Total number of printed pages–4

53 (CS 603) INSC

2018

INFORMATION SECURITY

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

Answer ***any ten*** *questions.*

1. *(a)* Explain encryption and decryption algorithm of Caesar cipher.

   (b) Explain how secure is Caesar cipher. 5+5=10

2. *(a)* Define the terms Threat and Attack according to X.800 security standard.

   (b) What do you understand by security services? Explain different types of security services.

   4+6=10

Contd.

3. *(a)* What are security vulnerability and security breach ?

(b) Explain how buffer overflow works.

5+5=10

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

(b) Prove that

$$(a * b) mod\ n = (a\ mod\ n * b\ mod\ n) mod\ n$$

(c) Show that if $c \mid a$ (meaning c divides a) and $c \mid b$ (c divides b) then c also divides d *i.e*, $c \mid d$ where $d = gcd(a, b)$.

2+3+5=10

5. *(a)* **Explain extended Euclid algorithm.**

(b) **Find the inverse of 113 mod 502.**

5+5=10

6. *(a)* Prove that GCD of two consecutive number is 1.

(b) Find $GCD(110, 540)$

(c) Find $GCD(x^5 + x^2 + x + 1,\ x^3 + x + 1)$.

3+3+4=10

7. *(a)* What do you understand by a symmetric key cipher?

(b) Explain the ith round DES encryption and decryption scheme.

2+8=10

8. *(a)* What is a public key cryptography?

(b) In a public key cryptography 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 message?

(c) Perform encryption and decryption using RSA algorithm for $p = 17$; $q = 31$; $e = 7$, $M = 2$.

2+4+4=10

9. *(a)* What is a MAC?

(b) Design MAC algorithm that guaranter source authencity, data integrity and confidentiality of message.

(c) Explain how digital signature works.

2+4+4=10

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

(b) Explain IPSEC protocol.

2+8=10

11. *(a)* How ARP spoofing works ? Explain.

(b) How MITM attack works ? Explain with example.

5+5=10

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

(a) Phishing

(b) DoS

(c) Botnet

(d) XSS.