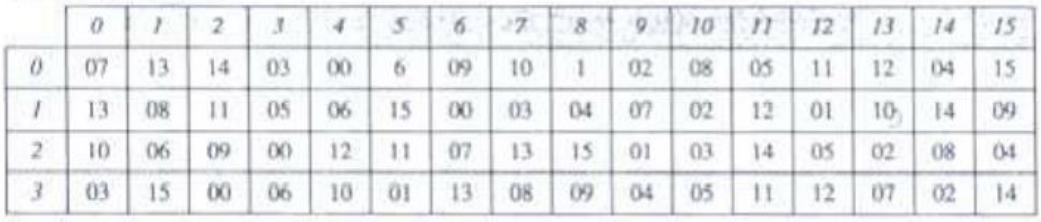
V SEMESTER B.TECH.
(Computer and Communication Engineering)
MAKEUP EXAMINATIONS, JAN 2022
SUBJECT: INFORMATION SECURITY [ICT 3172]
REVISED CREDIT SYSTEM PART A
22/2/2022

Question	M
1.What type of cipher relies upon changing the location of characters within a message to achieve confidentiality? A. Stream cipher **B. Transposition cipher** C. Block cipher D. Substitution cipher	1
2.Arya wishes to communicate a very secret message to Rehman. She uses the prime numbers 13 and 17 to generate her key pairs. If her public key is 35 , what is her private key? a. 9 b. 221 c. **11** d. 10	1
3.What kind of attack makes the Caesar cipher virtually unusable? A. Meet-in-the-middle attack B. Escrow attack **C. Frequency attack** D. Transposition attack	1
4.How many rounds does the AES-256 perform? a) 10 b) 12 **c) 14** d) 16	1
5. Show the result of passing 111111 through S-box 4 (Figure 1) of Data Encryption Standard.  Figure 1: S-Box 4 a.1101 b.1001 c.1100 **d. 1110**	1
6. The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key. a. True	1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	6	09	10	1	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

b. False	
7. In SHA-512, the message is divided into blocks of size ___ bits for the hash computation. **a) 1024** b) 512 c) 256 d) 1248	1
8. Which one of these is not a Whirlpool function? a) Add Key b) Substitute Bytes c) Mix Rows **d) Shift Rows**	1
9. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text **a) nlazeiibljji** b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki	1
10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 **b. 18** c. 28 d. 20	1
11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? **a) CTR, ECB** b) CTR, CFB c) CFB, OFB d) ECB, OFB	1
12. Using Rabin cryptosystem with p=23 and q=7,encrypt P=24 to find ciphertext. The Cipher text is a) 42 **b) 93** c) 74 d) 12	1
13. In ----------, a claimant proves her identity to the verifier. **a. entity authentication** b. message authentication c. message confidentiality d. message integrity	1
14. Myna tries to exchange some confidential information with Sabrina in a meeting having 20 members. Before actual data exchange, Myna authenticates herself to Sabrina without sending any secret. To do so she answered Sabrina's question :"Add 20 to your favorite number". The scheme used in this scenario is ……..	1

a. Zero knowledge scheme **b. Challenge response scheme** c. Encryption Scheme d. Hashing scheme e. None of the options.	
15. A MDC is a ----------message digest. **a. Keyless** b. Keyed c. Both the options d. Neither of the options	1
16. ---------- criteria of a hash function ensures that no two messages hash to the same digest. **a. Strong-collision resistance** b. One-wayness c. Pre-image resistance d. All of the options	1
17. Digital Signature cannot provide …….. a. Integrity **b. Confidentiality** c. Non-Repudiation d. Authentication	1
18. The Certification Authority (CA) signs the digital certificate to prevent forgery using…… a. user's public key b. user's private key c. its own public key **d. its own private key**	1
19. In Kerberos …….. issues the ticket to the user requesting a service. **a. Authentication Server** b. Ticket Granting Server c. PKI d. CA	1
20. A user has created a new program and wants to distribute it to everyone in the company. The user wants to ensure that when the program is downloaded that the program is not changed while in transit. What can the user do to ensure that the program is not changed when downloaded? a) Use Firewalls b) Encrypt the program and require a password after it is downloaded. c) Encrypt the session **d) Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded.** e) Provide IP security	1
21. Alice and Bob use the same password to login into the company network. This means both would have the exact same hash for their passwords. What could be implemented to prevent both password hashes from being the same? a) RSA	1

b) peppering **c) salting** d) pseudo-random generator	
22. What term is used to describe concealing data in another file such as a graphic, audio, or other text file? a) Masking and scrambling **b) steganography** c) obfuscation d) cryptology	1
23. A company is concerned with traffic that flows through the network. There is a concern that there may be malicious traffic that exists that is not being blocked or eradicated by antivirus. What technology can be put in place to detect potential malware traffic on the network in real time? **a) IDS** b) firewall c) IPS d) Session Hijacking	1
24. Compute the RSA digital signature for the following scenario. "Sign the message m=35. The private key used is (29,91) with the public key being (5,91)." a. 35 **b. 42** c. 41 d. 38	1
25. In an Elgammal Cryptosystem, Sender chooses p = 107, e1 = 2, d = 67, and the random integer is r=45. Find the plaintext to be transmitted if the ciphertext is (28,9). a) 45 b) 76 **c) 66** d) 13	1
26.HMAC is slower than CMAC and is similar to cipher block chaining mode. The given statement is a. True **b. False**	1
27. The responsibility of a certification authority for digital signature is to authenticate the _____ a) hash function used b) private keys of subscribers **c) public keys of subscribers** d) tickets generated	1
28. Data origin authentication cannot be provided using ---------- a. Digital signature b. MAC c. symmetric encryption d.**None of the answers.**	1

29. A PKI is not helpful for---------- a. Authentication b. Key Generation c. Certificate verification **d. None of the answers**	1
30. If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password? (a)Man-in-the middle attack (b)Birthday attack (c)Denial of service attack **(d)Dictionary attack**	1