Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Tutorial 1

Hieu Nguyen

Ngày 27 tháng 1 năm 2015

Questions

Question 1. What is the difference between passive and active security threats?

Question 2. List and briefly define categories of passive and active security attacks.

Question 3. List and briefly define categories of security services.

Exercises

Exercise 1. 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 , then E(k, p)E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps i1. nto 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.

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

Exercise 2. A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Break this code.
Note: The language of the plain text was English.
Exercise 3. A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword CIPHER, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

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

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

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

This yields the sequence

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

Such a system is used in the following example.

Ciphertext:

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD
TSVP QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
```

Plaintext: it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Determine the keyword.

Exercise 4. 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.
```