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 Solution

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

   Solution:

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
Shifted Alpha.	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

   Cipher Text: "ZMAQAB UCKP, WJMG TQBBTM".

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

   Cipher Text: "M XLMRO, XLIVIJSVI M IBMWX"

   Solution: Caesar Cipher could be easily broken with brute force in a maximum of 26 trials. But just as a practice let's break this code using cryptanalysis.

   The most common cryptanalysis attack is using frequency analysis. Applying that here, we see that the letter 'M' appears on its own, and single letter words are scarce in English; namely 'A' and 'I'.

   Therefore, to decipher the text, we need to consider only the shifts needed to turn 'M' into 'A' and 'M' into 'I', whichever produces a meaningful sentence is the correct shift. Twelve shifts backwards are needed to turn 'M' to 'A', this produces plain text: "A lzafc, lzwjwxgjw A wpakl".

   Fours shifts backwards are needed to turn 'M' to 'I', this produces: "I think, therefore I exist".

   Plain Text: "I think, therefore I exist"

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"

Solution: Plain Text: "Unbeing dead is not being alive".

1.3 Vigenère Cipher

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

Plain Text : "Attack Now".

Solution:

Plain Text.	A	T	T	A	C	K	N	O	W
Key.	P	L	A	Y	P	L	A	Y	P
Cipher Text.	P	E	T	Y	R	V	N	M	L

Cipher Text: " PETYRV NML".

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

Cipher Text : "LLVZHPKIIMBUSWU".

Solution:

Cipher Text.	L	L	V	Z	H	P	K	I	I	M	B	U	S	W	U
Key.	S	E	N	I	O	R	S	E	N	I	O	R	S	E	N
Plain Text.	T	H	I	R	T	Y	S	E	V	E	N	D	A	S	H

Plain Text: " Thirty Seven Dash".

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".

Solution: First, we find repetitions of sequences in the cipher:

"io ygx **wewq ss** tsw**mw** nzl eytluonnr. vs **wewq ss** hzo aj acw ysamdi yo **mw** eytluojd".

The distance between **wewq ss** repetitions is 25 characters and between the **mw** is 35 characters. Using prime factorization, we find that:

- 25 = 5 *5
- 35 = 5*7

Therefore the gcd = 5, this indicates a key length of 5.

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**.

Solution:

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

At position 10, the shift is:

$$T - C = 19 - 2 = 17 = R$$

Similarly, the remaining letters give the corresponding keyword: **rrectcorrect**. This is obviously not periodic with period 3 or 11, while period 7 is possible. A keyword of length 7 starts at position 15, resulting in the keyword: **correct**.

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".

Solution: To encrypt we need to create a table with the same number of rows as the key and then fill in the plain text column by column.

C	A	V	Y	K	W	G	W	H	Y	R	U	E
R	T	I	I	N	I	H	T	I	O	S	R	S
E	I	T	S	O	N	O	O	D	U	O	C	

After that we read the cipher text row by row.
Cipher Text: "CAVYKWGWHYRUERTIINIHTIOSRSEITSONOODUOC".

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

   Cipher Text: "PAEEISIHSIEECBGNWTAML"

Solution: To decrypt we do the same thing. But here we need first to know the number of columns. We do that by dividing the number of characters in the cipher text by the key. Therefore we have 2 rows and 11 columns. After that, we fill the table row by row and then read the plain text column by column.

P	A	E	E	I	S	I	H	S	I	E
E	C	B	G	N	W	T	A	M	L	

Plain Text: "Peace begins with a smile."

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".

Solution: Since we have 7 numbers in the key, we will create a table with 7 columns. Then we need to fill in the plain text in the table row by row.

7	5	2	1	3	4	6
W	H	A	T	E	V	E
R	Y	O	U	A	R	E
B	E	A	G	O	O	D
O	N	E	W	X	Y	Z

Now, the first segment of the cipher text is column number 1. This means that the first part is "TUGW" followed by the 2nd column and then the 3rd and so on.. giving us:

Cipher Text: "TUGWAOAEEAOXVROYHYENEEDZWRBO"

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

Cipher Text: "KATAHUMAANAT"

Solution: Here we have a 3 number key, meaning that we will have a 3 column table. Again we need to find out the number of rows. We get that by dividing the number of characters in the cipher by the length of the key. Therefore, we have a 4 by 3 table.

Now, we need to fill in the table but we have to do it in the correct way. To do that we divide our cipher text by the key length. We get:

KATA HUMA ANAT

Here, each of these 3 segments is a column in the table. Accordinglythe first segment is the 1st column of the table. So we fill it in. The next segment is the 2nd column. And the last segment is the 3rd column in the table. We then need to order the columns according to the key. After doing that, we just need to get the plaintext by reading the table row by row.

1	2	3
K		
A		
T		
A		

1	2	3
K	H	
A	U	
T	M	
A	A	

1	2	3
K	H	A
A	U	N
T	M	A
A	A	T

2	3	1
H	A	K
U	N	A
M	A	T
A	T	A

Plain Text: "HAKUNA MATATA".

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".

Solution: First applying the monoalphabetic cipher will give us

Cipher Text 1: "SDDSHASDISMQ"

Then applying the row transposition cipher, since we have 6 numbers in the key, we will create a table with 6 columns. Then we need to fill in the plain text (which is in this case Cipher Text 1) in the table row by row.

3	6	1	4	2	5
S	D	D	S	H	A
S	D	I	S	M	Q

Now, according to the key, the first segment of the cipher text is column number 1. This means that the first part is "DI" followed by the 2nd column and then the 3rd and so on.. giving us:

Cipher Text: "DIHMSSSSAQDD"

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"

Solution: We start by decryption railfence first; to get the number of columns we divide the string length by the key giving us a table of 3 rows and 5 columns;

A	S	W	J	V
H	M	Y	P	U
V	F	F	V	

Plain Text 1: "AHVSMFWYFJPVVU"

We then decrypt the vignere cipher by constructing a table with the ciphertext and the corresponding key;

Key.	H	A	R	R	Y	H	A	R	R	Y	H	A	R	R
Cipher Text.	A	H	V	S	M	F	W	Y	F	J	P	V	V	U

Now we will consult the vignere table, using the key, we will consult the row and in each row find the cipher letter, hence finding the corresponding plaintext letter.

Plain Text: "THE BOY WHO LIVED".

Plaintext

Key

	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
W	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