Sanjay Ghodawat University, Kolhapur 2019-20

Established as State Private University under Govt. of Maharashtra. Act No XL, 2017 EXM/P/09/01

Year and Program:2019-20 **School of Technology** **Department of TY B.Tech**

Course Code: CST309 **Course Title: Information Security** **Semester – V**

Day and Date Saturday 23/11/19 **End Semester Examination (ESE)** **Time: 3 hrs Max Marks: 100** 10.30 am to 1.30 pm

Instructions:
1) All questions are compulsory.
2) Assume suitable data wherever necessary.
3) Figures to the right indicate full marks.

		Marks	Bloom's Level	CO
Q.1	**Attempt the fallowing**			
a)	Distinguish between active and passive attacks and explain security services defined in ITU-T(X.800) standard	08	L4	CO1
	OR			
a)	With an example explain the followings i) Affine Cipher ii) Playfair Cipher	08	L2	CO1
b)	Explain Fiestel structure for Encryption/Description of block cipher	07	L2	CO1
	OR			
b)	With the neat diagram explain the structure and rounds in AES Encryption	07	L2	CO2
Q.2	**Solve any Two**			
a)	Describe RSA cryptosystem with an example.	07	L5	CO2
	OR			
a)	Explain Miller-Rabin Primality testing algorithm and check whether N =61 is prime or not	07	L2	CO2
b)	Identify the duties and explain the trust model of Public Key Infrastructure (PKI)	08	L3	CO2
	OR			
b)	Describe the signing and verifying process for Digital Signature Standards (DSS)	08	L2	CO2

Q.3		**Solve any Two**			
	a)	Solve the followings i) Using extended Euclidian algorithm find gcd (a,b) and also find the values of S and T given a=161 and b=28 ii) Find the multiplicative inverse of 11 in Z_{26}	08	L3	CO3
	b)	Describe Avalanche effect and the design criteria of S-Boxes for DES algorithm	08	L2	CO3
	c)	With a neat block diagram explain Modification destination code (MDC)	08	L2	CO3
	d)	Draw and explain the X.509 certificates used public key cryptosystem	08	L2	CO3
Q.4		**Solve any Two**			
	a)	Illustrate Diffie-Hellman key exchange algorithm with one example	09	L3	CO3
	b)	Define session key and show how a KDC can create a session key between Alice and Bob	09	L3	CO3
	c)	Describe header Multipurpose Internet Mail Extension (MIME) Protocol	09	L3	CO3
Q.5		**Solve any Two**			
	a)	List SSL services and explain key exchange algorithms	09	L1	CO4
	b)	Explain Authentication Header (AH) used in IPsec	09	L2	CO4
	c)	Describe the different phases of IKE (Internet Key Exchange)	09	L2	CO4
Q.6		**Solve any Three**			
	a)	Explain the services provided by SSL	06	L2	CO4
	b)	Describe the key rings used in PGP	06	L2	CO4
	c)	Describe IKE and Its components	06	L2	CO4
	d)	Explain ISAKMP general header format	06	L2	CO4

*****

ESE