



KINGS

COLLEGE OF ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
QUESTION BANK

SUB.NAME : CS 1029 - NETWORK SECURITY

YEAR / SEMESTER : IV / VIII

UNIT- I
SYMMETRIC CIPHER
Part A (2 Marks)

1. What are the essential ingredients of a symmetric cipher?
2. Define the Caesar cipher.
3. Define the monoalphabetic cipher.
4. Define the playfair cipher.
5. What is the difference between a block cipher and a stream cipher?
6. What are the two approaches to attacking a cipher?
7. What do you mean by stream cipher?
8. How many keys are required for two people to communicate via a cipher?
9. What do you mean by block cipher?
10. What do you mean by avalanche effect?
11. What are the advantages of DES?

PART-B (16 Marks)

1. Briefly explain Block Cipher modes of Operation (16)
2. Explain AES. (16)
3. Explain Classical Encryption Techniques. (16)
4. Explain DES with neat diagram (16)
5. Describe about Traffic Confidentiality. (16)

UNIT – II

PUBLIC KEY ENCRYPTION AND HASH FUNCTIONS

PART-A (2 Marks)

1. What are the characteristics of public key encryption?
2. Differentiate conventional & public key encryption?
3. What are the requirements of key distribution?
4. What are the techniques for distribution of public keys?
5. What do you mean by ECC?
6. Advantages of cryptography with elliptic curve?
7. What are the authentication requirements?
8. Define MAC?
9. What is meant by message authentication?
10. Define Hash function?
11. What are the properties of digital signature?
12. What are the requirements of digital signature?

PART-B (16 Marks)

1. What do you mean by Public key cryptography and explain the RSA -algorithm and it's security mechanisms? (16)
2. Explain about the various Key management techniques. (16)
3. Explain Elliptic Curve Architecture. (16)
4. Explain Authentication Functions. (16)
5. Explain Hash Functions. (16)
6. Explain Digital Signature Standard. (16)

UNIT - III

NETWORK SECURITY PRACTICE

PART-A (2 Marks)

1. Define Kerberos
2. What are the requirements of Kerberos?
3. Define X.509
4. Define Pretty Good Privacy
5. What are the reasons for the popularity of Pretty Good Privacy?
6. What are the services offered by PGP?
7. Define S/MIME
8. What are the MIME specifications?
9. What are the functions of S/MIME?
10. What are the steps for preparing an enveloped data for a MIME entity?
11. What are the applications of IP security?
12. Draw the IP Security ESP format
13. What are the steps for preparing a signed data MIME entity?
14. What are the benefits of IP Security?

PART-B (16 Marks)

1. Explain the authentication service provided by Kerberos? (16)
2. Explain X.509 authentication service? (16)
3. Briefly explain Pretty Good Privacy? (16)
4. Explain S/MIME? (16)
5. Explain the IP security architecture? (16)

UNIT – IV

SYSTEM SECURITY

PART-A (2 Marks)

1. What are the types of intruders?
2. Define masquerader
3. Define misfeasor
4. Define clandestine user

5. What are the techniques used for learning passwords?
6. What are the approaches used for intrusion detection?
7. How the Intrusion Detection provides security?
8. What are the password selection strategies?
9. Draw the architecture for distributed intrusion detection?
10. What do you mean by malicious software?
11. Name some malicious software's?
12. Define virus
13. Define a worm
14. Define a firewall
15. What are the design goals of firewall?
16. What are the advantages of firewall?
17. What are the limitations of firewalls?
18. What are the types of firewalls used?
19. Define a trusted system

PART-B (16 Marks)

1. Define intrusion and explain the methods used for intrusion detection? (16)
2. Explain password management? (16)
3. Define malicious software and explain different kinds of malicious software's? (16)
4. Explain firewall and their design principles? (16)
5. Explain trusted systems? (16)

UNIT – V

WIRELESS SECURITY

PART-A (2 Marks)

1. Gives some wireless security standards?
2. What do you mean by Wi-Fi?
3. What are the services provided by Wireless Equivalent Privacy (WEP)
4. Limitations of Wired Equivalent Privacy (WEP)
5. Give the structure of WEP
6. Service set identifier (SSID)
7. Media access control (MAC)
8. Wired equivalent privacy (WEP)

PART-B (16 Marks)

1. Write brief notes on wireless security standards. (16)
 2. Explain WEP and WPA. (16)
 3. Wireless LAN Security factors (16)
 4. Explain the issues in Wireless Security (16)
-