Total number of printed pages-5

53 (IT 702) ISCI

FATRAL INSTITU

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.

Contd.

- 0 Define Cryptanalysis. Explain the following cryptanalysis attack briefly:
- Known plaintext attack
- Ciphertext only attack
- Chosen plaintext attack
- (a) What do you mean by Network examples. network standard with the help of Standard? Explain different types of 1+4+2=7

2

- 6 Consider a Hill Cipher with block size = 2 and key K as given below: 5+8= 389AARY

CENTRAL

OK- TECHNOLO

(i) corresponding to the plaintext: What (SSIM) 18 ciphertext

MIRA

- (ii) What is corresponding to the ciphertext: (CIKK)? the plaintext
- ယ (a) Explain RSA algorithm.

ω

- 197(b) Taing intercept the ciphertext C = 10 sent to In a public-key system using RSA, you a user whose public key is e = 5, n = 35. What is the plaintext M?
- (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 why to justify your views. UDP session or a TCP session? Explain
- SAMIME ? . *(a)* **(b)** key exchange? Discuss Diffie-Hellman key exchange algorithm. 4+2+6=12 distributing keys? What is the need of What are the different ways of key and common secret key of A and algorithm, let the prime number be 353 In a Diffie-Hellman key exchange, $X_A = 97$ and $X_B = 233$. Compute public let A and B select their secret keys and one of its primitive root be 3 and
- 5.8 (a) What is digital signature? Describe a ddie attack. scheme to produce digital signature. 2+6=8

bus SIMIME and

ယ

- (b) With the help of play fair cipher encrypt key "SECURE" the plaintext "GOOD MORNING" using What is the p
- 0 why not? If yes, what are they? If no, explain Do each of the following inverses exist? толдугээр 3+3=6
- (i) 102⁻¹ (mod 125) b=Tr d

fw sust8

- (ii) 77⁻¹ (mod 401)
- (a) Why SSL layer is partitioned between Discuss the following sub protocol of application layer and transport layer? 2/6-8

6

Handshake protocol

111.

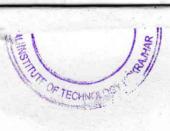
CENTRAL

- (ii) Record protocol
- (iii) Alert protocol. See AX

SEMME

- *(b)* What is the purpose of S/MIME? Pretty Good Privacy (PGP). 4+4=8 Compare and contrast S/MIME and
- 0 Describe Man in the Middle attack.

- 7 (any five) Write short note on the following:
- (a) Active attack and Passive attack
- 6 One way function
- 0 Firewalls
- (d) Avalanche effect
- (e) Buffer overflow
- S Stream cipher and Block cipher
- (9) **IPsec**



CI

4

23 (IL 105) IRCF/G