Hall Ticket Number:

Code No. : 17443 S N/O

VASAVI COLLEGE OF ENGINEERING *(AUTONOMOUS)*, HYDERABAD

Accredited by NAAC with A++ Grade

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

Network Security (PE-II)

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	PSO
1.	Which type of attack is this when the marks posted in the college website are modified?	2	1	1	1	2
2.	Give examples for classical and modern encryption techniques.	2	1	1	1	2
3.	Illustrate the end to end encryption and symmetrical encryption from daily applications.	2	1	2	1	2
4.	Encrypt the sentence "All the best for exam using key Vasavi using any encryption technique.	2	2	2	2	2
5.	Use Fermat's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29.	2	2	3	2	2
6.	Draw the block diagram of public key cryptography	2	2	3	1	2
7.	Describe the use of hash functions in network security.	2	1	4	1	2
8.	Illustrate digital signature standards with an example.	2	1	4	1	2
9.	Describe the use of firewalls in securing our data.	2	2	5	1	2
10.	Compare and contrast transport and tunnel modes.	2	1	5	1	2
	Part-B (5 × 8 = 40 Marks)					
11. a)	Is the DES decryption the inverse of DES encryption? Explain your answer.	4	2	1	1	2
b)	Using cryptographic and network security, encrypt the following message using rail fence cipher. Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends. Make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. Indicate what your assumptions are. b. Decrypt the cipher text. Show your work.	4	3	1	2	2
12. a)	What are the advantages and disadvantages of triple DES?	4	1	2	1	2
b)	Illustrate International data encryption algorithm with examples.	4	2	2	1	2

Contd... 2

10

13. a)	In what way is the Diffie–Hellman key exchange algorithm insecure against a man-in-the-middle attack?	4	3	3	2	2
b)	Design Fiestal structure and illustrate advantages of AES over DES.	4	3	3	2	2
14. a)	Examine if it is possible to use a hash function to construct a block cipher with a structure similar to DES?	4	3	4	2	2
b)	Design Kerberos to order things online with an example.	4	3	4	2	2
15. a)	List the direct approaches that can be implemented to counter insider attacks.	4	2	5	1	2
b)	Illustrate the secure electronic transaction with an example.	4	2	5	1	2
16. a)	Illustrate X.800 model with examples.	4	2	1	1	2
b)	Compare block cipher and stream cipher and classify types of block ciphers with examples.	4	3	2	1	2
17.	Answer any *two* of the following:					
a)	In an RSA system, the public key of a given user is $e = 7$, $n = 137$. What is the private key of this user?	4	3	3	2	2
b)	Illustrate Authentication protocols in daily applications.	4	2	4	1	2
c)	Illustrate intruder detection system with an example	4	3	5	1	2

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

i)	Blooms Taxonomy Level – 1	20%
ii)	Blooms Taxonomy Level – 2	40%
iii)	Blooms Taxonomy Level – 3 & 4	40%

*****