# Lab Manual

**Name : Yumna Mubeen**
**Seat No : B21110006165**
**Field: BSCS – A (4th Year)**

**Course: Network Security &Cryptogarphy**

**Course Code: 631**

**Teacher : Sir Bari Ahmed**

# Lab 1 : Caesar Cipher Algorithm Explanation :

### Introduction

The Caesar Cipher is one of the oldest and simplest encryption techniques used for encoding messages. It is a type of substitution cipher in which each letter in the plaintext is shifted a certain number of places down or up the alphabet.

### How It Works

1. Choose a shift value (also called the key). In our implementation, the shift value is set to 3.
2. Replace each letter in the plaintext with the letter that appears 'shift' positions later in the alphabet.
3. If the shift moves past 'Z' (for uppercase letters) or 'z' (for lowercase letters), it wraps around to the beginning of the alphabet.
4. Non-alphabetic characters remain unchanged.

### Example

#### Encoding the Cipher

- Plaintext: "HELLO"
- Shift: 3
- Ciphertext: "KHOOR"

**Decoding the Cipher** To decode an encoded message, the process is reversed by shifting each letter backward by the same shift value.

- Ciphertext: "KHOOR"
- Shift: -3
- Decoded text: "HELLO"

**Implementation in React** The following React component implements the Caesar Cipher with a fixed shift value of 3:

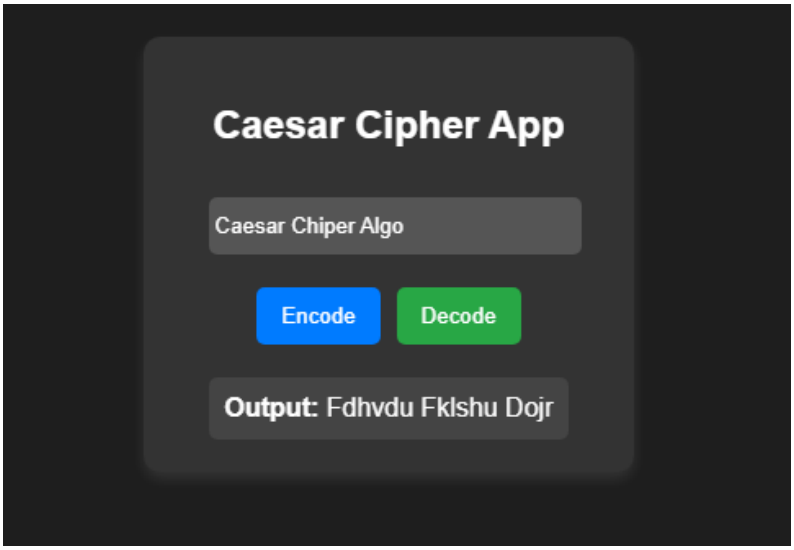
## Code:

```
import { useState } from "react";
import "./CaesarCipher.css";

const CaesarCipher = () => {
  const [text, setText] = useState("");
  const [output, setOutput] = useState("");

  const caesarCipher = (str, shift, encode = true) => {
```

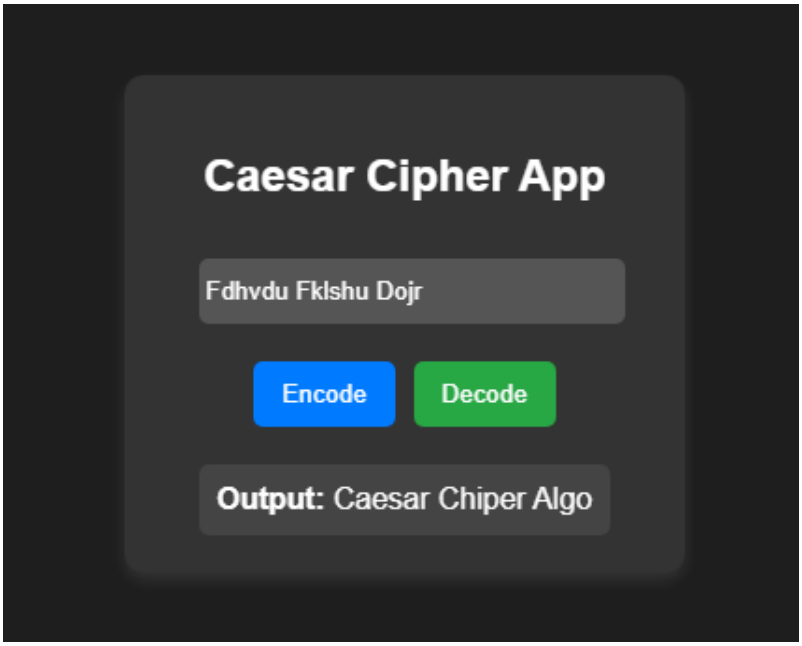
```
    return str
      .split("")
      .map((char) => {
        if (char.match(/[a-zA-Z]/)) {
          const base = char === char.toUpperCase() ? 65 : 97;
          return String.fromCharCode(
            ((char.charCodeAt(0) - base + (encode ? shift : -shift) + 26) % 26) +
base
          );
        }
        return char;
      })
      .join("");
  };

  return (
    <div className="container">
      <div className="card">
        <h2>Caesar Cipher App</h2>
        <input
          className="input"
          placeholder="Enter text"
          value={text}
          onChange={(e) => setText(e.target.value)}
        />
        <div className="button-group">
          <button className="button encode" onClick={() =>
setOutput(caesarCipher(text, 3, true))}>
            Encode
          </button>
          <button className="button decode" onClick={() =>
setOutput(caesarCipher(text, 3, false))}>
            Decode
          </button>
        </div>
        {output && (
          <div className="output">
            <strong>Output:</strong> {output}
          </div>
        )}
      </div>
    </div>
  );
};
export default CaesarCipher;
```

## Output:

### Encode:




### Decode:




## Conclusion

The Caesar Cipher is a simple yet classic encryption technique that helps understand the basics of cryptography. While it is not secure for modern applications, it is useful for educational purposes and basic text obfuscation.