University of Technology
Computer Science Department
Class: رابع-فرع الامنيه
Time: 3 hours

Subject: تحليل شفره
Examiner: د.هاله بهجت عبد الوهاب

Final Exam / First Trail / 2010 -2011

Note: choose five questions only

Q1/ Suppose that you have received the following ciphertext:

" ***Rzp djee uhlhmhu icfi lr fawjth iz rzp jb***
Gehfbh uhfa js rzpu ljsa szi js rzpu hrhb zser "

Find the plaintext corresponding to the ciphertext , when you know that affine transformation is used and additive key=25. (14 marks)

Q2/ Find the shortest LFBSR generating the sequence: **Sn= 101000** , and draw the flowchart of Berlekamp-Massy algorithm.

(14 marks)

Q3/ a- A keyword of length **3** is used in a polyalphabetic cipher with vigener table, where the shift forword value are **1&2=6, 1&3=20**. What is the plaintext and the keyword that used , where ciphertext is: ***Ltti qzhp ….."Iw mfqf".***

b- Write complet algorithm that descript kasiski test method and find the key length from the following ciphertext using kasiski test:

" ***sarbghlmuopkhklnhlkulonhtrcxsarhjkoputlmbgghtrolpkjmncxhjbnhgf fgrtjkmaylopiulkjewqanbhjkdsaemaycdfrewqaxzsghjukloplmnbv".***

(14 marks)

Q*4/* **a-** Differential cryptanalysis it can be used in an attempt to crypt analyze 3-round DES. Using the following pairs of PT/CT to find the equations that help you to deduce the information about the key: **PT1=0001 0100, PT2=0011 0100, CT1=0111 1111, CT2=0001 1100.**

b- Explain broad and related massage attacks with example.

(14 marks)

Q*5/* **a-** Fermat's factorization is main factoring method used in RSA attacks, write two examples that show the method work.

b- Explain in steps the complete algorithm to Cryptanalysis for polyalphabetic method.

(14 marks)

Q*6/* **a-** Explain basic consideration that should understood from letter frequencies in cryptanalysis and roughness that appears in unilateral frequency distribution.

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

(14 marks)