Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Lab 01

Hieu Nguyen
huuhieubk@gmail.com

Ngày 21 tháng 1 năm 2019

OBJECTIVE

The objective of this lab is to experiment with some cryptography methods. You will apply the substitution cipher such as Caesar algorithm and Vigenere Square methods. In addition, we will practice transposition ciphers such as permutation cipher and Vernam cipher.

EXPERIMENT

In Cipher methods there two methods for encrypting plaintext, the Bit Stream and Block cipher methods. In the Bit Stream each bit in the plain text is transformed into a cipher bit. Whereas the block ciphers the message is divided into blocks, of 8, 16 0r 64-bit blocks. In the block cipher each block is encrypted using an algorithm such as substitution, transposition, XOR, or combination of all as well as a key. Bit streams uses algorithmic functions like XOR and OR. In the coming sections you will be practicing some of the substitution and transposition methods.

a) Caesar Ciphers
Encrypt the following messages using three-position shifts to the right of the alphabet as it is illustrated below:

Position	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	26
Alphabets	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
3-posi-shift	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

Plaintext	Plaintext-arranged	Final ciphertext
MY EXAM IS EASY		PB HADP LV HDVB
I VISIT THE SCHOOL EVENT		L YLVLW WKH VFKRRO HYHQW
I LOVE EATING ICE-CREAM		L ORYH HDWLQJ LFHFUHDP

b) Vigenere Ciphers

Use the Vigenere algorithm to encrypt the following messages:

Plaintext	keyword	Final ciphertext
MY EXAM IS EASY	ITALY	VS FJZV CT QZBS
I VISIT THE SCHOOL EVENT	LONDON	U KWWXH FWS WRVADZ IKSZI
I LOVE EATING ICE-CREAM	PARIS	Y MGEX UBLRGW JUN-VHFSV

c) Transposition Cipher

Use the transposition Cipher to encrypt the followings Binary message:

Key Pattern: Key pattern: 1->4, 2->8, 3->1, 4->5,5->7,6->2,7->6,8->3			
Bit locations	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Plaintext(Binary)	0 0 1 0 0 1 0 1	0 1 1 0 1 0 1 1	0 0 1 1 0 1 1 1
Ciphertext	0 1 0 0 0 0 1 1	0 1 0 1 1 1 0 1	1 1 0 0 1 0 1 1
Bit location	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8

Use the transposition Cipher to encrypt the followings letters message:

"BOOK OR RUNNING KEY CIPHER"

Key Pattern: Key pattern: 1->4, 2->8, 3->1, 4->5,5->7,6->2,7->6,8->3			
Letter locations	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Plaintext(letters)	BOOK O R R U	N N I N G K E Y	C I P H E R B O
Ciphertext	KUBORORO	N Y N G E N K I	H O C E B I R P
Bit location	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8

d) Vernam Cipher

Encrypt the following message using the Vernam Approach: “BOOK OR RUNNING KEY CIPHER”

Plaintext	**B O O K**	**O R**	**R U N N I N G**	**K E Y**	**C I P H E R**
Plaintext value	2 15 15 11	15 18	18 21 14 14 9 14 7	11 5 25	3 9 16 8 5 18
One-time pad text	A B C A	B C	A B C A B C A	B C A	B C A B C A
One-time pad value	1 2 3 1	2 3	1 2 3 1 2 3 1	2 3 1	2 3 1 2 3 1
Sum of plaintext and pads	3 17 18 12	17 21	19 23 17 15 11 17 8	13 8 26	5 12 17 10 8 19
After Modulo subtraction					
Ciphertext	C Q R L	Q U	S W Q O K Q H	M H Z	E L Q J H S

Position	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	26
Alphabets	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

e) Solving a Cipher

Visit the Website for the American Cryptogram Association and click on “Solve a Cipher” (http://www.cryptogram.org/resource-area/solve-a-cipher/). Generate a new puzzle and try to solve it. [Try the hint option.] Document your results.

IFCJSAJH FL NPQWICINPJS IK OWIFBW AQWWBOJ XBSCPBWW XGWMPBZ: "HQBNJS FBGVTBSH CNJWWC SJNBQH. RPQZV BFIMR QR."

