Arab Academy for Science Technology and Maritime Transport
College of Computing and Information Technology

Course	**Computer System Security**
Course Code	**CS421**
Lecturer	**Prof. Dr Ayman Adel**
TA	**Maram Shouman, Menna Elmasry**

Sheet 2

Review Questions: (2 marks per each question)

1. Explain one time pad.
2. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2
3. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

Problems: (5 marks per each question)

1. Decrypt the following Cipher text
   i. Xly td detww esp xzde pieclzcotylcj nzxafepc zq lww
   ii. Hml qgmj xmlmjw af yggv zsfvk qgmj gof
2. Encrypt Jasper Fforde's words :"it remains, despite its non-existence, as one of the truly great wonders of Swindon",using playfair cipher with the keyword STZVLX
3. Encipher the following message using the Vigenere cipher and the keyword "IHS":
   1. There is a secret passage behind the picture frame
4. Encrypt the following message using Vignere Cipher with keyword "Security"
   i. The best way to predict your future is to create it
5. Repeat Q5 using the RailFence Cipher
6. Construct a Playfair matrix with the key largest.
7. Construct a Playfair matrix with the key occurrence. Make a reasonable assumption about how to treat redundant letters in the key.

8. Using this Playfair matrix

    i. M F H I/J K
    ii. U N O P Q
    iii. Z V W X Y
    iv. E L A R G
    v. D S T B C

    b. encrypt this message:

        1. Must see you over Cadogan West. Coming at once.

    c. Repeat part (a) using the Playfair matrix from Problem 9.

9. Using the Vigenère cipher, encrypt the word "explanation" using the key “leg”.

10. One of the transposition techniques is to write the message in rectangular row by row, and read the message off, column by column, but permute the order of columns. The order of columns becomes the key of the algorithm. It is required to implement the previous technique using a matrix of 6x6 to encrypt the following message using the key 431265.

    i. ARAB ACADEMY FOR SCIENCE AND TECHNOLOGY