# Assignment unit1 to unit 4 IANS June 2024-25

## Unit 1

1. Describe OSI security architecture and principles of security.
2. Define Security Attacks, Security Services, Security Mechanisms
3. Explain principles of security with possible attack example on each of them.
4. Explain model for network security with a labelled diagram.
5. Consider the message "THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS". Apply simple columnar transposition technique to encrypt it. Detail the steps.
6. Explain Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques
7. Discuss play fair cipher. Generate cipher text for "REPUBLIC DAY IS IN JANUARY" using LOTUS as the key.
8. Describe Steganography with an example.
9. Enlist and explain Block Cipher Principles,
10. Discuss AES algorithm.
11. Explain Block Cipher Modes of Operation
12. Explain RSA.
13. Explain Diffie-Hellman Key Exchange
14. Differentiate between passive and active security threats? List and briefly define categories of passive and active security attacks.
15. Define transposition cipher. Explain rail-fence cipher technique using suitable example.
16. What is meant by Asymmetric key algorithm? Using two prime numbers P=7 and Q=17 generate RSA private key and public key
17. Consider the message "THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS". Apply simple columnar transposition technique to encrypt it. Detail the steps.
18. Differentiate between block cipher and stream cipher.
19. Explain single round function of DES with suitable diagram and key generation.
20. Explain Diffie-Hellman algorithm. For Diffie-Hellman algorithm, two publicly known numbers are prime number 353 and 3. Person A selects the random integer 97 and Person B selects 233. Compute common secret key.
21. Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.
22. Brief Diffie-Hellman key exchange algorithm. Person A and B want to establish a secret key using the diffie-Hellman key exchange protocol. Assuming the values as n=11, g=5, x=2 and y=3, find out the values of A, B and secret key.

## Unit 2

Program Security: Secure programs: Fixing Faults, Unexpected Behavior, Types of Flaws. Non-malicious program errors: Buffer overflows, Incomplete Mediation. Viruses and other malicious code: Why worry about Malicious Code, Kinds of malicious code, how viruses attach, how viruses gain control, Prevention Control Example: The Brain virus, The Internet Worm, Web bugs. Targeted malicious code- Trapdoors, Salami Attack. Controls against program threats- Development Controls, Peer reviews, Hazard Analysis.

1. What are typical phases of operation of a virus or worm?
2. Describe some worm/virus countermeasures.
3. Explain the types of Malicious and Non-Malicious programming errors
4. What is Targeted Malicious code? Discuss Salami Attack in detail
5. Explain the following various controls against Program threats;
    a) Development Controls
    b) Peer reviews
    c) Hazard Analysis.
6. Explain Non-malicious program errors: Buffer overflows and Incomplete Mediation.
7. Explain different types of malicious programs:
    a) Backdoor
    b) Logic Bomb
    c) Trojan Horses
    d) Mobile Code
    e) Multiple-Threat Malware

8. explain various Viruses
    a) The Nature of Viruses
    b) Viruses Classification
    c) Virus Kits
    d) Macro Viruses
    e) E-Mail Viruses

## Unit 3

Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security of Hash Functions and Macs, Secure Hash Algorithm, HMAC Digital Signatures and Authentication: Digital Signatures, Authentication Protocols, Digital Signature Standard Authentication Applications: Kerberos, X.509 Authentication, Public-Key Infrastructure Network Access Control: Network Access Control, Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control. Wireless Network Security: Mobile Device Security, Wireless LAN Security

1. Discuss SHA-512 algorithm.
2. Summarize Kerberos Authentication System.
3. Describe X.509 authentication service.
4. What is MAC? Explain HMAC.
5. What is Kerberos? How Kerberos authenticates the users for authorized service access?
6. Discuss public key infrastructure.
7. Discuss hash function with its requirements. Explain birthday paradox and attack with respect to hash function.
8. Describe the contents of Digital certificate

9. Wireless Network Security
10. Mobile Device Security
11. Wireless LAN Security
12. Authentication protocols

**Unit 4**

Electronic Mail Security: Pretty Good Privacy, S/MIME, Domain Keys Identified Mail. IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management Web Security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, HTTPS standard , Secure Socket Shell Intrusion: Intruders, Intrusion Techniques, Intrusion Detection, Firewalls: Firewall Design Principles, Types of Firewalls Security in Online transactions

1. Where SSL is placed in TCP/IP?
2. Describe SSL handshake protocol in detail.
3. What is the purpose of PGP?
4. Explain PGP operations.
5. Discuss IPSec authentication header
6. Discuss the working of SSL record and alert protocol.
7. What is the purpose of PGP?
8. Discuss any three PGP operations. How PGP is different from S/MIME?
9. Discuss IPSec Encapsulating security header.
10. Give purpose of firewalls?
11. Explain firewall configurations.

**********