L.D.COLLEGE OF ENGINEERING AHMEDABAD
Department of Information Technology

Assignments

Subject: Information and Network Security (2170709)
Class: BE Sem. VII (IT)

Prepared By:- Prof JAHNAVI S VITHALPURA

Assignment-1:

1. Define the terms threat and attack. List and briefly define categories of security attacks.
2. List and briefly define the security services.
3. What is security mechanism? List and explain various security mechanisms.
4. Define the Cryptography.
5. Differentiate Symmetric and Asymmetric key cryptography.
6. Write the differences between conventional encryption and public key encryption.
7. Compare public key and private key cryptography. Also list various algorithms for each.
8. What is public key cryptography? Compare public it with conventional cryptography.
9. What is cryptography? Briefly explain the model of Asymmetric Cryptosystem.
10. Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.
11. Explain cryptanalysis. Discuss any one technique for it
12. Explain the conventional security model used for information security.
13. What is the objective of attacking an encryption system? Write the two approaches to attack a conventional encryption scheme.
14. Explain the terms diffusion and confusion.
15. List and explain various types of attacks on encrypted message.
16. Define the Caesar cipher.
17. Is playfair cipher monoalphabetic cipher? Justify. Construct a playfair matrix with the key “moonmission” and encrypt the message “greet”.
18. Explain the various types of cryptanalytic attack, based on the amount of information known to the cryptanalyst.
19. Explain play fair cipher with suitable example.
20. Construct 5 X 5 playfair matrix for the keyword “OCCURANCE”.
21. Let the keyword in playfail cipher is “keyword”. Encrypt a message “come to the window” using playfair cipher.
22. Construct a Playfair matrix with the key “engineering”. And encrypt the message “test this process”.
23. Construct a playfair matrix with the key “occurrence”. Generate the cipher text for the plaintext “Tall trees”.
24. Encrypt the message “Good morning” using the Hill Cipher with the key

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

25. Write short note on: Hill Cipher

26. Explain the one time pad scheme.
27. Explain Vegenere Cipher.
28. Explain monoalphabetic cipher and polyalphabetic cipher by giving an example.
29. Explain various types of attack on computer system.

Assignment-2:

1. Draw and explain Feistel's structure for encryption and decryption.
2. Define Block Cipher. Explain Design Principles of block cipher.
3. The exact realization of Feistel network depends on the choice of which parameters?
4. Explain DES algorithm with Figure.
5. Explain single round function of DES with suitable diagram.
6. Explain limitation of DES in detail.
7. Define the terms diffusion and confusion. What is the purpose of S-box in DES? Explain the avalanche effect in DES.
8. Explain the triple DES scheme with two keys and write about proposed attacks on 3DES.
9. Explain Sub key generation Process in Simplified DES algorithm with Example.
10. Explain key expansion Process in AES algorithm.
11. Explain AES with structure.

Assignment--3

12. List various modes of operations of block cipher. Explain any three of them briefly.
13. List and explain various block cipher modes of operation with the help of diagram.
14. Why mode of operation is defined? Explain the simplest mode for block cipher modes of operation?
15. Why mode of operation is defined? Explain the block cipher modes of operation?
16. Explain Modes of Operations.

Assignment--4:

1. List and explain four general categories of schemes for the distribution of public keys.
2. List and explain various key management techniques.
3. Explain different key distribution techniques.
4. Write the key distribution scenario in which each user shares a unique master key with key distribution centre.
5. What is KDC? With the help of diagram explain how KDC do key distribution.
6. Explain the key distribution scenario and write how does decentralized key control work?
7. Discuss the ways in which public keys can be distributed to two communication parties.
8. What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution canter.
9. Give the steps of RSA algorithm.
10. Explain Encryption and decryption in RSA algorithm. Also discuss various attacks on RSA.
11. Define the types of cryptanalytic attacks. Which cryptanalytic attack can occur on RSA algorithm?

12. Write four possible approaches to attacking the RSA algorithm.
13. Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7, M=5.
14. In a public key system using RSA, the ciphertext intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?
15. Calculate ciphertext in case of RSA if p=3,q=11,e=3,M=5.
16. How key exchange using elliptic curves can be done?
17. Write short note on:Elliptic Curve Cryptography
18. What is an elliptic curve? What is the zero point of an elliptic curve?
19. What is primitive root? Explain Diffi-Hellmen key exchange algorithm with proper example.
20. Explain Deffie Hellman key exchange scheme in detail.
21. Write Diffie Hellman key exchange algorithm. Explain man-in-the middle attack on this Diffie Hellman key exchange.
22. Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.

Assignment-5:

1. Is message authentication code same as encryption? How message authentication can be done by message authentication code?
2. What characteristics are needed in a secure hash function?
3. Write short note on: Message Authentication Code
4. Explain MD5 Hash Algorithm.
5. Explain four passes of MD5 message digest algorithm.
6. Explain SHA512 Algorithm.
7. Explain the operation of secure hash algorithm on 512 bit block.
8. Write the note on Digital Signature Algorithm.
9. What is digital signature? Explain its use with the help of example.
10. List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.
11. Illustrate variety of ways in which hash code can be used to provide message authentication.
12. Which parameters affect RC5 encryption algorithm. Explain RC5 encryption and decryption process.
13. Explain the general structure of secure hash functions.
14. Explain different characteristics of hash function.
15. Define MAC.
16. Explain briefly basic uses of MAC.
17. Illustrate the overall operation of HMAC. Define the terms.
18. What is MAC? Why it is required? Explain HMAC algorithm.
19. What is a trap-door one-way function? What is its importance in public key cryptography?
20. What is the difference between weak and strong collision resistance?
21. Explain the following properties of hash function

    (i) One way property, (ii) Weak collision resistance (iii) Compression function in hash algorithm.

22. What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is used.

Assignment -6

1. Define Digital Signature.
2. Explain X.509 authentication service.
3. Explain the one way and two way authentication in X.509.
4. Explain Kerberos in detail.
5. Explain the ticket granting server (TGS) scheme in Kerberos.
6. What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos.

Assignment -7

1. Explain SSL protocol in detail.
2. List and define the parameters that define secure socket layer connection state.
3. Which parameters define session state and which parameters define connection state in SSL (secure socket Layer).
4. Explain the pseudorandom function used by Transport layer security.
5. Explain the secure socket layer handshake protocol action.
6. How can we achieve web security? Explain with example.

****