SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

Academic Year 2025 – 2026 (ODD SEMESTER)

SEMESTER V

PCY301- MODERN CRYPTOGRAPHY

Regulation – 2023

Prepared by

Ms. K.R. Nandhashree AP (O.G) /CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT: PCY301- MODERN CRYPTOGRAPHY

SEM / YEAR: V SEMESTER/ III YEAR

UNIT-I: INTRODUCTION

Basics of Symmetric Key Cryptography- Basics of Asymmetric Key Cryptography- Hardness of Functions. Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI- Hard Core Predicate- Trap- door permutation- Goldwasser-Micali Encryption. Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations.

PART-A

Q.no	Question	BTL	Competence
1	Define symmetric key cryptography.	BTL1	Remembering
2	Define asymmetric key cryptography.	BTL1	Remembering
3	What is a cryptographic key?	BTL1	Remembering
4	List any two differences between symmetric and asymmetric encryption.	BTL1	Remembering
5	Define the term semantic security.	BTL1	Remembering
6	What is meant by message indistinguishability (MI)?	BTL1	Remembering
7	State the equivalence between semantic security and message indistinguishability.	BTL2	Understanding
8	What is a trapdoor permutation? Provide an example.	BTL2	Understanding
9	Define hard-core predicate in the context of one-way functions.	BTL1	Remembering
10	State the significance of the Goldreich–Levin Theorem.	BTL2	Understanding
11	What is a one-way function?	BTL1	Remembering
12	What are the essential properties of a secure encryption scheme?	BTL1	Remembering
13	Give the basic idea of Goldwasser–Micali Encryption.	BTL1	Remembering
14	Define indistinguishability under chosen plaintext attack (IND-CPA).	BTL1	Remembering
15	Differentiate between hard-core predicate and trapdoor permutation.	BTL2	Understanding
16	What is the role of randomness in modern encryption schemes?	BTL2	Understanding
17	Define the concept of message space and ciphertext space.	BTL1	Remembering
18	Explain the importance of semantic security in encryption schemes.	BTL2	Understanding

19	What is meant by probabilistic encryption?	BTL2	Understanding
20	Define ciphertext indistinguishability under chosen ciphertext attack.	BTL1	Remembering
21	What is a decryption oracle in the context of attack models?	BTL2	Understanding
22	Why is trapdoor one-way function important in public key cryptography?	BTL2	Understanding
23	What is the contribution of Goldwasser and Micali to public key encryption?	BTL1	Remembering
24	State any two applications of modern cryptographic primitives in cybersecurity.	BTL1	Remembering

PART - B

Q.no	Question	BTL	Competence
1	Illustrate the differences between symmetric and asymmetric key cryptography with suitable examples.	BTL3	Applying
2	Explain how semantic security and message indistinguishability are equivalent. Include a proof outline.	BTL4	Analyzing
3	Demonstrate the working of a trapdoor permutation with an appropriate example.	BTL3	Applying
4	Analyze the Goldwasser–Micali encryption scheme and explain how it achieves semantic security.	BTL4	Analyzing
5	Apply the concept of semantic security to explain how indistinguishability is maintained in a system.	BTL3	Applying
6	Compare and contrast chosen plaintext and chosen ciphertext attacks with suitable scenarios.	BTL4	Analyzing
7	Examine the Goldreich–Levin Theorem. How does it relate hard-core predicates to one-way functions?	BTL4	Analyzing
8	Evaluate the security assumptions behind the Goldwasser–Micali encryption.	BTL5	Evaluating
9	Design a scenario where trapdoor functions can be used to establish a secure communication channel.	BTL6	Creating
10	Analyze why hard-core predicates are crucial in constructing secure encryption schemes.	BTL4	Analyzing
11	Construct a pseudocode algorithm for basic semantic security-based encryption.	BTL6	Creating
12	Explain the concept of probabilistic encryption. How does it prevent deterministic attack models?	BTL3	Applying
13	Evaluate the use of randomness in public key encryption schemes.	BTL5	Evaluating
14	Justify the use of hard problems (e.g., factoring, discrete log) in building modern encryption systems.	BTL5	Evaluating
15	Propose a simplified version of Goldwasser–Micali encryption for educational demonstration.	BTL6	Creating
16	Identify limitations of symmetric key encryption in modern communication and how asymmetric systems help.	BTL3	Applying
17	Assess the relationship between hard-core predicates and semantic security using the Goldreich–Levin theorem.	BTL5	Evaluating

UNIT II - FORMAL NOTIONS OF ATTACKS

Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA)- ChosenCiphertext Attacks (IND-CCA1 and IND-CCA2)- Attacks under Message Non- malleability: NM-CPA and NM-CCA2- Inter- relations among the attack model

