53 (EC 711) CRYY

2014

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

   (b) Describe the RSA algorithm. 7

   (c) Mention some important application areas of public-key cryptosystems. 3

2. *(a)* Explain Diffie-Hellman Key exchange algorithm. 7

(b) What is a cryptographic hash function ? 3

(c) Cite some examples of the use of a hash function for message authentication. 10

3. (a) What is a message authentication code (MAC) ? Describe how does MAC ensure both authentication and confidentiality. 3+7=10

(b) List *two* disputes that can arise in the context of message authentication. Mention the properties of a digital signature. 5

(c) Describe a digital signature system using hash function. 5

4. (a) Write a brief note on web security threats. What are the approaches applied to web security threats ? 5+5=10

(b) Describe the operation of SSL Record Protocol. 7

(c) What is the purpose of change Cipher Spec Protocol of SSL ? 3

5. (a) What is PGP ? Describe its services. 2+8=10

(b) What are the IPSec protocols that can provide security ? Mention the functional areas and services of IPSec. 3+3·5+3·5=10

6. (a) Describe the working of a typical stream cipher. What is S/MIME ? 4+6=10

(b) What is the importance of block cipher modes ? Describe Cipher Feedback Mode (CFB) of operation. 2+8=10

7. (a) Describe the single round of DES algorithm. What are the classical examples of achieving steganography ? 7+4=11

(b) Write short notes on : *(i)* Polyalphabetic Cipher and *(ii) RC4* 4·5+4·5=9
