*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.***

*Question No.* ***1*** *is* ***compulsory*** *and answer* ***any seven*** *questions from the rest.*

1. *(a)* Answer the following questions. 2×10=20

   *(i)* What to you understand by encryption and decryption ?

   *(ii)* What is the difference between substitution and transposition techniques ?

   *(iii)* What is one-time pad ?

   *(iv)* Explain Vigenère Cipher ?

   *(v)* What are Confusion and Diffusion ?

*Contd.*

(vi) What is the role of public key in public key cryptosystem ?

(vii) What is the block size and key size of DES algorithm ?

(viii) Give *any two* examples where confidentiality may be violated.

(ix) Find $(100)^{-1}$ mod 29.

(x) What do you understand by email spoofing ?

(b) Fill in the blanks : 1×5=5

(i) The GCD of 55 and 56 is _____.

(ii) The inverse of 17 in mod 26 is _____.

(iii) If $n = p*q$, where $p$ & $q$ are prime, then $\phi(n)$= _____.

(iv) MITM stands for _____.

(v) Masquerade is a type of _____ attack.



(c) Write (True / False) : 1×5=5

(i) A good hash algorithm can generate multiple unique fixed string for same massage.

(ii) Passive attacks are very easy to detect.

(iii) In public key cryptosystem, to achieve confidentiality, public key of receivers are used during encryption.

(iv) DES is an example of symmetric key cipher.

(v) Checksum is used for verifying receiver of the data.

2. Explain the encryption and decryption algorithm of Caesar cipher that can support additional symbol space, $ and &. 10

3. Explain the encryption and decryption process of DES algorithm with proper diagram. 10

4. What do you understand by security services ? Explain *any four* security services. 2+8=10

5. Find : 5+5=10

(i) GCD (400, 651)

(ii) $15^{-1}$ mod 26

6. (a) Explain extended euclid algorithm.

(b) Using extended euclid algorithm, find the inverse of 30 in modulo 37. 5+5=10

7. (a) Explain RSA algorithm.

(b) Find $\phi(35)$ and $\phi(8)$. 5+5=10

8. (a) What is Message Authentication Code (MAC) ?

(b) Explain how MAC can be used as a method to detect or verify the sender of the message with neat diagram. 2+8=10

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

(a) Meet in the Middle

(b) Phishing

(c) IP Security.