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

Cryptography and Network Security Tutorial 1

Hieu Nguyen
huuhieubk@gmail.com

16/01/2017

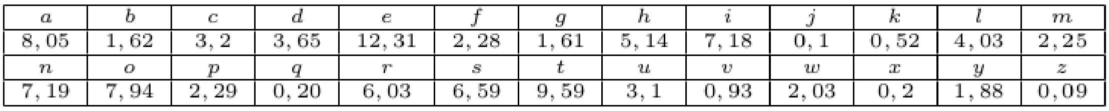
Basic Exercises

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:

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

(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?

(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.
```

Advanced Exercises

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

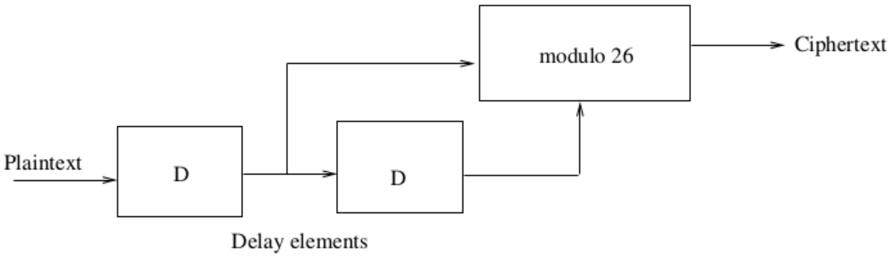
A basic requirement of any encryption algorithm is that it must be one-to-one. That is, if p $\neq$ q , then E(k, p) $\neq$ E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all 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