53 (EC 711) CRGR

2018

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 PGP ? What are its various services ? 2+3=5

   (b) Describe how PGP can provide confidentiality. 6

   (c) Describe a public-key cryptography system. How does it ensure authentication and secrecy ? 3+6=9

2. *(a)* What is a MAC ? How can it be used to provide message authentication and confidentiality ? 10

(b) Describe SSL specific protocols and SSL record protocol operation. 6+4=10

3. *(a)* Describe a digital signature process. Explain how digital signature can be achieved using cryptographic hash function. 10

(b) What requirements should a digital signature scheme satisfy ? 5

(c) In a public-key system using RSA, the ciphertext $C=10$ sent to a user is intercepted. The public key is $e=5$, $n=35$. What is the plaintext M ? 5

4. *(a)* What do you mean by Enveloped Data and Signed Data used by S/MIME ? 6

(b) What is IPSec ? What are its services ? 2+5=7

(c) Describe how stream generation is achieved through RC4 algorithm. 7

5. *(a)* Encrypt the following message : 7

"Must see you over the downtown street. Coming at once."

Using the playfair matrix :

M	*F*	*H*	*I/J*	*K*
U	*N*	*O*	*P*	*Q*
Z	*V*	*W*	*X*	*Y*
E	*L*	*A*	*R*	*G*
D	*S*	*T*	*B*	*C*

(b) Describe the various security services as cited in X800. 8

(c) Describe the mechanism of Vernam Cipher. 5

6. *(a)* Explain with the help of diagram, the Fiestel encryption and decryption. 7

(b) Explain the various criteria considered for the design of S-boxes. 6

(c) Describe the working of *any one* of the block cipher modes. 7

7. Write short notes on : 5×4=20

(i) Linear cryptanalysis

(ii) Triple DES

(iii) Cryptographic hash function

(iv) Confusion and diffusion.
