COMP/CBGS/VII/C&SC./ 01.12.2016

Cryptography & System Security

Q.P. Code : 811502

(3 Hours) [Total Marks : 80

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

Q1. (a) What are block ciphers? Explain with examples the CBC and ECB modes of block ciphers. 05

(b) Encrypt the string "This is an easy task" using a playfair cipher with key "monarchy". 05

(b) Define authentication and non-repudiation and show with examples how each one can be achieved. 05

(d) Describe triple DES with two DES keys. Is man in the middle attack possible on triple DES? 05

Q2. (a) A and B decide to use Diffie Hellman algorithm to share a key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. 10

(b) Compare DES and IDEA. Explain the round key generation scheme in both these algorithms. 10

Q3. (a) What are the different types of viruses and worms? How do they propogate? 10

Q3. (b) What are the various ways for memory and address protection in Operating systems? How is authentication achieved in O.S? 10

Q4. (a) Explain briefly with examples, how the following attacks occur: i)Salami attack ii) Denial of Service attack iii) session hijacking attack iv) Cross-cite scripting attack 10

Q4. (b) How is security achieved in the transport and tunnel modes of IPSec? Describe the role of AH and ESP. 10

Q5. (a)How is confidentiality achieved in emails using either S/MIME or PGP? 05

Q5. (b) A and B wish to use RSA to communicate securely. A chooses public key (e,n) as (7,247) and B chooses public key (e,n) as (5,221). Calculate their private keys. What will be the cipher text sent by A to B if A wishes to send message m=5 securely to B? 10

Q5. (c) What is a digital signature? Explain any digital signature algorithm. 05

Q6. (a) Compare and contrast (any two): 10

i) Block and stream ciphers

ii) MD-5 versus SHA

iii) KDC versus CA

Q6. (b) What are firewalls. Explain the different types of firewalls and mention the layer in which they operate. 10