Homework 2 Name: Abbas Shamshi Email: as10608n@pace.edu

The assignment consists of 2 parts. Part 1 (75%) and Part 2 (25%).

Exercise: Perform **Transposition cipher** and derive cipher text outcomes

Part 1 (Individual):

This must be completed individually.

Please read the attached pdf (**SpecialForcesCode.pdf**) and perform single transposition cipher, double transposition cipher on the given message below.

You might have to do additional web research to learn more about the transposition cipher to complete this part of work.

Upload your document with the name HW2_"LastName".pdf by replying to the discussion.

Part 1.1 : Single transposition cipher

Perform Single transposition cipher process using a key

Choose your own key and message.

KEY (memory word) of 10 alphabets. CHARACTERS

C	H	A	R	A	C	T	E	R	S

Write your permutation based on order of A to Z

3	6	1	7	2	4	10	5	8	9

My permutation below

Write down **PLAIN TEXT to be encrypted (choose any sentence of 60-80 characters length):**

T	H	I	S	T	E	X	T	H	A
S	B	E	E	N	E	N	C	R	Y
P	T	E	D	U	S	I	N	G	T
R	A	N	S	P	O	S	I	T	I
O	N	C	I	P	H	E	R	T	A
U	G	H	T	A	T	P	A	C	E
U	N	I	V	E	R	S	I	T	Y

Complete single transposition cipher process and Place the 5-letter groups of single transposition cipher below.

IEENC	HITNU	PPAET	SPROU
UEESO	HTRTC	NIRAI	HBTAN
GNSED	SITVH	RGTTC	TAYTI
AEYXN	ISEPS		

_____ _____

Part 1.2 : Double transposition cipher

Perform double transposition cipher process using 2 different keys (ex, cornflakes and Blockchain)

Choose your own keys and message.
KEY (memory word) of 10 alphabets: TECHNOLOGY

T	E	C	H	N	O	L	O	G	Y

My permutation below based on order of A to Z

9	2	1	4	6	7	5	8	3	10

KEY (memory word) of 10 alphabets: UNDERSTAND

U	N	D	E	R	S	T	A	N	D

My permutation below based on order of A to Z

10	5	2	4	7	8	9	1	6	3

Outcome after single transposition in 5-letter groups

UEUYA	TPOHT	RHTFC	TEHER
ECRSW	RHADI	GDITA	ATIOE
ESNHN	RGSSE	SMWVA	GYPXO
CAOIE	MINTX		

Outcome after double transposition in 5-letter groups

OHAIS	PNUTR	INWOT	RIEEO
XYFST	HVIEH	CDSMA	HEDOS
XTACW	ANAET	TRARG	MPEHT
GYIUR	EGESC		

Part 1.3 : Additional Research and commenting :

Question; Research and explain when it would be appropriate to use double transposition technique and what its advantages are. List your references.

Double Transposition is one of the strongest ciphers. It takes already encrypted text and cipher it again using different message key. Double transposition cipher makes it almost impossible to guess or decipher the message without knowing message key. It makes decrypting very difficult

This kind of method comes handy when security of data is high priority, thus this type of encryption is used in military to keep the text unreadable without the message key. This encryption can also be used to store data in banks which make it impossible to read the plain text data.

Advantages

It mixes letter better than some of the ciphers.

It can be applied more than once on the text which makes it very difficult to break.

Part 2 (Classes discussion):

Select at least 1 of your classmate's submitted HW2 assignment in classes and decrypt their cipher text to derive the plain text. This should validate their work. Let them know if it does.

In addition, share if you have any other information pertaining to the cipher, background, your findings, thoughts or any Cyber-attacks/Prevention from your corporate or personal experience.