SYED AMMAL ENGINEERING COLLEGE

(An ISO 9001:2008 Certified Institution)

Dr. E.M. Abdullah Campus, Ramanathapuram – 623502

DEPARTMENT OF INFORMATION TECHNOLOGY

CS6701 CRYPTOGRAPHY AND NETWORK SECURITY

UNIT- 1
INTRODUCTION & NUMBER THEORY

PART-A

1. Specify the four categories of security threads?
2. Explain active and passive attack with example?
3. Define integrity and nonrepudiation?
4. Differentiate symmetric and asymmetric encryption?
5. Define cryptanalysis?
6. Compare stream cipher with block cipher with example.
7. Define security mechanism
8. Differentiate unconditionally secured and computationally secured
9. Define steganography
10. Why network need security?
11. Define Encryption
12. Specify the components of encryption algorithm.
13. Define confidentiality and authentication
14. Define cryptography.
15. Compare Substitution and Transposition techniques.
16. Define Diffusion & confusion.
17. What are the design parameters of Feistel cipher network?
18. Define Product cipher.
19. Explain Avalanche effect.
20. Give the five modes of operation of Block cipher.

PART –B

1. Explain Playfair cipher & Vernam cipher in detail.
2. Write short notes on Steganography.
3. Explain classical Encryption techniques in detail.
4. Explain OSI Security Architecture.
5. Explain about Chinese Remainder Theorem.
6. Explain Euler's and Fermat's Theorem.

UNIT- 2
BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

PART-A

1. Differentiate public key and conventional encryption?
2. What are the principle elements of a public key cryptosystem?
3. What are roles of public and private key?
4. Specify the applications of the public key cryptosystem?
5. What requirements must a public key cryptosystem to fulfill to a secured algorithm?
6. What is a one way function?
7. What is a trapdoor one way function?
8. Define Euler's theorem and it's application?
9. Define Euler's totient function or phi function and their applications?
10. Describe in general terms an efficient procedure for picking a prime number?
11. Define Fermat Theorem?
12. List four general characteristics of schema for the distribution of the public key?
13. What is a public key certificate?
14. What are essential ingredients of the public key directory?
15. Find gcd (1970, 1066) using Euclid's algorithm?
16. User A and B exchange the key using Diffie-Hellman algorithm.
q=11 XA=2 XB=3. Find the value of YA, YB and k?
17. What is the primitive root of a number?
18. Determine the gcd (24140, 16762) using Euclid's algorithm.
19. Perform encryption and decryption using RSA Alg. for the following.
P=7; q=11; e=17; M=8.
20. What is an elliptic curve?

PART –B

1. Explain simplified DES with example.
2. Explain Block cipher modes of operation.
3. Explain about Feistel cipher structure.
4. Explain Data Encryption Standard (DES) in detail.
5. How AES is used for encryption/decryption? Discuss with example.
6. State and explain the principles of public key cryptography.
7. Explain Diffie Hellman key Exchange in detail with an example.
8. Explain the key management of public key encryption in detail.
9. Explain RSA algorithm in detail with an example.
10. Briefly explain the idea behind Elliptic Curve Cryptosystem.

UNIT -3
HASH FUNCTIONS AND DIGITAL SIGNATURES

PART-A

1. What is message authentication?
2. Define the classes of message authentication function.
3. What are the requirements for message authentication?
4. What you meant by hash function?
5. Differentiate MAC and Hash function?
6. Any three hash algorithm.
7. What are the requirements of the hash function?
8. What you meant by MAC?
9. Differentiate internal and external error control.
10. What is the meet in the middle attack?
11. What is the role of compression function in hash function?
12. What is the difference between weak and strong collision resistance?
13. Compare MD5, SHA1 and RIPEMD-160 algorithm.
14. Distinguish between direct and arbitrated digital signature?
15. What are the properties a digital signature should have?
16. What requirements should a digital signature scheme should satisfy?
17. Define Kerberos.
18. What 4 requirements were defined by Kerberos?
19. In the content of Kerberos, what is realm?
20. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?
21. What is the purpose of X.509 standard?

PART –B

1. Explain the classification of authentication function in detail.
2. Describe MD5 algorithm in detail. Compare its performance with SHA-1.
3. Describe SHA-1 algorithm in detail. Compare its performance with MD5.
5. Describe HMAC algorithm in detail.
6. Write and explain the Digital Signature Algorithm.

UNIT-4
SECURITY PRACTICE & SYSTEM SECURITY

PART-A

1. General format of IPsec ESP Format?
2. What is Authentication Header? Give the format of the IPsec Authentication Header?
3. Define Transport Adjacency and Iterated Tunnel?
4. Give features and weakness of Diffie Hellman?
5. Explain man in the middle attack?
6. List the steps involved in SSL record protocol?
7. Give SSL record format?
8. What are the different between SSL version 3 and TLS?
9. What is mean by SET? What are the features of SET?
10. What are the steps involved in SET Transaction?
11. What is dual signature? What it is purpose?
12. List the 3 classes of intruder?
13. Define virus. Specify the types of viruses?
14. What is application level gateway?
15. List the design goals of firewalls?
16. Differentiate Transport and Tunnel mode in IPsec?
17. Explain the format of ESP Transport Mode?

PART –B

1. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
2. Write short notes on Intrusion Detection.
3. Define virus. Explain in detail.
4. Describe trusted system in detail.
5. Explain in detail about password management.
6. Explain about Electronic Mail Security

UNIT-5
E-MAIL, IP & WEB SECURITY

PART-A

1. What are the services provided by PGP services
2. Explain the reasons for using PGP?
3. Why E-mail compatibility function in PGP needed?
4. Name any cryptographic keys used in PGP?
5. Define key Identifier?
6. List the limitations of SMTP/RFC 822?
7. Draw the diagram for PGP message transmission reception?
8. What is the general format for PGP message?
9. Define S/MIME?
10. What are the elements of MIME?
11. What are the headers fields define in MIME?
12. What is MIME content type and explain?
13. What are the key algorithms used in S/MIME?
14. Give the steps for preparing envelope data MIME?
15. What you mean by Verisign certificate?
16. What are the function areas of IP security?
17. Give the application of IP security?
18. Give the benefits of IP security?
19. What are the protocols used to provide IP security?
20. Specify the IP security services?

PART –B

1. Explain the operational description of PGP.
2. Write Short notes on S/MIME.
3. Explain the architecture of IP Security.
4. Write short notes on authentication header and ESP.
5. Explain in detail the operation of Secure Socket Layer in detail.
6. Explain Secure Electronic transaction with neat diagram.