(**Time: 3hrs**)   (**Marks 80**)

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

Q1. (a) Encrypt the message "Cryptography is fun" with a multiplicative cipher with key = 15. Decrypt to get back original plaintext.   **05**

(b) With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers?   **05**

(c) What are the properties of hash functions? What is the role of a hash function in security?   **05**

(d) What are the different protocols in SSL? How do the client and server establish an SSL connection   **05**

Q2. (a) What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format.   **10**

(b) With reference to DES comment on the following: **10**
   i)   Block size and key size
   ii) Need for expansion permutation
   iii) Avalanche and completeness effects
   iv) Weak keys and semi-weak keys
   v)   Role of S-box.

Q3. (a) What are the different types of viruses and worms? How do they propagate?   **10**
(b) What are the various ways for memory and address protection in Operating System?   **10**

Q4. (a) Explain briefly with examples, how the following attacks occur: **10**
   i)   Phishing attack
   ii) Denial of Service attack
   iii) SQL injection attack
   iv) Cross-site scripting attack

(b) How is security achieved in the transport and tunnel modes of IPSec? What are security associations?   **10**

Q5. (a) What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B.   **10**

(b) A and B wish to use RSA to communicate securely. A chooses public key as (7,119) and B chooses public key as (13,221). Calculate their private keys. A wishes to send message m=10 to B. What will be the ciphertext? With what key will A encrypt the message "*m*" if A needs to authenticate itself to B.   **10**

Page **1** of **2**

Q6. (a) Compare and contrast (any two): **10**
    i) Block and stream ciphers
    ii) MD-5 versus SHA
    iii) Key generation in IDEA and Blowfish

(b) What are the different components of an Intrusion Detection System? **10**
Compare the working of signature based IDS with anomaly based IDS.

……………………………………………………