

Total number of printed pages-4

53 (EC 711) CRGR

2021

(Held in 2022)

CRYPTOGRAPHY

Paper : EC 711

Full Marks : 100

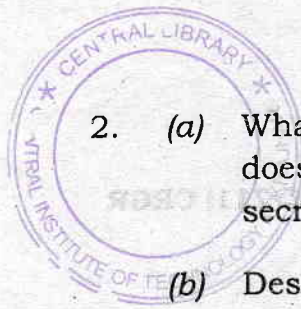
Time : Three hours

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

Answer **any five** questions.

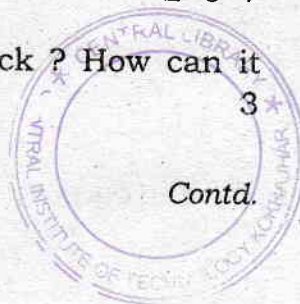
1. (a) Explain the working of DES detailing the Feistel structure. 7
- (b) What is man-in-the-middle attack that happens in double DES ? 5
- (c) What is the difference between diffusion and confusion ? 3
- (d) Describe triple DES using two keys. 5

Contd.



2. (a) What is public key cryptography ? How does it provide both authentication and secrecy ? 3+3=6
- (b) Describe linear cryptanalysis. 6
- (c) Describe a digital signature system citing the essential elements. Explain a digital signature scheme using cryptographic hash function. 8
3. (a) Explain the steps of RSA algorithm. 6
- (b) What is the difference between MAC function and a one-way hash function ? 3
- (c) Explain how does MAC provide authentication and confidentiality. 6
- (d) What are the design criteria of S-boxes ? 5
4. (a) What are the different Block Cipher modes of Operations ? What are their typical applications ? 5

- (b) Explain output feedback mode. What are its advantages and disadvantages? 6+3=9
- (c) Describe the key stream generation steps done in RC4 algorithm. 6
5. (a) What is secure socket layer (SSL)? Explain the SSL record protocol operation. 2+6=8
- (b) Explain the various SSL specific protocols. 7
- (c) What are the various functions provided by S/MIME? 5
6. (a) What is IP security (IPsec)? What are its various services? 5
- (b) Explain the transport mode of IPsec. 5
- (c) What is PGP? How does it provide both authentication and confidentiality? 2+5=7
- (d) What is a replay attack? How can it be dealt with? 3



7. (a) Perform encryption and decryption using the RSA algorithm for $p = 5$; $q = 7$; $e = 7$; $M = 12$. 4
- (b) Cite the differences between cryptography and steganography. 4
- (c) What are the application areas of public key cryptography ? 4
- (d) Explain in detail, a single round of DES. 8

