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

# CRYPTOGRAPHY AND NETWORK SECURITY

Lab 1

Nguyen Phuong Vuong - 1614186

## Exercise 1.

(a) What can be the main drawback of the substitution cipher given above?
The main drawback of the substitution is encrypted the following messages using five-position to the left of the alphabet.
(b) Caesar cipher is an example of classical cryptosystem. Is this statement true? Why or why not?
True because Caesar cipher is a cryptosystem which are too weak nowadays, too easy to break, especially with computers. However, it is simple to illustrate and it is basic to understanding ideas of cryptography.
(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.
The emerging message is FISHING FRESH WATER BEND SADMITS WORD FISH RAND OVERWHELMING ANY DAY.

## Exercise 2.

The first plaintext is W and the first cipher-text is A and you apply the rule C = (M + K) mod 26, you will compute the KEY is 4. The same as computation above you will take message which is WORLD CUP.

## Exercise 3.

We have:
(ap + b) mod 26 = 1 (the position of 'B')
(ap + b) mod 26 = 20 (the position of 'U')
We guess e = 4, t = 19:
E([a,b], 0) = (a*4 + b) mod 26 = 1
E([a,b], 19) = (a*19 + b) mod 26 = 20
So a = 3, b = 15.

## Exercise 4.

What are two problems with the one-time pad?
1. There is the practical problem of making large quantities of random key. Any heavily used system might require millions of random characters on regular basis.
2. Even more daunting is the problem of key distribution and protection. Because the length of key and cipher-text are the same, it creates many problem such as hacker might find out key base on length of cipher-text.

## Exercise 5.

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

Plain-text: MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX
Cipher-text: UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ
- Plain-text is encrypted 2 letters at a time.
- In this instance, insert filler like 'x' in the final of the plain-text.
- If both letters fall in the same row, replace each with letter to right.
- If both letters fall in the same column, replace each with letter below it.
- Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

## Exercise 6.

(a) Are there any limitations on the value of b? Explain why or why not.
No. A change in the value of b shifts relationship between plain-text letters and cipher-text letters to the left or right, so that if the mapping is one-to-one, it remains one-to-one.
(b) Determine which values of a are not allowed.
The values of a which are not allowed are 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. Any values larger than 25 is equivalent a mod 26.

## Exercise 7.

Plain-text: spyarrivesonthursday
Key 1: spyarrive (columns)
Key 2: sonthursday (lines)
Cipher-text: SSRTIVEDHROARNUYYASP