Reg. No															

B.Tech. DEGREE EXAMINATION, JUNE 2023

Fifth Semester

18CSE335T - PRINCIPLES OF CRYPTOGRAPHY

(For the candidates admitted during the academic year 2018-2019 to 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 40 minutes.

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

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

Part - A (20 × 1 Marks = 20 Marks)

Answer **All** Questions

		Marks	BL	CO
1.	Cryptography when its classical it is actually _____? (A) Art of coding (B) Art of riddles (C) Art of challenging (D) Art of writing or solving codes	1	1	1
2.	Cryptanalysis is _____? (A) Attacker's technique to find the plain text (B) Encryption with valid Key (C) Decryption with valid Key (D) Cryptology	1	2	1
3.	In secret key encryption, the two canonical applications are (A) the distinct parties are separated in space & same party can communicate over time (B) distinct parties are not separated & same party can communicate (C) the distinct parties are separated in space and different parties can communicate over time (D) the same parties are not separated in space and different parties can communicate over time	1	2	1
4.	Caesar Cipher is (A) Transposition cipher (B) Random cipher (C) Substitution cipher (D) One time pad	1	2	1
5.	A negligible function is one that is asymptotically _____ than any inverse polynomial function (A) Smaller (B) larger (C) equal (D) not equal	1	2	2
6.	A scheme is secure if for every _____ A carrying out an attack of some formally specified type, the probability that A succeeds in the attack (where success is also formally specified) is negligible. (A) Probaiistic adversary (B) probabilistic polynomial-time adversary (C) exponential adversary (D) asymptotic adversary	1	2	2
7.	A private-key encryption scheme has indistinguishable encryptions in the presence of an eavesdropper if and only if it is _____ in the presence of an eavesdropper (A) computationally secure (B) exponentially secure (C) semantically secure (D) not secure	1	2	2
8.	Technique for preventing replay attacks is to use _____ (A) frequency (B) error messages (C) authentication (D) Time stamps	1	1	2

9.	The primary requirement is to avoid collisions, or two inputs that map to the same _____		1	1	3
	(A) Message Digest	(B) encryption			
	(C) Decryption	(D) code			
10.	The _____ is a common approach for extending a compression function to a full-fledged hash function,		1	1	3
	(A) Caeser cipher	(B) Merkle–Damgard transform.			
	(C) Hashing algorithm	(D) avalanche			
11.	A commitment scheme has _____		1	1	3
	(A) Cryptography	(B) Encryption			
	(C) hiding and binding	(D) Hashing			
12.	An important property in any block cipher is that a small change in the input must "affect" every bit of the output. We refer to this as the_____		1	1	3
	(A) Avalanche effect	(B) Merkle–Damgard transform			
	(C) Hashing	(D) Cryptography			
13.	Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7		1	2	4
	(A) 1629	(B) 1665			
	(C) 1657	(D) 1628			
14.	Express 10110_{two} in base ten		1	2	4
	(A) 20	(B) 21			
	(C) 22	(D) 23			
15.	Study the following number pattern and add two more lines. $1 \cdot 9 + 2 = 11$ $12 \cdot 9 + 3 = 111$ $123 \cdot 9 + 4 = 1111$ $1234 \cdot 9 + 5 = 11111$ $12345 \cdot 9 + 6 = 111111$ $123456 \cdot 9 + 7 = 1111111$		1	2	4
	(A) $1234567 \cdot 9 + 8 = 1111111$; $12345678 \cdot 9 + 9 = 11111111$	(B) $1234567 \cdot 9 + 8 = 111111111$; $12345678 \cdot 9 + 9 = 1111111111$			
	(C) $1234567 \cdot 9 + 8 = 1111111$; $12345678 \cdot 9 + 9 = 111111111$	(D) $1234567 \cdot 9 + 8 = 11111111$; $12345678 \cdot 9 + 9 = 111111111$			
16.	Apply the Euclidean algorithm to find (4076, 1024)		1	2	4
	(A) 3	(B) 4			
	(C) 5	(D) 6			
17.	The _____ is an example of an encryption scheme that is homomorphic.		1	1	5
	(A) Rabin Trapdoor	(B) Paillier encryption scheme			
	(C) RSA Algorithm	(D) Digital Certificate			
18.	Rabin trapdoor permutation, which can be used to construct a _____scheme.		1	1	5
	(A) public-key encryption	(B) Private key encryption			
	(C) Hashing	(D) Digital Signature			
19.	_____, is simply a signature binding an entity to some public key		1	1	5
	(A) Digital signature	(B) Hashing			
	(C) Digital certificate	(D) Paillier encryption scheme			
20.	Diffie Hellman algorithm is _____		1	1	5
	(A) Key exchange algorithm	(B) Public key encryption			
	(C) Private Key encryption	(D) Classical encryption			

Part - B (5 × 4 Marks = 20 Marks) — Marks | BL | CO

Answer **any 5** Questions

		Marks	BL	CO
21.	Give the formal definitions for the process of 1) Generation of Keys 2) Encryption and 3) Decryption with respect to symmetric key algorithms.	4	2	1
22.	What is One time pad? Define the construction of One-time pad.	4	2	1
23.	Explain Block Cipher modes of operations.	4	2	2
24.	How Feistel networks build block ciphers?	4	2	3
25.	What is Division Algorithm? How it can be proved?	4	2	4
26.	Explain Chinese remainder theorem.	4	1	4
27.	Give the formal definition of Digital Signature.	4	1	5

Part - C (5 × 12 Marks = 60 Marks) — Marks | BL | CO

Answer **All** Questions

		Marks	BL	CO
28.	a. Explain the Classical Cryptography algorithms with suitable examples. **(OR)** b. Explain the threat model in the context of encryption in the order of increasing power of the attacker.	12	2	1
29.	a. Explain - A pseudorandom generator provides a natural way to construct a secure, fixed-length encryption scheme with a key shorter than the message. **(OR)** b. Explain Information-Theoretic MACs and its Limitations.	12	2	2
30.	a. The birthday problem is the following: if q people are in a room, what is the probability that two of them have the same birthday? How this helps to find collisions in hash functions. **(OR)** b. How to construct a pseudorandom function from any (length-doubling) pseudorandom generator.	12	2	3
31.	a. "The GCD of the positive integers a and b is a linear combination of a and b" – Prove this theorem. **(OR)** b. List the various divisibility tests with appropriate examples.	12	2	4
32.	a. Construct the Key Encapsulation mechanism in public key cryptography. **(OR)** b. Describe RSA Signatures including plain RSA and RSA- FDH.	12	2	5

* * * * *