1. a) Explain different kinds of threats to information security. 5

   b) Does a PKI use symmetric or asymmetric encryption? Explain your answer. 5

   c) What are the information security goals? Explain why the balance among different goals is needed. 5

   d) What are different types of malicious code? 5

2. a) Explain Advanced Encryption Standard Algorithm in detail. 10

   OR

   a) Use the Playfair cipher to encipher the message, "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row of a matrix with the word "GUIDANCE". Filling of rest of the matrix can be done with remaining alphabets. Consider alphabets 'Y', and 'Z' together in one cell of the matrix. 10

   b) Write a note on Kerberos system that supports authentication in distributed system. 10

3. a) Explain control of access to general objects in operating system. 10

   b) Explain nonmalicious program errors with examples. 10

4. a) If generator g = 2 and n or p = 11, using Diffie - Hellman algorithm solve the following.

      i) Show that 2 is a primitive root of 11. 4

      ii) If A has a public key '9', what is A's private key? 2

      iii) If B has a public key '3', what is B's private key? 2

      iv) Calculate the shared secret key. 2

   b) Explain different denial of service attacks. 10

5. a) List, explain and compare different kinds of firewalls used for network security. 10

   b) List and explain the contents of a security plan for administrative security. 10

6. Write a detail note on (any <u>two</u>) : 20

   a) E-mail security

   b) RSA algorithm (Public key algorithm)

   c) Data Encryption Standard (symmetric key algorithm)

   d) Covert channel .

7. a) What is the term Risk analysis? Explain in detail the steps in Risk analysis. 10

   b) How is physical security provided for protection needed outside the computer system? 10