Quiz-1
Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Each question part carries 2 marks. Please upload your answers in Microsoft Teams by **18/09/2020**. Your **Roll No.** and **Name** must be mentioned.]

1. (a) Use the Vigenère cipher with key **mole** to encrypt the string of plaintext: **two minutes until alarm sounds**.

   (b) Decrypt the following ciphertext that came from the Vigenère cipher with key **timbucktu** :

   UZUOAIHOKVUHBDOCLQAOAYZAEME $[2 \times 2 = 4]$

2. (a) Use the Playfair cipher with key **diskjockey** to encrypt the string of plaintext : **lay low until friday**.

   (b) Decrypt the following ciphertext that came from the Playfair cipher of part (a):

   REBSLUMNGYXYNBLFCR $[2 \times 2 = 4]$

3. (a) Using the affine cipher with key $(\alpha, \beta) = (5, 8)$, encrypt the plaintext message "**code blue alert**".

   (b) Use the above affine cipher to decrypt the following ciphertext message: **CJISEIZCZRCFPCUWXCVZ**.

   (c) A ciphertext is given along with a portion of the plaintext. An affine cipher of the form $\phi_{\alpha,\beta} : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} :: \phi_{\alpha,\beta}(x) \equiv \alpha x + \beta (\text{mod } 26)$ was used for encryption. Indicate whether the key can be uniquely determined mathematically from the given information. Explain why this is or is not possible; if possible, perform the decryption.

Ciphertext: **QMBUOBPXMDDYL**,
Plaintext: * * **n s** * * * * * * * * * $[3 \times 2 = 6]$

4. (a) Use the Hill cipher with encryption matrix $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ to encrypt the string of plaintext : **the phone is bugged**.

   (b) Decrypt the following ciphertext that was encrypted using the Hill cipher of part (a).
   Ciphertext: **PSAALAXGKXWAPZHKRZLYC**

   (c) A ciphertext is given below along with a portion of the plaintext. The Hill cryptosystem was used for encryption and the size of the encrypting matrix is also provided. Indicate whether the key (the encoding matrix) can be uniquely determined mathematically from the given information. Explain why this is or is not possible; if possible, perform the decryption.

   - A 2×2 encoding matrix was used.

   Ciphertext : **I G H O E S Z W J F P I T W B M L L P O F R X J O R T J Z I**
   Plaintext: * * * **r e o u** * * * * * **e r** * * * * **e l** * * * * * * * * **e** * $[3 \times 2 = 6]$