

SRM Nagar, Kattankulathur – 603 203.

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK



III SEMESTER

PMC503 CRYPTOGRAPHY AND CYBER SECURITY

Regulation – 2024

Academic Year 2026- 2027

Prepared by

Dr. K. Ponmozhi, Associate Professor



SRM VALLIAMMAI ENGINEERING COLLEGE

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

SUBJECT : PMC503 - CRYPTOGRAPHY AND CYBER SECURITY

SEM / YEAR: III/2026-27

UNIT I INTRODUCTION TO SECURITY				
Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.				
Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define Computer Security.	BTL -1	Remembering	CO 1
2.	What is the OSI Security Architecture?	BTL -1	Remembering	CO 1
3.	Define Security Attack.	BTL -1	Remembering	CO 1
4.	What are passive attacks?	BTL -1	Remembering	CO 1
5.	What are active attacks?	BTL -1	Remembering	CO 1
6.	Define Security Service.	BTL -1	Remembering	CO 1
7.	What is a Security Mechanism?	BTL -1	Remembering	CO 1
8.	Define Network Security Model.	BTL -1	Remembering	CO 1
9.	What is substitution cipher?	BTL -1	Remembering	CO 1
10.	Define transposition cipher.	BTL -1	Remembering	CO 1
11.	What is Steganography?	BTL -1	Remembering	CO 1
12.	Define Cryptanalysis.	BTL -1	Remembering	CO 1
13.	What is Product Cryptosystem?	BTL -1	Remembering	CO 1
14.	Differentiate between active and passive attacks.	BTL -2	Understanding	CO 1
15.	Distinguish between substitution and transposition techniques.	BTL -2	Understanding	CO 1

16.	Explain the purpose of confidentiality in network security.	BTL -2	Understanding	CO 1
17.	Why is authentication important in computer security?	BTL -2	Understanding	CO 1
18.	Explain the role of security mechanisms in protecting information.	BTL -2	Understanding	CO 1
19.	Compare encryption and steganography.	BTL -2	Understanding	CO 1
20.	Explain the concept of perfect security.	BTL -2	Understanding	CO 1
21.	How does information theory relate to cryptography?	BTL -2	Understanding	CO 1
22.	Explain why product ciphers are more secure than simple ciphers.	BTL -2	Understanding	CO 1
23.	Describe the objectives of network security.	BTL -2	Understanding	CO 1
24.	Explain the relationship between security services and security mechanisms.	BTL -2	Understanding	CO 1
25.	Give an example of cryptanalysis and explain its purpose.	BTL -2	Understanding	CO 1
PART – B				
1.	Apply the OSI Security Architecture to classify various security services and mechanisms used in an online banking system.	BTL -3	Applying	CO 1
2.	Apply the network security model to explain secure communication between two organizations.	BTL -3	Applying	CO 1
3.	Illustrate the Caesar cipher encryption and decryption process using a suitable example.	BTL -3	Applying	CO 1
4.	Encrypt and decrypt a message using the Playfair cipher with a suitable key.	BTL -3	Applying	CO 1
5.	Apply the Hill cipher algorithm to encrypt a given plaintext.	BTL -3	Applying	CO 1
6.	Demonstrate the encryption and decryption process using the Rail Fence transposition cipher.	BTL -3	Applying	CO 1
7.	Apply the Columnar Transposition technique to encrypt a given message.	BTL -3	Applying	CO 1
8.	Demonstrate how steganography can securely hide information within an image.	BTL -3	Applying	CO 1
9.	Apply product cipher principles to improve the security of a simple substitution cipher.	BTL -3	Applying	CO 1

10.	Apply information theory concepts to determine the security strength of a cryptographic system.	BTL -3	Applying	CO 1
11.	Analyze the different types of security attacks with suitable real-world examples.	BTL -4	Analyzing	CO 1
12.	Analyze the OSI Security Architecture and explain how it addresses network security requirements.	BTL -4	Analyzing	CO 1
13.	Compare and analyze various security services and mechanisms in terms of their effectiveness.	BTL -4	Analyzing	CO 1
14.	Analyze the advantages and limitations of substitution and transposition ciphers.	BTL -4	Analyzing	CO 1
15.	Compare classical encryption techniques with modern cryptographic techniques.	BTL -4	Analyzing	CO 1
16.	Analyze the concept of perfect security using the One-Time Pad.	BTL -4	Analyzing	CO 1
17.	Analyze the role of information theory in evaluating cryptographic security.	BTL -4	Analyzing	CO 1
18.	Compare steganography and cryptography with respect to security, applications, and limitations.	BTL -4	Analyzing	CO 1

UNIT II SYMMETRIC CIPHERS

Number theory – Algebraic Structures – Modular Arithmetic - Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudo random Number Generators – RC4 – Key distribution.

