

SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
&
DEPARTMENT OF INFORMATION TECHNOLOGY**

QUESTION BANK



VII SEMESTER

CY3765 - CRYPTOGRAPHY AND CYBER SECURITY

Regulation – 2023

Academic Year 2026 – 2027

(ODD SEMESTER)

Prepared by

Ms. I. Kavitha, Assistant Professor (O.G)/ IT

Ms.M.Sophiya Sugantha Grace,Assistant Professor(O.G)/CSE

Ms.M.Priyadharshini,Assistant Professor (O.G)/CSE



SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT : CY3765 - CRYPTOGRAPHY AND CYBER SECURITY

SEM / YEAR: VII/IV

UNIT I -INTRODUCTION & NUMBER THEORY			
Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). FINITE FIELDS AND NUMBER THEORY: Modular arithmetic-Euclid's algorithm- Prime numbers-Fermat's and Euler's Theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms			
PART – A			
Q.No	Questions	BT	Competence
1	Differentiate active attacks and passive attacks.	BTL-2	Understanding
2	Define cryptography	BTL-1	Remembering
3	List the types of attack.	BTL-1	Remembering
4	Define cryptanalysis.	BTL-1	Remembering
5	List out the components of encryption algorithm.	BTL-1	Remembering
6	Compare Substitution and Transposition techniques.	BTL-2	Understanding
7	Explain how brute force attack is used in Network?	BTL-2	Understanding
8	List the four categories of security threats.	BTL-1	Remembering
9	Compute GCD of 1970 and 1066 using Euclid algorithm.	BTL-2	Understanding
10	Define primitive root.	BTL-1	Remembering
11	Give examples for substitution cipher.	BTL-2	Understanding
12	Define Steganography	BTL-1	Remembering
13	Explain why Modular arithmetic has been used in cryptography.	BTL-2	Understanding
14	Compare threats and attacks.	BTL-2	Understanding
15	Classify the basic functions used in encryption algorithms.	BTL-2	Understanding
16	Describe security mechanism.	BTL-2	Understanding
17	Identify the original text from the following cipher text using brute force attack: CMTMROEOORW (Hint: Algorithm-Rail fence).	BTL-1	Remembering
18	Explain why network need security.	BTL-2	Understanding
19	Convert the given text "VALLIAMMAI" into cipher text using Rail fence Technique.	BTL-2	Understanding
20	How many keys are required by two people to communicate via a cipher.	BTL-2	Understanding
21	Describe Euler's theorem.	BTL-2	Understanding
22	Explain why asymmetric cryptography is bad for huge data?	BTL-2	Understanding
23	State Fermat's theorem	BTL-2	Understanding
24	Compute $117 \bmod 13$	BTL-2	Understanding

PART – B

1	List and explain the categories of passive and active security attacks. (16)	BTL-4	Analyzing
2	Tabulate the substitution Techniques in detail. (16)	BTL-3	Applying
3	Illustrate the Transposition Techniques in detail. (16)	BTL-3	Applying
4	Explain the OSI security architecture in detail. (16)	BTL-4	Analyzing
5	i) Discuss Play fair cipher in detail. (8) ii) Encrypt the following using play fair cipher using the keyword MONARCHY. Use X for blank spaces “SWARAJ IS MY BIRTH RIGHT” (8)	BTL-3	Applying
6	i) Apply Caesar cipher and k=5 decrypt the given Cipher text “YMJTYMJWXNIJTKXNQJSHJ”. (8) ii) Apply Vigenere cipher, encrypt the word “explanation” Classical cryptosystems and its types using the key “leg”. (8)	BTL-3	Applying
7	Explain the following encryption methods in detail: (i) Play fair cipher (6) (ii) Railfence cipher (5) (iii) Vigenere cipher (5)	BTL-4	Analyzing
8	(i) What is Steganography? Briefly examine any three techniques. (8) (ii) What is mono-alphabetic cipher? Examine how it differs from Caesar cipher? (8)	BTL-4	Analyzing
9	Demonstrate the encryption of the message “PAY” using hill cipher with the following key matrix and show the decryption. (16) $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	BTL-3	Applying
10	Explain the following (i) Security services. (8) (ii) Security mechanisms. (8)	BTL-4	Analyzing
11	State and Describe Fermat’s theorem. (8) Evaluate $3^{21} \bmod 11$ using Fermat’s theorem. (8)	BTL-5	Evaluating
12	State Chinese Remainder theorem Find X for the given set of congruent equations using CRT. $X \equiv 2 \pmod{3}$ $X \equiv 3 \pmod{5}$ $X \equiv 2 \pmod{7}$ (16)	BTL-5	Evaluating
13	Explain the properties that are satisfied by modular arithmetic. (16)	BTL-4	Analyzing
14	State and prove: i) Euler’s theorem. (8) ii) Euclid’s Algorithm. (8)	BTL-4	Analyzing

