Total number of printed pages–4

53 (CS 603) INFS

2019

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.*

1. (a) Define Security services. List the categories of Security services. 5

(b) Consider an Automated teller machine (ATM) in which users provide a Personal Identification Number (PIN) and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system and in each case, indicate the degree of importance of the requirement. 5

Contd.

2. *(a)* What are symmetric and asymmetric key ciphers ? Give examples. 5

   (b) Modify Caesar Cipher to support the following 5 characters along with 26 english alphabet

   "@, #, $, %, &". 5

3. *(a)* What do you understand by substitution and transposition techniques ? Give examples. 5

   (b) Explain Playfair Cipher with example, take the key as CIPHER. 5

4. *(a)* Encrypt the message "SECURITY" using the Hill Cipher with the key

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}.$$

   Show your calculations. 5

   (b) Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. 5

5. *(a)* What do you understand by a stream cipher and block cipher ? 5

   (b) Show how a n-bit-n-bit block cipher works. 5

6. *(a)* What do you understand by the terms Confusion and Diffusion ? 5

   (b) Explain the i^{th} round DES algorithm. 5

7. *(a)* What is the difference between modular arithmetic and ordinary arithmetic ? 5

   (b) Find : 5

   (i) 500 *mod* 55

   (ii) 125 *mod* 26.

8. *(a)* Determine *gcd* (24140, 16762). 5

   (b) Using extended euclid algorithm, find the multiplicative inverse of

   1234 *mod* 4321. 5

9. *(a)* What is Euler's Totient Function ? 2

   (b) Find ϕ (77) and ϕ (231). 8

10. *(a)* What are the roles of public key and private key in public cryptosystem? 5

(b) Explain RSA algorithm with example. 5

11. *(a)* Perform encryption and decryption using RSA algorithm for the following $p = 7$; $q = 11$; $e = 17$ and $M = 8$. 5

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

12. Write short notes on : ***(any two)*** 2×5=10

(a) Message Authentication Code

(b) Firewall

(c) Meet in the Middle Attack

(d) Masquerade.