



KINGS



COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT CODE:

YEAR : III

SUBJECT NAME: CRYPTOGRAPHY AND NETWORK SECURITY

SEM : VI

UNIT I - FUNDAMENTALS

PART-A (2 MARKS)

UNIT I

1. Specify the four categories of security threats?
2. Explain active and passive attack with example?
3. Define integrity and non repudiation?
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

Cryptography and Network Security

12. Specify the components of encryption algorithm.
13. Define confidentiality and authentication Confidentiality.
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.
21. State advantages of counter mode.
22. Define Multiple Encryption.
23. Specify the design criteria of block cipher.
24. Define Reversible mapping.
25. Specify the basic task for defining a security service.
26. What is the difference between link and end to end encryption?
27. What is traffic Padding? What is its purpose?
28. List the evaluation criteria defined by NIST for AES?
29. What is Triple Encryption? How many keys are used in triple encryption?

PART-B

1. Explain (a) Playfair cipher (8)
(b) Vernam cipher in detail. (8)
2. Explain simplified DES with example. (16)
3. Write short notes on i) Steganography (16)
4. Explain classical Encryption techniques in detail. (16)
5. Write short notes on
(a) Security services (8)
(b) Feistel cipher structure (8)

Cryptography and Network Security

6. Explain Data Encryption Standard (DES) in detail. (16)
7. How AES is used for encryption/decryption? Discuss with example. (16)
8. List the evaluation criteria defined by NIST for AES. (16)

UNIT II - PUBLIC KEY CRYPTOGRAPHY

PART-A (2 MARKS)

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 its 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 are essential ingredient of the public key directory?
14. Find gcd (1970, 1066) using Euclid's algorithm?
15. What is the primitive root of a number?
16. Determine the gcd (24140,16762) using Euclid's algorithm.
17. Perform encryption and decryption using RSA Alg. for the following. $P=7$; $q=11$; $e=17$;
 $M=8$.
18. What is an elliptic curve?

PART-B

1. State and explain the principles of public key cryptography. (16)
2. Explain Diffie Hellman key Exchange in detail with an example (16)
3. Explain the key management of public key encryption in detail (16)
4. Explain RSA algorithm in detail with an example (16)
5. Briefly explain the idea behind Elliptic Curve Cryptosystem. (16)

UNIT III - AUTHENTICATION AND HASH FUNCTION

PART-A (2 MARKS)

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?

PART-B

1. Explain the classification of authentication function in detail. (16)
2. Describe MD5 algorithm in detail. Compare its performance with SHA-1. (16)
3. Describe SHA-1 algorithm in detail. Compare its performance with MD5 and RIPEMD-160 and discuss its advantages. (16)
4. Describe RIPEMD-160 algorithm in detail. Compare its performance with MD5 and SHA-1.
5. Describe HMAC algorithm in detail. (16)
6. Write and explain the Digital Signature Algorithm. (16)
7. Assume a client C wants to communicate with a server S using kerberos protocol. How can it be achieved? (16)

UNIT IV - NETWORK SECURITY

PART-A (2 MARKS)

1. Define Kerberos.
2. What is Kerberos? What are the uses?
3. What 4 requirements were defined by Kerberos?
4. In the content of Kerberos, what is realm?
5. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?
6. What is the purpose of X.509 standard?
7. What are the services provided by PGP services.
8. Explain the reasons for using PGP?
9. Why E-mail compatibility function in PGP needed?
10. Name any cryptographic keys used in PGP?
11. Define key Identifier?
12. List the limitations of SMTP/RFC 822?
13. Draw the diagram for PGP message transmission reception?

Cryptography and Network Security

14. What is the general format for PGP message?
15. Define S/MIME?
16. What are the elements of MIME?
17. What are the headers fields define in MIME?
18. What is MIME content type and explain?
19. What are the key algorithms used in S/MIME?
20. Give the steps for preparing envelope data MIME?
21. What you mean by Verisign certificate?
22. What are the function areas of IP security?
23. Give the application of IP security?
24. Give the benefits of IP security?
25. What are the protocols used to provide IP security?
26. Specify the IP security services?
27. What do you mean by Security Association? Specify the parameters that identifies the Security Association?
28. What does you mean by Reply Attack?
29. General format of IPsec ESP Format?
30. Differentiate Transport and Tunnel mode in IPsec?
31. What is Authentication Header? Give the format of the IPsec Authentication Header?
32. Explain the format of ESP Transport Mode?
33. Define Transport Adjacency and Iterated Tunnel?
34. Give features and weakness of Diffie Hellman?
35. Explain man in the middle attack?
36. List the steps involved in SSL record protocol?

PART-B

1. Explain the operational description of PGP (16)
2. Write Short notes on S/MIME (16)

Cryptography and Network Security

3. Explain the architecture of IP Security (16)
4. Write short notes on authentication header and ESP (16)
5. Explain in detail the operation of Secure Socket Layer in detail. (16)
6. Explain Secure Electronic transaction with neat diagram. (16)

UNIT V - SYSTEM LEVEL SECURITY

PART-A (2 MARKS)

1. List the 3 classes of intruder?
2. Define virus. Specify the types of viruses?
3. What is application level gateway?
4. List the design goals of firewalls?
5. What are the steps involved in SET Transaction?
6. What is dual signature? What is its purpose?
7. Give SSL record format?
8. What are the differences between SSL version 3 and TLS?
9. What is meant by SET? What are the features of SET?

PART-B

1. Explain the technical details of firewall and describe any three types of firewall with neat diagram. (16)
2. Write short notes on Intrusion Detection. (16)
3. Define virus. Explain in detail. (16)
4. Describe Trusted system in detail. (16)