Guideline

File 01. Overview of Cryptography:

1. Define cryptography. List four main objectives of modern cryptography. Briefly discuss the parts of a cryptographic system.
2. Illustrate the general idea behind symmetric-key and asymmetric-key cryptography.
3. Differentiate between symmetric-key and asymmetric-key cryptography.
4. How does asymmetric-key cryptography provide message confidentiality and prove the authenticity of the message originator?
5. What services are provided by cryptography? What is Three Pass protocol? Give an illustration.

File 02. Mathematics for Cryptography:

1. Define binary operation with example. Why division is not a binary operation?
2. Find the result of the following operations:
   (i) 0 mod 35, (ii) -4 mod 7, (iii) 15 mod 27, (iv) 57 mod 19
3. What does Z, Z_{12} and Z^{*}_{12} mean?
4. How to express the following set of integers?
   (i) Set of all integers
   (ii) Set of all positive/ negative integers
   (iii) Set of all non-negative/ non-positive integers
   (iv) Set of integers ranging from zero to 100
   (v) Set of integers who have multiplicative inverse in 10 modulus
5. When integers ***a*** and ***b*** are coprimes or mutually primes? Determine the GCD of 24 and 48 using Euclidean Algorithm.
6. Assume that ***A*** and ***B*** are two integers in ***N*** modulus. Write the appropriate condition such that -
   i) ***A*** is the multiplicative inverse of ***B***.
   ii) ***A*** is the additive inverse of ***B***.
7. What do you mean by *additive inverse* and *multiplicative inverse* of an integer? Determine the multiplicative inverse of 31 in Z_{33} using Extended Euclidean Algorithm/ Does multiplicative inverse of 5 exist in 15 modulus? Why or why not?
8. Find the number of elements in $Z*_{25}$ / $Z*_{23}$ / $Z*_{33}$ using Euler's Phi-Function.

File 04. DES & RSA Cryptosystem:

1. What is DES? Draw the function block diagram of DES algorithm.
2. Describe four stages of round function f(x,k) used in DES.
3. What do you mean by Feistel and Non-Feistel ciphers? Give examples.
4. What do you mean by Confusion and Diffusion?
5. What is RSA? Briefly describe three steps involved in RSA algorithm with an illustration.
6. What is P-Box and S-Box? An S-Box used for encryption is given below. If an input to this S-box is 1111, then what is the output?

		LSBs of Input			
		00	01	10	11
MSBs of Input	00	0001	0101	0100	1101
	01	1011	1000	1110	0010
	10	1010	1111	0110	0000
	11	1100	0111	1001	0011

File 05. Digital Signature & Cryptographic Hash Function (1 Set of Question)

1. Define digital signature. State the general idea behind it. Why is it needed?
   Illustrate the process of signing and verification used in digital signature.
2. What three purposes are served by a digital signature? Differentiate between conventional signature and digital signature.
3. Differentiate between (i) conventional signature and digital signature (ii) MAC Algorithm and Hash Algorithm (iii) Digital Signature and Cryptosystem
4. What is hashing and hash function? What are the importance of hash function? List two widely used hash functions used in cryptography.
5. Briefly describe some desirable properties a cryptographic hash function should have.

File 06. Traditional Transposition Ciphers

1. Define transposition cipher. What are the various types of transposition ciphers?
2. Encrypt the message 'we are facing new difficulties' using keyless transposition cipher. Check your answer by decrypting the message after encryption.
3. An encryption key is given as 2 5 4 3 6 1. Determine the corresponding decryption key. Encrypt the message 'set up the bomb' using keyed transposition cipher. Check your answer by decrypting the message after encryption. [use encryption and decryption keys found previously]
4. Encrypt the message "we love our country" using Columnar transposition cipher with the help of given key.

File 07. Traditional Substitution Ciphers

1. Define two classes of traditional symmetric-key ciphers?
2. Define monoalphabetic and polyalphabetic ciphers with example. Suppose you want to encrypt a message using 47 modulus. What will be the possible key domain if Affine cipher is used?
3. Differentiate between- i) Additive Cipher and Autokey Cipher ii) Additive Cipher and Vigenere Cipher
4. Given some traditional ciphers. Identify which are monoalphabetic and polyalphabetic?
   Affine cipher, Hill cipher, Additive cipher, Autokey cipher, Multiplicative cipher,
   Playfair cipher, Caesar cipher, Vigenere cipher.
5. Encrypt the message 'bogus' using the following ciphers. (Ignore the space between words, and use modulo 26). Decrypt the message to get the original plaintext.
   (a) Multiplicative cipher with key = 15
   (b) Playfair cipher with the key created in the text.
   (c) Additive cipher with key = 23
   (d) Autokey cipher with key = 14