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define Number Theory.	BTL -1	Remembering	CO 2
2.	What is Modular Arithmetic?	BTL -1	Remembering	CO 2
3.	State Euclid's Algorithm.	BTL -1	Remembering	CO 2
4.	Define Congruence relation.	BTL -1	Remembering	CO 2
5.	What is a Group?	BTL -1	Remembering	CO 2
6.	Define Ring.	BTL -1	Remembering	CO 2
7.	Define Field.	BTL -1	Remembering	CO 2
8.	What is a Finite Field?	BTL -1	Remembering	CO 2
9.	What is the identity element in a group?	BTL -1	Remembering	CO 2
10.	Define multiplicative inverse.	BTL -1	Remembering	CO 2

11.	Differentiate between a Group and a Ring.	BTL -2	Understanding	CO 2
12.	Explain the significance of Modular Arithmetic in Cryptography.	BTL -2	Understanding	CO 2
13.	Why is Euclid's Algorithm used in cryptography?	BTL -2	Understanding	CO 2
14.	Explain the properties of finite fields.	BTL -2	Understanding	CO 2
15.	Distinguish between prime fields and extension fields.	BTL -2	Understanding	CO 2
16.	Explain matrix representation in modular arithmetic.	BTL -2	Understanding	CO 2
17.	Why are congruence relations important in encryption?	BTL -2	Understanding	CO 2
18.	Explain the closure property of algebraic structures.	BTL -2	Understanding	CO 2
19.	Expand SDES and DES.	BTL -1	Remembering	CO 2
20.	What is a Block Cipher?	BTL -1	Remembering	CO 2
21.	What is Differential Cryptanalysis?	BTL -1	Remembering	CO 2
22.	What is Linear Cryptanalysis?	BTL -1	Remembering	CO 2
23.	Define RC4.	BTL -1	Remembering	CO 2
24.	What is a Pseudo Random Number Generator (PRNG)?	BTL -1	Remembering	CO 2
25.	What is Key Distribution?	BTL -1	Remembering	CO 2
PART -B				
1.	Apply Euclid's Algorithm to find the GCD of two given integers and explain each step.	BTL -3	Applying	CO 2
2.	Solve modular arithmetic problems involving addition, subtraction, multiplication, and division.	BTL -3	Applying	CO 2
3.	Demonstrate how congruence relations are used to solve modular equations.	BTL -3	Applying	CO 2
4.	Construct examples of Groups, Rings, and Fields and verify their properties.	BTL -3	Applying	CO 2
5.	Apply finite field arithmetic in cryptographic computations.	BTL -3	Applying	CO 2
6.	Perform SDES encryption and decryption for a given plaintext and key.	BTL -3	Applying	CO 2
7.	Illustrate the DES encryption process with a neat block diagram.	BTL -3	Applying	CO 2

8.	Apply various DES modes of operation (ECB, CBC, CFB, OFB, CTR) for secure communication.	BTL -3	Applying	CO 2
9.	Generate pseudo-random numbers using a suitable PRNG algorithm.	BTL -3	Applying	CO 2
10.	Illustrate RC4 key scheduling and stream generation with an example.	BTL -3	Applying	CO 2
11.	Explain the concepts of Groups, Rings, Fields, and Finite Fields with suitable examples. Discuss their applications in modern cryptography.	BTL -4	Analyzing	CO 2
12.	Describe the DES algorithm with a neat diagram and explain each round of encryption. Discuss why DES is no longer considered fully secure.	BTL -4	Analyzing	CO 2
13.	Explain different Block Cipher Modes of Operation (ECB, CBC, CFB, OFB, and CTR). Compare their advantages, disadvantages, and applications.	BTL -4	Analyzing	CO 2
14.	Explain Differential Cryptanalysis and Linear Cryptanalysis in detail. Compare both attack methods and discuss how modern block ciphers resist these attacks.	BTL -4	Analyzing	CO 2
15.	Compare Euclid's Algorithm and Extended Euclid's Algorithm with suitable examples.	BTL -4	Analyzing	CO 2
16.	Analyze the internal architecture of DES and discuss its strengths and weaknesses.	BTL -4	Analyzing	CO 2
17.	Compare Differential and Linear Cryptanalysis techniques.	BTL -4	Analyzing	CO 2
18.	Analyze the design principles of block ciphers.	BTL -4	Analyzing	CO 2

UNIT – III ASYMMETRIC CRYPTOGRAPHY

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -- Elliptic curve arithmetic – Elliptic curve cryptography.

