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.*

FIRST HALF

1. *(a)* What do you mean by security attack, security mechanism and security service ? 6

   (b) Briefly explain the *three* important categories of security services. 4

2. *(a)* Explain what is substitution cipher, transposition cipher, stream cipher and a block cipher. 4

(*b*) Briefly explain the model for network security. 6

3. Given a key : 10

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

decrypt the following message using Hill Cipher.

"LNSHDLEWMIRW"

4. (*a*) Explain Vernam Cipher. 3

(*b*) What do you mean by one time pod ? 3

(*c*) Using Vernam cipher technique encrypt the following binary message with the key

K=01101011

M=10001101 4

5. *(a)* The following message has been encrypted using transposition technique in such a way that plaintext were placed in 7×4 matrix table (where 7 nos of column and 4 nos of rows) with the given key 4 3 1 2 5 6 7. The encrypted message is TTNAAPTMTSUOAODWCOIXKNLYPETZ. Decrypt this message. 8

(b) What is ciphertext ? 2

SECOND HALF

6. *(a)* What do you mean by prime and co prime numbers ? 4

(b) Find whether the following numbers are co prime with respect to 26 or not 6

(i) 7

(ii) 19

(iii) 15

(iv) 20

7. *(a)* Prove that 2

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

(*b*) Find the additive inverse of –33 mod 26. 3

(*c*) Using Extended Euclid's algorithm find the multiplicative inverse of –33 mod 26. 3

(*d*) Find gcd (1970, 1066). 2

8. (*a*) What do you mean by confusion and diffusion ? 2

(*b*) Explain DES algorithm with proper diagram indicating encryption part as well as for decryption part. 8

9. (*a*) What do you mean by public cryptosystem ? 2

(*b*) Explain RSA algorithm. 6

(*c*) Using RSA algorithm decrypt the following ciphertext message 2

$$C = 10$$

Given public key $C = 5$ and $n = 35$.

10. (*a*) What is a digital signature ? 3

(*b*) Explain how digital signature works. 5

(c) Mention any known digital signing software. 2

11. (a) Explain Man in The Middle Attack (MITM) with example. 5

(b) Explain how key distribution works (consider that there is a key distribution authority involved). 5

12. (a) Write short notes on : 6

(i) Masquerade

(i) DNS spoofing

(b) Encrypt / decrypt the following using RSA. Given $p = 5; q = 11; e = 3; M = 9$. 4
