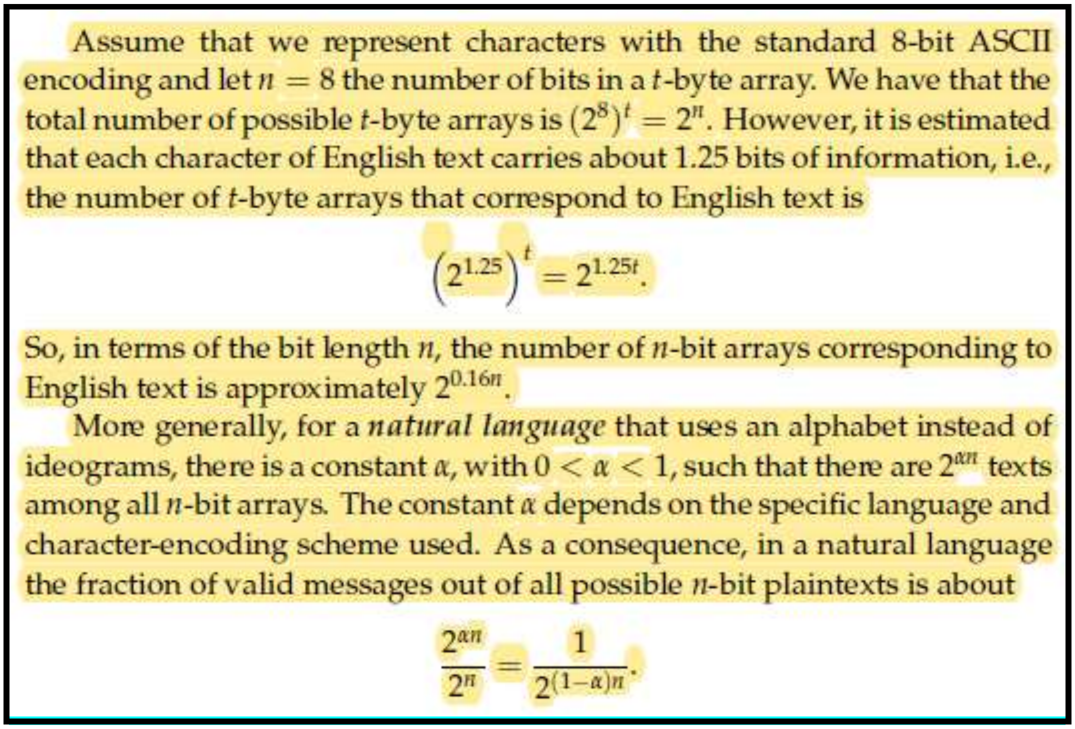
FURTHER QUESTIONS MODULE 1 & MODULE 2

1. Compare and contrast symmetric encryption with public-key encryption, including the strengths and weaknesses of each.

2. Give an example of the false sense of security that can come from using the “security by obscurity" approach.

3.



Assume that we represent characters with the standard 8-bit ASCII encoding and let $n = 8$ the number of bits in a t-byte array. We have that the total number of possible t-byte arrays is $(2^8)^t = 2^n$. However, it is estimated that each character of English text carries about 1.25 bits of information, i.e., the number of t-byte arrays that correspond to English text is

$$\left(2^{1.25}\right)^t = 2^{1.25t}.$$

So, in terms of the bit length n, the number of n-bit arrays corresponding to English text is approximately $2^{0.16n}$.

More generally, for a *natural language* that uses an alphabet instead of ideograms, there is a constant α, with $0 < \alpha < 1$, such that there are $2^{\alpha n}$ texts among all n-bit arrays. The constant α depends on the specific language and character-encoding scheme used. As a consequence, in a natural language the fraction of valid messages out of all possible n-bit plaintexts is about

$$\frac{2^{\alpha n}}{2^n} = \frac{1}{2^{(1-\alpha)n}}.$$

The English language has an information content of about 1.25 bits per character. Thus, when using the standard 8-bit ASCII encoding, about 6:75 bits per character are redundant. Compute the probability that a random array of t bytes corresponds to English text.

