Network Security and Cryptography (23CY501)

Tutorial Sheet – Unit II

Symmetric Key Ciphers and Asymmetric Key Ciphers

Part A: Short Answer Questions

Symmetric Key Ciphers

1. Define a block cipher.
2. What is a stream cipher?
3. State the basic principles of block cipher design.
4. What is DES?
5. What is the key size of DES?
6. Expand AES.
7. What are the standard key sizes used in AES?
8. What is Blowfish?
9. What is RC5?
10. What is IDEA?
11. What is the block size of IDEA?
12. What is RC4?
13. Differentiate between block ciphers and stream ciphers.
14. What is meant by encryption round?
15. What is Feistel structure?
16. What is substitution in block ciphers?
17. What is permutation in block ciphers?
18. What are the advantages of AES over DES?
19. What is avalanche effect?
20. Define confusion and diffusion.

Asymmetric Key Ciphers

21. What is public key cryptography?
22. Define public key and private key.
23. State the principles of public key cryptosystems.
24. What is RSA?
25. Expand RSA.
26. What is the purpose of the Diffie–Hellman algorithm?
27. What is ElGamal cryptography?
28. What is a digital signature?
29. What is key exchange?
30. What is the Knapsack algorithm?

Part B: Long Answer Questions

Symmetric Key Ciphers

1. Explain the principles of block ciphers with a neat diagram.
2. Discuss the structure and working of the DES algorithm.
3. Explain the DES encryption process with suitable illustrations.
4. Describe the architecture and working of AES.
5. Explain the AES encryption process in detail.
6. Compare DES and AES.
7. Explain the Blowfish algorithm and its features.
8. Describe the RC5 encryption algorithm.
9. Explain the structure and working of IDEA.
10. Discuss various modes of block cipher operation.
11. Compare ECB, CBC, CFB, OFB, and CTR modes.
12. Explain stream ciphers and their characteristics.
13. Describe the RC4 algorithm and its working.
14. Differentiate between block ciphers and stream ciphers.
15. Discuss the advantages and limitations of DES, AES, Blowfish, RC5, and IDEA.

Asymmetric Key Ciphers

16. Explain the principles of public key cryptosystems.
17. Describe the RSA algorithm with key generation, encryption, and decryption steps.
18. Explain RSA with a suitable numerical example.
19. Discuss the advantages and limitations of RSA.
20. Explain the ElGamal cryptographic algorithm.
21. Describe the Diffie–Hellman key exchange algorithm with an example.
22. Explain the working of the Knapsack cryptosystem.
23. Compare RSA and ElGamal cryptographic systems.
24. Compare symmetric key cryptography and asymmetric key cryptography.
25. Explain how public key cryptography provides authentication and confidentiality.

Part C: Analytical and Conceptual Questions

1. Why is AES considered more secure than DES?
2. Analyze the importance of multiple rounds in block ciphers.
3. Why are stream ciphers generally faster than block ciphers?
4. Discuss the security weaknesses of DES.
5. Why is key management easier in public key cryptography?
6. Explain why RSA is computationally expensive.
7. Compare RSA and Diffie–Hellman algorithms.

8. Why is Diffie–Hellman vulnerable to man-in-the-middle attacks?
9. Analyze the role of prime numbers in RSA.
10. Explain the significance of public and private keys.

Part D: Problem-Solving Questions

DES and AES

1. Explain the round structure of DES.
2. Draw and explain the Feistel network used in DES.
3. List the transformations performed in one round of AES.
4. Explain the SubBytes, ShiftRows, MixColumns, and AddRoundKey operations in AES.

RSA

5. Generate RSA keys using:
   - p = 3
   - q = 11
   - e = 7

   Find:

   - n
   - φ(n)
   - Private key d
6. Encrypt the message M = 5 using the RSA parameters:
   - p = 3
   - q = 11
   - e = 3
7. Decrypt a given RSA ciphertext using the private key.

Diffie–Hellman

8. Using:
   - Prime number p = 23
   - Primitive root g = 5
   - User A private key = 6
   - User B private key = 15

   Calculate:

   - Public keys Shared secret key

ElGamal

9. Explain the encryption and decryption steps of ElGamal with an example.
10. Compare RSA and ElGamal based on:
    - Key generation
    - Security
    - Performance
    - Applications

Part E: Multiple Choice Questions (MCQs)

1. DES uses a key length of:
    - A) 56 bits
    - B) 64 bits
    - C) 128 bits
    - D) 256 bits

    Answer: A

2. AES supports key lengths of:
    - A) 32, 64, 128
    - B) 128, 192, 256
    - C) 64, 128, 512
    - D) 56, 112, 168

    Answer: B

3. Blowfish is a:
    - A) Stream cipher
    - B) Block cipher
    - C) Hash algorithm
    - D) Public key algorithm

    Answer: B

4. RC4 is a:
    - A) Block cipher
    - B) Hash function
    - C) Stream cipher
    - D) Digital signature algorithm **Answer:** C

5. RSA is based on:
    - A) Discrete logarithm
    - B) Integer factorization
    - C) Hashing
    - D) Transposition

    Answer: B

6. Diffie–Hellman is primarily used for:
    - A) Encryption
    - B) Key exchange
    - C) Hashing
    - D) Compression

    Answer: B

7. ElGamal security is based on:
    - A) Discrete logarithm problem
    - B) Factorization
    - C) Hash functions
    - D) DES

    Answer: A

8. AES block size is:
    - A) 64 bits
    - B) 128 bits
    - C) 256 bits
    - D) 512 bits

    Answer: B

9. DES consists of:
    - A) 8 rounds
    - B) 12 rounds
    - C) 16 rounds
    - D) 32 rounds

    Answer: C

10. Which algorithm is used for public key cryptography?
    - A) AES
    - B) DES
    - C) Blowfish D) RSA **Answer:** D

Part F: Assignment Questions

1. Prepare a comparative study of DES, AES, Blowfish, RC5, and IDEA.
2. Analyze the strengths and weaknesses of stream ciphers and block ciphers.
3. Implement a simple RSA algorithm and demonstrate encryption and decryption.
4. Study the working of Diffie–Hellman key exchange with a numerical example.
5. Compare RSA, ElGamal, and Knapsack cryptosystems.
6. Investigate real-world applications of AES in secure communication systems.
7. Analyze the security vulnerabilities of RC4.
8. Study modern replacements for DES and RC4.

Viva Questions

1. What is a block cipher?
2. What is a stream cipher?
3. What is the key size of DES?
4. Why was AES introduced?
5. What is the difference between DES and AES?
6. What is Blowfish?
7. What is RC4?
8. What is RSA?
9. What is the role of public and private keys?
10. What is Diffie–Hellman key exchange?
11. What is ElGamal cryptography?
12. What is the Knapsack algorithm?
13. What are block cipher modes of operation?
14. What is a digital signature?
15. Why is RSA more secure than traditional symmetric algorithms for key distribution?