15	Explain how to test for primality? (8) Calculate a solution for $11^{13} \bmod 53$ using modular exponentiation. (8)	BTL-3	Applying
16	Summarize the relationship between security services and security mechanisms. (16)	BTL-5	Evaluating
17	(i) Rewrite the rules to perform encryption using play fair cipher and encrypt 'snowshooos' using 'monarchy' I and J count as one letter and x is the filler letter. (8) (ii) Encrypt the word "Semester Result" with the keyword "Examination" using play fair cipher. List the rules used (8)	BTL-6	Creating

UNIT II - SYMMETRIC KEY CRYPTOGRAPHY

SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES – Block cipher design principles – Block cipher mode of operation – Advanced Encryption Standard – RC4 – Key distribution.

PART – A

Q.No	Questions	BT Level	Competence
1	What is the difference between a block cipher and a Stream cipher?	BTL-2	Understanding
2	Define Diffusion.	BTL-1	Remembering
3	Differentiate substitution and permutation.	BTL-2	Understanding
4	Explain S box in DES Structure.	BTL-2	Understanding
5	List the five modes of operation of block cipher.	BTL-1	Remembering
6	What is called as avalanche effect?	BTL-1	Remembering
7	Compare Forward and reverse substitute byte transformation.	BTL-2	Understanding
8	Give the strengths of Triple DES.	BTL-2	Understanding
9	Show general design of S-AES encryption cipher.	BTL-1	Remembering
10	State Data units used in AES.	BTL-2	Understanding
11	List the four different stages of each round in AES.	BTL-1	Remembering

12	Explain why the middle portion of triple DES is a decryption rather than encryption?	BTL-2	Understanding
13	List the function of state array.	BTL-1	Remembering
14	Point out is it possible to use the DES algorithm to generate message authentication code.	BTL-1	Remembering
15	Differentiate between sub bytes and sub words.	BTL-2	Understanding
16	Describe the triple encryption. How many keys are used in triple encryption?	BTL-2	Understanding
17	Compare DES and AES.	BTL-2	Understanding
18	Identify the parameters (block size, key size and no. of rounds) for the three AES versions.	BTL-1	Remembering
19	Explain idea of RC4 stream cipher.	BTL-2	Understanding
20	List the evaluation criteria for AES algorithm.	BTL-1	Remembering

21	Discuss the relationship between the key length and state vector in RC4 algorithm.	BTL-2	Understanding
22	Discover the use of nonce in key distribution.	BTL-3	Applying
23	Explain the need of key-distribution center.	BTL-2	Understanding
24	Explain Hierarchical Multiple KDCs.	BTL-2	Understanding

