(10 Marks)

Important Note: 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. 2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

USN

Second Semester M.Tech. Degree Examination, June/July 2016 Information and Network Security

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions.

		Title Till Sires and Till Till Till Till Till Till Till Til	1
		Explain the Feistal Cipher structure. Also explain the various parameter and design	an choices
1	a.	which determine the actual algorithm of Feistal Cipher.	(12 Marks)
	b.	Explain the Avalanche effect.	(08 Marks)
	U.	Explain the Avaianche effect.	
2	a.	Explain with an example the Elgamal cryptosystem.	(12 Marks)
-	b.	Perform encryption and decryption using the RSA algorithm for $p = 3$, $q = 11$,	e = 7 and
		M = 5.	(08 Marks)
		10	
3	a.	Explain the following: i) Caesar cipher ii) Vernam cipher.	(10 Marks)
	b.	Explain Diffie-Hellman key exchange.	(10 Marks)
			(00 M 1-)
4	a.	Explain with neat diagram the general format of X.509 certificate.	(08 Marks)
	b.	Briefly explain four general categories of scheme for distribution of public keys.	(12 Marks)
		Differentiate between conventional encryption and public key encryption.	(05 Marks)
5	a.	List and briefly define types of cryptanalytic attacks based on what is known to the	
	b.		(05 Marks)
	c.	Explain packet exchanges and packet formation of secure shell transport layer pro	tocol.
		20	(10 Marks)
			(10 M l-a)
6	a.	Explain in detail the IEEE 802.11 WLAN.	(10 Marks)
	b.	Briefly explain architecture and record protocol operations of secure sockets layer	. (10 Marks)
		What is an all the forestions of S/MIME	(05 Marks)
7	a.	What is S/MIME? Write the functions of S/MIME.	(05 Marks)
	b.	Explain application of IPsec. Explain with a neat diagram encapsulating security payload format.	(10 Marks)
	c.	Explain with a heat diagram encapsulating security payload format.	
8	0	Write the differences between version 4 and version 5 of Kerberos.	(10 Marks)
0	a.	while the difference between terms being identified mail	(10 Marks)

* * * * *

Describe the function flow of domain keys identified mail.