

Name of Student: Pushkar Sane		
Roll Number: 45	Lab Assignment Number: 1	
Title of Lab Assignment: Implement Caesar Cipher (Symmetric Encryption) and show the encryption as well as decryption process.		
DOP: 06-08-2024	DOS: 13-08-2024	
CO Mapped:	PO Mapped:	Signature:

Practical No. 1

Aim: Implement Caesar Cipher (Symmetric Encryption) and show the encryption as well as decryption process.

Theory:**What is Cryptography?**

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and the suffix “graphy” means “writing”. In Cryptography, the techniques that are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Features Of Cryptography:

1. Confidentiality: Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. Integrity: Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. Non-repudiation: The creator/sender of information cannot deny his intention to send information at a later stage.
4. Authentication: The identities of the sender and receiver are confirmed. As well, the destination / origin of the information is confirmed.
5. Interoperability: Cryptography allows for secure communication between different systems and platforms.
6. Adaptability: Cryptography continuously evolves to stay ahead of security threats and technological advancements.

Types Of Cryptography:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

What is Symmetric Encryption?

It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely. The most popular symmetric key cryptography systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES).

Explanation about caesar cipher

The Caesar Cipher is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications. This technique involves shifting the letters of the alphabet by a fixed number of places. For example, with a shift of three, the letter 'A' becomes 'D', 'B' becomes 'E', and so on. Despite its simplicity, the Caesar Cipher formed the groundwork for modern cryptographic techniques. In this article, we'll explore how the Caesar Cipher works, its significance, and its impact on the development of cryptography with its advantages and disadvantages

Advantages:

1. Easy to implement and use thus, making it suitable for beginners to learn about encryption.
2. Can be physically implemented, such as with a set of rotating disks or a set of cards, known as a scytale, which can be useful in certain situations.
3. Requires only a small set of pre-shared information.
4. Can be modified easily to create a more secure variant, such as by using multiple shift values or keywords.

Disadvantages:

1. It is not secure against modern decryption methods.
2. Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
3. The small number of possible keys means that an attacker can easily try all possible keys until the correct one is found, making it vulnerable to a brute force attack.
4. It is not suitable for long text encryption as it would be easy to crack.
5. It is not suitable for secure communication as it is easily broken.
6. Does not provide confidentiality, integrity, and authenticity in a message.

Rules for the Caesar Cipher:

1. Choose a number between 1 and 25. This will be your "shift" value.
2. Write down the letters of the alphabet in order, from A to Z.
3. Shift each letter of the alphabet by the "shift" value. For example, if the shift value is 3, A would become D, B would become E, C would become F, and so on.
4. Encrypt your message by replacing each letter with the corresponding shifted letter. For example, if the shift value is 3, the word "hello" would become "khood".
5. To decrypt the message, simply reverse the process by shifting each letter back by the same amount. For example, if the shift value is 3, the encrypted message "khood" would become "hello".

Code:

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

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

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

        # Encrypt lowercase characters
        elif char.islower():
            result += chr((ord(char) + key - 97) % 26 + 97)
        else:
            result += char

    return result

def decrypt(text, key):
    result = ""

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

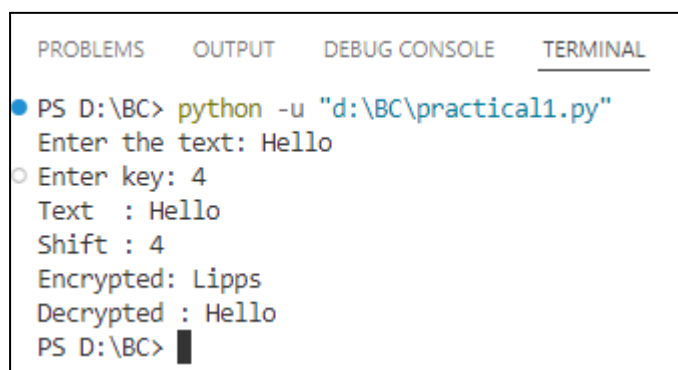
```
# Encrypt uppercase characters
if (char.isupper()):
    result += chr((ord(char) - key - 65) % 26 + 65)

# Encrypt lowercase characters
elif char.islower():
    result += chr((ord(char) - key - 97) % 26 + 97)
else:
    result += char
return result

#check the above function
text = input("Enter the text: ")
key = int(input("Enter key: "))
print ("Text : " + text)
print ("Shift : " + str(key))

encrypted_text = encrypt(text, key)
print ("Cipher: " + encrypted_text)

decrypted_text = decrypt(encrypted_text, key)
print ("Original Text : " + decrypted_text)
```

Output:

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL
● PS D:\BC> python -u "d:\BC\practical1.py"
Enter the text: Hello
○ Enter key: 4
Text : Hello
Shift : 4
Encrypted: Lipps
Decrypted : Hello
PS D:\BC> █
```

Conclusion:

Implemented Caesar Cipher (Symmetric Encryption) and show the encryption as well as decryption process successfully