EECS710: Information Security and Assurance

Professor Hossein Saiedian

Fall 2014

Assignment 2: Encryption and Cryptography
Points: 20
Due: 9/5/2014

PART 1: : You must be familiar with an encryption technology (tool) to encrypt a file or directory (minimally) or a hard drive partition, or an entire (virtual) hard drive. Download and install one of the existing encryption tools and apply it. Summarize your experience in a short PowerPoint presentation and include screen captures. Interesting experiences will be shared with the rest of the classroom.

PART 2: : Form 2-member teams. Download and install one of the PGP tools. Share your public keys with your teammate. Exchange short encrypted emails. Summarize experience (include screen captures) and the emails exchanged.

PART 3: : 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 appreciate to use this technique and what its advantages are.

FM 31-4

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 C	8 O	9 R	7 N	4 F	6 L	1 A	5 K	3 E	10 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 B	7 L	1 A	3 C	6 K	5 H	8 O	9 R	10 S	4 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