53 (EC 711) CRYY

2017

CRYPTOGRAPHY

Paper : EC 711 (Back)

Full Marks : 100

Time : Three hours

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

*Answer **any five** questions.*

1. *(a)* What is a Message Authentication Code (MAC) ? Describe how does MAC ensure authentication, confidentiality and both. 3+7=10

   (b) Describe encryption and decryption of Feistel block cipher. 10

2. *(a)* Explain how does meet-in-the-middle attack take place in Double DES. 6

(b) Describe the technique of Differential Cryptanalysis. 8

(c) Describe the design criteria of S-boxes in DES. 6

3. (a) What is a Digital Signature ? Explain a digital signature scheme using hash function. 3+7=10

(b) Explain the working of any of the block chaining model. Find out expressions for its plaintext and ciphertext. 10

4. (a) How Stream Generation is achieved through RC4 algorithm ? 10

(b) What is a SSL protocol stack ? Explain the operation of SSL Record Protocol. 3+7=10

5. (a) What is PGP ? Describe its services. 3+7=10

(b) Explain various Security services outlined in ITU-T recommendation X·800 Security Architecture. 10

6. *(a)* Describe the RSA algorithm. 10

(b) Write different approaches used for traditional ciphers. Explain *one* of them, citing its merits and demerits. 2+8=10

7. *(a)* What is public-key cryptography ? How does it ensure authentication and secrecy ? 3+7=10

(b) Write short notes on : 5+5=10

(i) Steganography and

(ii) Active Attacks.
