Hall Ticket Number:

Code No. : 22915

VASAVI COLLEGE OF ENGINEERING *(Autonomous)*, HYDERABAD

M.Tech. (CSE: CBCS) II-Semester Main Examinations, June-2018

Network Security

Time: **3** hours

Max. Marks: **60**

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

Part-A (10 × 2 = 20 Marks)

1. Compare monoalphabetic and polyalphabetic cipher.
2. Differentiate worms and viruses.
3. What is the purpose of Substitution operation in DES?
4. Compute Caeser cipher using k = 5 for the sentence ***"He is my friend".***
5. What are the differences between RSA and DSA digital signature?
6. Draw Public Key Infrastructure (PKIX) model.
7. What are the requirements of message authentication?
8. Why zero knowledge protocols are suitable for smart card protection?
9. How dual signature is useful in SET protocol?
10. What is the role of cipher suit protocol in SSL?

Part-B (5 × 8 = 40 Marks)

11. a) Differentiate between DOS and replay attack [4]

b) Using the given play fair matrix encrypt the message **"Must see you over cadogan west"** [4]

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

12. a) Explain DES algorithm with neat sketch. [4]

b) Explain Diffie-Hellman key exchange algorithm and compute Y_A and Y_B using Diffie-Hellman key exchange algorithm based on the prime number q = 353, primitive root $\alpha = 3$, $X_A = 97$ and $X_B = 233$. [4]

13. a) Explain the working of SHA 5 with neat diagrams. [4]

b) Compute 8 bit hash value for $B23C_X$ using following hash function [4]
Hash Function: XOR the given data by $AAAA_X$, rotate the result by 4 bits left and select alternate 8 bits.

14. a) Draw the structure of X.509 certificate format and explain all the components. [4]

b) Explain Zero knowledge protocol and verify Fiat-Shamir Identification Protocol using prime numbers 3, 5. [4]

15. a) Explain Secure Socket Layer (SSL) Handshake Protocol. [5]

b) Differentiate between tunnel and transport mode of IPsec. [3]

16. a) Compare active and passive attacks. Explain active attacks. [4]

b) Explain key generation algorithm for AES. [4]

17. Answer any *two* of the following:

a) Sketch the diagram for signing and verification in digital signature algorithm. [4]

b) Define fermats little theorem and calculate 2^{27}mod27 using fermats little theorem. [4]

c) What are the security services provided by ESP in IPsec? [4]