARENTL
          YAWDSTODVG
          YONPHOTOGR
          RHQDLPXEOW
          APHICMISSI
          MKCLCDSTQI
          ONS
          QGZ
```

Cryptogram:

```
DGEAM CBDWH NNYZH KHHCA XNFZZ ERVQX MGFBS
WVPIT LNZUC NSOML
ENYZM TBVBF YAWDS TODVG
RHQDL PXEOW MKCLC  DSTQI QGZXX
```

5 2. Polyalphabetic substitution.

5 3. *a.* $C_p\ (R_k) = M_c$.

5 *b.* $N_p\ (B_k) = O_p\ (V_k)$.

4 4. *a.* 26.

4 *b.* Polyalphabetic substitution.

4 *c.* In polyalphabetic substitution, the different equivalents for the same plain-text letter are fixed more or less automatically by the elements of the system, whereas in monoalphabetic substitution with variants the different equivalents are subject to the whim or caprice of the encipherer.

Solutions
Elementary Military Cryptography, 10–p. 2
1943

Weight

3 5. *a.* Number of elements in the key.
b. Identity of each element of the key.
c. Specific sequence of the elements of the key.

25 6. *a.* Enciphering diagram:

Key word: CONTRACT
Plain: ENEMYPAT
Cipher: YBJHTLCA
ROLSRUSH
LACBAGKM
EDOURADV
YLZZAAZY
ANCELINE
CBLPGSPP
SINQUEST
KGADXWKA
OFPRISON
OJYCJIOG
ERSBUTAL
YXVSXHCI
LWEREDRI
RSJCNXLL
VENBACK
HKASRYS

Cryptogram:

YBJHT LCALA CBAGK MYLZZ AAZYC BLPGS PPKGA
DXWKA OJYCJ IOGYX VSXHC IRSJC NXLLH KASRY
SXXXX

Solutions
Elementary Military Cryptography, 10–p. 3
1943

Weight

20 *b.* Deciphering diagram:

Key word: PENSION
Cipher: YALKTXZ
Plain: RECIPRO
NECSRVF
CALARTI
ETJBKOL
LLERYAC
WWZFEOV
TIONEAS
WEAPMKV
TANDWES
WQIZBKV
TOFTHES
PEWRIWF
AARBASI
C
N

Plain-text message:

RECIPROCAL ARTILLERY ACTION EAST AND WEST OF THE SAAR BASIN

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.

LESSON 11 —Sliding Alphabets and Square Tables; More Complicated Substitution Methods.

Weight

4 1. *a.* Mechanical (usually hand-operated) devices or instruments employed to facilitate cryptographing and decryptographing and to increase the degree of cryptographic security of cipher messages.

2 *b.* Converter M–209A.

6 2. *a.* Because they exhibit phenomena of a cyclic or periodic nature.

6 *b.* Break up periodicity by employing a variable-length key, or applying key to variable lengths of plain text, or a combination of both.

4 3. *a.* Polygraphic substitution is the name applied to cryptographic methods in which the cryptographic treatment is applied to sets of two or more letters taken as units.

4 *b.* Its object is the suppression, so far as possible, of the characteristic frequencies of individual letters.

2 *c.* Polygraphic substitution.

10 4. *a.* Slow.
b. Cumbersome.
c. Subject to error.
d. Degree of cryptographic security not very great.
e. Not economical.

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Weight

12 5. *a.* GEORWASHINTUVYBCDFJKLMPQXZ
EORWASHINTUVYBCDFJKLMPQXZG
ORWASHINTUVYBCDFJKLMPQXZGE
RWASHINTUVYBCDFJKLMPQXZGEO
WASHINTUVYBCDFJKLMPQXZGEOR
ASHINTUVYBCDFJKLMPQXZGEORW
SHINTUVYBCDFJKLMPQXZGEORWA
HINTUVYBCDFJKLMPQXZGEORWAS
INTUVYBCDFJKLMPQXZGEORWASH
NTUVYBCDFJKLMPQXZGEORWASHI
TUVYBCDFJKLMPQXZGEORWASHIN
UVYBCDFJKLMPQXZGEORWASHINT
VYBCDFJKLMPQXZGEORWASHINTU
YBCDFJKLMPQXZGEORWASHINTUV
BCDFJKLMPQXZGEORWASHINTUVY
CDFJKLMPQXZGEORWASHINTUVYB
DFJKLMPQXZGEORWASHINTUVYBC
FJKLMPQXZGEORWASHINTUVYBCD
JKLMPQXZGEORWASHINTUVYBCDF
KLMPQXZGEORWASHINTUVYBCDFJ
LMPQXZGEORWASHINTUVYBCDFJK
MPQXZGEORWASHINTUVYBCDFJKL
PQXZGEORWASHINTUVYBCDFJKLM
QXZGEORWASHINTUVYBCDFJKLMP
XZGEORWASHINTUVYBCDFJKLMPQ
ZGEORWASHINTUVYBCDFJKLMPQX

Solutions
Elementary Military Cryptography, 11–p. 2
1943

Weight

20 *b.* Encipherment:

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

Cryptogram:

CLDBF ORCVF KBLLP RZMNL MXLKS BZCEJ XGCFZ
QKLAC CYIYK BMFMM VWYKA BFOBN JCFCK JZCRQ
HYXKX KVDJT KXBOQ ATOLM XYSTN DFKCW AONAX
OTLCE

Solutions
Elementary Military Cryptography, 11–p. 3
1943

Weight

c. Enciphering alphabet:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: BQXZTGNDFEORWJUASVCKLMYHPI

Deciphering alphabet:

Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: PASHJIFXZNTUVGKYBLQEORMCWD

d. Decipherment:

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

Plain-text message:

THREE SUCCESSFUL BOMBING RAIDS ON AN ENEMY AIRFIELD AT KOBLENZ TODAY DESTROYED MANY AIRPLANES AND AN AMMUNITIONS DUMP

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 12 —Code Systems.

