Computer Sciences

University of Technology

Date: 28th May, 2012

Time: 3 Hr.

Lecturer: Dr. Hala Bahjat

Final Exam. 2011-2012

First trail

Subject: Cryptanalysis

Class: Fourth

Branch : Security

Note: choose five questions only

Q1) In the following the cipher text is obtained from affine method:

"NYLUYHVYNNYNYLU,....."

When you know that frequency of letters of cipher text is given in the following table:

characters	*No. of occurrences*
R	9 occurrences
K	7 occurrences
N,Y	4 occurrences
H,L	3 occurrences
F,S,V,U	2 occurrences

Find the plaintext and the keys that used to encrypt the cipher text?

(12 marks)

Q2)a- letter frequencies can be used to aid identification and solution in cryptogram, explain some basic consideration that should understood from letter frequencies in cryptanalysis.

b- Write complete algorithm that show cryptanalysis using letter frequency method.

(12 marks)

Q3) a- A keyword of length 3 is used in a polyalphabetic cipher with vigener table, where shift forward value are 1&2=6 , 1&3=20. What is the plaintext and keyword used, where ciphertext is: **GVSOJGPMJYUALELGSF**

b- Decrypt the following ciphertext, when you know that simple subsitiution(additive method) is used. The cipher text = **LTLXAALXC.**

(12 marks)

Q4) Suppose you obtain the following cipher text:

VOESA IVENE MRTNL EANGE WTNIM HTMEE ADLTR NISHO DWOEH

Note: you believe was encrypted using a keyword columnar transposition.

Please find the following:-

a- The plain text corresponding ciphertext.

b- The key that used.

c- Encrypt the following massage using the key that obtained in

The message is: **"GOOD LUCK TO ALL .**

(12 marks)

Q5) a- Write complete algorithm for Berlekamp-Massy and prove that the sequence=011 generate from LFSR polynomial $f(x)=1+x+x^2$.

b- Explain broad and related massage attacks with example .

(12 marks)

Q6) a- Explain in steps the Cryptanalysis method for 3-round of DES using *linear cryptanalysis* method (Known plain text attack) with block diagrams .

b- Find the key length from the following ciphertext using kasiski test:

" sarbghlmuopkhklnhlkulonhtrcxsarhjkoputlmbgghtrolpkjmncxhjbnhgf fgrtjkmaylopiulkjewqanbhjkdsaemaycdfrewqaxzsghjukloplmnbv".

(12 marks)

Computer Sciences

University of Technology

Date: 28th May, 2012

Time: 3 Hr.

Lecturer: Dr. Hala Bahjat

Final Exam. 2011-2012

First trail

Subject: Cryptanalysis

Class: Fourth

Branch : Security

Note: choose five questions only

Q1) In the following the cipher text is obtained from affine method:

"NYLUYHVYNNYNYLU,....."

When you know that frequency of letters of cipher text is given in the following table:

characters	*No. of occurrences*
R	9 occurrences
K	7 occurrences
N,Y	4 occurrences
H,L	3 occurrences
F,S,V,U	2 occurrences

Find the plaintext and the keys that used to encrypt the cipher text?

(12 marks)

Sol:

Additive key=5, multiplication key= 3, inverse the multiplication key=9

The plain text= **I hope to all good future.**

Q2)**a-** letter frequencies can be used to aid identification and solution in cryptogram, explain some basic consideration that should understood from letter frequencies in cryptanalysis.

b- Write complete algorithm that show cryptanalysis using letter frequency method.

