



Prodigy InfoTech Cyber Security Report

Week 1: Implementation of a Caesar Cipher

Full Name: Sairaj Turalkar

Date: 01/06/2024

1. Introduction

In the first week of my cybersecurity internship at Prodigy Infotech, I was tasked with implementing a Caesar Cipher. The Caesar Cipher is a simple and well-known encryption technique where each letter in the plaintext is shifted a certain number of places down or up the alphabet. It is one of the earliest known and simplest ciphers, historically used by Julius Caesar.

2. Objective

The objective of this task was to develop a Python program that can encrypt and decrypt text using the Caesar Cipher algorithm. The program should allow the user to input a message and a shift value to perform encryption and decryption operations.

3. Methodology

3.1. Python Program

The implementation consists of three main functions: encrypt, decrypt, and main.

Encrypt Function

The encrypt function takes two parameters: text and shift. It processes each character of the input text, shifting it by the specified number of positions according to the Caesar Cipher algorithm. It handles both uppercase and lowercase letters and leaves non-alphabetic characters unchanged.

python

Copy code

```
def encrypt(text, shift):
```

```
    result = ""
```

```
    for i in range(len(text)):
```

```

char = text[i]

if char.isupper():
    result += chr((ord(char) + shift - 65) % 26 + 65)

elif char.islower():
    result += chr((ord(char) + shift - 97) % 26 + 97)

else:
    result += char

return result

```

Decrypt Function

The decrypt function simply calls the encrypt function with a negative shift value, effectively reversing the encryption process.

python

Copy code

```

def decrypt(text, shift):
    return encrypt(text, -shift)

```

Main Function

The main function serves as the user interface, prompting the user to choose between encryption and decryption, enter the message, and specify the shift value. It then calls the appropriate function and displays the result. The process repeats until the user decides to exit.

python

Copy code

```

def main():
    while True:
        choice = input("Do you want to (e)ncrypt or (d)ecrypt? ")
        message = input("Enter your message: ")
        shift = int(input("Enter the shift value: "))

        if choice.lower() == 'e':
            encrypted_message = encrypt(message, shift)

```

```

        print("Encrypted message:", encrypted_message)
    elif choice.lower() == 'd':
        decrypted_message = decrypt(message, shift)
        print("Decrypted message:", decrypted_message)
    else:
        print("Invalid choice. Please choose 'e' for encryption or 'd' for decryption.")

    repeat = input("Do you want to perform another operation? (if yes press 'y' / if no press 'n'): ")
    if repeat.lower() != 'y':
        print("Goodbye!")
        break

if __name__ == "__main__":
    main()

```

4. Testing and Results

To ensure the correctness of the implementation, the program was tested with various inputs. Below are some test cases and their results:

- **Test Case 1:**
 - Input: "Hello Sir", Shift: 2
 - Encrypted: "Jgnnq Ukt"
 - Decrypted: " Hello Sir "

```

>>> ===== RESTART: D:\Prodify Info\Task 01.py =====
Do you want to (e)ncrypt or (d)ecrypt? e
Enter your message: Hello Sir
Enter the shift value: 2
Encrypted message: Jgnnq Ukt
Do you want to perform another operation? (if yes press 'y' / if no press 'n'): y
Do you want to (e)ncrypt or (d)ecrypt? d
Enter your message: Jgnnq Ukt
Enter the shift value: 2
Decrypted message: Hello Sir
Do you want to perform another operation? (if yes press 'y' / if no press 'n'): |

```

- **Test Case 2:**
 - Input: "hello", Shift: 3
 - Encrypted: "Khoor"

- Decrypted: "hello"

```
>>> ===== RESTART: D:\Prodify Info\Task 01.py =====
Do you want to (e)ncrypt or (d)ecrypt? e
Enter your message: Hello
Enter the shift value: 3
Encrypted message: Khoor
Do you want to perform another operation? (if yes press 'y' / if no press 'n'): y
Do you want to (e)ncrypt or (d)ecrypt? d
Enter your message: Khoor
Enter the shift value: 3
Decrypted message: Hello
Do you want to perform another operation? (if yes press 'y' / if no press 'n'): |
```

- **Test Case 3:**

- Input: " Prodigy InfoTech ", Shift: 4
- Encrypted: " Tvshmkc MrjsXigl"
- Decrypted: " Prodigy InfoTech "

```
===== RESTART: D:\Prodify Info\Task 01.py =====
Do you want to (e)ncrypt or (d)ecrypt? e
Enter your message: Prodigy InfoTech
Enter the shift value: 4
Encrypted message: Tvshmkc MrjsXigl
Do you want to perform another operation? (if yes press 'y' / if no press 'n'): y
Do you want to (e)ncrypt or (d)ecrypt? d
Enter your message: Tvshmkc MrjsXigl
Enter the shift value: 4
Decrypted message: Prodigy InfoTech
Do you want to perform another operation? (if yes press 'y' / if no press 'n'):
```

5. Conclusion

This task provided a practical understanding of how simple encryption techniques like the Caesar Cipher work. Implementing the algorithm in Python reinforced my programming skills and introduced me to the basics of cryptography. The knowledge gained from this exercise will be foundational for more advanced studies in cybersecurity.

6. References

- Caesar Cipher: [Wikipedia](https://en.wikipedia.org/wiki/Caesar_cipher)