Reg. No															

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Seventh Semester

18CSE435J - ADVANCED CRYPTOGRAPHY

(For the candidates admitted during the academic year 2020 - 2021 & 2021 - 2022)

Note:

i. **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

PART - A (20 × 1 = 20 Marks)

Answer **all** Questions

Marks BL CO

1. Which of the following best describes private key encryption in cryptography? 1 2 1
   (A) It uses two different keys for encryption and decryption.
   (B) It uses a public key for encryption and a private key for decryption.
   (C) It uses a single key for both encryption and decryption.
   (D) It uses a public key for both encryption and decryption.

2. Which principle of modern cryptography involves clearly specifying what security means for a cryptographic system? 1 1 1
   (A) Provable Security and Real-World Security
   (B) Principle 1 - Formal Definitions
   (C) Principle 2 - Precise Assumptions
   (D) Principle 3 - Proofs of Security

3. Perfect secrecy in cryptography implies that: 1 1 1
   (A) The ciphertext reveals no information about the plaintext.
   (B) The encryption algorithm is unbreakable.
   (C) The encryption keys are perfectly secure.
   (D) The encryption process is extremely fast.

4. Shannon's Theorem is related to: 1 1 1
   (A) Cryptanalysis techniques.
   (B) Proving the security of cryptographic systems.
   (C) The maximum achievable compression ratio for data.
   (D) The limitations of perfect secrecy.

5. Which cryptographic concept involves generating a long stream of pseudorandom bits to be combined with plaintext for encryption, often used in stream ciphers? 1 2 2
   (A) Chosen-Plaintext Attacks
   (B) A Secure Fixed-Length Encryption Scheme
   (C) Pseudorandom Generators
   (D) Proofs by Reduction

6. Which security property ensures that an attacker cannot distinguish between two different plaintexts encrypted with the same key, even if the attacker knows both plaintexts and ciphertexts? 1 2 2
   (A) Semantic Security
   (B) The Asymptotic Approach
   (C) The Concrete Approach
   (D) Computational Security

7. Which mode of operation in block ciphers provides security against chosen-plaintext attacks (CPA) by randomizing the encryption of each block? 1 1 2
   (A) Stronger Security Notations
   (B) Cipher Block Chaining (CBC) mode
   (C) Constructing CPA Secure Encryption Schemes
   (D) Implement DES Algorithm

8. Which cryptographic algorithm is known for its block size of 64 bits and variable key length, making it suitable for various encryption applications? 1 1 2

(A) Proofs by Reduction (B) Semantic Security

(C) Security for Multiple Encryptions (D) Implement Blowfish Algorithm

9. In public key cryptography, which mathematical concept is crucial for operations like encryption and decryption? 1 1 3

(A) Prime numbers (B) Isomorphism

(C) Group Theory (D) Modular Arithmetic

10. What is the fundamental property of prime numbers that makes them essential in public key cryptography, particularly in algorithms like RSA? 1 1 3

(A) They are even numbers. (B) They have no divisors other than 1 and themselves.

(C) They are always odd numbers. (D) They are composite numbers.

11. The Diffie-Hellman key exchange protocol is used for: 1 1 3

(A) Digital signatures. (B) Key exchange over an insecure channel.

(C) Public key encryption. (D) Symmetric encryption.

12. In RSA encryption, what is the primary assumption that forms the basis of the security of the algorithm? 1 1 3

(A) The intractability of the factoring problem. (B) The difficulty of computing discrete logarithms.

(C) The isomorphism of groups. (D) The commutative property of modular multiplication.

13. Which of the following algorithms is specifically designed to factor large integers, a problem that is relevant in cryptography? 1 2 4

(A) The Pohlig-Hellman Algorithm (B) The Index Calculus Algorithm

(C) Setup a Honeypot and Honeypot on Network (D) Constructing Collision-Resistant Hash

14. Digital signatures are used in cryptography primarily for: 1 1 4

(A) Factoring large integers. (B) Encrypting data.

(C) Verifying the authenticity and integrity of data. (D) Performing discrete logarithm calculations.

15. One-way functions in cryptography are functions that: 1 1 4

(A) Produce the same output for every input. (B) Are always reversible.

(C) Require a public key and a private key. (D) Are easy to compute in one direction but hard to reverse.

