NETWORK ADMINISTRATION AND SECURITY

Unit – I (NAS)

(W- 10)

Q. 1) What is Security Attack? Explain general categories of attack with examples. 7

(S - 11)

Q. 2) List and define the five security services. 5

(W - 11)

Q. 3) Define and explain the types of security attack in each of the following cases. 6
i) A student breaks into a professor's office to obtain a copy of the next day's test,
ii) A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.

Q. 4) Define and explain eight security Mechanism. 8

(S - 12)

Q. 5) List and define five security services. 5

Q. 6) Discuss the following: 8
i) Cryptography ii) Cryptoanalysis.

(W - 12)

Q. 7) What is RFC? Describe the RFC publication process. 7

Q. 8) What is cipher block chaining mode and cipher feedback mode. 6

Q. 9) Explain the Model for Network Security. 7

Unit – II (NAS)

(S - 06)

Q. 1) What is cryptanalysis? Explain the DES algorithm in detail. 9

Q. 2) What do the following terms mean in key distribution : 4
i) Session key ii) Permanent key
iii) Key Distribution centre iv) Front-end processor

Q. 3) Explain the RSA public key encryption algorithm. 6

Q. 4) What is message authentication ? Explain the digital signature. 7

(W - 06)

Q. 5) What are various requirements for public key cryptography? 7

(W - 09)

Q. 6) Explain any two block cipher conventional encryption algorithms. 8

Q. 7) With neat diagrams explain how the I-way hash function is used for message authentication. 6

Q. 8) Explain: i) ECB ii) CFB 5

Q. 9) Compare Link encryption & end-to-end encryption. 4

(W - 10)

Q. 10) Explain Public Key Cryptography with respect to Private Key Cryptography. Write RSA algorithm. 7

Q. 11) Define a Session Key. How a KDC can create a session key between Alice and Bob. Explain. 7

Q. 12) What is SHA-SIZ? Explain compression function is used in SHA-SIZ. 6

(S - 11)

Q. 13) Explain DES and Triple DES algorithms on the following issues- 10

i) No of rounds ii) Key size

iii) Mathematical operation iv) Applications

Q. 14) What is the need of public key cryptography ? Explain RSA algorithm. 8

(W - 11)

Q. 15) Discuss public-key encryption structure. Give diagrammatic representation of encryption and authentication. 7

Q. 16) In a public-key using RSA, you intercept that ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? 7

Q. 17) Compare and control DES, 3DES and AES. 6

Q.18) Explain the secure hash function requirements. 6

Q. 19) Explain the DES algorithm in detail with its strength and drawbacks. 8

Q. 20) Distinguish between a substitution cipher and a transposition cipher. 5

Q. 21) Explain the DES algorithm. How is the Triple DES algorithm different from DES. 8

Q. 22) Explain the concept of Digital Signature. 5

Q. 23) Explain RSA algorithm giving a suitable example. 8

Unit – III (NAS)

(W - 09)

Q. 1) List the limitations of SMTP 822 scheme which are addressed by MIMME. What are the elements of MIME specification. 6

(S - 10)

Q. 2) What is Kerberos? Give the difference between Kerberos version 4 and version 5. 5

Q. 3) Compare MIME and SMTP. 4

(S - 11)

Q. 4) What is MINE? Explain the need and functionality. 6

Q. 5) Explain PCP services. 6

(W - 11)

Q. 6) What is Kerberos? Explain it's requirements. 6

Q. 7) State the problem that Kerberos address. Explain simple authentication dialogues with AS & TGS for Kerberos version 4. 7

(S - 12)

Q. 8) Define Kerberos and name its server. Explain in detail the duties of each server. 8

Q. 9) What is pretty Good Privacy? Explain PGP services. 6

Q. 10) What are the different types of function provided by the S/MIME. 6

(W - 12)

Q. 11) Discuss PGP message transmission and reception using key rings. 7

Q. 12) Describe the authentication procedure for X.509. 7

Q. 13) What is multiple Kerberi ? Compare Kerberos version 4 and 5. 7

Q. 14) Explain the key management functions performed by S/MIME user. 7

Unit - IV

(S - 09)

