Uka Tarsadia University (Diwaliba Polytechnic)

Diploma in Computer Engineering

Assignment (Information Security)

Unit 1: Introduction to Information Security

1. Write down difference between active attacks and passive attacks.
2. Define: Information security.
3. Define: Authentication and Integrity
4. Which attacks are hard to detect? Why?
5. Explain OSI security architecture model.
6. Describe CIA.
7. Enlist types of authentication. Explain them in detail.
8. Enlist types of active attack.
9. Explain following terms each with a suitable diagram:
    a. Release of message contents
    b. Traffic analysis
10. What is the requirement of security?
11. Explain following terms each with a suitable diagram:
    a. Masquarade
    b. Denial of service

Unit 2: Encryption Techniques

1. Explain symmetric cipher model with a suitable diagram.
2. Describe steganography in brief.
3. Find the cipher text for following plain text and key using hill cipher:

   PT: $\begin{bmatrix} 11 & 20 & 9 \end{bmatrix}$

   Key: $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{bmatrix}$
4. Find the cipher text for following plain text and key using caesar cipher:

PT: Computer Engineering

Key: 7

5. Differentiate substitution technique and transposition technique.
6. Find the cipher text for following plain text and key using rail fence technique:

   PT: Work for it more than you hope for it.

   Key: 3
7. Find the cipher text for following plain text and key using columnar technique:

   PT: Do not stop until you are proud.

   Key: worth
8. Find the cipher text for following plain text and key using playfair cipher:

   PT: Hill cipher is a multi-letter cipher.

   Key: cryptography
9. Find the cipher text for following plain text and key using polyalphabetic cipher:

   PT: One time pad uses random keys.

   Key: accept

Unit 3: Block Ciphers

1. What is confusion and diffusion?
2. Explain avalanche effect.
3. What is the size of plaintext and how many numbers of round used in DES algorithm?
4. Given 10 bit key K=1110000111. Determine k1, k2 where

   P10 = 3 5 2 7 4 10 1 9 8 6

   P8 = 6 3 7 4 8 5 10 9

   by using S-DES key generation method.
5. Write down the strength of DES.
6. Given the following data find cipher text using S-DES encryption algorithm:

IP
2 6 3 1 4 8 5 7

IP^{-1}
4 1 3 5 7 2 8 6

P4
2 4 3 1

E/P
4 1 2 3 2 3 4 1

$$S0=\begin{bmatrix}1 & 0 & 3 & 2\\ 3 & 2 & 1 & 0\\ 0 & 2 & 1 & 3\\ 3 & 1 & 3 & 2\end{bmatrix}, S1=\begin{bmatrix}0 & 1 & 2 & 3\\ 2 & 0 & 1 & 3\\ 3 & 0 & 1 & 2\\ 2 & 1 & 0 & 3\end{bmatrix}$$

Plaintext = 10101001, K1 = 10100100, K2 = 01000011.

9. Explain block cipher.
10. What is timing attack?
11. Draw the diagram of single round of feistel structure.

Unit 4: Public Key Cryptography

1. List out ingredients of public key encryption scheme.
2. Write down difference between private key and public key algorithm.
3. Draw the diagram of encryption with private key.
4. Brief the concept of key exchange.
5. What is probable message attack?
6. Find n and $\varnothing(n)$, where p = 3 and q = 11.
7. What is a meet-in-the-middle attack?
8. Explain the concept of public key cryptosystem.
9. Explain public key cryptosystem to achieve secrecy.
10. Explain simple secret key distribution.
11. Explain the concept of public announcement of public keys and publicly available directory.
12. Perform encryption and decryption using RSA system for p = 11, q = 3, e = 3 & M = 4. Also show the steps to generate the public and private keys.
13. Explain public-key authority.

Unit 5: Message Authentication And Hash Function

1. Enlist applications of cryptographic hash function.
2. Describe MAC.
3. What are the requirements of hash function?
4. Enlist types of attacks addressed by message authentication.

5. Describe strong collision resistance.
6. Describe one way property in hash function.
7. Draw and explain the following statements:
    a. Message authentication and confidentiality tied to plaintext
    b. Message authentication and confidentiality tied to ciphertext
8. Describe the requirements of MAC function.
9. Describe basic authentication function.
10. Enlist and explain various ways in which hash code can be used to provide message authentication with suitable diagram.

Unit 6: Digital signatures and Authentication protocols

1. Explain requirements of digital signature.
2. Describe arbitrated digital signature technique.
3. Explain direct digital signature technique.
4. Draw the diagram for DSA approach to provide digital signature.
5. Enlist steps of digital signature algorithm.
6. Write down difference between RSA approach and DSA approach.
7. Write down use of authentication protocols.
8. How to provide one-way authentication in email?
9. List any two properties a digital signature should essentially have.
10. What are some threats associated with a direct digital signature scheme?