Total number of printed pages–5

53 (IT 702) ISCL

2019

INFORMATION SECURITY AND CYBER LAWS

Paper : IT 702

Full Marks : 100

Time : Three hours

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

*Answer **any five** questions.*

1. *(a)* What do you mean by security services ? Explain various types of security services in X.800 architecture. 2+5=7

   (b) State the advantages of PUBLIC KEY cryptography over SECRET KEY Cryptography with the help of examples. 6

Contd.

(c) Define Cryptanalysis. Explain the following cryptanalysis attack briefly : 1+6=7

(i) Known plaintext attack

(ii) Ciphertext only attack

(iii) Chosen plaintext attack.

2. (a) What do you mean by Network Standard ? Explain different types of network standard with the help of examples. 1+4+2=7

(b) Consider a Hill Cipher with block size = 2 and key K as given below : 5+8=13

$$K = \begin{pmatrix} 3 & 25 \\ 24 & 17 \end{pmatrix}$$

(i) What is the ciphertext corresponding to the plaintext : (M I S S) ?

(ii) What is the plaintext corresponding to the ciphertext : (C I K K) ?

3. (a) Explain RSA algorithm. 3

(b) In a public-key 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 M? 5

(c) With the help of RSA algorithm, show the complete process of encryption and decryption for the following parameters : $p = 11$, $q = 13$ and plaintext $(m) = 9$. 8

(d) State which one is easier to hijack : a UDP session or a TCP session ? Explain why to justify your views. 4

4. (a) What are the different ways of distributing keys ? What is the need of key exchange ? Discuss Diffie-Hellman key exchange algorithm. 4+2+6=12

(b) In a Diffie-Hellman key exchange, algorithm, let the prime number be 353 and one of its primitive root be 3 and let A and B select their secret keys $X_A = 97$ and $X_B = 233$. Compute public key and common secret key of A and B. 8

5. (a) What is digital signature ? Describe a scheme to produce digital signature. 2+6=8

(b) With the help of play fair cipher encrypt the plaintext "GOOD MORNING" using key "SECURE". 6

(c) Do each of the following inverses exist? If yes, what are they? If no, explain why not? 3+3=6

(i) 102^{-1} (mod 125)

(ii) 77^{-1} (mod 401)

6. (a) Why SSL layer is partitioned between application layer and transport layer? Discuss the following sub protocol of SSL: 2+6=8

(i) Handshake protocol

(ii) Record protocol

(iii) Alert protocol.

(b) What is the purpose of S/MIME? Compare and contrast S/MIME and Pretty Good Privacy (PGP). 4+4=8

(c) Describe Man in the Middle attack. 4

7. Write short note on the following: ***(any five)*** 4×5=20

(a) Active attack and Passive attack

(b) One way function

(c) Firewalls

(d) Avalanche effect

(e) Buffer overflow

(f) Stream cipher and Block cipher

(g) IPsec.