Hall Ticket Number:

Code No. : 17453 (B) N/O

VASAVI COLLEGE OF ENGINEERING *(AUTONOMOUS)*, HYDERABAD

Accredited by NAAC with A++ Grade

B.E. (E.C.E.) VII-Semester Main & Backlog Examinations, Dec.-23/Jan.-24

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.	Encrypt the message "Hello World " by using Caesar cipher with key =10	2	3	1	2/2
2.	Justify this statement "Passive attacks are very difficult to detect".	2	3	1	2/2
3.	Define Confusion and Diffusion properties of Modern Ciphers?	2	1	2	1/2
4.	Compare link encryption and end to end encryption methods.	2	2	2	2/2
5.	Draw the structure of the Conventional Public-key encryption with relevant illustrations	2	1	3	1/2
6.	Define Fermats theorem and find GCD of two numbers (1970,1066)	2	3	3	2/2
7.	Compare Transport mode and Tunnel mode?	2	2	4	2/2
8.	Justify the statement-"Message encryption by itself can provide a measure of authentication".	2	3	4	2/2
9.	Describe IPSEC protocols used in IP security?	2	2	5	1/2
10.	Compare TLS and SSL protocols	2	2	5	2/2
	Part-B (5 × 8 = 40 Marks)				
11. a)	Explain the Play Fair cipher algorithm? Encrypt the message "Network Security" using the key 'MONACHRY'	4	3	1	2/2
b)	Illustrate X.800 model with examples?	4	2	1	1/2
12. a)	Write about the round functions and key expansion of IDEA algorithm. How it is different from DES?	4	1	2	1/2
b)	Give the structure of AES. Explain how Encryption/Decryption is done in AES.	4	1	2	1/2
13. a)	Discuss Deffie Hellman key exchange algorithm with an example and how the vulnerability of Deffie Hellman algorithm is removed?	4	2	3	1/2
b)	Describe RSA Algorithm and Estimate the encryption and decryption values for the RSA algorithm parameters. Find n, d if p=11, q=3, e=3.	4	3	3	1/2

Contd... 2

Code No. : 17453 (B) N/O

14. a)	Illustrate the usage of digital signature algorithm (DSA) to perform signing and verifying operations	4	2	4	1/2
b)	Analyze PGP cryptographic functions for authentication only, confidentiality only and both confidentiality and authentication	4	3	4	2/2
15. a)	Illustrate SET for E-commerce transaction with a diagram	4	3	5	2/2
b)	Discuss the role of firewalls in our daily applications? Which firewall architecture offers more security for information assets on trusted network?	4	2	5	2/2
16. a)	Enumerate the various cipher block modes of operation	4	1	1	1/2
b)	Illustrate how Triple Data encryption algorithm is used for encryption and decryption. How do you remove demerits in DES?	4	2	2	2/2
17.	Answer any ***two*** of the following:				
a)	Illustrate the five ingredients of public key cryptosystem and compare with symmetric key cryptosystem.	4	2	3	2/2
b)	Analyze the applications of e.commerce website by using Kerberos	4	3	4	2/2
c)	Illustrate various intruder detection systems	4	3	5	2/2

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%

*****