53 (CS 603) INSC

2017

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Answer **any five** questions.*

1. *(a)* What do you understand by the term Threat and Vulnerability? 5

   (b) Explain the concepts of *three* parameters of Security Services i.e., CIA with neat diagrams. 7

   (c) What do you understand by security attacks? Explain all the categories of Security attacks. 8

2. *(a)* What do you understand by modular arithmetic? Prove that $a \equiv b \ mod\, n$ if $n \mid (a-b)$ for any integer a, b and n. 5

(b) Prove that GCD of two consecutive integer numbers is 1 i.e.
GCD $(k, k+1) = 1$ for any integer k. 5

(c) Solve : $(a \bmod n \times b \bmod n) \bmod n$
$= (a+b) \bmod n$ 5

(d) Find GCD (536, 274). 5

3. *(a)* Write the Extended Euclid algorithm for finding the multiplicative inverse modulo. 5

(b) Find the multiplicative inverse of 9 in modulo 31 using the Extended Euclid algorithm. 5

(c) Determine the multiplicative inverse of the polynomial $x^3 + x + 1$ in GF (2^3) with $m(x) = x^4 + x + 1$. 5

(d) Assume the Advanced Encryption Standard (AES) uses arithmetic in the finite field GF (2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials

$$f(x) = x^6 + x^4 + x^2 + 1 \text{ and}$$

$$g(x) = x^7 + x + 1.$$

Find GCD of $g(x) \times f(x)$ and $m(x)$. 5

4. (a) What is the difference between a block cipher and a stream cipher? 5

(b) Explain the i^{th} round encryption scheme of DES algorithm. 7

(c) Explain the general encryption and decryption strategy of AES cipher. 8

5. (a) What do you understand by public key cryptography? Can a public cryptography be used for encrypting personal data? Justify. 5

(b) Explain the RSA algorithm. 5

(c) In a public key system using RSA, you intercept $C = 10$ sent to a user whose public key is $e = 5$ and $n = 35$. What is plaintext M? 5

(d) Can RSA be used in Digital Signature ? Justify your answer. 5

6. (a) Explain the steps needed to be taken by two entities involving in a communication to shared a secret key using public key distribution strategy. 7

(b) What is MAC (Message Authentication Code) and where is it used ? 5

(c) Explain MAC function for maintaining Message Authentication and Confidentially assume the authentication is tied to plain text. 8

7. Explain the following concepts : ***(any four)*** 5×4=20

(a) Buffer Overflow Attack

(b) Format String Vulnerability

(c) Cross Site Request Forgery

(d) SQL-Injection

(e) DDoS

(f) Digital Certificate.