4. Compare and contrast the C.I.A. concepts for information security with the A.A.A. concepts.

5. Explain why someone need not worry about being a victim of a social engineering attack through their cell phone if they are inside of a Faraday cage.

6. What is the ciphertext in an English version of the Caesar cipher for the plaintext “ALL ZEBRAS YELP.”

7. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality,
integrity, and availability requirements associated with the system and, in each case indicate the degree of importance of the requirement.

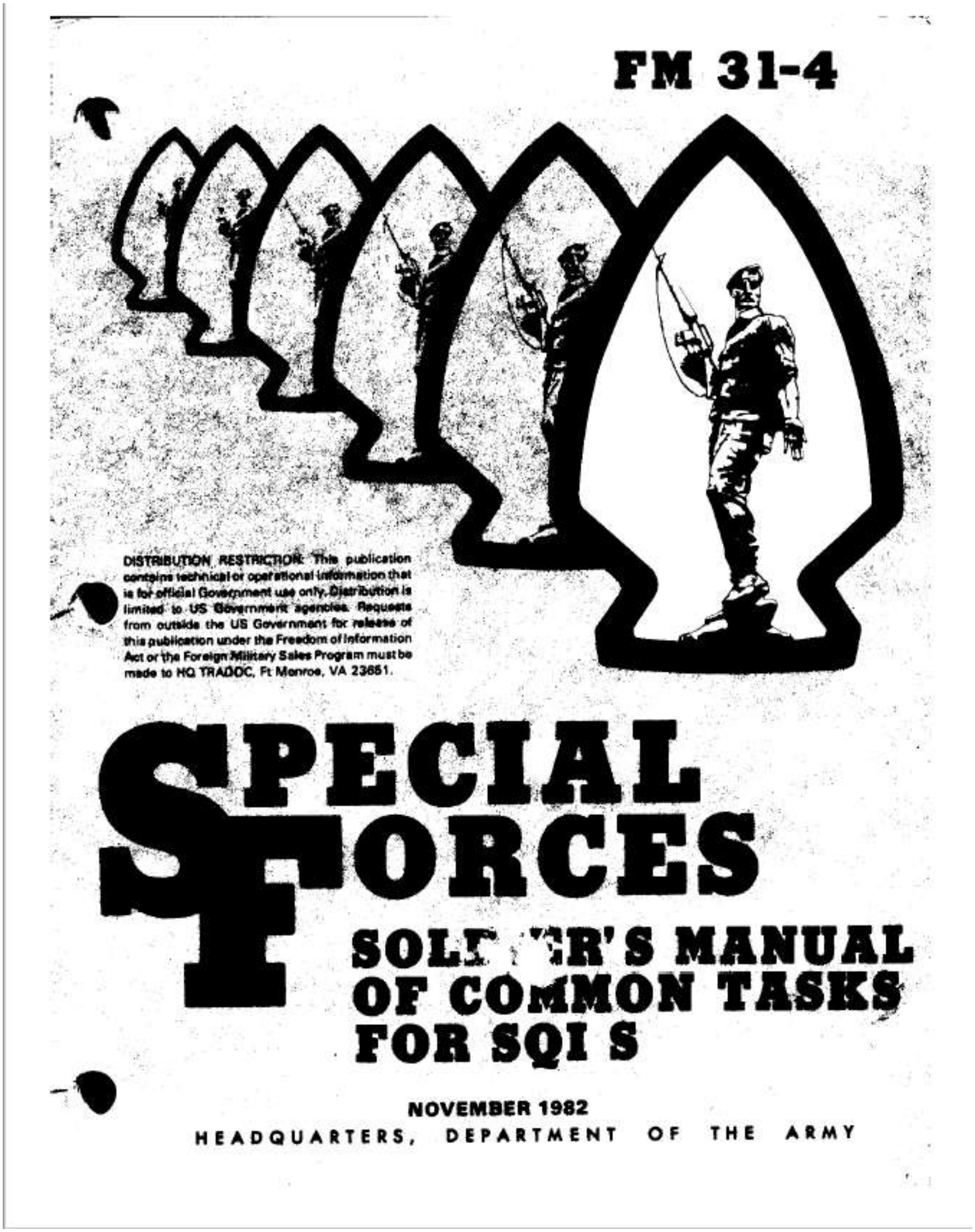
8. The Administrators of TCOM3003 are entertaining the possibility of an online end of term Exam. What security issues are raised when implementing such a design. Consider the Material in Module 1. Your answer should be at least half a page long.