Sol: Some basic considerations should be understood now.

a. In transposition systems, the letter frequencies of a cryptogram will be identical to that of the plaintext. A cryptogram in which the ciphertext letters occur with the expected frequency of plaintext will usually be enciphered by a transposition system.

b. In the simplest substitution systems, each plaintext letter has one ciphertext equivalent. The ciphertext letter frequencies will not be identical to the plaintext frequencies, but the same numbers will be present in the frequency count as a whole.

c. More complex substitution cipher systems, such as the polyalphabetic systems in ,will keep changing the equivalents. E might be enciphered by a K the first time it occurs and by different cipher letters each time it recurs. This will produce a very different looking frequency count.

d. Each one is a frequency count of the message listed above it. The four messages are different, but each has the same plaintext. The first shows the plaintext and its frequency count. The second shows the frequencies of the same message enciphered by a transposition system. The third shows a simple substitution system encipherment. The fourth shows a polyalphabetic substitution encipherment.

(12 marks)

Q3) a- A keyword of length 3 is used in a polyalphabetic cipher with vigener table, where shift forward value are 1&2=6 , 1&3=20. What is the plaintext and keyword used, where ciphertext is: **GVSOJGPMJYUALELGSF**

Sol: goo morning Iraq

b- Decrypt the following ciphertext, when you know that simple subsitiution(additive method) is used. The cipher text = **LTLXAALXC.**

Sol: M= we will win

(12 marks)

Q4) Suppose you obtain the following cipher text:

VOESA IVENE MRTNL EANGE WTNIM HTMEE ADLTR NISHO DWOEH

Note: you believe was encrypted using a keyword columnar transposition.

Please find the following:-

a- The plain text corresponding ciphertext.

b- The key that used.

c- Encrypt the following massage using the key that obtained in

The message is: **"GOOD LUCK TO ALL .**

Sol: Which we believe was encrypted using a keyword columnar transposition. Our goal is to recover the key and the plaintext. First, note that there are 45 letters in the ciphertext. Assuming the array is not a single column or row,

the array could have any of the following dimensions: 9 *x* 5. 5 x 9. 15 x 3 or 3 x 15. Suppose that we first try a 9 x 5 array. Then we have the ciphertext array in Table 1.1. We focus our attention on the top row of the array in Table 1.1. If we permute the columns as shown in Table 1.2, we see the word **GIVE** in the first row and we see words or partial words in the other rows. Therefore, we have almost certainly recovered the key. This method is somewhat ad hoc, but the process could be automated, provided we can automatically recognize likely plaintexts. In this example, we have recovered the encryption key 24013 and the plaintext is

GIVE ME SOMEWHERE TO STAND AND I WILL MOVE THE EARTH.

b- The key that used = 24013

(12 marks)

Q5) a- Write complete algorithm for Berlekamp-Massy and prove that the sequence=011 generate from LFSR polynomial $f(x)=1+x+x^2$.

Sol: Algorithm : Berlekamp- Massy

1- F(x)=1, B(x)=1, D=1, l=0, b=1, N=0

2- Read(n, sn)

3- If N=n then stop
Else compute
$d=sn+\sum_{i=1}^{l} ci.sn-i$

4- If d=0 , then D=D+1 go to 7

5- If d<>= and 2L>N then
$F(x)= f(x)+d/b.x^{D}.B(x)$
D=D+1 , and go to 7

6- If d<> 0 and 2l<= N then
$F(x)= f(x)+d/b.x^{D}.B(x)$
L=N+1-L
B(x)=T(x)
b=d
D=1

7- N=N+1 and return to step 3

Example : when apply sn=100 on the algorithm
$F(x)=1+x+x^2$

b- Explain broad and related massage attacks with example . **(12 marks)**

Q6) **a-** Explain in steps the Cryptanalysis method for 3-round of DES using *linear cryptanalysis* method (Known plain text attack) with block diagrams .

Sol : lectures no.7

b- Find the key length from the following ciphertext using kasiski test:
" sarbghlmuopkhklnhlkulonktrcxsarhjkoputlmbgghtrolpkjmncxhjbnhgf fgrtjkmaylopiulkjewqanbhjkdsaemaycdfrewqaxzsghjuklopimnbv".

Sol: key length= 4

(12 marks)