Total number of printed pages–4

53 (CS 603) INSC

2018

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)* What do you understand by Encryption and Decryption ?

   (b) Explain *any three* Security services. 4+6=10

2. *(a)* What do you understand by Security attack and Security vulnerability ?

   (b) Explain *any two* Security vulnerability. 4+6=10

Contd.

3. *(a)* What do you understand by modular arithmetic ?

   (b) Prove :

   $(a\,mod\,n \times b\;mod\;n \times c\;mod\,n)mod\,n =$

   $(a \times b \times c)mod\,n.$

   5+5=10

4. *(a)* Explain extended Euclidean algorithm for finding multiplicative inverse.

   (b) Find $(1001)^{-1}$ *mod* 517.

   5+5=10

5. *(a)* What is an ARP ?

   (b) Explain the purpose of ARP.

   (c) How ARP spoofing can be carried out in a LAN ?

   2+3+5=10

6. *(a)* Given :

   $f(x) = x^5 + x^4 + x + 1$ and

   $g(x) = x^3 + x^2 + 1$ where field multiplication are performed in the modulo of 2. Find $gcd[f(x), g(x)]$.

   (b) Prove :

   $x \equiv y\,mod\,n$ and

   $y \equiv z\,mod\,n$

   imply $x \equiv z\,mod\,n$.

   5+5=10

7. *(a)* What do you understand by Confusion and Diffusion ?

   (b) Explain DES encryption and decryption algorithm.

   4+6=10

8. *(a)* What do you understand by Public Key Cryptosystem ?

   (b) Explain RSA algorithm with example.

   2+8=10

9. *(a)* What is MAC ?

   (b) What do you understand by Digital Signature ?

   (c) With mathematical formulation prove that Digital Signature can guarantee source authenticity.

   2+3+5=10

10. *(a)* What is a Firewall ?

(b) Explain general security architecture of Firewall design.

(c) Explain your firewall strategy to secure a particular organization.

2+3+5=10

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

(a) Masquerade Attack

(b) Cross Site Request Forgeny

(c) IPSec

(d) Botnet.