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define a prime number.	BTL-1	Remembering	CO 3
2.	What is primality testing?	BTL-1	Remembering	CO 3
3.	Define factorization.	BTL-1	Remembering	CO 3
4.	State Euler's Totient Function.	BTL-1	Remembering	CO 3

5.	State Fermat's Little Theorem.	BTL-1	Remembering	CO 3
6.	State Euler's Theorem.	BTL-1	Remembering	CO 3
7.	What is the Chinese Remainder Theorem (CRT)?	BTL-1	Remembering	CO 3
8.	Define modular exponentiation.	BTL-1	Remembering	CO 3
9.	What is a discrete logarithm?	BTL-1	Remembering	CO 3
10.	Define multiplicative inverse in modular arithmetic.	BTL-1	Remembering	CO 3
11.	What is a composite number?	BTL-1	Remembering	CO 3
12.	Define relatively prime numbers.	BTL-1	Remembering	CO 3
13.	Explain the significance of prime numbers in public-key cryptography.	BTL-2	Understanding	CO 3
14.	Differentiate between primality testing and factorization.	BTL-2	Understanding	CO 3
15.	Why is Euler's Totient Function important in RSA?	BTL-2	Understanding	CO 3
16.	Explain the application of Fermat's Little Theorem in cryptography.	BTL-2	Understanding	CO 3
17.	Describe the purpose of the Chinese Remainder Theorem in RSA computations.	BTL-2	Understanding	CO 3
18.	Explain why modular exponentiation is preferred over ordinary exponentiation in cryptography.	BTL-2	Understanding	CO 3
19.	Compare Euler's Theorem and Fermat's Little Theorem.	BTL-2	Understanding	CO 3
20.	Explain the computational difficulty of the discrete logarithm problem.	BTL-2	Understanding	CO 3
21.	Define RSA cryptosystem.	BTL-1	Remembering	CO 3
22.	What is Diffie–Hellman Key Exchange?	BTL-1	Remembering	CO 3
23.	Define key management.	BTL-1	Remembering	CO 3
24.	What is Elliptic Curve Cryptography (ECC)?	BTL-1	Remembering	CO 3
25.	Define elliptic curve arithmetic.	BTL-1	Remembering	CO 3
PART –B				
1.	Apply Fermat's Little Theorem to solve modular exponentiation problems.	BTL-3	Applying	CO 3
2.	Calculate Euler's Totient Function for given integers and demonstrate its application in cryptography.	BTL-3	Applying	CO 3

3.	Solve congruence equations using the Chinese Remainder Theorem.	BTL-3	Applying	CO 3
4.	Perform modular exponentiation using the square-and-multiply algorithm.	BTL-3	Applying	CO 3
5.	Generate RSA public and private keys for given prime numbers.	BTL-4	Analyzing	CO 3
6.	Demonstrate RSA encryption and decryption using a numerical example.	BTL-3	Applying	CO 3
7.	Apply the Diffie–Hellman Key Exchange algorithm to establish a shared secret key.	BTL-3	Applying	CO 3
8.	Perform point addition and point doubling operations on an elliptic curve.	BTL-4	Analyzing	CO 3
9.	Apply Elliptic Curve Cryptography (ECC) to encrypt and decrypt a message.	BTL-3	Applying	CO 3
10.	Demonstrate RSA key generation using Euler's Totient Function and modular inverse.	BTL-3	Applying	CO 3
11.	Explain the RSA cryptosystem with a neat block diagram. Describe the key generation, encryption, and decryption processes using a suitable numerical example.	BTL-3	Applying	CO 3
12.	Describe the Diffie–Hellman Key Exchange algorithm with an example. Explain its working, advantages, limitations, and applications in secure communication.	BTL-3	Applying	CO 3
13.	Explain Elliptic Curve Cryptography (ECC) in detail. Discuss elliptic curve arithmetic, point addition, point doubling, and compare ECC with RSA.	BTL-3	Applying	CO 3
14.	Analyze the mathematical principles that ensure the security of RSA.	BTL-4	Analyzing	CO 3
15.	Compare primality testing algorithms with integer factorization methods.	BTL-4	Analyzing	CO 3
16.	Analyze the advantages and limitations of Fermat's and Euler's Theorems in cryptographic applications.	BTL-4	Analyzing	CO 3
17.	Compare RSA and Diffie–Hellman algorithms in terms of key generation, security, and applications.	BTL-4	Analyzing	CO 3
18.	Analyze the mathematical principles that ensure the security of RSA.	BTL-4	Analyzing	CO 3
UNIT – IV INTEGRITY AND AUTHENTICATION ALGORITHMS				

