UNIT - I: INTRODUCTION TO CRYPTOGRAPHY

2 Marks

1. Define Cryptography.
2. List types of Cryptography.
3. List any 4 Applications of cryptography.
4. Define Plain Text.
5. Define Cipher text.
6. What is the cipher text of **"defend the east wall of the castle"** with a shift of 3 keys?
7. What is encryption?
8. What is decryption?
9. List Encryption and Decryption Keys
10. Define Symmetric Key cryptography.
11. Define Asymmetric Key cryptography.
12. What is the Key Range?
13. What is Key Size?
14. Define cryptanalysis.
15. List Cryptanalysis Attacks.
16. List Cryptanalysis tools.

4 Marks

1. Explain Features of Cryptography.
2. Explain types of cryptography.
3. Write differences between plain text and cipher text.
4. Explain Encryption and Decryption Keys.
5. Write a note on Key Range and Key Size.
6. Explain Symmetric Cipher Model.
7. Write a note on Cryptanalysis Tools.

8 Marks

1. Explain Applications of Cryptography.
2. Explain plain text and cipher text in detail with examples.
3. Explain Encryption and decryption with a neat diagram.
4. Write Differences between Encryption and Decryption.
5. Explain Symmetric and Asymmetric Key cryptography in detail.
6. Explain Cryptanalysis Attacks and techniques.

UNIT - II: Public Key Cryptography and RSA

2 Marks:

1. Define Public key encryption.
2. List Components of Public Key Encryption.
3. What is RSA?
4. List two broad components of RSA.
5. Define Diffie-Hellman key exchange.
6. List applications of Diffie Hellman Exchange algorithm.

4 Marks:

1. Explain Components of Public Key Encryption.
2. Explain Applications of the Public Key Encryption.
3. Explain RSA Algorithm.
4. Explain RSA Algorithm steps.
5. Write Diffie Hellman Exchange algorithm Steps.
6. Explain applications of Diffie Hellman Exchange algorithm.
7. P=33, G (Primitive Root) =8, A=3, B=2. Find the D-H Key shared between them.
8. P=23, G =7, A=3, B=6, Find D-H Key shared between them.
9. P=23, G =5, A=4, B=3. Find the D-H Key shared between them.
10. P=7, G =3, A=2, B=5 Find D-H Key shared between them.

8 Marks:

1. Explain RSA Algorithm steps with one example.
2. In an RSA cryptosystem, a particular A uses two prime numbers, P=3 and q=11, to generate the public and private keys. If the public key of A is e=7, then find the private key of A. Perform Encryption and Decryption when plain text=2.
3. P and Q are two prime numbers P=5, Q=7. Take public key E=5, If Plain text value is 3, then what will be the cipher text value according to the RSA algorithm? Again calculate Plain text value from cipher text.
4. P and Q are two prime numbers P=5, Q=7. Take public key E=5, If Plain text value is 2, then what will be the cipher text value according to the RSA algorithm? Also calculate Plain text value from cipher text.
5. Write the steps for Diffie Hellman Algorithm and solve the following algorithm. P=33, G=8, A=3, B=2 find D-H Key shared between the users.

UNIT - III

Block ciphers and Data encryption standards

2 Marks:

1. Define Stream cipher.
2. List types of stream cipher.
3. Define Block Cipher.
4. List examples of stream and block ciphers.
5. List various modes of operation of a Block Cipher.
6. Define DES.
7. Define AES.
8. List AES features.

4 Marks:

1. Explain Advantages and Disadvantages of stream cipher.
2. Write differences between Stream and block ciphers.
3. Write a note on Stream Cipher.
4. Write a note on Block Cipher.
5. Explain ECB mode with a neat diagram.
6. Explain Cipher Block Chaining Mode with a neat diagram.
7. Explain broad level steps of DES with a neat diagram.
8. Explain steps involved in the encryption process of AES.

8 Marks:

1. Solve the problem P=‘RLS BCA’, Key=’E’ using stream cipher. Perform Encryption and Decryption.
2. Solve the problem P=‘KIWI’, Key=’D’ using stream cipher. Perform Encryption and Decryption.
3. Solve the problem P=‘APPLE’, Key=’F’ using stream cipher. Perform Encryption and Decryption.
4. Solve the Problem using RC4’s PRGA Algorithm. Consider **S= [2, 3, 7, 4, 6, 0, 1, 5]**, **P= [1,2,2,2], K= [5,1,0,1]** and perform Encryption and Decryption.
5. Explain various modes of operation of a Block Cipher.

UNIT – IV - CRYPTOGRAPHY

2 Marks:

1. What is data integrity?
2. Define Cryptographic Hash Functions.
3. List Message Authentication Requirements.
4. List Message Authentication Functions.
5. What is the MD5 Algorithm?
6. What is digital signature?
7. Define DSA algorithm.
8. List DSA algorithm Steps.

4 Marks:

1. Explain message authentication.
2. Explain Working of MD5 Algorithm.
3. Explain Advantages of MD5.
4. Explain Digital Signature Process.
5. Explain block diagram of digital signature.
6. Explain Importance of Digital Signature.

8 Marks:

1. Explain Message Authentication Requirements
2. Explain Message Authentication Functions.
3. Explain DSA Algorithm steps.
4. Solve the following with the DSA Algorithm.
   H (m) =3, p=7, h=2, k=2, q=3, x=2