Reg. No															

B.Tech DEGREE EXAMINATION, MAY 2024

Fifth & Sixth Semester

18ECE224T - CRYPTOGRAPHY AND NETWORK SECURITY

(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 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.	In symmetric key cryptography, the secret key is kept by _____ (A) sender (B) receiver (C) sender and receiver (D) Intruder	1	1	1
2.	In cryptography, the order of the letters in a message is rearranged by _____ (A) Substitution ciphers (B) Transpositional ciphers (C) Repudiation (D) Replay	1	1	1
3.	What is data encryption standard (DES)? (A) Block cipher (B) Stream cipher (C) Bit cipher (D) Byte cipher	1	1	1
4.	What is the maximum size of the key in blowfish algorithm? (A) 256 bits (B) 512 bits (C) 56 bytes (D) 48 bytes	1	1	1
5.	A curve over Zp, we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p-1 and in which calculations are performed modulo p is called as _____ (A) Prime curve (B) Binary curve (C) Elliptic curve (D) Trapezoidal curve	1	1	1
6.	Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not ..... (A) Authenticated (B) Joined (C) Submitted (D) Separated	1	1	2
7.	The multiplicative inverse of 550 mod 1769 is _____ (A) 434 (B) 224 (C) 550 (D) 1	1	1	2
8.	If three points on an elliptic curve lies on a straight line their sum is _____ (A) 0 (B) 1 (C) 6 (D) 3	1	1	2
9.	SHA-1 has a message digest of (A) 160 bits (B) 512 bits (C) 628 bits (D) 820 bits	1	1	2
10.	Which of the following is not a property of Hash function? (A) Pre-Image Resistance (B) Compression (C) Fixed length output (D) Fixed length input	1	1	2

11.	What is a one-way password file? (A) A scheme in which the password is jumbled and stored (B) A scheme in which the password is XOR with a key and stored (C) A scheme in which the hash of the password is stored (D) A scheme in which the password is passed through a PRF, which is then stored	1	1	3
12.	For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is _____kk (A) 2^k (B) 2^n (C) Min $(2^k, 2^n)$ (D) $2^k/2^n$	1	1	3
13.	IPsec is designed to provide security at the _____ (A) Transport layer (B) Network layer (C) Application layer (D) Session layer	1	1	3
14.	An attempt to make a computer resource unavailable to its intended users is called _____ (A) Denial-of-service attack (B) Virus attack (C) Worms attack (D) Botnet process	1	1	3
15.	For a client-server authentication, the client requests from the KDC a _____for access to a specific asset. (A) token (B) local (C) ticket (D) user	1	1	3
16.	Pretty good privacy (PGP) is used in _____ (A) Browser security (B) Email security (C) FTP security (D) WiFi security	1	1	4
17.	SPI stands for _____ (A) Scalable payload index (B) Scalable parameter index (C) Security physical index (D) Security parameters index	1	1	4
18.	_____algorithm is used for data encryption in GSM. (A) A7 (B) A5 (C) A3 (D) A1	1	1	4
19.	A multilevel security enforces _____ rules. (A) No read down and no read up (B) No read up and no write down (C) No read up and no write up (D) No read down and no write down	1	1	4
20.	A_____ replicate itself and send copies to another computer across network connections. (A) Trajan horse (B) Bacteria (C) Virus (D) Worms	1	1	4

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

		Marks	BL	CO
21.	Discuss in brief about security attacks.	4	1	1
22.	Explain Rail Fence Encryption with Example.	4	1	1
23.	Find the gcd (161,28) using Extended Euclidean algorithm.	4	1	2
24.	Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. If user B has private key is 6, find his public key?	4	1	3
25.	Illustrate the Process of PGP.	4	1	4
26.	Explain Password Management Techniques.	4	1	5

		Marks	BL	CO
27.	Illustrate the Firewall types.	4	1	5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

28.	(a) Perform encryption and decryption using Hill cipher method. Plain Text : VLKH , Key : ACTW.	12	1	1
	(OR)			
	(b) Describe the working steps of Blowfish with neat diagrams.			
29.	(a) Perform encryption and decryption using RSA Algorithm for the following. Plain text=88, e=7, p=17, q=11.	12	1	2
	(OR)			
	(b) Explain in detail the Elliptic curve cryptography.			
30.	(a) Explain in detail about MD-5 Algorithm in detail.	12	1	3
	(OR)			
	(b) Explain in detail the generation and verification processes of Digital Signature standard.			
31.	(a) Illustrate the working of Kerberos V4 with its dialogues.	12	1	4
	(OR)			
	(b) Explain the AH and ESP protocols of IPSec with neat sketches.			
32.	(a) Explain the Password Selection Strategies. Also illustrate the UNIX password protection scheme.	12	1	5
	(OR)			
	(b) Explain in detail about Reference monitor concept and show how Trojan attack can be detected.			

* * * * *