PART – B

1	Explain in detail, AES algorithm with round functions. (16)	BTL-3	Applying
2	Explain in detail about (i) Cipher block chaining. (8) (ii) Cipher feedback mode. (8)	BTL-3	Applying
3	Explain in detail about (i) Electronic codebook mode (8) (ii) Output feedback mode. (8)	BTL-4	Analyzing
4	(i) Formulate the single round of DES algorithm. (8) (ii) Design the key generation process of DES. (8)	BTL-6	Creating
5	Explain the RC4 method used for encryption and decryption. (16)	BTL-4	Analyzing
6	Examine the General structure of DES with diagrams. (16)	BTL-4	Analyzing
7	(i) Analyze how men in middle attack is performed on double Data Encryption Standard. (8) (ii) Explain the substitution bytes transformation and add round key transformation of AES cipher. (8)	BTL-4	Analyzing
8	Explain in detail the key generation in AES algorithm and its key expansion format. (16)	BTL-4	Analyzing
9	For each of the following elements of DES, determine the comparable element in AES if available.	BTL-3	Applying

	(i) XOR of sub key material with the input to the function. (ii) f function. (iii) Permutation p. (iv) Swapping of halves of the block. (16)		
10	Summarize the block cipher design principles. (16)	BTL-5	Evaluating
11	Explain the modes of operation in block cipher. (16)	BTL-4	Analyzing
12	Illustrate Evaluation criteria for AES (16)	BTL-3	Applying
13	(i) Describe Triple DES and its applications. (8) (ii) Identify the strength of DES algorithm. (8)	BTL-3	Applying
14	Explain the stream generation process in RC4 algorithm. (16)	BTL-5	Evaluating
15	What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. (16)	BTL-5	Evaluating
16	Design the Structure of Simplified DES (S-DES) with Ciphering and Reverse Ciphering. (16)	BTL-6	Creating
17	Compose public key and secret key distribution mechanisms in detail. (16)	BTL-6	Creating

UNIT III ASYMMETRIC KEY CRYPTOGRAPHY

ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange – ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.

PART A

Q.No	Questions	BT Level	Competence
1	Give the applications of the public key crypto systems.	BTL-2	Understanding
2	Write the roles of public and private key.	BTL-1	Remembering
3	Differentiate public key and conventional encryption.	BTL-2	Understanding
4	Write the three broad categories of applications of public key cryptosystems.	BTL-2	Understanding
5	Explain the purpose of Diffie Hellman key exchange.	BTL-2	Understanding
6	Define the principle elements of a public key crypto system.	BTL-1	Remembering
7	Examine the requirements for public key cryptosystems.	BTL-1	Remembering

8	List four general characteristics of schema for the distribution of the public key.	BTL-1	Remembering
9	What are requirements that a public key crypto system need to fulfil security.	BTL-1	Remembering
10	Give the formula for encryption and decryption using RSA algorithm.	BTL-2	Understanding
11	Explain elliptic curve cryptography.	BTL-2	Understanding
12	Express the key generation process of RSA algorithm.	BTL-2	Understanding
13	Compare public key and private key.	BTL-2	Understanding
14	Explain whether symmetric and asymmetric cryptographic algorithm need key exchange.	BTL-2	Understanding
15	List four general categories of schemes for the distribution of public keys.	BTL-1	Remembering
16	Draw a neat sketch showing the key distribution scenario.	BTL-1	Remembering
17	Describe the purpose of Diffie Hellman key exchange.	BTL-2	Understanding
18	Distinguish Elliptic Curves over Real Numbers	BTL-2	Understanding
19	Point out the attacks of RSA cryptosystem	BTL-1	Remembering
20	Compute encryption and decryption using RSA algorithm for the following. $p=7$, $q=11$; $e=17$; $m=8$.	BTL-2	Understanding
21	Define abelian group	BTL-1	Remembering
22	Give the counter measures for timing attacks in RSA.	BTL-2	Understanding
23	Give the role of certificate authority in the exchange of public keys.	BTL-2	Understanding
24	Point out whether strong primes are necessary in RSA.	BTL-1	Remembering

PART B

1	Explain about RSA algorithm highlighting its computational aspects. (16)	BTL-4	Analyzing
2	Summarize the security aspects of RSA algorithm. (16)	BTL-5	Evaluating

