Practical 1 and 2:

- Caesar Cipher is a Substitution encryption technique.
- In Caesar Cipher every letter of the plain text is shift by a fixed value. And non alphabetic character remains unchanged.
- During decryption, each letter in the ciphertext is shifted backward by the same key value used during encryption to recover the original plaintext.
- Give one example:

Practical 3:

- Rail Fence Cipher is a transposition cipher.
- the plaintext is written in a zigzag pattern across a certain number of "rails" (or rows) based on the key value, and then read row by row to form the ciphertext. For eg: key= 4 then for the plain text is written in zigzag pattern across a 4 "rails"
- During decryption, the cipher text is rearranged according to the same zigzag pattern to reconstruct the original message.

Practical 4:

- One-Time Pad (OTP) Cipher is a symmetric encryption technique
- A **random key** is generated, having the **same length as the plaintext**.
  Each character of the plaintext is then **XORed (⊕)** with the corresponding value in the key to produce the ciphertext
- **For decryption**, the same key is applied again using XOR, which reverses the encryption process and perfectly restores the original plaintext.

Practical 5:

Columnar Transposition Cipher is a transposition encryption technique.

In this the plaintext letters are written in rows under the columns determined by the key, and then columns are rearranged based on the alphabetical order of the key to form ciphertext.

During decryption, the process is reversed using the same key to retrieve the original plaintext.

For multiple the transposition process is done more than one time but here ct is plaintext for second time transposition

Practical 6:

- **DES (Data Encryption Standard)** is a **symmetric key block cipher**.
- It encrypts data in **blocks of 64 bits (8 bytes)** using an **8-character key**.
- **Padding** is added to plaintext if its length is not a multiple of 8.
- **Encryption:** The plaintext is converted into bytes and encrypted using the DES algorithm in **ECB mode**.
- **Decryption:** The ciphertext is decrypted using the same key to retrieve the original plaintext.

Practical 7:

- Monoalphabetic Cipher is a **substitution encryption technique**.
- Each letter in the plaintext is **replaced by a corresponding letter** from a fixed substitution key of 26 letters.
- Non-alphabetic characters (spaces, punctuation) **remain unchanged**.
- **Decryption** uses the inverse of the substitution key to retrieve the original plaintext.

Practical 9:

- **RSA** is an **asymmetric key encryption technique**, meaning it uses **two different keys**: a **public key** for encryption and a **private key** for decryption.
- It relies on the mathematical difficulty of **factoring large prime numbers**.
- **Steps:**

1. Select two prime numbers p and q and calculate n = p * q.
2. Compute Euler's totient: phi = (p-1)*(q-1).
3. Choose a public exponent e such that 1 < e < phi and gcd(e, phi) = 1.
4. Compute the private key d such that (d * e) % phi = 1.
5. Encrypt plaintext m using C = m^e mod n.
6. Decrypt ciphertext C using m = C^d mod n.

Practical 11:

- **Blowfish** is a **symmetric key block cipher** used for secure encryption of data.
- It encrypts data in **blocks of 64 bits (8 bytes)** using a variable-length key (up to 16 characters in this example).
- **Padding** is applied to plaintext so that its length is a multiple of 8 bytes.
- **Encryption:** The plaintext is encrypted using **Blowfish in ECB mode**, and the ciphertext is often **encoded in Base64** for readability.
- **Decryption:** The ciphertext is decoded from Base64, decrypted using the same key, and unpadded to retrieve the original plaintext.