Q. 1) What is IPSec ESP packet format? Explain scope of ESP encryption and authentication. 7

Q. 2) What are set components ? give the sequence of events that are required for a transaction. 4+3=7

(W – 09)

Q. 3) Discuss SSL record protocol operation & SSL record format. 7

Q. 4) Explain SSL handshake protocol. 5

(S - 10)

Q. 5) Explain SSL architecture in detail. 10

Q. 6) Explain the secured Electronic Transaction (SET), giving its key features. 3

(W - 10)

Q. 7) What are various Secure Electronic Commerce Components? 5

(S - 11)

Q. 8) Explain security provided at transport layer in detail. 8

Q. 9) What is Web security? Explain its need and requirements. 5

(W - 11)

Q. 10) What is secured Electronic Transaction.
i) Explain key features and participants of SET.
ii) Briefly describe the sequence of events, that are required for transaction.

Q. 11) What is an IPsec ? List and explain its Application and benefits. 9

Q. 12) List the different types of threats faced in using a web. 5

(S - 12)

Q. 13) Explain : i) SSL session ii) SSL connection 8

Q. 14) Explain Anti-Replay Services. 6

(W – 12)

Q. 15) What is IP sec ? Explain the authentication header with its scope. 8

Unit - V

(S - 09)

Q. 1) Explain :
i) Management Station ii) Management agent iii) MIB 6.

(W - 09)

Q. 2) Describe SNMPV3 message format with USM. 6

Q. 3) What is SNMP community? Explain with authentication, access control & proxy service. 8

(S - 10)

Q. 4) Explain the VSM message processing mechanism. 6

Q. 5) What is SNMP ? Explain with authentication, access control & proxy service. 8

Q. 6) Explain the Network Management Protocol Architecture. 8

(W - 10)

Q. 7) Explain SNMP Architecture. 6

Q. 8) What are the Elements of VACM ? Explain view-based access control logic for access policy. 7

(S - 11)

Q. 9) Compare $SNMPV_1$, $SNMPV_2$ and $SNMPV_3$. 6

Q. 10) Explain the User Security Model Message Processing. 6

(W - 11)

Q. 11) What is proxy ? Why it is developed ? Explain the protocol architecture involving proxy. 7

Q. 12) What are the different strengths and deficiencies of SNMPV2. 6

Q. 13) Explain SNMP protocol architecture. 7

Q. 14) Explain in brief view – based access control. 6

(S - 12)

Q. 15) What is proxy ? Explain the protocol architecture involving proxy. 6

Q. 16) Discuss authentication service and access policies of SNMPV1. 7

Q. 17) Explain the role of SNMP for network management protocol architecture. 7

(W - 12)

Q. 18) Why do we need proxy? Explain its protocol architecture. 6

Q. 19) Discuss the USM message processing mechanism. 7

Unit – VI

(W - 08)

Q. 1) What is Virus ? Give its different types. 4

Q. 2) Explain Firewall :
i) Characteristics ii) Techniques used to control access iii) Limitations. 9

(S - 09)

Q. 3) What are the common types of firewalls ? Explain. 6

Q. 4) List and explain the different Antivirus approaches. 7

(S - 10)

Q. 5) Explain in detail taxonomy of malicious programs. 7

Q. 6) What is a Firewall ? Explain its characteristics and limitations. 7

(W - 10)

Q. 7) What are various types of firewalls ? discuss any two types of firewalls. 7

Q. 8) What is the nature of viruses ? Give lifetime four typical stages of virus. 7

(S - 11)

Q. 9) Explain the distributed intrusion detection architecture. 7

Q. 10) What are Trusted systems ? Explain the concepts. 7

Q. 11) Explain the following malicious programs :- 8

i) Worms ii) Trap doors

iii) Trojan Horses iv) Bacteria

Q. 12) Explain in brief :- 6

i) Rule based intrusion detection system.

ii) Distributed Intrusion detection system

(W – 11)

Q. 13) How many generations of Antivirus software ? Explain in detail. 6

(S - 12)

Q. 14) Explain in detail the UNIX password scheme. 6

(W - 12)

Q. 15) What is Intrusion Detection System? Explain the rule based Intrusion Detection and Distributed Intrusion Detection in brief. 7

Q. 16) Explain the types, characteristics and Limitations of Firewall. 7