53 (CS 603) INSC

2014

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Time : Three hours

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

Answer ***any ten*** *questions out of* ***twelve.***

1. Find the following : (show all the steps) 4+3+3=10

   (a) ged (1970, 1066)

   (b) Multiplicative inverse of

      (i) 89 mod 113

      (ii) 99 mod 69

2. *(a)* What is encryption and decryption ?

(b) Design your own encryption and decryption algorithm based on Caesar Cipher, where your algorithm must support the english alphabets as well as inclusion of Space ( ), Dollar ($) and Ampersand (&) characters. 4+6=10

3. (a) What is Symmetric Cipher ?

(b) Explain the Symmetric Cipher model.

(c) You have been given a key having name CYBER. Use the play-fair Cipher algorithm to encrypt the following message :

BALLOON 2+4+4=10

4. (a) Solve (algebraically) 4+6=10

$[(a \bmod n) \times (b \bmod n) \times (c \bmod n)] \bmod n =$

(b) Given a key K having

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Find the inverse of this matrix K. Show all the steps.

5. *(a)* Explain Vernam Cipher.

(b) What is one time pad ?

(c) Using Vernam Cipher technique encrypt the following message with the key

K = 011 01 011

M= 100 011 01 3+3+4=10

6. *(a)* What do you mean by confusion and diffusion ?

(b) Explain DES algorithm with proper diagram indicating encryption and decryption. 4+6=10

7. *(a)* What is a digital signature ?

(b) Explain how digital signature works.

(c) What is the purpose of digital signature ? 2+6+2=10

8. *(a)* Explain Man in the middle (MITM) attack with example.

(b) Explain the centralized authentication system. 5+5=10

9. *(a)* Explain RSA algorithm.

(b) Using RSA algorithm decrypt the following Ciphertext message $C = 10$. Given public key $e = 5$ and $n = 35$. 6+4=10

10. *(a)* What is block cipher ?

(b) Is the RSA and DES a block cipher ?

(c) Explain the Security Services. 2+2+6=10

11. *(a)* According to OSI security architecture, what do you mean by attacks ?

(b) Explain the various security attacks. 2+8=10

12. Write short notes on : 2·5×4=10

(a) Virus

(b) DoS attack

(c) Worms

(d) Bruteforce
