Cryptography Lab Assignments - Real Detailed Explanations with Examples

1. Caesar Cipher

The Caesar cipher is a substitution cipher where each letter in the plaintext is shifted a fixed number of places along the alphabet. It is named after Julius Caesar, who used it in his private correspondence. For example, with a shift of 3, A becomes D, B becomes E, and so on. After Z, it wraps around back to A. Example: Plaintext = HELLO, Shift = 3, Ciphertext = KHOOR.

2. Playfair Cipher

The Playfair cipher encrypts pairs of letters (digraphs) using a 5x5 matrix filled with a keyword and the alphabet. If a pair is in the same row, each letter is replaced with the one to its right; if in the same column, with the one below; otherwise, use rectangle rules. Example: Keyword = MONARCHY, Plaintext = BALLOON, Ciphertext = IBSUPMOP.

3. Polyalphabetic Cipher

The Polyalphabetic cipher uses multiple Caesar ciphers based on letters of a keyword. Each letter of the plaintext is shifted according to the corresponding keyword letter, making it stronger against attacks. Example: Plaintext = ATTACK, Keyword = LEMON, Ciphertext = LXFOPV.

4. Rail Fence Cipher

The Rail Fence cipher writes the message in a zigzag pattern across multiple rails (lines) and reads the letters row by row to form the cipher text. It rearranges the characters without changing them. Example: Plaintext = MEETMEAFTERTHEPARTY, Rails = 3, Ciphertext = MTAEERMTPETEFHAY.

5. Hill Cipher

The Hill cipher encrypts groups of letters using a matrix multiplication approach where plaintext is turned into numbers. The result is taken modulo 26 to remain within the alphabet range. Example: Key matrix [[3,3],[2,5]], Plaintext HI becomes Ciphertext TC.

6. Simple Columnar Transposition

This cipher writes the message into rows and reads the columns according to a predefined columnar key order. It is a method of transposition and shuffles the characters without altering them. Example: Plaintext =

ATTACKATDAWN, Key = 4312567, Ciphertext rearranged accordingly.

7. RSA Algorithm (Encryption)

RSA is a public key cryptography technique where encryption is performed using a public exponent and modulus derived from two large prime numbers. It is based on the difficulty of factoring large numbers. Example: Primes p=3, q=11, n=33, e=7, message=5; encrypted as 14.

8. RSA Algorithm (Decryption)

RSA decryption is done using the private key. It involves raising the cipher text to the power of the private exponent modulo the public modulus. Only the intended receiver knows the private key. Example: Encrypted 14, decrypted with d=3 back to 5.

9. Diffie-Hellman Key Exchange

Diffie-Hellman enables two parties to establish a shared secret over an insecure channel by exchanging computed values, not the secret itself. They both calculate the same secret key independently. Example: Public prime 23, base 5, private secrets 6 and 15 result in shared secret 2.

10. Chinese Remainder Theorem

The Chinese Remainder Theorem helps to find a unique solution to a system of modular equations when the moduli are pairwise coprime. It combines the separate modular constraints into one final solution. Example: x leaves remainder 2 when divided by 3, 3 when divided by 5, and 2 when divided by 7; solution is x=23.

11. ElGamal Cryptographic Algorithm

ElGamal encryption uses asymmetric keys based on the discrete logarithm problem. Each encryption operation uses a random value, making the cipher text different even for the same plaintext. Example: p=467, g=2, private key=127, message=88, results in a cipher pair (96,203).

12. Hashing with Collision Resolution

Hashing involves mapping data into a table based on a hash function. When collisions happen (two data items map to same location), methods like chaining (linked lists) or linear probing (find next empty slot) are

used. Example: Inserting numbers into a table of size 7 using these techniques handles overlaps properly.