Model question paper

VIII Semester Electronics & Communication Engineering

13.806. Elective VI – INFORMATION SECURITY

Time: 3 hours Maximum: 100 Marks

PART A

(Answer all questions. Each question carries 2 marks)

1. What is the difference between linear and differential cryptanalysis?
2. Define CIA triad?
3. What is the difference between private key and public key encryption?
4. Define balancing information security and access?
5. Why is it important to study Feistel cipher?
6. What is the importance of digital signatures?
7. State one advantage of an H-MAC over a CBC-MAC.
8. What are the difference between X.509 & Kerberos?
9. What is firewall? How does it differ from gateway?
10. What are the features of Internet Protocol security(IPsec)?

(10*2=20 Marks)

PART B

(***Answer one question from each module. Each question carries 20 marks)***

Module I

11. (a) Explain in detail about Security System Development Life Cycle (SecSDLC)? (14)

(b) List the advantages of Top down over Bottom up approaches to information security implementation . (6)

OR

12.(a) Explain in detail about components of information system? (12)

(b) Describe the CNSS security model. What are its three dimensions? (8)

Module II

13(a) Explain Feistel Cipher structure of Data Encryption Standard also describe the strength of DES algorithm. (10)

(b)With neat illustration explain Advanced Encryption Standard algorithm (AES). (10)

OR

14(a) In an RSA system public key of a given user is e = 31,n =3599. What is the private key of the user? (12)

(b) Explain the procedure involved in RSA public-key encryption (8)

Module III

15(a) Illustrate how a hash code is used to provide digital signature? (13)

(b) Briefly explain whirlpool cryptographic hash function. (7)

OR

16(a) Explain HMAC design objective and its algorithm? (15)

(b) Briefly explain the security of MACs (5)

Module IV

17(a) List the sequence of events that are required for a secure electronic transaction? (10)

(b)What is pretty good privacy (PGP)? (10)

OR

18(a) What is SSL session? Can a session be shared among multiple connections?

What are the parameters that define a session state? (10)

(b) Discuss about the different types of intrusion detection and prevention system with Suitable example. (10)