22CS401 – Cryptography and Network Security
III B.Tech I Semester
Module Bank - 1

1. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
   a. A student maintaining a blog to post public information.
   b. An examination section of a university that is managing sensitive information about exam papers.
   c. An information system in a pathological laboratory maintaining the patient's data.
   d. A student information system used for maintaining student data in a university that contains both personal, academic information and routine administrative information (not privacy related). Assess the impact for the two data sets separately and the information system as a whole.
   e. A University library contains a library management system which controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.

2. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C:
   $$C = E([a, b], p) = (ap + b) \bmod 26$$
   A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3,
   then E([a, b], 0) = E([a, b], 13) = 3.
   a. Are there any limitations on the value of b? Explain why or why not.
   b. Determine which values of a are not allowed.
   c. Provide a general statement of which values of *a* are and are not allowed. Justify your statement.

3. Using this Playfair matrix:

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

   Encrypt this message:
   "I only regret that I have but one life to give for my country"
   a. 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.
   b. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

4. Consider a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first eight round keys, k1, k2, c k8, and then sets

   k9 = k8, k10 = k7, k11 = k6, ……., k16 = k1

   Suppose you have a ciphertext c. Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the device are not known to you and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)

5. Using S-DES, decrypt the string 01000110 using the key 1010000010 by hand. Show intermediate results after each function (IP, FK, SW, FK, IP-1). Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2 (i.e., A = 0000, B = 0001, c, P = 1111). Hint: As a midway check, after the xoring with K2, the string should be 11000001.

6. Compute the output of the MixColumns transformation for the following sequence of input bytes "A1 B2 C3 D4." Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from "A1" to "A3" perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output.

7. Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.
   a. XOR of subkey material with the input to the f function
   b. XOR of the f function output with the left half of the block
   c. f function
   d. permutation P
   e. swapping of halves of the block

8. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption? For the ECB, CBC, and CFB modes, the plaintext must be a sequence of one or more complete data blocks (or, for CFB mode, data segments). In other words, for these three modes, the total number of bits in the plaintext must be a positive multiple of the block (or segment) size. One common method of padding, if needed, consists of a 1 bit followed by as few zero bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?

9. a. In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M?
   b. In an RSA system, the public key of a given user is e = 65, n = 2881. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).

If each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

10. Analyse the design principles and security properties of the RSA algorithm, including its key generation and encryption/decryption processes. Compare the security levels of elliptic curve cryptography (ECC) and RSA, and the advantages of ECC in terms of key size and computational efficiency.