German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Practice Assignment 1

Discussion 01/02/2020 - 06/02/2020

---

1 Substitution Ciphers

1.1 Caesar Cipher

1. **Encrypt** the following plain text using Caesar cipher with key **8**.

   Plain Text: "Resist much, obey little".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. **Decrypt** the following cipher text using Caesar cipher, knowing that the key is less than 5.

   Cipher Text: "M XLMRO, XLIVIJSVI M IBMWX"

1.2 Monoalphabetic Cipher

1. **Decrypt** the following cipher text using Monoalphabetic Substitution Cipher.

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

Cipher Text:"IDOWADE FWLF AT DBY OWADE LPAUW"

1.3 Vigenère Cipher

1. **Encrypt** the following plain text using the Vigenère cipher with key **"Play"**.

   Plain Text : "Attack Now".

2. **Decrypt** the following cipher text using Vigenère cipher with key **"Senior"**.

   Cipher Text : "LLVZHPKIIMBUSWU".

3. **Perform** an examination to find the length of the key that was used to produce the following Vigenère cipher text.

   Cipher Text: "io ygx wewq ss tswmw nzl eytluonnr. vs wewq ss hzo aj acw ysamdi yo mw eytluojd".

4. **Assume** that Vigenere cipher was used to convert the following plaintext into ciphertext:

Plain Text.	C	R	Y	P	T	O	G	R	A	P	H	Y
Cipher Text.	T	I	C	R	M	Q	U	I	R	T	J	R

If the sequence of characters TICRMQUIRTJR was found twice in the ciphertext, once starting at the 10th character position and again starting at the 241st character position (numbering starts from 1), we can use the Kasiski method to estimate that the key length can be multiples of:

$$241 - 10 = 231 = 3*7*11$$

Thus, we estimate that the length of the key is 3, 7 or 11 characters. **Discover the key**.

2 Transposition Ciphers

2.1 Railfence Cipher

1. **Encrypt** the following plain text using the Rail Fence cipher with key **3**.

   Plain Text: "Creativity is knowing how to hide your sources".

2. **Decrypt** the following plain text using the Rail Fence cipher with key **2**.

   Cipher Text: "PAEEISIHSIEECBGNWTAML"

2.2 Row Transposition

1. **Encrypt** the following plain text using the Row Transposition cipher with key **7521346**.

   Plain Text: "Whatever you are, be a good one".

2. **Decrypt** the following cipher text which is encrypted using the Row Transposition cipher knowing that the key is **231**.

   Cipher Text: "KATAHUMAANAT"

3 Double Layer Encryption

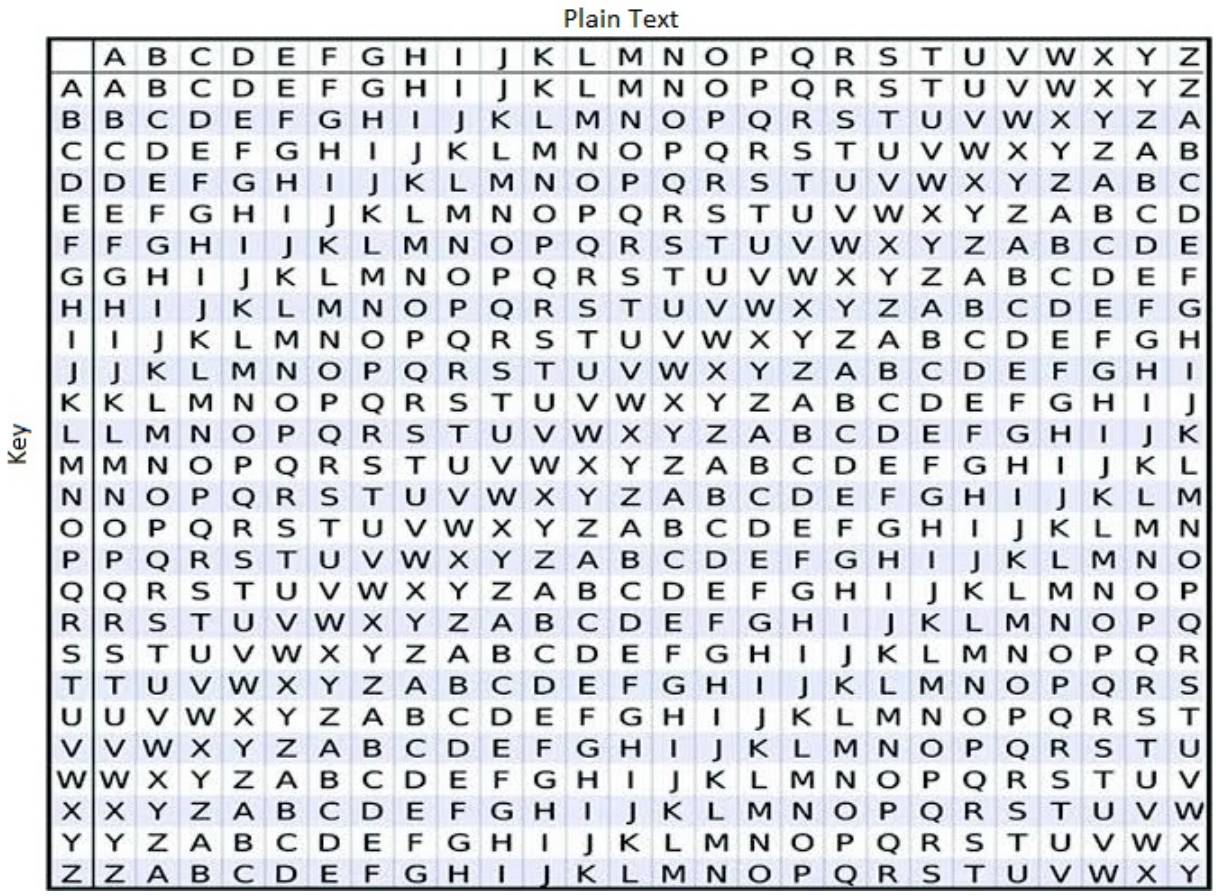
1. **Encrypt** using Monoalphabetic cipher with the below substitution key then row transposition cipher with the key **361425**.

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

Plain Text: "Attack at Dawn".

2. **Decrypt** knowing that the following text has been encrypted using Vignere cipher with the key **"HARRY"** then railfence cipher with the key **3**.

   Cipher Text: "ASWJVHMYPUVFFV"



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