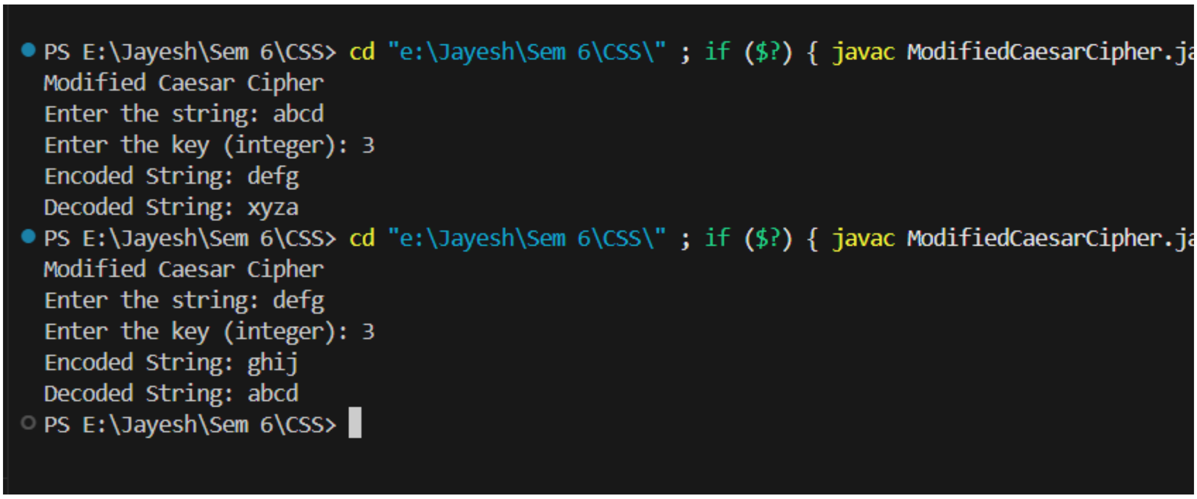
CSSL:
EXPERIMENT 1:

```
import java.util.Scanner;

public class ModifiedCaesarCipher {

    public static String encode(String input, int key) {
        StringBuilder encoded = new StringBuilder();

        for (char c : input.toCharArray()) {
            if (Character.isLetter(c)) {
                char base = Character.isLowerCase(c) ? 'a' : 'A';
                encoded.append((char) ((c - base + key) % 26 + base));
            } else {
                encoded.append(c);
            }
        }

        return encoded.toString();
    }

    public static String decode(String input, int key) {
        StringBuilder decoded = new StringBuilder();

        for (char c : input.toCharArray()) {
            if (Character.isLetter(c)) {
                char base = Character.isLowerCase(c) ? 'a' : 'A';
                decoded.append((char) ((c - base - key + 26) % 26 + base));
            } else {
                decoded.append(c);
            }
        }

        return decoded.toString();
    }

    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);

        System.out.println("Modified Caesar Cipher");
        System.out.print("Enter the string: ");
        String input = scanner.nextLine();

        System.out.print("Enter the key (integer): ");
        int key = scanner.nextInt();

        String encoded = encode(input, key);
        System.out.println("Encoded String: " + encoded);
```

CSSL:
EXPERIMENT 1:

```
        String decoded = decode(input, key);
        System.out.println("Decoded String: " + decoded);

        scanner.close();
    }
}
```

OUTPUT :



```
PS E:\Jayesh\Sem 6\CSS> cd "e:\Jayesh\Sem 6\CSS\" ; if ($?) { javac ModifiedCaesarCipher.ja
Modified Caesar Cipher
Enter the string: abcd
Enter the key (integer): 3
Encoded String: defg
Decoded String: xyza
PS E:\Jayesh\Sem 6\CSS> cd "e:\Jayesh\Sem 6\CSS\" ; if ($?) { javac ModifiedCaesarCipher.ja
Modified Caesar Cipher
Enter the string: defg
Enter the key (integer): 3
Encoded String: ghij
Decoded String: abcd
PS E:\Jayesh\Sem 6\CSS>
```

CSSL:
EXPERIMENT 1:

Theory on Cryptography and Caesar Cipher

What is Cryptography?

Cryptography is the practice and study of techniques for securing communication and data from unauthorized access or alterations. It ensures confidentiality, integrity, and authentication of information. Cryptography is a cornerstone of modern digital security and plays a critical role in protecting sensitive information from cyber threats. It is widely used in various fields, including banking, e-commerce, healthcare, and secure communications.

