	UNIT-I / PART-A
1	List the types of security attacks with examples.
2	Decipher the following cipher text using brute force attack: CMTMROOEOORW (Hint : Algorithm – Railfence)
3	What are diffusion and confusion in cryptography?
4	Apply Miller Rabin primality testing to determine whether 221 is prime.
5	Find GCD (21,300) using Euclid's Algorithm.
6	Define Steganography.
7	Why modular arithmetic has been used in cryptography?
8	What is discrete logarithm problem?
	UNIT-I / PART-B (Any Four)
1	Explain any two classical ciphers and describe their security limitations.
2	i)Find the solution to the following equations $X \equiv 2 \bmod 3$ $X \equiv 3 \bmod 5$ $X \equiv 2 \bmod 7$ ii) Write short notes on brute force attacks and crypt analysis.
3	i) Explain in detail about the relationships between the security services and security mechanism. ii) Brief about OSI Security architecture and network security model.
4	Write short notes on i) Fermat's and Euler's theorem ii) Chinese Remainder theorem.
5	Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text. K = 17 17 5 21 18 21 2 2 19
	UNIT-II / PART-A
1	Write short notes on triple DES.
2	Mention the need and parameters for AES.
3	What are the disadvantages with ECB mode of operation?
4	State the cons and pros of RSA algorithm over Elliptic Curve Cryptography.
5	What requirements must a public key cryptosystem to fulfill a secured algorithm?
6	Specify the security issues in Elliptic Curve Cryptography.
7	In a public key system using RSA, you intercept the cipher text C= 15 sent to a user whose public key is e = 9, n = 45, What is the plain text M?

8	What is the purpose of S- box in DES?
	UNIT-II / PART-B
1	Explain DES structure including key generation phase. Also explain the modes of operations.
2	Explain – RSA crypto system with the following values P= 7 q = 13 e = 5 and M = 10 . Mention the possible attacks on RSA.
3	Explain diffie-Hellman key exchange algorithm with an example . consider a Diffie- Hellman scheme with a common prime q = 353 and a primitive root α = 3. Users A and B have private keys Xa = 17 , Xb= 21 respectively. What is the shared secret key K1 and K2?
4	How a data can be encrypted using ECC? Explain with an example.

	UNIT-III / PART-A
1	Define hashing function.
2	How digital signature is different from conventional?
3	What are the schemes of MAC where authentication is tied to plain text and authentication is tied to cipher text?
4	What requirements should a digital signature scheme should satisfy?
5	What is a message digest?
6	What is the role of a compression function in a hash function?
7	What are the two approaches of digital signature?
8	What types of attacks are addressed by message authentication?
	UNIT – III / PART-B
1	While communicating across a network what are the authentication requirements and what are the authentication functions to produce an authentication? Discuss.
2	What are the properties of hashing function in cryptography? Explain Secure Hash Algorithm.(SHA)
3	i) Describe MD5 algorithm in detail. Compare its performance with SHA-1 ii) Explain the concept of message digest and digital signature on online fund transfer.
4	i) Explain Elgamal digital signature procedure with suitable example. ii) Explain the need for DSA compared to ElGamal digital signature procedure. Explain the creation and verification procedures of signatures in DSA.
	UNIT-IV / PART-A
1	What is X.509 certificate and its revocation?
2	Specify the requirements of Kerberos.
3	Differentiate spyware and virus.
4	What is the advantage of Intrusion detection system over firewall?
5	Differentiate macro virus and boot virus.
6	What are three threats associated with user authentication over a network or Internet?
7	List and briefly define three classes of intruders.

8	List three design goals for a firewall.

	UNIT-IV/PART-B
1	Explain the characteristics and types of firewalls
2	i) Explain – kerberos authentication procedure. ii) Describe any one advanced anti-virus technique in detail.
3	Explain Statistical anomaly detection and rule based intrusion detection.
4	i) Explain in detail about trusted systems. ii) Explain the format of the X.509 Certificate.
	UNIT-V/PART-A
1	What is PKI?
2	What is the difference between transport mode and tunnel mode?
3	What are the protocols used to provide IP Security?
4	What is PGP and list out its services?
5	Expand and define SPI.
6	Write short notes on SET.
7	List and briefly define the parameters that define an SSL session state.
8	What is a dual signature and what is its purpose?
	UNIT-V / PART-B
1	i)With a neat sketch explain the architecture of IPSEC. ii)Explain the hand shake protocol actions of SSL.
2	Explain in detail about Pretty Good Privacy in detail.
3	Explain about S/MIME in detail.
4	i)Explain in detail about web security ii) Brief – SSL and TLS