USN □□□□□□□□□□

14SCN13

First Semester M.Tech. Degree Examination, Dec.2014/Jan.2015
Information and Network Security

Time: 3 hrs. Max. Marks: 100

Note: ***Answer any FIVE full questions.***

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.

1 a. Define cryptanalysis. List various types of cryptanalytic attacks. **(04 Marks)**

b. Briefly explain model of conventional cryptosystem. **(08 Marks)**

c. Encrypt the plaintext "MONDAY" using Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show that calculation and ciphertext [Hint : a = 0, b = 1 - - - - - z = 25]. **(08 Marks)**

2 a. Draw the single round of DES algorithm and explain the process. **(10 Marks)**

b. Explain RSA algorithm in detail. **(06 Marks)**

c. Briefly public key cryptosystem for secrecy. **(04 Marks)**

3 a. Explain ECC Diffie- Helman key exchange. **(10 Marks)**

b. If A and B are the users use the Diffie – Hellman key exchange technique with a common prime q = 11 and a primitive root $\alpha = 5$.

i) If user A has private key $X_A = 3$, what is A's public key Y_A?

ii) If user B has primate key $X_B = 2$, what is B's public key Y_B?

iii) What is the shared secret key K_A and K_B? **(06 Marks)**

c. Discuss various elements of X-509 certificate format. **(04 Marks)**

4 a. List distribution of public key and briefly explain public – key authority. **(10 Marks)**

b. What is Kerberos? Explain overview of Kerberos with neat sketch. **(10 Marks)**

5 a. Compare the threats on the web. **(04 Marks)**

b. Explain SSL protocol stack along with SSL record protocol operations. **(14 Marks)**

c. Draw SSL record format. **(02 Marks)**

6 a. Explain hand shake protocol of SSL. **(10 Marks)**

b. Explain IEEE 802·11 protocol architecture along with IEEEE 802·11i services. **(10 Marks)**

7 a. Explain PGP message generation and PGP message reception techniques. **(10 Marks)**

b. Describe S/MIME functionality. **(04 Marks)**

c. Briefly explain IPSec documentation overview. **(06 Marks)**

8 Write short notes for the following :

a. Fiestel cipher structure

b. Transport layer security

c. Mutual authentication

d. ESP format. **(20 Marks)**

* * * * *