29. a.	Categorize the different headers in IP Sec protocol and explain them in detail with diagram.	10	4	4	3
	(OR)				
b.	Explain the stages and intricate steps involved in Secured Electronic Transaction (SET).	10	4	4	3
30. a.	Distinguish the various intrusion techniques and detection mechanisms.	10	4	5	1
	(OR)				
b.	Interpret the possible attacks due to various malwares.	10	4	5	3

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, MAY 2022
Fifth and Sixth Semester

18ECE224T – CRYPTOGRAPHY AND NETWORK SECURITY
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

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** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

		Marks	BL	CO	PO
	PART – A (25 × 1 = 25 Marks) Answer **ALL** Questions				
1.	List the number of subkey arrays in Blowfish algorithm. (A) 2 (B) 3 (C) 4 (D) 5	1	1	1	1
2.	If the loss due to attack is limited, them the attack is classified as _____ level. (A) High (B) Low (C) Medium (D) Severe	1	2	1	3
3.	Identify the attack that is hard to stop and easy to detect. (A) Active (B) Passive (C) Local (D) Corporate	1	2	1	3
4.	Express ECB in block cipher modes of operation. (A) Electronic cipher book (B) Electronic code book (C) Easy code book (D) Easy code block	1	2	1	1
5.	Indicate the number of entries in 'P' array and in 'S' array in Blowfish algorithm. (A) 15, 216 (B) 18, 256 (C) 22, 512 (D) 18, 512	1	2	1	3
6.	The computational complexity of factorization in RSA algorithm is expressed as _____. (A) $O(e\hat{}\log n \log \log n)$ (B) $O(e \log n \log n)$ (C) $O(e\hat{}\log n)$ (D) $O(\log n \log \log n)$	1	2	2	3
7.	The expression ~~for~~ $(ab) \bmod p$ according to modulo arithmetic is _____. (A) $(a \bmod p)(b \bmod p)$ (B) $((a \bmod b)(b \bmod p)) \bmod p$ (C) $((a \bmod p)(b \bmod a)) \bmod p$ (D) $((a \bmod p)(b \bmod p)) \bmod p$	1	2	2	3

8. State the attack which is prevented by strong collision resistance property of Hash. 1 1 3 7
   (A) Birthday attack (B) Non repudiation
   (C) Forgery (D) Brute force attack

9. Identify the number of elements in reduced set of residues in set. 1 2 2 7
   (A) Euler function (B) Fermat function
   (C) Euler totient function (D) Littls function

10. Predict the method to solve $x\hat{}y \bmod n$, when 'n' is prime. 1 2 2 1
   (A) Euler's theorem (B) Modulo exponentiation
   (C) Fermat's theorem (D) Miller's theorem

11. Express the attack associated with Deffie Hellman algorithm. 1 2 2 1
   (A) Brute force (B) Statistical
   (C) Birthday (D) Man in middle attack

12. Select the output of a Message Authentication Code algorithm (MAC). 1 1 3 1
   (A) Cryptographic checksum (B) Variable length message
   (C) Variable sized authenticator (D) Fixed message

13. Predict the prime requirement in symmetric encryption. 1 2 3 7
   (A) Public gateway (B) Common secret key
   (C) Private key (D) Private gateway

14. Identify the algorithm that has masking keys. 1 2 3 3
   (A) IDEA (B) DES
   (C) RSA (D) CAST

15. Relate the certificate of X.509 with the source who generates it. 1 2 3 3
   (A) License authority (B) Arbiter
   (C) Certificate authority (D) Third party

16. Interpret the service achieved by combining MAC with shared secrete key in SSL record protocol. 1 2 4 1
   (A) Integrity (B) Confidentiality
   (C) Availability (D) Security

17. Identify the protocol which conveys SSL related alerts to peer entity. 1 2 4 1
   (A) SSL peer (B) SSL change cipher specification
   (C) SSL alert (D) SSL record

18. Recall the strongest authentication in X.509 certificate format. 1 2 4 1
   (A) One way authentication (B) Two way authentication
   (C) Three way authentication (D) Many way authentication

19. Identify the part of SSL architecture that associated the client and server. 1 2 4 1
   (A) SSL session (B) SSL record
   (C) SSL connectionless (D) SSL change cipher

20. Name the entity which verifies all the certificates in Secured Electronic Transaction (SET). 1 1 4 7
   (A) Bank (B) Payment gateway
   (C) Merchant (D) Customer

21. Identify the malware that is very hard to block in operating system. 1 2 5 7
   (A) Logic bomb (B) Trap door
   (C) Trojan horse (D) Virus

22. Classify the anomaly detection method of intrusion detection. 1 2 5 1
   (A) Statistical (B) Rule – based
   (C) Operation based (D) Threshold based

23. Indicate the types of intrusion detection when varying audit records formats and dealt. 1 2 5 1
   (A) Hierarchical (B) Centralized
   (C) Distributed (D) Stand alone

24. Identify the method for defining a threshold independent of user, for the frequency of occurrence of various events. 1 2 5 7
   (A) Statistical anomaly detection (B) Rule – based detection
   (C) Reactive audit records (D) Profile based detection

25. Classify the malware code red into the corresponding category. 1 2 5 1
   (A) Trojan horse (B) Zombie
   (C) Virus (D) Worm

PART – B (5 × 10 = 50 Marks)

Answer **ALL** Questions

		Marks	BL	CO	PO
26. a.i.	Sketch the network security model and explain.	5	3	1	3
ii.	Compare stegnogrpahy and cryptography with examples.	5	4	1	3
	(OR)				
b.	Explain all block cipher modes of operation.	10	4	1	3
27. a.	Relate Euler's theorem to RSA algorithm and prove the logic of RSA.	10	3	2	3
	(OR)				
b.	Explain elliptic curve cryptography in detail.	10	4	2	3
28. a.i.	Illustrate the requirements of Hash function.	5	3	3	1
ii.	Demonstrate MD5 algorithm with block diagram.	5	3	3	3
	(OR)				
b.	With neat sketch, explain the digital signature algorithm.	10	3	3	3