Weight	
5	1. *a.* Decodement.
5	*b.* Code book or code.
5	*c.* By means of a syllabary.
5	*d.* Code groups.
5	2. *a.* Primary, economy; secondary, secrecy.
5	*b.* Primary, secrecy; secondary, economy.
5	3. Code A.
6	4. *a.* Economy in terms of money.
	b. Economy in time.
	c. Economy in labor.
20	5. Messages *a* and *e*.
	Messages *b* and *f*.
	Messages *c* and *d*.
12	6. Any four of the following:
	a. Bona fide words.
	b. Artificial words.
	c. Groups of letters presenting no appearance of bona fide or artificial words.
	d. Groups of figures.
	e. Groups of letters and figures.
4	7. *a.* A permutation table is a table which permits the more or less automatic and systematic construction of code groups of the form desired.
3	*b.* The two-letter differential.

All concerned are requested to be careful that neither this solution nor information concerning the same comes into the possession of students or prospective students who have not completed the work to which it pertains.

Weight			
20	8. *a.* Position.	*f.* Identity.
	b. Position.	*g.* Position.
	c. Identity.	*h.* Position.
	d. Position.	*i.* Identity.
	e. Position.	*j.* Identity.

Solutions
Elementary Military Cryptography, 12–p. 2.
1943

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 13 —One-Part and Two-Part Codes; Enciphered Code; Comparison of Code and Cipher Systems.

Weight

4 1. *a.* A strictly alphabetical code is one in which a strict alphabetical arrangement is adhered to in the sequence, progression, or arrangement of the phrases included in the vocabulary of the code.

A caption code is one in which the phrases are listed under separate headings based upon the principal word or idea in the whole expression.

2 *b.* Advantage: A caption code permits, perhaps, of more precise and more economical encoding then does a strictly alphabetical code, because it is easier under the former type of arrangement to assemble under each specific principal heading a rather extended variety of expressions and different shades of expressions than under the latter type of arrangement.

Disadvantage: The use of a caption code involves more time and labor in encoding, especially by untrained or unskilled personnel.

15 2. *a.* (1) A basic or unchangeable method or process termed the general system.

(2) A specific or variable factor which controls the steps under the general system and is termed the specific key.

b. The specific key.

c. Because it must be assumed that the enemy is in full possession of all the details concerning the general system, since the circumstances of employment are such that the enemy has prolific sources of information,

---

and since he can in any case, sooner or later, solve messages on account of blunders, piling up of traffic, etc. If secrecy depended only on keeping the general system secret, then every time a method became compromised, it would be necessary to prepare a new one, distribute it to numerous individuals and train them in its use. This cannot be done frequently in the military service.

Weight

14. 3.

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

4. *a.* Additive method of encipherment is that in which a code group is replaced by the one which stands 1, 2, 3, . . . *n* places after it in the sequence of code groups of the code book, whereas the subtractive method of encipherment is that in which a code group is replaced by the one which stands 1, 2, 3, . . . *n* places before it in the sequence of code groups of the code book.

b. Yes. They may be combined by having addition and subtraction take place alternately, or at regular or irregular intervals as controlled by a key.

5. *a.* One-part and two-part codes. A one-part code is that in which the plain-text elements (the words, phrases, sentences, etc.) are arranged in a systematic order, usually alphabetically accompanied by their code groups which are also arranged in alphabetical or numerical order. One book serves for encoding as well as for decoding. A two-part code is that in which the plain-text elements (the words, phrases, sentences, etc.) are arranged in a systematic order, usually alphabetical, accompanied by their code groups in a nonsystematic or random order. Two sections are necessary, one for encoding, the other for decoding. In the latter the code groups are listed alphabetically or numerically, accompanied by their meanings as given in the encoding section.