PART-A

Q.no	Question	BTL	Competence
1	What is a chosen plaintext attack?	BTL1	Remembering
2	Define chosen ciphertext attack.	BTL1	Remembering
3	Define chosen ciphertext attack.	BTL1	Remembering
4	What is non-malleability under chosen plaintext attack (NM-CPA)?	BTL1	Remembering
5	Define non-malleability under chosen ciphertext attack (NM-CCA2).	BTL1	Remembering
6	Differentiate IND-CPA and IND-CCA2.	BTL2	Understanding
7	What is a cryptographic adversary?	BTL1	Remembering
8	What is a decryption oracle?	BTL1	Remembering
9	What is indistinguishability in cryptography?	BTL2	Understanding
10	State the relation between NM and IND security.	BTL2	Understanding
11	What is message non-malleability?	BTL1	Remembering
12	Define attack model in cryptography.	BTL1	Remembering
13	What is adaptive chosen ciphertext attack?	BTL2	Understanding
14	What is a security experiment in cryptographic models?	BTL2	Understanding
15	State any two types of adversarial goals.	BTL1	Remembering
16	What is an indistinguishability game?	BTL2	Understanding
17	Define advantage of an adversary in an IND game.	BTL2	Understanding
18	What is meant by semantic equivalence?	BTL1	Remembering
19	State the purpose of NM-CCA2 security.	BTL2	Understanding
20	Differentiate between CPA and CCA.	BTL2	Understanding
21	What is malleability in encryption schemes?	BTL2	Understanding
22	Explain chosen message attack briefly.	BTL2	Understanding
23	Mention a real-world example of a chosen ciphertext attack.	BTL1	Remembering
24	What is the significance of attack models in cryptography?	BTL2	Understanding

PART - B

Q.no	Question	BTL	Competence
1	Explain IND-CPA and describe a scenario where this attack can occur.	BTL3	Applying
2	Illustrate the difference between IND-CCA1 and IND-CCA2 with examples.	BTL4	Analyzing
3	Examine the NM-CCA2 model and its real-world implications.	BTL4	Analyzing

4	Apply the concepts of IND and NM attacks in secure email systems.	BTL3	Applying
5	Compare the effectiveness of IND-CCA2 over IND-CPA in protocol design.	BTL4	Analyzing
6	Design an attack model to evaluate a new encryption scheme.	BTL6	Creating
7	Evaluate a cryptographic scheme based on its resistance to NM-CPA.	BTL5	Evaluating
8	Construct a proof for equivalence of NM-CCA2 and IND-CCA2.	BTL6	Creating
9	Differentiate malleability and indistinguishability using a case study.	BTL4	Analyzing
10	Analyze the limits of chosen plaintext attacks in real-world systems.	BTL4	Analyzing
11	Apply adversarial goals to assess the strength of a symmetric cipher.	BTL3	Applying
12	Justify the need for NM security in public key encryption.	BTL5	Evaluating
13	Develop a model attack demonstrating NM failure in ElGamal encryption.	BTL6	Creating
14	Describe an experiment to test resistance against chosen ciphertext attacks.	BTL5	Evaluating
15	Explain how the attacker’s advantage is calculated in IND-CPA model.	BTL3	Applying
16	Critically assess RSA-OAEP in the context of IND-CCA2.	BTL5	Evaluating
17	Design an attack-resistant message transmission protocol.	BTL6	Creating

UNIT - III - RANDOM ORACLES

Provable Security and asymmetric cryptography- hash functions. One-way functions: Weak and Strong one-way functions. Pseudo-random Generators (PRG): Blum-Micali-Yao Construction- Construction of more powerful PRG- Relation between One-way functions and PRG- Pseudo random Functions (PRF)

PART-A

Q.no	Question	BTL	Competence
1	What is a one-way function?	BTL1	Remembering
2	Differentiate between weak and strong one-way functions.	BTL2	Understanding
3	Define provable security in cryptographic protocols.	BTL1	Remembering
4	State the role of hash functions in modern cryptography.	BTL1	Remembering
5	What is a pseudo-random generator (PRG)?	BTL1	Remembering
6	List any two properties of a good hash function.	BTL1	Remembering
7	What is the use of pseudo-random functions (PRFs)?	BTL2	Understanding
8	Define the Blum-Micali generator.	BTL1	Remembering
9	What is the Yao PRG construction?	BTL1	Remembering