9. This problem is a real-world example of a symmetric cipher from an old US Special Forces manual. See the attached document. Using the two keys (memory words) **“cryptographics” and “network security,”** encrypt the following message: “**Be at the third pillar from the left outside the Iyceum theater tonight at seven. If you are distrustful bring two friends.”** Make reasonable assumptions about how to treat redundant letters and excess letters in the keys (memory words) and how to treat space and punctuation. Indicate

what your assumptions are.

Decrypt the ciphertext. Show your work.

Comment on when it would be appropiate to use this technique and what its advantages are.



FM 31-4

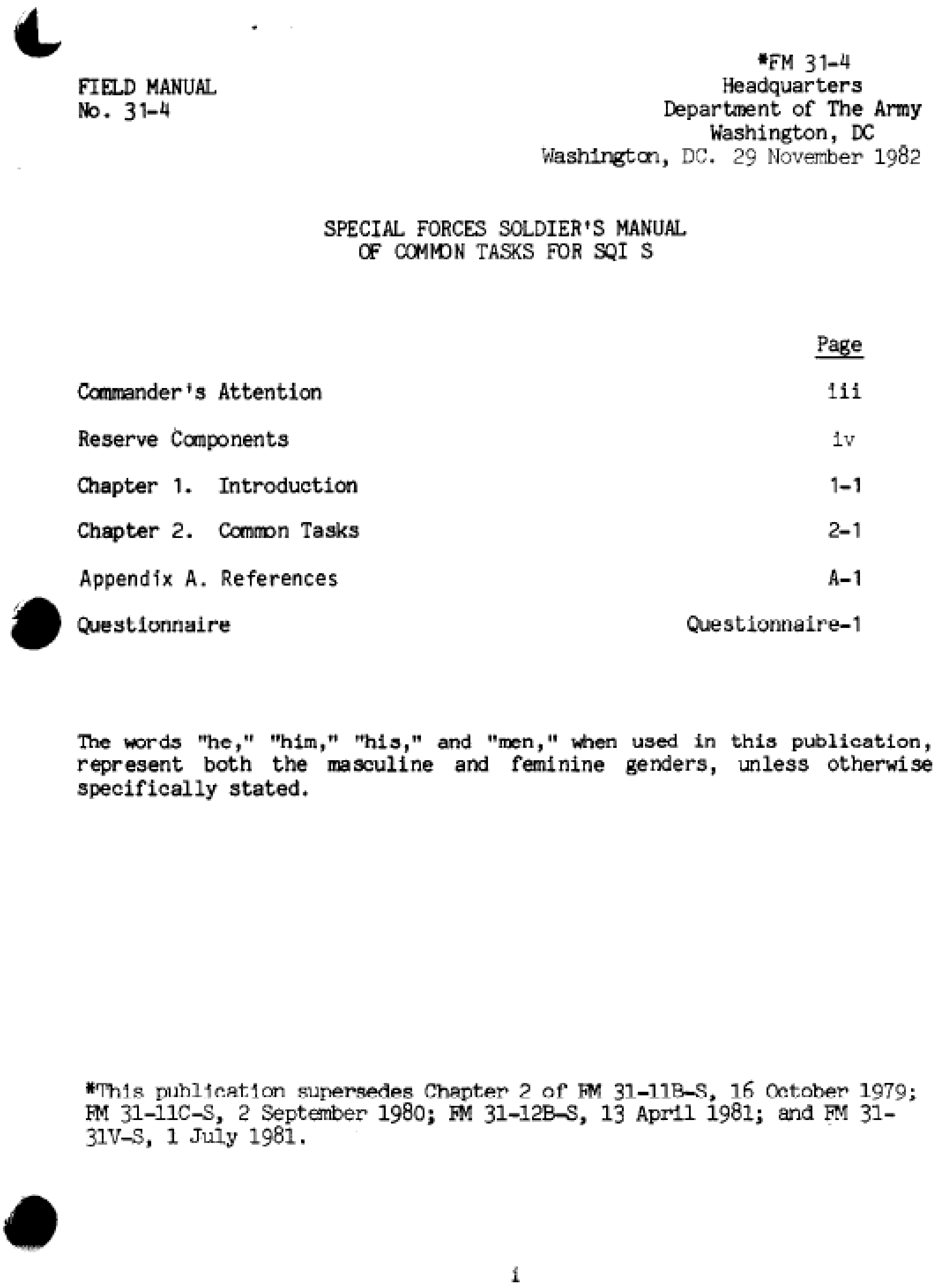
DISTRIBUTION RESTRICTION: This publication contains technical or operational information that is for official Government use only. Distribution is limited to US Government agencies. Requests from outside the US Government for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to HQ TRADOC, Ft Monroe, VA 23651.

