Name: Devanshu Surana
Roll No.: 23
Prn:1032210755
Panel: C batch:C1

Lab A1: Implement any classical cryptographic technique using java or python or C++

Objective of Lab

1. To study understand and implement at least two classical cryptographic algorithms

Theory

Theory :

1. Caesar Cipher: The Caesar cipher is one of the simplest and most well-known encryption techniques. It's a type of substitution cipher that shifts each letter in the plaintext by a fixed number of positions down or up the alphabet. This fixed number is called the "key" or "shift."

Here's how the Caesar cipher works:

- Choose a shift value (key), typically a number between 1 and 25.

- For each letter in the plaintext, replace it with the letter that is "key" positions down the alphabet.

- Wrap around the alphabet if necessary. For example, if the key is 3, and you're encoding 'X,' it would become 'A.'

Example:

Let's say we want to encrypt the message "HELLO" with a Caesar cipher using a key of 3.

- H -> E

- E -> B

- L -> I

- L -> I

- O -> L

So, "HELLO" would be encrypted as "EBIIL."

To decrypt, you simply reverse the process by shifting the letters back by the key positions.

2. Monoalphabetic Cipher: The monoalphabetic cipher is another type of substitution cipher, but instead of a fixed shift like the Caesar cipher, it involves a one-to-one mapping of each

letter in the plaintext to a corresponding letter in the ciphertext. In other words, each letter in the plaintext is replaced by a different letter in the ciphertext according to a predefined mapping.

Example:

Here's a simple example of a monoalphabetic cipher:

- Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

- Ciphertext alphabet: XYZABCDEFGHIJKLMNOPQRSTUVW

In this example, 'A' is mapped to 'X,' 'B' to 'Y,' 'C' to 'Z,' and so on.

Using this mapping, if we want to encrypt the word "HELLO," it would become "SVYYI."

To decrypt the message, you'd simply reverse the mapping.

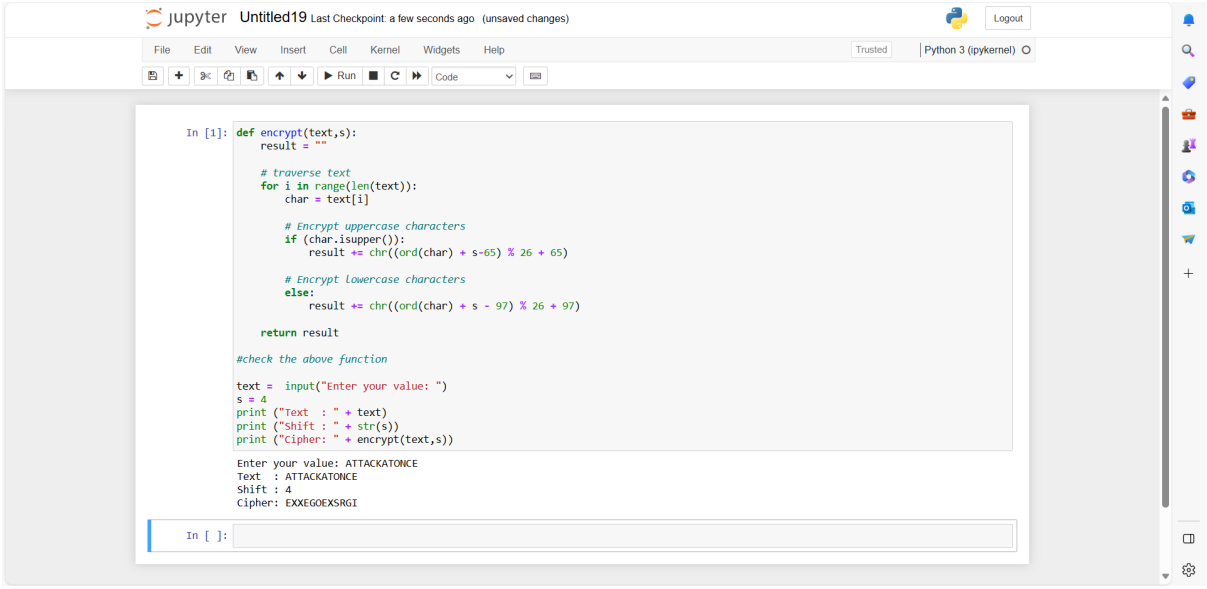
The monoalphabetic cipher is not very secure, as it is vulnerable to frequency analysis. Because each letter is replaced by a fixed letter, patterns in the plaintext can often be discerned in the ciphertext. Modern encryption methods use more complex algorithms and techniques to provide a higher level of security.

Code (ceasar cipher)

```
def encrypt(text,s):
    result = ""

    # traverse text
    for i in range(len(text)):
        char = text[i]

        # Encrypt uppercase characters
        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)

        # Encrypt lowercase characters
```

```
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)

    return result
text =  input("Enter your value: ")
s = 4
print ("Text  : " + text)
print ("Shift : " + str(s))
print ("Cipher: " + encrypt(text,s))
```

Output Screen shots (Ceasar Cipher)



Code (Mono alphabetic cipher)

```
import java.io.*;
class GFG {
        public static char normalChar[]
                = { 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i',
                        'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r',
                        's', 't', 'u', 'v', 'w', 'x', 'y', 'z' };

        public static char codedChar[]
                = { 'Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I', 'O',
                        'P', 'A', 'S', 'D', 'F', 'G', 'H', 'J', 'K',
                        'L', 'Z', 'X', 'C', 'V', 'B', 'N', 'M' };
```

```
public static String stringEncryption(String s)
{

	String encryptedString = "";

	for (int i = 0; i < s.length(); i++) {
		for (int j = 0; j < 26; j++) {

			if (s.charAt(i) == normalChar[j])
			{
				encryptedString += codedChar[j];
				break;
			}

			if (s.charAt(i) < 'a' || s.charAt(i) > 'z')
			{
				encryptedString += s.charAt(i);
				break;
			}
		}
	}

	return encryptedString;
}

public static String stringDecryption(String s)
{
	String decryptedString = "";

	for (int i = 0; i < s.length(); i++)
	{
		for (int j = 0; j < 26; j++) {

			if (s.charAt(i) == codedChar[j])
			{
				decryptedString += normalChar[j];
				break;
			}

			if (s.charAt(i) < 'A' || s.charAt(i) > 'Z')
			{
				decryptedString += s.charAt(i);
```

```
                                    break;
                                }
                            }
                        }

                        return decryptedString;
                }
                public static void main(String args[])
                {
                        String str = "asssignmentone";

                        System.out.println("Plain text: " + str);

                        String encryptedString = stringEncryption(str.toLowerCase());

                        System.out.println("Encrypted message: "
                                                + encryptedString);


                        System.out.println("Decrypted message: "
                                + stringDecryption(encryptedString));

                }
}
```

Output Screen chots (Monoalphabetic cipher)

Conclusion:

Thus, we have successfully learned and implemented Ceasar cipher and Mono alphabetic cipher.

FAQs:

1. What are various classical ciphers?
2. Compare steganography and Cryptography.

3. State the reasons why classical ciphers are obsolete.
4. How to carry our cryptanalysis of classical cryptography?
5. Write how different disciplines of art, science and engineering have contributed forinformation security.