16. Which cryptographic concept is related to ensuring that it is computationally infeasible to find two different inputs that hash to the same output? 1 2 4

(A) Discrete Logarithms from Collisions (B) Permutations

(C) Working in Subgroups of Zp (D) Algorithms for Computing Discrete Logarithms

17. What is the primary challenge in key management for public key encryption? 1 1 5

(A) Creating strong encryption keys. (B) Encrypting and decrypting messages.

(C) Generating digital signatures. (D) Distributing encryption keys securely.

18. The man-in-the-middle attack can endanger the security of the diffie-hellman if two parties are not 1 1 5

(A) authenticated (B) joined
(C) separate (D) submit

19. Which cryptographic paradigm combines the Key Encapsulation Mechanism (KEM) with the Data Encapsulation Mechanism (DEM) for secure encryption? 1 2 5

(A) The Paillier Encryption Scheme (B) Hybrid Encryption
(C) Public-Key Encryption from Trapdoor Permutations (D) Trapdoor Permutations

20. The Paillier Encryption Scheme is known for its ability to perform operations like: 1 1 5

(A) Homomorphic encryption on encrypted data. (B) Fast symmetric key encryption.
(C) Digital signatures. (D) Factoring large integers.

PART - B (5 × 4 = 20 Marks)
Answer **any 5** Questions

		Marks	BL	CO
21.	Explain the significance of Shannon's Theorem in the field of cryptography.	4	2	1
22.	Explain the concept of Semantic Security in private key encryption and its significance in modern cryptographic systems.	4	2	2
23.	Describe the key principles that make a scheme CPA secure, and discuss the importance of CPA security in encryption schemes.	4	2	2
24.	Explain the basic principles of primality testing and its relevance in cryptographic applications like RSA.	4	2	3
25.	Discuss the concept of isomorphism in the context of group theory and its relationship with the Chinese Remainder Theorem in number theory. Provide a simple example to illustrate this connection.	4	2	3
26.	Explain the purpose and benefits of constructing collision-resistant hash functions in cryptographic applications.	4	2	4
27.	Explain the basic concept of a Trapdoor Permutation in cryptography and why it is significant in public key encryption.	4	2	5

PART - C (5 × 12 = 60 Marks)
Answer **all** Questions

		Marks	BL	CO
28.	(a) Explain the process of implementing a Substitution Cipher. Provide a step-by-step description of how this type of encryption works, and discuss its strengths and weaknesses. Illustrate your answer with a real-world example of a Substitution Cipher. **(OR)** (b) Consider a scenario where you need to implement data encryption for a secure communication channel. Describe the key principles of modern cryptography (Principle 1 - Formal Definitions, Principle 2 - Precise Assumptions, Principle 3 - Proofs of Security) and explain how these principles can guide the design and implementation of a secure encryption scheme. Provide a hypothetical example to demonstrate your understanding.	12	3	1
29.	(a) Describe the key aspects of the Data Encryption Standard (DES) algorithm, including key generation, encryption, and decryption processes. Assess its security and significance in the history of encryption standards. **(OR)** (b) Illustrate how the Blowfish encryption algorithm operates, focusing on its unique Feistel network structure and the key-expansion process. Elaborate on the practical applications of Blowfish in modern cryptography and highlight any considerations for its security in contemporary contexts.	12	3	2

30. (a) Describe the Diffie-Hellman key exchange algorithm, its mathematical foundation, and how it enables secure communication. Discuss a practical scenario where the Diffie-Hellman algorithm can be employed for secure key exchange. 12 3 3

(OR)

(b) Explain the fundamental concepts of public key cryptography, focusing on how it differs from private key cryptography and its real-world applications. Discuss the significance of number theory, modular arithmetic, and group theory in the development of public key encryption systems.

31. (a) Illustrate how the Pohlig-Hellman Algorithm operates to solve the discrete logarithm problem within a finite cyclic group. 12 3 4

(OR)

(b) Describe the concept of elliptic curves in cryptographic systems and explain how they contribute to secure encryption.

32. (a) Write in detail about the the Paillier Encryption Scheme 12 2 5

(OR)

(b) Detail the KEM/DEM paradigm in public key encryption. Discuss how it combines key management and data encryption. Provide a real-world scenario where KEM/DEM is advantageous for ensuring secure communication.

* * * * *