SPECIAL FORCES

SOLDIER'S MANUAL OF COMMON TASKS FOR SQI S

NOVEMBER 1982

HEADQUARTERS, DEPARTMENT OF THE ARMY



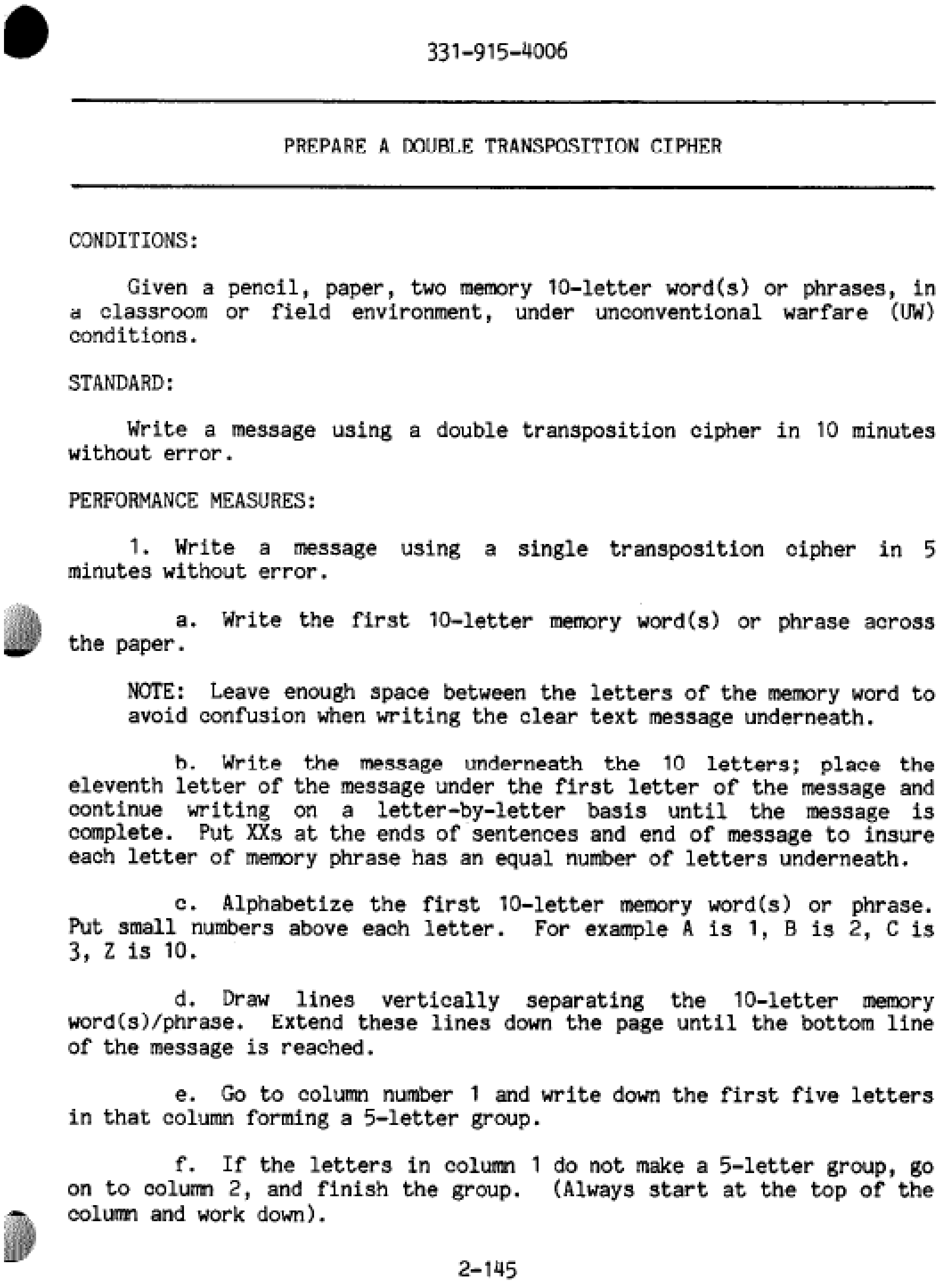
FIELD MANUAL
No. 31-4

*FM 31-4
Headquarters
Department of The Army
Washington, DC
Washington, DC. 29 November 1982

SPECIAL FORCES SOLDIER'S MANUAL
OF COMMON TASKS FOR SQI S

The words "he," "him," "his," and "men," when used in this publication, represent both the masculine and feminine genders, unless otherwise specifically stated.

*This publication supersedes Chapter 2 of FM 31-11B-S, 16 October 1979; FM 31-11C-S, 2 September 1980; FM 31-12B-S, 13 April 1981; and FM 31-31V-S, 1 July 1981.



PREPARE A DOUBLE TRANSPOSITION CIPHER

CONDITIONS:

Given a pencil, paper, two memory 10-letter word(s) or phrases, in a classroom or field environment, under unconventional warfare (UW) conditions.

STANDARD:

Write a message using a double transposition cipher in 10 minutes without error.

PERFORMANCE MEASURES:

1. Write a message using a single transposition cipher in 5 minutes without error.

a. Write the first 10-letter memory word(s) or phrase across the paper.

NOTE: Leave enough space between the letters of the memory word to avoid confusion when writing the clear text message underneath.

