Hall Ticket Number:

Code No. : 17642 S (B) N/O

VASAVI COLLEGE OF ENGINEERING *(AUTONOMOUS)*, HYDERABAD

Accredited by NAAC with A++ Grade

B.E. (I.T.) VII-Semester Supplementary Examinations, May/June-2023

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.	State Fermat's theorem. Find the value of 2^{35} mod 7 using Fermat's theorem.	2	3	1	2
2.	List and briefly define the different categories of security attacks.	2	1	1	1
3.	What is the necessity of block cipher modes of operation?	2	2	2	1
4.	Why is it important to use the Feistel cipher in DES?	2	2	2	1
5.	What is meant by EIGamal cryptosystem?	2	1	3	1
6.	Specify the applications of the public key cryptosystem?	2	2	3	1
7.	Compare and Contrast SHA algorithm with MD5 algorithm.	2	2	4	1
8.	Differentiate between Hashing and Encryption. List the different hash functions family.	2	1	4	1
9.	Differentiate between linear cryptanalysis and differential cryptanalysis.	2	2	5	1
10.	List the different types of attacks on cryptosystems.	2	1	5	1
	Part-B (5 × 8 = 40 Marks)				
11. a)	Draw and explain the model for network security.	4	2	1	1
b)	Use Euler Theorem to find a number a between 0 and 9 such that a is congruent to 3^{500} modulo 10.	4	3	1	2
12. a)	Consider the plain text "TECHNOLOGICAL INSTITUTE". Convert into cipher text with the key value '52345' using simple columnar transposition technique.	4	3	2	2
b)	Explain the concept of shift rows in AES Algorithm. How many bytes in State array of AES affected by Shift Rows?	4	2	2	1
13. a)	Consider a Diffie-Hellman scheme with a common prime q = 13, and a primitive root $\alpha = 7$. i) Show that 7 is a primitive root of 13. ii) If Alice has a public key $Y_A = 5$, what is Alice's private key X_A? iii) If Bob has a public key $Y_B = 12$, what is the secret key shared with Alice?	4	3	3	2

Contd... 2

b)	Describe in detail about Elliptic Curve Encryption/Decryption. Is (5,9) a point on the elliptic curve $y^2=x^3-5x+5$ over real numbers?	4	3	3	2
14. a)	Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single blocks and discuss single round function in SHA-512 algorithm.	4	3	4	2
b)	Describe the operation of implementing HMAC with help of neat diagram.	4	2	4	1
15. a)	Define Time/Memory Trade-off (TMTO) attack. What is the basic idea of TMTO? Identify the different phases of Time/Memory Trade-off attack.	4	1	5	1
b)	Illustrate Attribute-based Encryption (ABE). Explain how it is different from Identity- based Encryption (IBE).	4	2	5	1
16. a)	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
b)	Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it 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) The f function iv) Permutation P	4	3	2	2
17.	Answer any ***two*** of the following:				
a)	Perform encryption and decryption using RSA for the following: p=3; q=13; e=5; M=10	4	3	3	2
b)	Describe in detail about Digital Signature with a neat sketch.	4	1	4	1
c)	Explain about Shamir's secret sharing algorithm.	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	37.5%
iii)	Blooms Taxonomy Level – 3 & 4	42.5%

*****