Total number of printed pages–4

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 ***all*** *questions.*

1. Short answer question : 4×10=40

   (i) What do you understand by security services and security attacks ?

   (ii) What are secret key and public key cryptography ?

   (iii) What are the differences between Monoalphabetic Ciphers and Polyalphabetic Ciphers ?

   (iv) What is a Threat and a Defense ?

Contd.

(v) Define Confusion and Diffusion in terms of Cryptography.

(vi) What are the differences between Block Ciphers and Stream Ciphers ?

(vii) Mention the Block size, Numbers of Rounds and Key size of DES Algorithm.

(viii) What are phishing and spoofing ?

(ix) What are viruses and trojans ?

(x) Why Cybercrime is a growing concern ? How to prevent cybercrime ?

2. (a) Explain the model of conventional cryptography.

(b) Explain the different types of attack on Encrypted messages.

5+5=10

3. (a) For a particular encryption algorithm given the key size is 32 bits. Find the number of alternative keys. Calculate the average time required for exhaustive key search of the 32 bits key size, if 1 decryption mode per milliseconds.

(b) What do you understand by a brute force attack ? Explain with an example.

5+5=10

4. A generalisation of the Caesar cipher, knows as the affine Caesar cipher, has the following : For each plaintext letter p, substitute the ciphertext letter C :

$$C = E([a,b], p) = (ap + b) mod 26$$

A basic requirement of any encryption algorithm is that it to be one-to-one. That is, if $p \neq q$, then $E(k,p) \neq E(k,q)$. Otherwise, decryption is impossible, because more than one plaintext character maps in to the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for $a = 2$ *and* $b = 3$, then $E = ([a,b],0) = E([a,b],13) = 3$.

(a) Are there any limitations on the value of b ? Explain why or why not.

(b) Determine which values of a are not allowed.

(c) Provide a general statement of which values of a are allowed and are not allowed. Justify your answer.

10

5. *(a)* Encrypt the message "MEET ME AT USUAL PLACE AT TEN RATHER THAN EIGHT O'CLOCK" using the Hill Cipher with the hey $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.

Show your calculations and result.

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

5+5=10

6. *(a)* Compare AES and DES algorithm.

(b) Explain the i^{th} round Encryption and Decryption structure of DES algorithm.

5+5=10

7. *(a)* What do you understand by a Digital Signature and Digital Certificate ?

(b) Explain MAC algorithm for achieving Digital Signature as well as confidentiality of the message.

5+5=10