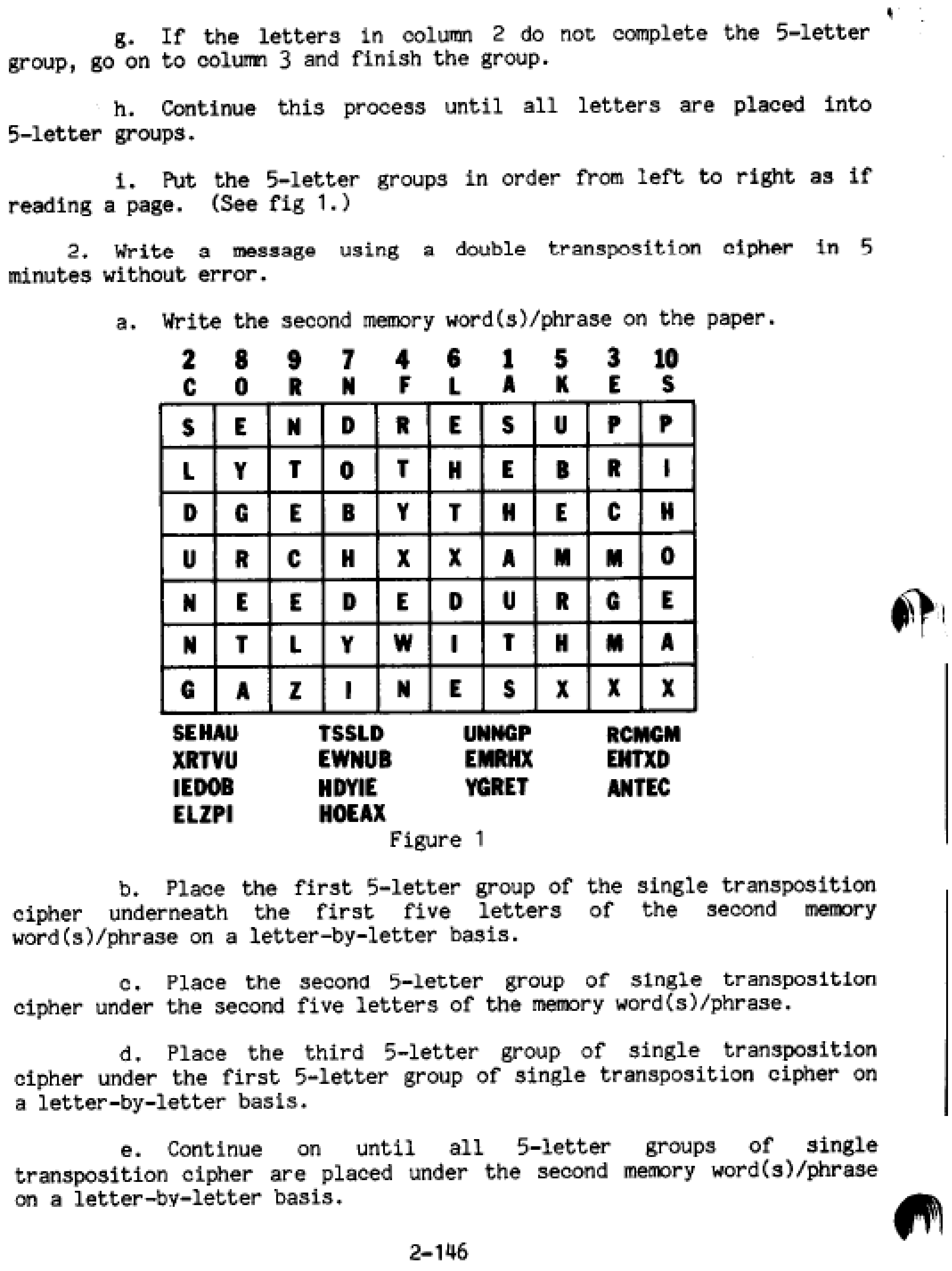
b. Write the message underneath the 10 letters; place the eleventh letter of the message under the first letter of the message and continue writing on a letter-by-letter basis until the message is complete. Put XXs at the ends of sentences and end of message to insure each letter of memory phrase has an equal number of letters underneath.

c. Alphabetize the first 10-letter memory word(s) or phrase. Put small numbers above each letter. For example A is 1, B is 2, C is 3, Z is 10.

d. Draw lines vertically separating the 10-letter memory word(s)/phrase. Extend these lines down the page until the bottom line of the message is reached.

e. Go to column number 1 and write down the first five letters in that column forming a 5-letter group.

f. If the letters in column 1 do not make a 5-letter group, go on to column 2, and finish the group. (Always start at the top of the column and work down).



g. If the letters in column 2 do not complete the 5-letter group, go on to column 3 and finish the group.

h. Continue this process until all letters are placed into 5-letter groups.

i. Put the 5-letter groups in order from left to right as if reading a page. (See fig 1.)

2. Write a message using a double transposition cipher in 5 minutes without error.

a. Write the second memory word(s)/phrase on the paper.