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates				
Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define authentication.	BTL-1	Remembering	CO 4
2.	What are authentication requirements?	BTL-1	Remembering	CO 4
3.	Define an authentication function.	BTL-1	Remembering	CO 4
4.	What is a Message Authentication Code (MAC)?	BTL-1	Remembering	CO 4
5.	Define a cryptographic hash function.	BTL-1	Remembering	CO 4
6.	What is HMAC?	BTL-1	Remembering	CO 4
7.	What is CMAC?	BTL-1	Remembering	CO 4
8.	Expand SHA and DSS.	BTL-1	Remembering	CO 4
9.	Define a digital signature.	BTL-1	Remembering	CO 4
10.	What is an authentication protocol?	BTL-1	Remembering	CO 4
11.	Explain the purpose of message authentication.	BTL-2	Remembering	CO 4
12.	Differentiate between MAC and a hash function.	BTL-2	Understanding	CO 4
13.	Explain the role of HMAC in message authentication.	BTL-2	Understanding	CO 4
14.	Compare HMAC and CMAC.	BTL-2	Understanding	CO 4
15.	Why are cryptographic hash functions considered one-way functions?	BTL-2	Understanding	CO 4
16.	Explain the importance of collision resistance in hash functions.	BTL-2	Remembering	CO 4
17.	Describe the working principle of the SHA algorithm.	BTL-2	Remembering	CO 4
18.	Explain the role of digital signatures in ensuring data integrity and non-repudiation.	BTL-2	Remembering	CO 4
19.	What is the Digital Signature Standard (DSS)?	BTL-1	Remembering	CO 4
20.	Define the Schnorr Digital Signature Scheme.	BTL-1	Remembering	CO 4
21.	What is the ElGamal Cryptosystem?	BTL-1	Remembering	CO 4
22.	What is Kerberos?	BTL-1	Remembering	CO 4

23.	What is an X.509 Certificate?	BTL-1	Remembering	CO 4
24.	Define biometrics in authentication.	BTL-1	Remembering	CO 4
25.	What is a Challenge–Response Protocol?	BTL-1	Remembering	CO 4
PART –B				
1.	Demonstrate the generation and verification of a Message Authentication Code (MAC) using a suitable example.	BTL3	Applying	CO 4
2.	Apply the SHA algorithm to generate a message digest for a given message.	BTL3	Applying	CO 4
3.	Illustrate the HMAC generation process and explain how it provides message authentication.	BTL3	Applying	CO 4
4.	Demonstrate the working of CMAC with a suitable block cipher example.	BTL3	Applying	CO 4
5.	Apply the Digital Signature Standard (DSS) to generate and verify a digital signature.	BTL3	Applying	CO 4
6.	Demonstrate the Schnorr Digital Signature Scheme with a suitable example.	BTL3	Applying	CO 4
7.	Illustrate the ElGamal Cryptosystem for encryption and decryption using a numerical example.	BTL3	Applying	CO 4
8.	Demonstrate a Challenge–Response authentication protocol for secure entity authentication.	BTL3	Applying	CO 4
9.	Illustrate the Kerberos authentication process using a neat block diagram.	BTL3	Applying	CO 4
10.	Demonstrate symmetric key distribution using both symmetric and asymmetric encryption techniques.	BTL3	Applying	CO 4
11.	Analyze the authentication requirements necessary for secure communication systems.	BTL4	Analyzing	CO 4
12.	Compare MAC, HMAC, and CMAC based on security, performance, and applications.	BTL4	Analyzing	CO 4
13.	Analyze the security properties of cryptographic hash functions and discuss common attacks on hash algorithms.	BTL4	Analyzing	CO 4
14.	Compare DSS, Schnorr, and ElGamal Digital Signature Schemes in terms of security, efficiency, and applications.	BTL4	Analyzing	CO 4

15.	Analyze different entity authentication techniques such as passwords, biometrics, and challenge–response protocols.	BTL4	Analyzing	CO 4
16.	Compare symmetric key distribution and public key distribution mechanisms.	BTL4	Analyzing	CO 4
17.	Analyze the architecture and working of the Kerberos authentication protocol.	BTL4	Analyzing	CO 4
18.	Compare different public key distribution methods, including X.509 Certificates and trusted public key authorities.	BTL4	Analyzing	CO 4