10	How does a one-way function relate to PRGs?	BTL2	Understanding
11	Explain the term 'random oracle model'.	BTL2	Understanding
12	What is a collision-resistant hash function?	BTL1	Remembering
13	Define unpredictability in PRGs.	BTL1	Remembering
14	How does a PRG extend a short seed to a long pseudo-random output?	BTL2	Understanding
15	Mention two applications of hash functions.	BTL1	Remembering
16	What is a cryptographic seed?	BTL1	Remembering
17	Define entropy in the context of randomness.	BTL1	Remembering
18	Differentiate between PRG and PRF.	BTL2	Understanding
19	What is an initialization vector (IV)?	BTL1	Remembering
20	State the use of randomness in asymmetric cryptography.	BTL2	Understanding
21	What is meant by deterministic versus probabilistic encryption?	BTL2	Understanding
22	What does the term 'stretching function' refer to in PRG context?	BTL2	Understanding
23	What is meant by 'forward security'?	BTL2	Understanding
24	Define input and output length of a PRG.	BTL1	Remembering

PART - B

Q.no	Question	BTL	Competence
1	Explain how a one-way function can be used to construct a PRG.	BTL3	Applying
2	Demonstrate the Blum-Micali construction for generating pseudo-random bits.	BTL3	Applying
3	Analyze the security properties of the Yao PRG.	BTL4	Analyzing
4	Compare weak and strong one-way functions with examples.	BTL4	Analyzing
5	Evaluate the effectiveness of collision resistance in hash functions.	BTL5	Evaluating
6	Construct a pseudo-code for a PRF using a given seed.	BTL6	Creating
7	Assess the role of PRGs in symmetric key generation.	BTL5	Evaluating
8	Design a secure hashing mechanism using compression functions.	BTL6	Creating
9	Illustrate how random oracles are applied in signature schemes.	BTL3	Applying
10	Interpret the relationship between unpredictability and security in PRGs.	BTL4	Analyzing
11	Create a simplified model to demonstrate the working of a PRF.	BTL6	Creating
12	Apply the concept of entropy in generating secure random bits.	BTL3	Applying
13	Analyze how hash functions contribute to data integrity.	BTL4	Analyzing

14	Evaluate the reliability of PRFs in MAC construction.	BTL5	Evaluating
15	Develop a method to extend PRG output using hybrid techniques.	BTL6	Creating
16	Differentiate between the security proofs of PRG and PRF constructions.	BTL4	Analyzing
17	Propose improvements to increase the efficiency of hash-based PRFs.	BTL5	Evaluating

UNIT - IV: BUILDING A PSEUDORANDOM PERMUTATION

The LubyRackoff Construction: Formal Definition- Application of the LubyRackoff Construction to the construction of Block Ciphers- The DES in the light of LubyRackoff Construction.

PART-A

Q.no	Question	BTL	Competence
1	Define Luby-Rackoff construction.	BTL1	Remembering
2	What is the purpose of Feistel networks in block cipher design?	BTL2	Understanding
3	State the significance of pseudorandom permutations.	BTL2	Understanding
4	Define block cipher.	BTL1	Remembering
5	What are the rounds in Luby-Rackoff construction?	BTL1	Remembering
6	How does Luby-Rackoff construction achieve security?	BTL2	Understanding
7	Mention two applications of block ciphers.	BTL1	Remembering
8	What is a round function in the context of block ciphers?	BTL2	Understanding
9	Define ideal cipher model.	BTL1	Remembering
10	What is DES?	BTL1	Remembering
11	What is the role of key mixing in DES?	BTL2	Understanding
12	State the number of rounds in DES.	BTL1	Remembering
13	What is the function of permutation in DES?	BTL1	Remembering
14	Define S-box.	BTL1	Remembering
15	What is the expansion permutation in DES?	BTL2	Understanding
16	State the size of the block in DES.	BTL1	Remembering
17	What is the key schedule in DES?	BTL1	Remembering
18	Mention the difference between pseudorandom function and permutation.	BTL2	Understanding
19	What is the Feistel structure?	BTL2	Understanding
20	Define invertibility in the context of block ciphers.	BTL1	Remembering
21	What is the avalanche effect?	BTL1	Remembering
22	Explain the diffusion property of block ciphers.	BTL2	Understanding
23	What is the significance of substitution in block ciphers?	BTL2	Understanding

