Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester End-Semester Examination, 2023

Information Security and Cryptography (CS 3204)

Time: 3 Hours **Full Marks: 50**

[Answer any five questions]

1. (a) What is Euler's Totient Function and how is it related with RSA algorithm?
   (b) Prove that [(a mod n) × (b mod n)] mod n = (a × b) mod n for any three integers a, b and n.
   (c) Apply Miller-Rabin Primality Test on 11 and subsequently write down your observation.
   (d) Considering $(10101)_2$ as the plain text in Merkle-Hellman hard Knapsack Cryptosystem, show the steps of both encryption and decryption Assume a private key correctly and find out the corresponding public key for the above encryption and decryption.

[1 + 2 + 2 + 5]

2. (a) Which principle of security is assured using message-digest algorithms?
   (b) Suppose you are to find out the digest of a 6,590 bit message using MD-5 algorithm. Determine the padding that you need to concatenate to this message for further processing.
   (c) Compare and contrast MD-5 and SHA-1 algorithms.
   (d) What is the difference between message-digest and message authentication code?
   (e) Write down the disadvantages of HMAC?

[1 + 2 + 3 + 2 + 2]

3. (a) Compare and contrast RSA based Digital Signature Algorithm and Digital Signature Algorithm (DSA) Introduced by Digital Signature Standard (DSS).
   (b) Is there any role of message digest during creation of digital signature?
   (c) Explain the working principle of digital envelope?
   (d) Write down the motivations behind the use of digital envelope.

[3 + 2 + 3 + 2]

4. (a) What is digital certificate?
   (b) What is the role of a CA and RA during creation of digital certificate?
   (c) Explain the steps of digital certificate creation.
   (d) How can we verify a digital certificate?

[1 + 3 + 4 + 2]

5. (a) What do you mean by protection state of a system?

(b) What is access control matrix and how is it related with protection state of a system?

(c) Let, P denotes the possible protection states of a protection system and Q denotes the states in which the system is authorised to reside. Now, explain how (P – Q) is dealt with in designing a secure system.

(d) What do you mean by Principle of Attenuation of Privilege? Explain with an example.

(e) Explain different phases that a typical virus goes through during its lifetime and also comment critically on its effects during different phases on the protection state of the affected system

[1 + 2 + 2 + 1 + 4]

6. (a) Cryptographic operations can be very slow, especially for large numbers. One of the operations we need to perform is to first raise a number to a certain exponent, and then find the modulus of the result. This can be very expensive for very large numbers. Now, write down one efficient solution to this problem. Also explain every steps of your approach with a suitable example.

(b) Computerized voting would become quite common in the next few decades. As such, it is important that the protocol for virtual elections should protect individual privacy and should also disallow cheating. Now, design a secure protocol that provides comfort both to the voters as well as to the Election Authority by preventing fake and duplicate votes. Also prove the correctness of your design by explaining the logic behind each and every steps of your virtual election process.

(c) Write a short note on any one of the following

(i) Biometric Authentication

(ii) Authentication Token

[3 + 3 + 4]