Unit-1

1) Find g.c.d(252,198) by Euclidean Algorithm.
2) Find the inverse of 3 mod 5.
3) Define Euler Tuotient function. Find (32).
4) State Euler's criteria for quadratic residue mod prime. Verify whether 2 is a quadratic residue mod 13.
5) Find the quadratic residue mod 5.
6) State Law of Quadratic Reciprocity.
7) Find the value of $3^{31}(\text{mod } 7)$ by applying Fermat's Little theorem.
8) Show that 8 is a Quadratic residue mod 17.
9) Find an x between 0 and 19 such that $x^2 \equiv 5\,(\text{mod}\,19)$.
10) Find $\varphi(125)$, where $\varphi(n)$ is Euler 'Phi" function of an integer "n".
11) Explain Euclidean Algorithm. Write the g.c.d(1547,560) as linear combination of 1547 and 560.
12) Distinguish between Legendre Symbol and Jacobi Symbol. Find $\left(\frac{1999}{2315}\right)$.
13) Find the remainder when 24^{1947} is divided by 17 by using Fermat's Little theorem.
14) Express the G.C.D of (726, 275) in the form of *m*726+*n*275, where *m* and *n* are any integers and find the values of *m* and *n*.
15) Suppose a and n are relatively prime such that g.c.d(a, n)=1, prove that

    a) If $x^2 \equiv a$ (mod n) has a solution then $\left(\frac{a}{n}\right) = 1$.

    b) If $\left(\frac{a}{n}\right) = 1$, we cannot conclude that $x^2 \equiv a$ (mod n) has solutions.

16) State and Prove Fermat's Theorem.
17) State and Prove Chinese Remainder Theorem.
18) Explain Miller-Rabin Algorithm. Test the primality of 561.
19) Using Chinese Remainder Theorem solve the following congruence's x≡1 (mod 3), x≡1 (mod 4), x≡1 (mod 5) and x≡0 (mod 7).
20) Solve $x \equiv 3(\text{mod } 4)$, $x \equiv 1(\text{mod } 5)$, $x \equiv 2(\text{mod } 3)$ by using Chinese Remainder theorem.

Unit-2

1) Construct a Playfair matrix with the key "*largest*".

2) What are two problems with the one-time pad?

3) Differentiate between a monoalphabetic cipher and a polyalphabetic cipher.

4) Distinguish between a substitution cipher and a transposition cipher.

5) What is "Symmetric encryption":

6) Briefly define the Caesar cipher.

7) Briefly define the monoalphabetic cipher.

8) Briefly define the Playfair cipher.

9) Construct a Playfair matrix with the key "*occurrence*". Make a reasonable assumption about how to treat redundant letters in the key.

10) What is encryption and decryption?

11) Differentiate between Transposition Cipher and Substitution Cipher. Apply two stage (Double) transposition cipher on the text " meet me soon".

12) Discuss the substitution techniques?

13) Describe the monoalphabetic ciphers in detail.

14) Explain the symmetric cipher model.

15) What is Vigenere Ciphers?

16) Discuss about the Hill Ciphers?

17) **a).** Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is full of surprises".

b). The cipher ext "VHFUHW" has been generated with the Caesar cipher. Determine the plain text with the key k=3.

18) Use the Playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.

19) Encrypt the message "meet me" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.

20) Use the Hill cipher with matrix $\begin{pmatrix} 3 & 2 \\ 13 & 1 \end{pmatrix}$ to encrypt the message *"GOLD*".

Unit-3

Short answer questions

1. What are the operations used in AES?
2. Write down the purpose of S-boxes in DES.
3. What are the operations used in AES?
4. Name the 5 block cipher modes of operation.
5. Which two algorithms are used in RC4?
6. With a neat diagram, show the Classical Feistel Cipher structure for encryption.
7. Draw the general structure of Data Encryption Standard(DES).
8. Using stream cipher technique encrypt the data 11010111 with the key 01010110.
9. What is the role of IP in DES algorithm?
10. What type of encryption is RC4?

Essay Questions

1. With a neat diagram, describe Classical Feistel Cipher structure for encryption and decryption.
2. Explain Stream cipher and block cipher in detail.
3. What is RC4? Explain the two algorithms used in RC4.
4. Explain any two block cipher modes of operations.
5. Explain the overall structure of AES encryption process.
6. Explain the general structure of Data Encryption Standard(DES).
7. Explain RC4 algorithm.
8. Explain Data Encryption Standard(DES) algorithm .
9. Define Stream cipher. Explain RC4 algorithm.
10. Write the different Cipher block modes of operation. Explain any two in detail.

Unit-4

1) In RSA algorithm find private key if the public key is (e, n) where p & q are primes with 1<e<ϕ(n).
2) Using Diffie-Hellman key exchange find the common key 'k' with p=353, α=3, a=97 & b=233.
3) Using RSA algorithm, find the public key if the private key is (7,33) for p=3 and q=11.
4) Define one-way function.
5) Write applications of public key cryptosystems.
6) Define Probabilistic encryption.
7) Using Diffie-Hellman key exchange find the common key 'k' with p=7, α=5, X_A=3 & X_B=4.
8) Define Public-key cryptography.
9) What are the two basic principles of public-key cryptosystem?
10) Define trap-door one-way function.
11) Explain about Public Key Cryptography.
12) Explain about RSA Algorithm.
13) Explain about Diffie-Hellman Key Exchange Algorithm.
14) Explain about Elliptic Curve Cryptosystem.
15) Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q= 17 and a primitive root α = 5.
    a. If Alice has a private key X_A = 9, find her public key *YA*.
    b. If Bob has a private key X_B= = 8, find his public key *YB*.
    c. What is the shared secret key between Alice and Bob?
16) Write Diffie-Hellman Key exchange algorithm. Using Diffie-Hellman key exchange algorithm, find the common key 'k' with p=29, α=2, X_A=11 & X_B=19.
17) Write RSA Algorithm. In RSA algorithm find private key if the public key is (7, 187) where p =17 and q=11.
18) Perform encryption and decryption using RSA algorithm for the plain text 'NO' with encipher key (public key) (n,e) = (77, 19) where p=11 and q=7.
19) What is Elliptic Curve Cryptography? Explain in detail about encryption and decryption in ECC.
20) Write and explain five possible approaches to attack the RSA algorithm.

Unit-5

1. What is Message Authentication Code(MAC)?
2. What is Message authentication?
3. What is Message digest?
4. Distinguish between a Hash function and a Hash value.
5. Comment on the statement ” Cryptographic hash function is a one-way function.”
6. Draw a neat diagram where authentication is tied to plaintext w.r.t. MAC.
7. Draw a neat diagram where authentication is tied to ciphertext w.r.t. MAC.
8. Distinguish between the collision free property and one-way property of a hash function?
9. What is Digital signature? Why is it used in cryptography?
10. Write the difference between RSA algorithm and DSA.
11. Explain about cryptographic Hash functions.
12. Explain about Message Authentication functions
13. Define MAC. Write the requirements for Message Authentication codes.
14. List the type of attacks and forgeries in Digital Signatures.
15. Write applications of cryptographic Hash functions.
16. Explain the two approaches to digital signatures with a neat diagram.
17. Explain different methods to provide authentication using Hash functions.
18. Write briefly about (a) Message Authentication Code(MAC) (b) Hash function (c) Message digest (d) digital signature
19. Explain about Digital signature and also write the Digital signature requirements.
20. Explain about DSA with diagram.