24	Define confusion in cryptographic algorithms.	BTL1	Remembering

PART - B

Q.no	Question	BTL	Competence
1	Explain the Luby-Rackoff construction and its use in building block ciphers.	BTL3	Applying
2	Illustrate the structure and components of the DES algorithm.	BTL3	Applying
3	Analyze how the Luby-Rackoff model ensures pseudorandomness.	BTL4	Analyzing
4	Evaluate the security of a 3-round Feistel network under chosen plaintext attack.	BTL5	Evaluating
5	Construct a simplified Feistel network and simulate one encryption round.	BTL6	Creating
6	Differentiate between DES and Luby-Rackoff construction.	BTL4	Analyzing
7	Design a Feistel-based block cipher using a PRF.	BTL6	Creating
8	Apply the principles of Luby-Rackoff to derive pseudorandom permutations.	BTL3	Applying
9	Compare the DES round structure with that of the Luby-Rackoff approach.	BTL4	Analyzing
10	Evaluate the role of diffusion and confusion in DES.	BTL5	Evaluating
11	Develop a mini DES-like cipher with 2 rounds and describe its working.	BTL6	Creating
12	Analyze how key scheduling affects DES security.	BTL4	Analyzing
13	Explain the relevance of round functions in block cipher security.	BTL3	Applying
14	Construct a diagram of a Luby-Rackoff 3-round Feistel cipher.	BTL6	Creating
15	Design a test case to evaluate DES avalanche effect.	BTL5	Evaluating
16	Assess the weaknesses in DES using differential cryptanalysis.	BTL5	Evaluating
17	Propose enhancements to Luby-Rackoff based construction for modern ciphers.	BTL6	Creating

UNIT – V: MESSAGE AUTHENTICATION CODES

Left or Right Security (LOR). Formal Definition of Weak and Strong MACs- Using a PRF as a MAC- Variable length MAC. Public Key Signature Schemes: Formal Definitions- Signing and Verification- Formal Proofs of Security of Full Domain Hashing. Assumptions for Public Key Signature.
Schemes: One-way functions Imply Secure One-time Signatures. Shamir's Secret Sharing Scheme. Formally Analyzing Cryptographic Protocols. Zero Knowledge Proofs and Protocols.

PART-A

Q.no	Question	BTL	Competence
1	Define Message Authentication Code (MAC).	BTL1	Remembering
2	What is the difference between weak and strong MAC?	BTL2	Understanding
3	Define the term 'Left or Right Security (LOR)'.	BTL1	Remembering
4	State the use of a PRF in MAC construction.	BTL2	Understanding
5	What is a variable length MAC?	BTL1	Remembering
6	Define digital signature.	BTL1	Remembering
7	What is a public key signature scheme?	BTL2	Understanding
8	Define signing and verification functions.	BTL1	Remembering
9	What is full domain hashing?	BTL2	Understanding

10	State the assumptions required for a secure public key signature scheme.	BTL1	Remembering
11	What is Shamir's secret sharing?	BTL1	Remembering
12	What is meant by Zero Knowledge Proof?	BTL1	Remembering
13	Differentiate between MAC and digital signature.	BTL2	Understanding
14	What is non-repudiation in digital communication?	BTL2	Understanding
15	List applications of secret sharing schemes.	BTL1	Remembering
16	Define cryptographic protocol analysis.	BTL2	Understanding
17	What is meant by authentication tag?	BTL1	Remembering
18	State the significance of nonce in authentication.	BTL2	Understanding
19	What are one-time signatures?	BTL1	Remembering
20	Define adversarial model in authentication.	BTL1	Remembering
21	What is signature forgery?	BTL1	Remembering
22	State the goal of message authentication.	BTL1	Remembering
23	What is the need for integrity in messages?	BTL2	Understanding
24	Differentiate between confidentiality and authentication.	BTL2	Understanding

PART - B

Q.no	Question	BTL	Competence
1	Explain the construction of MAC using a PRF. Provide an example.	BTL3	Applying
2	Illustrate the working of a public key signature scheme.	BTL3	Applying
3	Analyze the security of full domain hashing in digital signatures.	BTL4	Analyzing
4	Evaluate the role of variable length MACs in protocol design.	BTL5	Evaluating
5	Construct a one-time signature scheme using a one-way function.	BTL6	Creating
6	Compare weak and strong MACs with relevant use cases.	BTL4	Analyzing
7	Develop a signature scheme using RSA and explain its steps.	BTL6	Creating
8	Apply Shamir’s Secret Sharing for secure key distribution.	BTL3	Applying
9	Design a MAC that supports variable-length input securely.	BTL6	Creating
10	Evaluate the authentication and integrity properties of MACs.	BTL5	Evaluating
11	Analyze the trade-offs between MACs and digital signatures.	BTL4	Analyzing
12	Demonstrate how non-repudiation is ensured using digital signatures.	BTL3	Applying
13	Design a protocol with zero-knowledge proof authentication.	BTL6	Creating

14	Assess the security implications of using hash-based MACs.	BTL5	Evaluating
15	Apply full domain hashing in designing a secure digital signature scheme.	BTL3	Applying
16	Justify the need for secret sharing in distributed systems.	BTL5	Evaluating
17	Propose a hybrid authentication mechanism using both MAC and digital signature.	BTL6	Creating