Check your result: observed by philosopher of global village marshall mcluhan: "diaper backward spells repaid. think about it."

HOMEWORK

Exercise 1. (2pts) We consider a Caesar cipher and assume that the plaintext message is in English. Decrypt the following ciphertext by giving a brief explanation:

```
KNXMNSLKWJXMBFYJWGJSIXFIRNYXB
TWIKNXMWFSITAJWMJQRNSLFSDIFD
```

Note: Use the following frequency distribution of the letters in the English language for the cryptanalysis:
(a) What can be the main drawback of the substitution cipher given above?

(b) Caesar cipher is an example of classical cryptosystem. Is this statement true? Why or why not?

Table 1:

a	b	c	d	e	f	g	h	i	j	k	l	m
8, 05	1, 62	3, 2	3, 65	12, 31	2, 28	1, 61	5, 14	7, 18	0, 1	0, 52	4, 03	2, 25
n	o	p	q	r	s	t	u	v	w	x	y	z
7, 19	7, 94	2, 29	0, 20	6, 03	6, 59	9, 59	3, 1	0, 93	2, 03	0, 2	1, 88	0, 09

(c) Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Take the third letter in each word of the encrypted message above and find the emerging message.

Exercise 2. (1pts) Given is the following string of ciphertext which was encrypted with substitution cipher:

asvphgyt

The encryption rule is given as

$$C = (M + K) \bmod 26$$

where C is the ciphertext, M is the plaintext and K is the key. We assume that the plaintext is in English. You know that the first plaintext letter is a W . Find the key and decrypt the message.

Exercise 3. (1pts) A ciphertext has been generated with an affine cipher.

$$C = E([a, b], p) = (ap+b) \bmod 26$$

The most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Break this code (Find values of a, b)
Note: The language of the plain text was English.

Exercise 4. (1pts) What are two problems with the one-time pad?

Exercise 5. (1pts) Using this Playfair matrix:

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

Encrypt this message:

`Must see you over Cadogan West. Coming at once.`

Exercise 6. Affine Cipher (2pts)
A generalization of the Caesar cipher, knows as the affine Caesar cipher, has the following form:

For each plaintext letter p, substitute the ciphertext letter C:

C = E([a, b], p) = (ap+b) mod 26

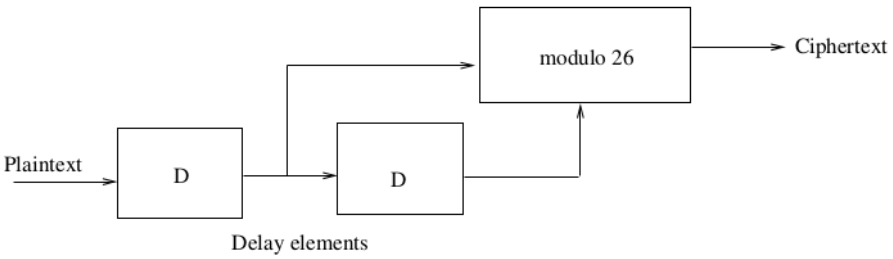
A basic requirement of any encryption algorithm is that it must be one-to-one. That is, if p $\neq$ q , then E(k, p) $\neq$ E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3.

(a) Are there any limitations on the value of b? Explain why or why not.
(b) Determine which values of a are not allowed.
(c) Provide a general statement of which values of a are and are not allowed. Justify your statement.

Exercise 7. Permutation Cipher (2pts)

Encrypt the message ***spyarrivesonthursday*** using the **double Transposition**. Choose Key1 and Key2 as your first and second name. (Ex.: anil mengi, then the Key1=anil and Key2=mengi).

Exercise 8. Vigenere Cipher (2pts)
Consider a Vigenere type of cipher with the encryption scheme given in figure.



(a) D represents the delay elements in time where C_i and P_i are the ciphertext and plaintext with the time index i. Write the encryption function from the figure.
(b) Determine the decryption function.
(c) Draw the equivalent decryption implementation.

THE END