(Time: 3hrs)   (Total Marks 80)

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

Q1. **Solve any four**: (5 marks for each)
 (a) Why is padding done in MD5 and SHA?   **05**
 (b) What are the properties of cryptographic hash functions?   **05**
 (c) Explain with examples, poly-alphabetic & mono-alphabetic ciphers.   **05**
 (d) What are the different types of viruses? Explain in brief.   **05**
 (e) With examples explain Denial of service attack.   **05**

Q2. (a) Justify why DES is a fiestel cipher. Explain the different operations in DES.   **12**
        How are the subkeys generated in each round different from each other?
 (b) Design a double transposition cipher and use it to encrypt "Enemy attacks tonight".   **08**
     Column Key to be used is [5,2,4,3,1].

Q3. (a) What is a digital certificate? Explain the significance of X.509 certificate in   **10**
     PKI. How is a digital certificate verified by the receiver during a communication?
Q3. (b) How is single sign-on achieved in Kerberos? What is the role of each server in   **10**
     the protocol?

Q4   (a) A and B use RSA to communicate securely. B choses public key (**e,n**) as   **10**
     (7,221). Calculate p,q and Φn. Compute the private key, **d**. A choses public key as
     (Ea,Na). A wishes to send message m=5 to B such that confidentiality is maintained.
     With what key will A encrypt the message?

Q4. (b) What is session hijacking? What are the different ways to prevent session   **10**
     hijack attacks?

Q5. (a) What are the different types of firewalls? Differentiate between working of the **10**
     statefull and stateless inspection firewalls.

Q5. (b) Discuss how authentication and integrity is achieved in SET payment protocol?   **10**

Q6. (a)   Write in brief about (any two):   **10**
     i)   Database Security.
     ii)   Key generation in IDEA
     iii)   SSL record protocol.

Q6. (b) How does the IPSec protocol help in achieving authentication and integrity?   **10**

…………………………………