[Total No. of Questions - 8] [Total No. of Printed Pages - 2]
(2123)

1618

M. Tech 3rd Semester Examination

Information Securities

EC-305

Time : 3 Hours **Max. Marks : 100**

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : All Questions carry equal marks. Attempt any five.

1. List and briefly define categories of security attacks. Distinguish between cryptography and steganography. Give an example of a situation in which compromise of confidentiality leads to a compromise in Integrity. **(20)**

2. Explain the network security model. Define and explain different traditional symmetric-key cipher. In GF(2^4), find the inverse of (x^2+1) modulo (x^4+x+1). **(20)**

3. Explain the concept of block cipher and stream cipher with suitable example. Why it is important to study Feistel cipher? Give and explain the block diagram of AES. **(20)**

4. What are the three broad categories of application of the public key cryptography? What requirements must a public key cryptosystems fulfill to be secure algorithm? Define elliptic curves and explain its applications with example in cryptography. **(20)**

5. Define an iterated cryptographic hash function. What characteristics are needed in secure hash function? Suppose H(m) is a collision resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all message x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer. **(20)**

6. Explain different basic and logical functions used in MD5. Define and explain the RSA digital signature scheme and compare it with RSA cryptosystem. Write the algorithm using RSA scheme: one for the signing the process and one for the verifying process. **(20)**

7. (a) Write short note on the followings:
   (i) PGP
   (ii) Access control Policies
   (iii) meet-in-middle attack for double DES

   (b) Consider the following electronic voting protocol:

   Each voter signs his vote with his private key, encrypts the vote with the public key of the Commissioner of Elections (CE) and sends it to the CE. Once all the votes are received, CE decrypts them, validates the signatures, tabulates the votes and announces the results. Discuss the pluses and minuses of the above protocol. **(15+5=20)**

8. (a) Write short note on the followings:
   (i) Intrusion detection techniques
   (ii) Electronic Codebook mode and Cipher Codebook Mode
   (iii) Distributed Denial of service attacks

   (b) Suppose we want to use the RSA scheme for an encryption and have chosen the integer value 77 as the product of two (2) prime numbers p and q. For the private key d and public key e, we have the relation e*d=1 modulo (p-1) (q-1).

   (i) What is the public key e for a private key with d = 43?

   (ii) What is the cipher C for a message with M =5? **(15+5=20)**