3	(i) Explain RSA Algorithm. (8) (ii) Estimate the encryption and decryption values for the RSA algorithm parameters. $P=7$, $Q=11$, $E=17$, $M=8$. (8)	BTL-5	Evaluating
4	(i) Apply the mathematical foundations of RSA algorithm. (8) (ii) Perform encryption and decryption using RSA algorithm for $p=17$, $q=11$, $e=7$ $m=88$. (8)	BTL-3	Applying
5	. Perform encryption decryption for the following data. $P=17$, $q=7$, $e=5$, $n=119$, message="6". Use Extended Euclid's algorithm to find the private key. (16)	BTL-3	Applying
6	Explain Diffie-Hellman key exchange with an example. (16)	BTL-4	Analyzing
7	Explain with necessary example the concept of man-in-the-middle attack. (16)	BTL-4	Analyzing
8	Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime $q=11$ and a primitive root $\alpha=7$. (16)	BTL-5	Evaluating

	(i) If user A has private key $X_A=3$. What is A's public key Y_A ? (ii) If user B has private key $X_B=6$. What is B's public key Y_B ? (iii) What is the shared secret key? Also write the algorithm.		
9	(i) Summarize the role of discrete log in the Diffie-Hellman key exchange in exchanging the secret key among two users. (8) (ii) What are elliptic curves? Describe how the elliptic curves are useful for Cryptography? (8)	BTL-5	Evaluating
10	With a neat sketch explain the Elliptic curve cryptography with an example. (16)	BTL-4	Analyzing
11	User A and B use Diffie-Hellman key exchange a common prime $q=71$ and a primitive root $\alpha = 7$. Calculate the following. If user A has private key $X_A=5$, what is A's public key Y_A . If user A has private key $X_B=12$, what is B's public key Y_B and what is shared secret key? (16)	BTL-4	Analyzing
12	Generalize the Key generation, encryption, and decryption in ElGamal. (16)	BTL-6	Creating
13	(i) Explain briefly about Diffie-Hellman key exchange algorithm with its pros and cons. (8) (ii) Explain public key cryptography and when is it preferred. (8)	BTL-4	Analyzing
14	Illustrate the key management of public key encryption in detail. (16)	BTL-3	Applying
15	Explain in detail about the public key distribution of secret keys. (16)	BTL-5	Evaluating

16	i) In a public-key system using RSA, you intercept the cipher text $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M ? (8) ii) In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. Determine the private key of this user? (8)	BTL-6	Creating
17	Discuss the ElGamal cryptosystem and elliptic curve cryptosystem. (16)	BTL-5	Evaluating

UNIT IV-INTRODUCTION TO CYBER SECURITY

Introduction – Computer Security – Threats – Harm – Vulnerabilities – Controls – Authentication – Access Control and Cryptography – Web—User Side – Browser Attacks – Web Attacks Targeting Users – Obtaining User or Website Data – Email Attacks.

PART – A

Q.No	Questions	BT Level	Competence
1	Define Cyber Security.	BTL-1	Remembering
2	What are the objectives of Computer Security?	BTL-1	Remembering
3	Explain the CIA triad in Computer Security.	BTL-2	Understanding
4	Define Confidentiality with an example.	BTL-1	Remembering
5	What is Integrity? How is it maintained?	BTL-2	Understanding
6	Define Availability. Give an example.	BTL-1	Remembering
7	What is a cyber threat? Mention any two examples.	BTL-2	Understanding
8	Define vulnerability. How does it differ from a threat?	BTL-2	Understanding
9	What is meant by harm in cyber security?	BTL-1	Remembering
10	What are security controls? List their categories.	BTL-2	Understanding
11	Define authentication. Mention its factors.	BTL-1	Remembering

12	What is Multi-Factor Authentication (MFA)?	BTL-2	Understanding
13	Define access control.	BTL-1	Remembering
14	List any four access control models.	BTL-1	Remembering
15	What is cryptography?	BTL-1	Remembering
16	Differentiate between symmetric and asymmetric encryption.	BTL-2	Understanding
17	Define browser attack. Mention any two browser attacks.	BTL-2	Understanding
18	What is a cryptographic hash function?	BTL-2	Understanding
19	Define browser attack. Mention any two browser attacks.	BTL-2	Understanding
20	What is Clickjacking?	BTL-2	Understanding

