4-12-15

Indian Institute of Engineering Science and Technology, Shibpur

B. E. (CST) 7th Semester Final Examination, 2015

Information Security

Elective II (CS704/6)

Time: 3 Hours **Full Marks: 70**

Answer question number 1 and any four from the rest.

1. Answer any **five** questions:
   (a) What is masquerade? Which principle of security is breached because of that?
   (b) What is the role of FAR and FRR in biometric authentication?
   (c) What is the main feature of Polygram substitution cipher?
   (d) How fabrication attack can be prevented?
   (e) What is packet spoofing?
   (f) What is the basic difference between message-digest and message authentication code?
   (g) Write any two disadvantages of HMAC?

   [2 x 5 = 10]

2. (a) i) What do you mean by algorithm mode?
   ii) What is the problem of Electronic Code Book (ECB) mode?
   iii) How Cipher Block Chaining (CBC) mode solves this problem?
   (b) Consider that the 10-bit initial key in Simplified Data Encryption Standard (S-DES) is (1010000010). Find out the corresponding two 8-bit keys where the P10 and P8 boxes are as follows.

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

   (c) i) Explain the mechanism of S-box substitution in a round of Data Encryption Standard (DES).
   ii) Why S-box substitution is so important in DES? [(1 + 2 + 3) + 4 + (3 + 2)]

3. (a) i) Why modular arithmetic is so important in the study of cryptography?
   ii) Prove that [(a mod n) + (b mod n)] mod n = (a + b) mod n, where a, b, n are integers.
   iii) What do you mean by residue classes modulo n, where n is an integer? Give example.
   (b) Prove the correctness of Diffie-Hellman Key-exchange algorithm mathematically.
   (c) What is authentication token? Briefly explain its features.

   [(2 + 2 + 3) + 3 + 5]

4. (a) Explain the steps of MD5 algorithm with block diagram.
   (b) What are the differences between MD5 and SHA-1?

   [10 + 5]

5. (a) Considering $(10101)_2$ as the plain text in Merkle-Hellman hard Knapsack Cryptosystem, show the steps of both encryption and decryption. Select the private key correctly and find out the corresponding public key?

   (b) Briefly explain the method of cryptanalysis of Merkle-Hellman Knapsack cipher using some suitable evolutionary algorithm.

   [9 + 6]

6. (a) What is digital certificate?

   (b) How digital certificate is verified?

   (c) What is the role of a CA and RA?

   (d) Briefly explain the four key steps of digital certificate creation.

   [1 + 3 + 3 + 8]

7. (a) Comment critically on the strength of RSA algorithm.

   (b) (i) Why AES is popular than DES?

   (ii) What is the role of L-Table and E-table in AES?

   (iii) Briefly explain the method of key expansion in AES?

   (c) What is the usefulness of key wrapping?

   [3 + (2 + 3 + 4) + 3]