Solutions
Elementary Military Cryptography, 13–p. 2
1943

REF ID:A64682

14352

B R O W N

QYLED	TLAZL	NGOKI	XALDA	BEPUX
14352	14352	14352	14352	14352
QDLYE	TLAEZ	NIOGK	XALAD	BXPEU

OXQAV
14352
OVQXA

Cryptogram:

QDLYE TLAEZ NIOGK XALAD BXPEU OVQXA

Elementary Military Cryptography
(1943) Lesson 13. Question 6

Weight

b. One-part code is smaller and the cost of compilation and printing is less than for the two-part code. It has the disadvantages, however, of being less secret and less accurate than the two-part code.

6. Derived numerical key:

		1 4 3 5 2			
		B R O W N			
QYLED	TEAZL	NGOKI	XALDA	BEPUX	OXQAV
14352	14352	14352	14352	14352	14352
QELDY	TZALE	NKOIG	XDLAA	BUPXE	OAQVX

Cryptogram:

QELDY	TZALE	NKOIG	XDLAA	BUPXE	OAQVX

7. *a.* (1) Simplicity, rapidity, practicability.
(2) Secrecy.
(3) Accuracy.
(4) Economy.

b. Code systems are, in general, more rapid, simple, and practicable than cipher systems. Enciphering and deciphering involves closer attention and more mental strain than do encoding and decoding. Code systems are more secret than cipher systems; the solution of a single code message does not entail the immediate breakdown of the whole system, as is the case of ciphers. But code books must be handled carefully at all times to safeguard them from compromise. Code systems are less accurate than cipher systems because a mistake in one code group may obscure, alter, or render unintelligible the meaning of a whole message, whereas a mistake in one cipher group can usually be corrected easily from the context. Code is more economical than cipher; messages can be condensed or abbreviated, since a single code group may represent a long phrase or a whole sentence. On the other hand, codes are expensive to compile, print, and distribute.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
LESSON 14 —Corrections of Errors; Fundamental Rules for Safeguarding Cryptograms.

Weight

10 1. Paraphrase the message and then transmit it in the old code.

10 2. In substitution ciphers, nulls may be added at any time, but in transposition ciphers the necessary nulls must be added before cryptographing. If added after cryptographing, the message will not yield to quick decryptographing, if it yields at all.

10 3. *a.* (1) Those made in cryptographing and decryptographing including copying.

(2) Those made in transmission and reception.

15 *b.* By systematizing the work, doing it carefully, and invariably checking it. Suitable offices for cryptographic personnel should be provided. Checking should preferably be done by having a second operator perform the work. If the cryptographing of a message is to be checked, it should be done by decryptographing it, not merely checking the original work. If the decryptographing is to be checked, the final text should be checked against the original work sheets by another operator. Cryptographic personnel should know the telegraph alphabets thoroughly and the most common types of errors in transmission and receiption so as to be able to correct simple errors quickly. The word count of every cryptographed message, as indicated on the message blank as received, should be examined, and likewise each group should be examined to see that it

Weight

has its proper quota of letters. In the case of transposition ciphers, nulls (if necessary) must be added before cryptographing. Carefulness, accuracy, and attention to detail are absolutely essential in cryptographic personnel and those with the latter qualification should be especially selected for the work.

4. *a.* Telegraphing (incorrect grouping of signals, DE=B).
   b. Telegraphing (incorrect grouping of signals, FEU=I).
   c Telegraphing (incorrect transmission of S for H).
   d. Copying (psychological).
   e. Telegraphing (incorrect grouping of signals, IN=F).
   f. Telegraphing (incorrect grouping of signals, KR=NC).
   g. Copying (faulty writing, D made like O).
   h. Telegraphing (final dash of M shortened to a dot) or copying.
   i. Copying (transposition in writing, phychological).
   j. Copying (psychological).
   k. Copying (transposition in writing, psychological).
   l. Telegraphing (incorrect grouping of signals, AM=WT).
   m. Copying (transposition in writing, psychological).
   n. Copying (faulty writing, G made like C).
   o. Telegraphing (incorrect grouping of signals, EY=AW).

5. The instructor should examine the student's summary in the light of the data given in section XX of the text.

FOR USE OF INSTRUCTORS ONLY

Serial No.....

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE—Elementary Military Cryptography.
EXAMINATION

Weight

10 1. Substitution and transposition.

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 retain their original identities but merely undergo some change in their relative positions or sequences so that the message becomes unintelligible.

9 2. *a.* *A* is using a one-part code.
b. *B* is using a two-part code.
c. Two-part code.

15 3. Literal key: C A T F I S H
Numerical key: 2 1 7 3 5 6 4

2173564 2173564 2173564 2173564 2173564
ENEMYRA IDERSOV ERNORTH SEAWILL BEMETBY
2173564 2173564 2173564
FASTFIG HTINGPL ANESRD

Cryptogram:

NDREE ATNEI ESBFH AMROW ETNSA VHLYG
LYSRI TFGRR OTLBI PDEEN AMSIE

Note.—Underlined letters (R and D) are nulls to complete the last group.

4 4. Because such letters are infrequent in plain English and, if found in a transposition cipher, offer clues to its solution, since they may be identified as nulls.