21	What is Cross-Site Scripting (XSS)?	BTL-2	Understanding
22	Mention any four best practices to protect against email attacks.	BTL-3	Applying
23	Define phishing. How does it affect users?	BTL-2	Understanding
24	What is email spoofing?	BTL-2	Understanding

PART – B

1	A software company has experienced repeated cyber attacks due to weak passwords and outdated systems. Explain the different cyber threats, vulnerabilities, and security controls that can be implemented to improve the company's security posture.	BTL 3	Applying
2	An organization is planning to strengthen its authentication mechanism. Explain the various authentication methods and recommend suitable access control models for different organizational roles with justification.	BTL 3	Applying
3	Analyze the differences between symmetric and asymmetric cryptography. Compare their advantages, disadvantages, applications, and suitability for different security scenarios.	BTL 4	Analyzing
4	Analyze various browser attacks and web attacks targeting users. Explain how attackers exploit browser vulnerabilities and recommend suitable preventive measures.	BTL 4	Analyzing
5	Analyze different methods used by attackers to obtain user or website data. Discuss the impact of these attacks on individuals and organizations and suggest effective countermeasures.	BTL 4	Analyzing
6	Evaluate different authentication techniques and access control models. Recommend the most appropriate security mechanism for a banking application with proper justification	BTL 5	Evaluate
7	Evaluate the effectiveness of different email security techniques in preventing phishing, spoofing, spam, and Business Email Compromise (BEC) attacks.	BTL 5	Evaluate
8	Evaluate the role of cryptography in protecting modern web applications. Justify the use of encryption, hashing, and digital signatures in ensuring secure communication.	BTL 5	Evaluate
9	Explain different categories of cyber threats with suitable examples. (8) Explain different types of vulnerabilities and security controls with suitable examples.(8)	BTL3	APPLY

10	Explain authentication methods used in cyber security.(8). Analyze the working of Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC).(8)	BTL 4	Analyzing
11	Compare symmetric and asymmetric encryption techniques with suitable examples.(8) Analyze the applications of cryptographic hash functions in maintaining data integrity and password security.(8)	BTL 4	Analyzing
12	Analyze different browser attacks such as clickjacking, cookie theft, and drive-by downloads. (8) Analyze web attacks such as Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Session Hijacking.(8)	BTL 4	Analyzing
13	Evaluate different techniques used to protect user and website data against cyber attack(8) Evaluate the effectiveness of encryption, authentication, and access control in securing web applications.(8)	BTL5	Evaluate
14	Evaluate various email attack prevention techniques adopted by organizations.(8) Assess the effectiveness of spam filters, digital signatures, and Multi-Factor Authentication in securing email communication.(8)	BTL5	Evaluate
15	Explain the CIA triad and its application in protecting organizational information systems.(8) Analyze the relationship between confidentiality, integrity, availability, authentication, and access control in cyber security.(8)	BTL 4	Analyzing
16	Analyze the impact of browser vulnerabilities on user privacy and data security.(8) Evaluate the effectiveness of browser security mechanisms in protecting users from cyber attacks.(8)	BTL5	Evaluate
17	A university plans to implement a secure online examination system. Evaluate the security	BTL5	Evaluate