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

SEHAU TSSLD UNNGP RCMGM
XRTVU EWNUB EMRHX EHTXD
IEDOB HDYIE YGRET ANTEC
ELZPI HOEAX

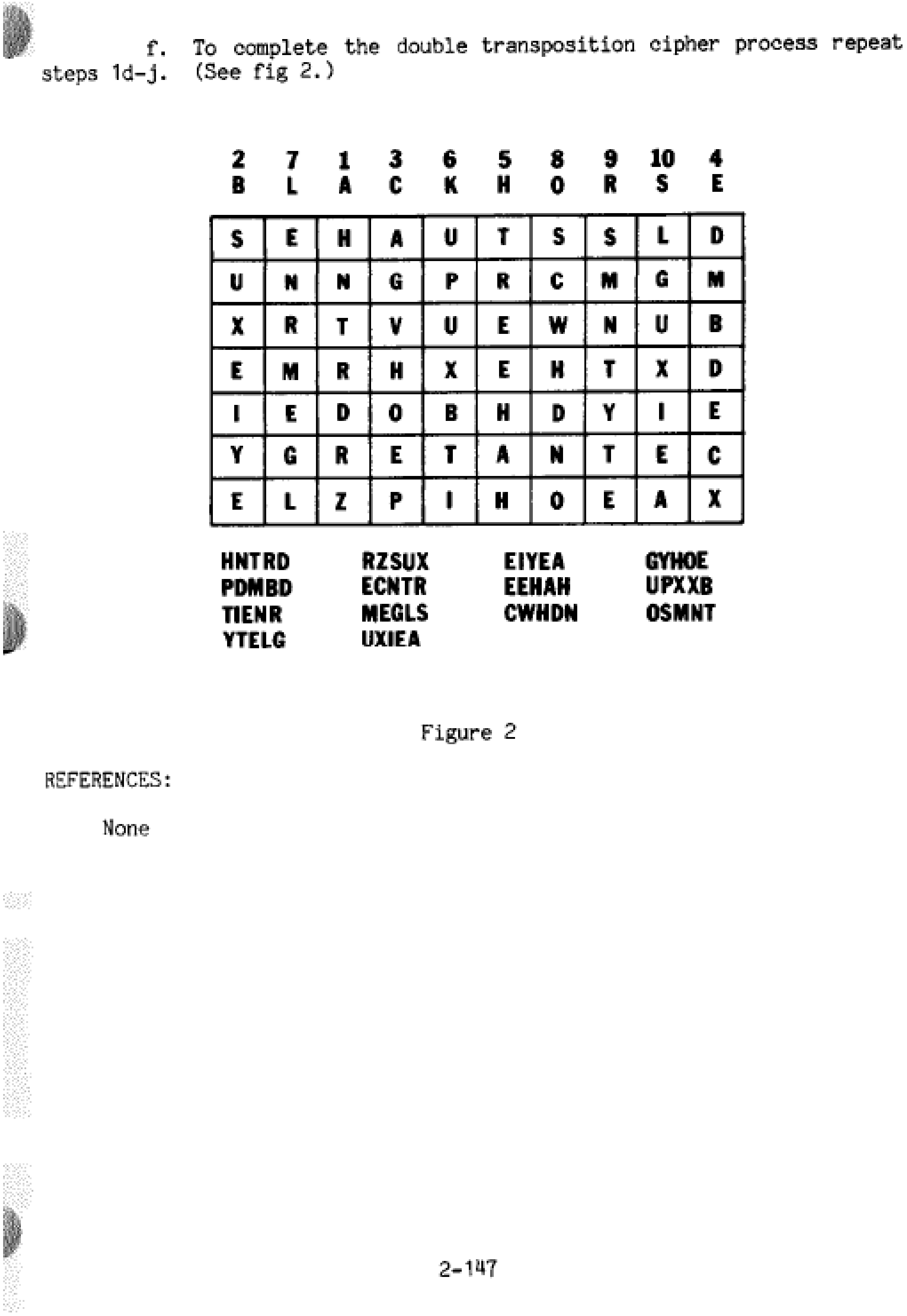
Figure 1

b. Place the first 5-letter group of the single transposition cipher underneath the first five letters of the second memory word(s)/phrase on a letter-by-letter basis.

c. Place the second 5-letter group of single transposition cipher under the second five letters of the memory word(s)/phrase.

d. Place the third 5-letter group of single transposition cipher under the first 5-letter group of single transposition cipher on a letter-by-letter basis.

e. Continue on until all 5-letter groups of single transposition cipher are placed under the second memory word(s)/phrase on a letter-by-letter basis.



f. To complete the double transposition cipher process repeat steps 1d-j. (See fig 2.)

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

```
HNTRD   RZSUX   EIYEA   GYHOE
PDMBD   ECNTR   EEHAH   UPXXB
TIENR   MEGLS   CWHDN   OSMNT
YTELG   UXIEA
```

Figure 2

REFERENCES:

None

2-147

10. Using the Vigenère cipher, encrypt the word “cryptographic” using the word “eng”.

11. This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

a. Encrypt the plaintext sendmoremoney with the key stream

3 11 5 7 17 21 0 11 14 8 7 13 9

b. Using the ciphertext produced in part (a), find a key so that the ciphertext decrypts to the plaintext cashnotneeded.