

Total number of printed pages-3

53 (IT 702) ISCL

2021

(Held in 2022)

**INFORMATION SECURITY AND
CYBER LAWS**

Paper : IT 702

Full Marks : 100

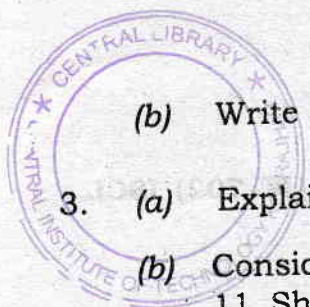
Time : Three hours

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

Answer any five questions.

1. (a) Define cryptanalysis. Explain three cryptanalysis attack. 1+9=10
- (b) Explain various types of security services in X.800 architecture. 5
- (c) What are the advantages of public key cryptography over secret key cryptography? Explain. 5
2. (a) Explain the AES. 10

Contd.



- (b) Write the RC4 algorithm. 10
- 3. (a) Explain RSA algorithm. 10
- (b) Consider two prime numbers 17 and 11. Show how Alice generates the public key and private key pair using RSA algorithm. Using RSA algorithm, encrypt a message $M=88$ using the public key and decrypt the cipher text using the private key. 10
- 4. (a) Discuss Diffie-Hellman key exchange algorithm. 10
- (b) What is a digital signature? Describe a scheme to produce digital signature. 10
- 5. (a) How are public keys distributed? Explain X.509 certificate format. 3+7=10
- (b) What do you understand by transport layer security? Explain. 10
- 6. (a) What are PGP and S/MIME? Write the algorithms for PGP transmission and reception. 2+8=10
- (b) What is Kerberos? Explain how Kerberos works. 2+8=10

7. Write short notes on the following :

5×4=20

- (a) Active and passive attack
- (b) Firewalls
- (c) Stream cipher and block cipher
- (d) IPSec
- (e) SNMP