UNIT – V CYBER CRIMES AND CYBER SECURITY

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define Cyber Crime.	BTL-1	Remembering	CO 5
2.	What is Information Security?	BTL-1	Remembering	CO 5
3.	List any four classifications of cyber crimes.	BTL-1	Remembering	CO 5
4.	Define Password Cracking.	BTL-1	Remembering	CO 5
5.	What is a Keylogger?	BTL-1	Remembering	CO 5
6.	Define Spyware.	BTL-1	Remembering	CO 5
7.	What is SQL Injection?	BTL-1	Remembering	CO 5
8.	Define Network Access Control (NAC).	BTL-1	Remembering	CO 5
9.	What is Cloud Security?	BTL-1	Remembering	CO 5
10.	Define Web Security.	BTL-1	Remembering	CO 5
11.	Explain the importance of Information Security in cyber space.	BTL-2	Remembering	CO 5
12.	Differentiate between cyber crime and cyber attack.	BTL-2	Understanding	CO 5
13.	Explain how password cracking threatens system security.	BTL-2	Understanding	CO 5
14.	Compare Keyloggers and Spyware.	BTL-2	Understanding	CO 5
15.	Explain the working principle of SQL Injection attacks.	BTL-2	Understanding	CO 5
16.	Describe the purpose of Network Access Control (NAC).	BTL-2	Understanding	CO 5

17.	Explain the importance of Cloud Security in modern organizations.	BTL-2	Understanding	CO 5
18.	Describe common threats to Web Security.	BTL-2	Understanding	CO 5
19.	Explain the significance of Wireless Security in Wi-Fi networks.	BTL-2	Understanding	CO 5
20.	Compare wired network security and wireless network security.	BTL-2	Understanding	CO 5
21.	Explain the role of authentication in preventing cyber crimes.	BTL-2	Understanding	CO 5
22.	Describe the objectives of Network Access Control.	BTL-2	Understanding	CO 5
23.	Explain why cyber crime prevention is important for organizations.	BTL-2	Understanding	CO 5
24.	Explain the importance of Information Security in cyber space.	BTL-2	Understanding	CO 5
25.	Differentiate between cyber crime and cyber attack.	BTL-2	Understanding	CO 5
PART –B				

1.	Demonstrate how password cracking attacks are performed and suggest suitable countermeasures.	BTL-3	Evaluating	CO 5
2.	Illustrate the working of a keylogger and recommend preventive measures against keylogging attacks.	BTL-3		
3.	Demonstrate how spyware infects a computer system and explain methods to detect and remove it.	BTL-3	Applying	CO 5
4.	Apply SQL Injection prevention techniques to secure a web application.	BTL-3	Analyzing	CO 5
5.	Illustrate the implementation of Network Access Control (NAC) in an enterprise network.	BTL-3	Analyzing	CO 5
6.	Demonstrate cloud security mechanisms for protecting data confidentiality and integrity.	BTL-3	Analyzing	CO 5
7.	Apply web security techniques to protect websites from common cyber attacks.	BTL-3	Analyzing	CO 5
8.	Demonstrate wireless security mechanisms such as WPA2/WPA3 for securing Wi-Fi networks.	BTL-3	Applying	CO 5
9.	Illustrate different cyber crime investigation steps using a real-world scenario.	BTL-3	Applying	CO 5
10.	Apply information security best practices to secure an organization's IT infrastructure.	BTL-3	Applying	CO 5
11.	Analyze different classifications of cyber crimes with suitable real-world examples.	BTL-4	Applying	CO 5
12.	Compare password cracking, keylogging, spyware, and SQL Injection based on attack methods, impact, and prevention.	BTL-4	Analyzing	CO 5

13.	Analyze the architecture and benefits of Network Access Control (NAC).	BTL-4	Analyzing	CO 5
14.	Compare different cloud security threats and the techniques used to mitigate them.	BTL-4	Analyzing	CO 5
15.	Analyze common web application vulnerabilities and recommend suitable security controls.	BTL-4	Analyzing	CO 5
16.	Compare web security and wireless security in terms of threats, vulnerabilities, and protection mechanisms.	BTL-4	Analyzing	CO 5
17.	Analyze different authentication and authorization techniques used in securing enterprise networks.	BTL-4	Analyzing	CO 5
18.	Examine the role of information security policies in preventing cyber crimes.	BTL-4	Analyzing	CO 5

