Uka Tarsadia University (Diwaliba Polytechnic)
Diploma in Information Technology
Assignment (Web & Network Security-020070602)

Unit 1: Public Key Crypto Systems

1. Describe one way function.
2. Two prime numbers are 11 and 13. Find public key and private key using RSA algorithm.
3. Enlist counter measure of timing attack.
4. Find GCD of 54 and 888.
5. Explain requirements for public key cryptography.
6. In RSA algorithm user A uses p=13 and q=17 to generate public key and private key. If public key is 35 then what will be the private key?
7. Explain asymmetric public key cryptography.
8. Draw the diagram of encryption with public key.
9. Explain principles of public key cryptosystem.
10. Explain how authentication and secrecy is achieved in public key cryptosystem.

Unit 2: MAC and Hash Functions

1. Enlist uses of hash function.
2. Enlist and explain requirement of cryptographic hash function.
3. Explain man-in-the-middle attack with suitable diagram.
4. Write the block size of SHA-1 and SHA-512.
5. Define the following terms:
    a. Hash function
    b. Message digest
6. Write the full form of PRF and PRNG.
7. Explain digital signature with suitable diagram.
8. Explain compression function of MD5 hash algorithm with suitable diagram.
9. Explain message authentication using hash function.
10. Describe one-way property of hash function.

Unit 3: Network Security Application

1. Enlist properties of digital signature.
2. Write full form of MIME and S/MIME.
3. Explain MIME transfer encoding.
4. Explain confidentiality service in S/MIME.
5. Explain process of generating and using of digital signature.
6. Define email compatibility in S/MIME.
7. Explain format of PGP message.
8. Explain S/MIME message content types.
9. What is weak collision resistant?
10. Define MAC.

Unit 4: IPSec

1. Define SSL session.
2. Explain transport layer security with its benefits.
3. Enlist services provided by IPSec.
4. Draw and explain authentication header.
5. Draw the structure of ESP encryption and authentication in tunnel mode for IPv4.
6. Enlist and briefly define the parameters that define SSL connection state.
7. Write the difference between SSL and TLS.
8. Enlist Benefits of IPSec.
9. Enlist and briefly define the parameters that define SSL session state.
10. Draw IPv6 header. Describe any four field of IPv6 header.

Unit 5: Web Security

1. Explain web security consideration.
2. Explain HTTPS connection initiation.
3. Define SET.
4. Explain issuer domain in 3D secure protocol.
5. Define web security. Why web security is required?

6. Explain web security threats that violate the integrity and confidentiality with its consequences and counter measures.
7. Define the following terms:
    a. Issuer
    b. Acquirer
8. Explain difference between HTTP and HTTPS.
9. Explain any two web traffic security approaches with suitable diagram.
10. List the elements which are encrypted when are when HTTPS communication is used.

Unit 6: System Security

1. Enlist techniques that are used to avoid guessable passwords.
2. Explain rule-based detection.
3. What is the difference between statistical anomaly detection and rule-based intrusion detection?
4. Enlist and explain types of intruders.
5. What are the benefits that can be provided by an intrusion detection system?
6. Explain types of malicious software.
7. What are the limitations of firewall?
8. Explain UNIX password management scheme with suitable diagram.
9. Draw the hierarchy of malicious program.
10. Explain reactive password checking and proactive password checking techniques for avoid guessable passwords.