Hall Ticket Number:

□□□□□□□□□□□□

Code No. : 17632 S (B)

VASAVI COLLEGE OF ENGINEERING *(AUTONOMOUS)*, HYDERABAD

Accredited by NAAC with A++ Grade

B.E. (I.T.) VII-Semester Supplementary Examinations, July-2022

Cryptography and Network Security (PE-I)

Time: **3 hours** Max. Marks: **60**

*Note: Answer all questions from **Part-A** and any **FIVE** from **Part-B***

Part-A (10 × 2 = 20 Marks)

Q. No.	Stem of the question	M	L	CO	PO
1.	Use Fermat's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29.	2	3	1	2
2.	What is the need for security? Draw the model for network security.	2	1	1	1
3.	Encrypt the message "this is an exercise" using additive Cipher with key=20.	2	3	2	2
4.	What is the necessity of block cipher modes of operation? List out the advantages and disadvantages of output feedback mode.	2	2	2	1
5.	Explain Encryption/Decryption procedure using Elliptic Curve Cryptography.	2	1	3	1
6.	Two parties use the Diffie-Hellman key exchange protocol with p=23 and g=5. If the common secret that both sides compute=21, then what are the possible values of the initial secrets chosen by each of them?	2	3	3	2
7.	Identify the Security Requirements of message authentication?	2	1	4	1
8.	Compare and Contrast MACs based on Hash functions (HMAC) and MACs based on Block Ciphers (CMAC).	2	4	4	2
9.	List and briefly define types of cryptanalytic attacks.	2	1	5	1
10.	List important design considerations for a stream cipher. Why is not desirable to reuse a stream cipher key?	2	2	5	1
	Part-B (5 × 8 = 40 Marks)				
11. a)	Define Euler's Totient Function. Prove that, $\phi(pq) = (p-1)(q-1)$, where p and q are prime numbers.	4	3	1	2
b)	Prove the following: i) [(a mod n) - (b mod n)] mod n = (a - b) mod n ii) [(a mod n) * (b mod n)] mod n = (a * b) mod n	4	3	1	2
12. a)	Use Playfair Cipher with key "COMPUTER" to encrypt the message "CRYPTOGRAPHY".	4	3	2	2
b)	Explain the S-box design of DES algorithm. Describe single round of DES algorithm.	4	2	2	1

Contd... 2

20

13. a)	Perform encryption and decryption using RSA Algorithm for the following: P=7; q=11; e=13; M=8.	4	3	3	2
b)	Consider a Diffie-Hellman scheme with a common prime q = 11 and primitive root α = 2. i) Show that 2 is a primitive root of 11. ii) If user A has public key $Y_A = 9$, what is A's private key? iii) If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A.	4	3	3	2
14. a)	List different types of attacks addressed by message authentication.	4	1	4	1
b)	Illustrate the working of SHA-1 with neat sketch.	4	2	4	1
15. a)	What is ciphertext only attack, known plaintext attack and chosen plaintext attack? Explain in detail.	4	1	5	1
b)	Explain Shamir's Secret sharing scheme with an example.	4	2	5	1
16. a)	Find the least residue of 9^{794} modulo 73.	4	3	1	2
b)	Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why is not needed in AES. i) XOR of subkey material with the input to the **f** function ii) XOR of the **f** function output with the left half of the block iii) **f** function iv) Permutation **P**	4	3	2	2
17.	Answer any *two* of the following:				
a)	Consider an ElGamal scheme with a common prime q = 71 and a primitive root a = 7. i) If B has public key $Y_B = 3$ and A choose the random integer k = 2, what is the Ciphertext of M = 30? ii) If A chooses a different value of k and the encoding of M = 30 is C = (59, C_2), what is the integer value of C_2?	4	3	3	2
b)	How digital signature is implemented using RSA approach.	4	2	4	1
c)	Describe about Identity Based Encryption (IBE) with an example.	4	2	5	1

M : Marks; L: Bloom's Taxonomy Level; CO; Course Outcome; PO: Programme Outcome

i)	Blooms Taxonomy Level – 1	20%
ii)	Blooms Taxonomy Level – 2	30%
iii)	Blooms Taxonomy Level – 3 & 4	50%

*****