In today's interconnected world, cryptography is essential for safeguarding digital interactions. From securing online banking transactions to protecting personal data on social media platforms, cryptography underpins the trustworthiness of digital communication. It provides a mechanism to prevent unauthorized access to information, ensuring that private data remains secure even when transmitted over potentially insecure channels like the internet.

Why is Cryptography Used?

Cryptography serves several essential purposes:

1. Confidentiality: Ensures that only authorized individuals can access the information, keeping sensitive data private.
2. Integrity: Verifies that the data has not been altered during transmission or storage.
3. Authentication: Confirms the identity of the sender or receiver, ensuring secure interactions.
4. Non-repudiation: Prevents denial of sending or receiving the data, providing accountability.

By leveraging cryptographic techniques, organizations and individuals can safeguard their communications, maintain trust, and reduce the risk of data breaches. It is an essential tool for ensuring security in a world where data breaches and cyber-attacks are becoming increasingly sophisticated and frequent.

What is a Cipher?

A cipher is a method of transforming readable data, called plaintext, into an unreadable format, called ciphertext, using a specific algorithm and key. The reverse process, known as decryption, converts ciphertext back into plaintext using the same or a related key. Ciphers can be classified into two main types:

- Substitution Ciphers: Replace each element of the plaintext with another element.
- Transposition Ciphers: Rearrange the elements of the plaintext according to a defined system.

Ciphers have been used throughout history to protect sensitive communications. In modern times, they have evolved into highly complex systems that form the backbone of digital security.

CSSL:
EXPERIMENT 1:

What is Caesar Cipher?

The Caesar Cipher, also known as a shift cipher, is one of the simplest and most widely known encryption techniques. Named after Julius Caesar, who reportedly used it in his private correspondence, this cipher is a type of substitution cipher. It works by shifting each letter in the plaintext by a fixed number of positions down the alphabet.

How Does the Caesar Cipher Work

- Encryption: Each letter of the plaintext is shifted by a fixed number (key) down the alphabet. For example, with a key of 3:
- A becomes D, B becomes E, C becomes F, and so on. After Z, the alphabet wraps around to A again.
- Non-alphabetic characters such as numbers, spaces, and punctuation remain unchanged.
- Decryption: The ciphertext is shifted back by the same fixed number (key) to retrieve the original plaintext.

Working of the Program

1. Input: The user provides a string to encode or decode and a numeric key.
2. Encoding: The program shifts each character of the plaintext by the key value to produce the encoded string.
3. Decoding: The program reverses the shift using the same key to retrieve the original text.
4. Handling Special Characters: Non-alphabetic characters remain unchanged to preserve the original structure of the message.

Advantages of Caesar Cipher

1. Simplicity: Easy to understand and implement, making it ideal for educational purposes.
2. Speed: Requires minimal computational resources, allowing for quick encryption and decryption.
3. Basic Security: Offers a simple method for obscuring data, sufficient for non-critical applications.

Disadvantages of Caesar Cipher

1. Weak Security: Vulnerable to brute force attacks as there are only 25 possible keys (for the English alphabet).
2. Letter Frequency Analysis: Susceptible to statistical attacks since the structure of the plaintext is preserved in the ciphertext.
3. Limited Applicability: Not suitable for modern encryption needs where advanced algorithms are required.

Examples

- Encryption Example:
  - Plaintext: HELLO
  - Key: 3
  - Ciphertext: KHOOR

- Decryption Example:
    - Ciphertext: KHOOR
    - Key: 3
    - Plaintext: HELLO
- Handling of Non-Alphabetic Characters:
    - Plaintext: Hello World 123
    - Key: 5
    - Ciphertext: Mjqqt Btwqi 123

Applications of Caesar Cipher

1. Educational Tools: Used to teach the fundamentals of cryptography and encryption.
2. Games and Puzzles: Encoding messages for fun or as part of challenges like treasure hunts and escape rooms.
3. Basic Message Security: Suitable for low-level security applications where advanced methods are unnecessary.
4. Historical Use: Used by Julius Caesar for secure military communications, highlighting its historical importance.

Conclusion

The Caesar Cipher is a fundamental encryption technique that exemplifies the principles of cryptography. While it lacks the robustness required for modern security, its simplicity makes it an excellent educational tool. It also finds niche applications in games, puzzles, and low-risk message encoding. Cryptography as a whole remains a critical tool in today’s digital society, protecting information and ensuring secure communication in a wide range of applications.