Time (3 Hours) [Total Marks 80]

N. B:

1. Question No. 1 is Compulsory.
2. Solve any THREE from Question No. 2 to 6.
3. Draw neat well labeled diagram wherever necessary.

Q. 1	a)	Enlist security goals. Discuss their significance.	(5)
	b)	Compare and contrast HMAC and CMAC.	(5)
	c)	SHA provides better security than MD. Justify.	(5)
	d)	Design Sample Digital Certificate and explain each field of it.	(5)
Q. 2	a)	Explain Transposition Ciphers with illustrative examples.	(10)
	b)	Given modulus n=91 and public key, e=5, find the values of p, q, phi(n), and d using RSA. Encrypt M=25. Also perform decryption.	(10)
Q. 3	a)	What are Block Cipher Modes. Describe any two in detail.	(10)
	b)	Using Affine cipher, encrypt the Plaintext 'SECURITY' with key pair (5, 2).	(10)
Q. 4	a)	Given generator g= 2 and n=11. Using Diffie Hellman algorithm solve the following: 1. Show that 2 is primitive root of 11 2. If A's public key is 9 , what is A's private key? 3. If B's public key is 3, what is B's private key? 4. Calculate the shared secret key.	(10)
	b)	Explain different types of Denial of Service attacks.	(10)
Q. 5	a)	What is Authentication? Explain Needham Schroeder Authentication protocol.	(10)
	b)	What is a firewall? Explain different types of firewall.	(10)
Q. 6		Write short notes on any **FOUR:** 1. Email Security 2. SSL/TLS 3. IPSec 4. Port Scanning. 5. Honey pots	(20)

****