Homework 2

Name: Anusha Balasubramanian
Email: ab19533n@pace.edu

Exercise: Perform Transposition cipher process and derive cipher text outcomes

Section 1: Exercise - (25 points)

SINGLE TRANSPOSITION CIPHER

KEY:

D	U	P	L	I	C	A	T	E	S

PERMUTATION:

3	10	7	6	5	2	1	9	4	8

MESSAGE TO BE ENCRYPTED:

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

5-LETTER GROUPS OF SINGLE TRANSPOSITION ARE CIPHER BELOW:

EESDI	LEUTI	EGATT	NGKUI
TILOE	AENRN	ELAXS	TICWM
XNEFN	OINIG	ITBTR	XSLNG
NBIHO	ENTOE		

Section 2: Exercise - (50 points)

For extra credit, perform double transposition cipher process using 2 different keys of (ex, cornflakes and blackhorse) instead of single transposition for the text message above and place the 5-letter groups of transposition cipher below. Show the table/steps in detail

DOUBLE TRANSPOSITION CIPHER:

STEP 1: SINGLE TRANSPOSITION

KEY:

D	U	P	L	I	C	A	T	E	S

PERMUTATION:

3	10	7	6	5	2	1	9	4	8

MESSAGE TO BE ENCRYPTED:

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

OUTCOME AFTER SINGLE TRANSPOSITION IN 5-LETTER GROUPS:

EESDI	LEUTI	EGATT	NGKUI
TILOE	AENRN	ELAXS	TICWM
XNEFN	OINIG	ITBTR	XSLNG
NBIHO	ENTOE		

STEP 2:DOUBLE TRANSPOSITION

KEY:

F	R	U	I	T	C	A	K	E	S

PERMUTATION:

4	7	10	5	9	2	1	6	3	8

ENCRYPTED MESSAGE TO BE ENCRYPTED AGAIN:

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

OUTCOME AFTER DOUBLE TRANSPOSITION IN 5-LETTER GROUPS:

EGEII	SNLNA	TOXET	URWIN
OEETE	XINDT	OXFTH	UKNCN
LTEGI	LNTBI	INMGG	EITES
NROSA	LAEBI		

Section 3: Exercise - (25 points)

Question; Comment on when it would be appropriate to use double transposition technique and what its advantages are.

The double transposition technique can be used at the place where strong encryption is needed.That is stronger than single transposition, as single transposition uses only one key and message is encrypted only once. Whereas, in double transposition, two keys are used and is encrypted twice to make it difficult for an attacker/hacker to crack it. It is still breakable using divide and conquer technique(Was done at " Solving the Double Transposition Challenge with a Divide and Conquer Approach.").But this technique has been combined with various substitutions methods to make it hard for hackers to crack.

This technique was used at difficult field conditions like World War I, World War II, and even sometimes later. This is used in algorithms which requires strong permutations along with the other techniques like substitution. Hence i feel that it can be used in these difficult filed conditions provided it is made more stronger along with other techniques.

Advantages of Double Transposition Technique

- A double transposition technique with keys and messages so long will be difficult to break because there is a lot of efforts required(lots of permutations) to do that. However, with the recent computers, this can be done easily.
- It requires attacker/hacker to know two keys that is being used.
- Can be used along with other techniques(substitution) to make it more strong.
- Easy to create.
- Simple and easy algorithm to understand.