King Saud University
College of Computer and Information Sciences
Department of Information Technology
IT324 Information Security
Assignment 1
1st semester 1443

كلية علوم الحاسب والمعلومات
قسم تقنية المعلومات

Instructions:

- Solve the assignment **individually**.
- Your work must be organized, comprehensible, and easy to read and follow.
- Submission should be **typed by computer, not handwritten**. Handwritten assignments are penalized **zero**
- **Answer all of the questions. Questions 1-3 have to be submitted.** Questions 4 and 5 solve it but don't submit it (it will be discussed during tutorial time.)
- Submission will be through LMS ***(Due Date: Monday Oct 11th at 7:30 a.m.)***

Question 1:

Vigenere cipher is another variation of Additive cipher. It just uses a keyword instead of a single key.

a) Consider the character set: "**a---z**" and key value: "**hash**".
Encrypt the following plaintext using Vigenere cipher:
Plaintext = "**yes we can**"
Show all the steps to the final ciphertext

b) Is Vigenere cipher monoalphabetic or polyalphabetic cipher? Justify your answer.

Question 2:

Considering the English alphabet, use Playfair cipher to encrypt the following plaintext= **"start"**

You have to create the secret key matrix as follows:

- First write the letters of the word **"sun"** in the second column of the five by five matrix starting from the upper left corner.
- Then finish filling the remaining cells of the matrix row by row with the remaining letters of the alphabet, in alphabetical order.
    - Notes:
        1. Put the letters **I** and **J** in one cell
        2. Follow the encryption steps in the textbook (Forouzan). Refer to page 71.

Show all the steps to the final ciphertext.

Question 3:

a. Let k = (2 4 1 3) be the decryption key used in a transposition cipher. What is the encryption key?

b. Encrypt the following plaintext: Good morning

Question 4:

Consider the alphabet set: “**a---z, $, (,) , % , 0---9**”. Fill the table with the required answers along with justifications. For details about cryptanalysis attacks, refer to textbook (Forouzan), chapter 3.

Cipher	**Key Domain**	**Resistant to Brute Force Attack? Why?**	**Resistant to statistical Attack? Why?**	**Monoalphabetic or Polyalphabetic?**
Additive				
Transposition cipher				
Playfair				

Question 5:

We discussed in the lecture that using one-time pad, if the plaintext is made of 0’s, the ciphertext will be equal to the key, which is random.

What is the pattern of the ciphertext of **one-time pad** cipher in each of the following cases? (for each case, show an example with all steps and specify for each case whether the resulted ciphertext is random or not):

1. The plaintext is made of 1’s (e.g. 11111111111...).
2. The plaintext is made of alternating 0’s and 1’s (e.g. 0101010101...)
3. The plaintext is a random string of bits.