	mechanisms required to protect users, websites, and sensitive examination data.(8) An e-commerce company has experienced phishing attacks, session hijacking, and data theft. Recommend and justify a comprehensive cyber security strategy to protect the organization.(8)		
UNIT - V: DEFENCES: SECURITY COUNTERMEASURES			
Cryptography in Network Security – Firewalls – Intrusion Detection and Prevention Systems – Network Management – Databases – Security Requirements of Databases – Reliability and Integrity – Database Disclosure – Data Mining and Big Data.			
PART A			
1	Define network security.	BTL1	Remembering
2	What is cryptography in network security?	BTL1	Remembering
3	State the objectives of cryptography.	BTL1	Remembering
4	Define firewall.	BTL1	Remembering
5	List the different types of firewalls.	BTL1	Remembering
6	What is packet filtering firewall?	BTL1	Remembering
7	Define Intrusion Detection System (IDS).	BTL1	Remembering
8	What is an Intrusion Prevention System (IPS)?	BTL1	Remembering
9	Differentiate between IDS and IPS.	BTL 2	Understanding
10	What is network management?	BTL1	Remembering
11	List the objectives of network management.	BTL1	Remembering
12	Define database security.	BTL1	Remembering
13	What are the security requirements of databases?	BTL 2	Understanding
14	Define database reliability.	BTL1	Remembering
15	What is data integrity?	BTL1	Remembering
16	Differentiate between reliability and integrity.	BTL 2	Understanding
17	What is database disclosure?	BTL1	Remembering
18	Mention any four database disclosure threats.	BTL 2	Understanding
19	Define data mining.	BTL1	Remembering
20	What is Big Data?	BTL1	Remembering
21	List the characteristics (5Vs) of Big Data.	BTL 2	Understanding
22	Mention any four applications of data mining.	BTL 2	Understanding
23	How does cryptography improve network security?	BTL 2	Understanding
24	Why is firewall considered the first line of defense in network security?	BTL 2	Understanding
PART B			
1	Explain the role of cryptography in network security. Discuss how encryption, decryption, digital signatures, and hashing provide secure communication.	BTL 3	Apply

2	Analyze the working principles of different types of firewalls. Compare their advantages, limitations, and real-world applications.	BTL 4	Analyze
3	Analyze the architecture and working of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Compare signature-based and anomaly-based detection techniques.	BTL 4	Analyze
4	An organization is planning to implement a secure network infrastructure. Evaluate the combined role of cryptography, firewalls, IDS, and IPS in protecting enterprise networks.	BTL 5	Evaluate
5	Evaluate the security requirements of databases and recommend suitable mechanisms to ensure confidentiality, integrity, availability, authentication, and authorization.	BTL 5	Evaluate
6	Design a secure database protection framework for a healthcare organization by considering database reliability, integrity, disclosure prevention, and access control.	BTL6	Create
7	Evaluate various techniques used to prevent database disclosure. Justify the importance of privacy-preserving database systems in modern organizations.	BTL 5	Evaluate
8	Design a security framework for an e-commerce company using data mining and big data analytics to detect cyber threats while ensuring customer privacy.	BTL 6	Create
9	Explain the applications of cryptography in network security. (8) Analyze the importance of encryption techniques in protecting network communication. (8)	BTL 4	Analyze
10	Explain different types of firewalls with suitable diagrams.(8) Compare packet filtering, stateful inspection, proxy, and next-generation firewalls.(8)	BTL 4	Analyze
11	Explain the working of Intrusion Detection Systems (IDS). (8) Evaluate the effectiveness of IDS and IPS in preventing cyber attacks.(8)	BTL 5	Evaluate
12	Explain the objectives and functions of network management.(8) Analyze the role of network management tools in maintaining network security.(8)	BTL 4	Analyze

13	Explain the security requirements of databases with suitable examples. (8) Evaluate different database security mechanisms used to protect organizational data.(8)	BTL 5	Evaluate
14	Analyze the concepts of database reliability and integrity with examples.(8) Design a strategy to improve database reliability and integrity in a banking system.(8)	BTL 6	Create
15	Analyze different types of database disclosure attacks and their consequences.(8) Evaluate various techniques used to prevent database disclosure.(8)	BTL 5	Evaluate
16	Explain the concepts of data mining and big data with suitable applications.(8) Analyze the role of big data analytics in cyber security and threat detection.(8)	BTL 4	Analyze
17	Evaluate the benefits and security challenges of using big data in modern organizations.(8) Design an integrated cyber security framework incorporating cryptography, firewalls, IDS/IPS, secure databases, and big data analytics for a smart city application.(8)	BTL 6	Create