Code No: **R41051** **R10** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, February/March - 2018

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1	a)	What are block ciphers? Explain how diffusion and confusion are used in Block Ciphers. Explain about the Fiestel Structure.	[8]
	b)	How is SQL injection performed? Explain.	[7]
2	a)	What are the operations performed in each round of CAST-128 block cipher? Explain.	[8]
	b)	Explain about the Encryption and decryption functions Triple DES. Evaluate its strength with DES.	[7]
3	a)	Find the value of congruence using the Chinese Remainder Theorem. $x \equiv 2 \bmod 7$ and $x \equiv 3 \bmod 9$, $x \equiv 7 \bmod 13$ and $x \equiv 11 \bmod 12$	[8]
	b)	Explain Miller Rabin Algorithm for Primality Testing. Find out if the number '561' pass Miller Rabin Test.	[7]
4	a)	Explain the characteristics of a good hash function, clearly bringing out the difference between Strong Collision Resistance and Weak Collision Resistance. Which one requires more effort to break?	[8]
	b)	How is the message Digest calculated in SHA-1?	[7]
5	a)	Perform RSA for Data Confidentiality. Perform RSA Encryption/Decryption for the following set of data: P=11, Q=13, e=11,M=7	[8]
	b)	Explain about elliptic curves, encryption in ECC.	[7]
6	a)	Write the message exchanges done in Kerberos version 4. Explain the role of Authentication Server (AS) and Ticket Granting Server (TGS).	[8]
	b)	What are the five services provided by PGP? Explain briefly.	[7]
7	a)	What do you mean by Security Association? What are the parameters? Briefly explain the basic Combinations of security associations.	[8]
	b)	Discuss the scope of ESP encryption and authentication in both IPV4 and IPV6?	[7]
8	a)	What is a firewall? List the characteristics of a good firewall implementation.	
	b)	What is an audit record? What is the use of audit record in intrusion detection?	
	c)	Explain statistical anomaly detection in detail.	[15]