SRI JAYACHAMARAJENDRA COLLEGE OF ENGINEERING
A Constituent College of
JSS SCIENCE & TECHNOLOGY UNIVERSITY

Additive Cipher & Multiplicative Cipher

Mini project report submitted in partial fulfillment of curriculum prescribed for the : Cryptography and Network Security (20CS552) course for the award of the degree of

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE AND ENGINEERING

PROJECT REPORT

Submitted by

S.No.	NAME	ROLLNO.	USN
1	Adithya Deepthi Kumar	28	01JST21CS005
2	E Shreyas Herale	35	01JST21CS037
3	Eshwar J	8	01JCE21CS033
4	Harsha N P	10	01JCE21CS038

D-SECTION

Under the Guidance of
Shwethashree G C
Assistant Professor
Dept.of CS & E,
SJCE, JSSSTU, Mysuru

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
November 2023

SRI JAYACHAMARAJENDRA COLLEGE OF ENGINEERING
A Constituent College of
JSS SCIENCE & TECHNOLOGY UNIVERSITY

CERTIFICATE

This is to certify that the work entitled“ **Additive Cipher & Multiplicative Cipher ”** is a bonafied work carried out by **Adithya Deepthi Kumar, E Shreyas Herale, Eshwar J, Harsha N P** in partial fulfillment of the award of the degree of **Bachelor of Engineering in Computer Science and Engineering of JSS Science and Technology University, Mysuru during the year 2023**. It is certified that all corrections / suggestions indicated during CIE have been incorporated in the report. The mini project report has been approved as it satisfies the academic requirements in respect of mini project work for event 1 prescribed for the Cryptography and Network Security (20CS552) course.

Course in Charge and Guide

Shwethashree G C
Assistant Professor
Dept.of CS & E,
SJCE, JSSSTU, Mysuru

Place: Mysuru **Date : 07/11/2023**

ABSTRACT

In this report, we have delved into the principles and applications of two classical encryption techniques, the Additive Cipher and the Multiplicative Cipher. These ciphers, although rudimentary in their design, hold intrinsic educational value as they introduce foundational concepts in the world of cryptography. While the Additive Cipher serves as a simple and swift illustration of letter shifting, it comes with notable security vulnerabilities, making it unsuitable for modern cryptographic needs. On the other hand, the Multiplicative Cipher offers a larger key space and heightened resistance to certain attacks, yet it too falls short of providing robust data security in the contemporary digital landscape. These ciphers find their niche in educational contexts, historical references, recreational puzzles, and casual communication. However, their limitations underscore the necessity of adopting more advanced encryption methods for the protection of sensitive information in our digitally interconnected world.

TABLE OF CONTENTS

Introduction

Introduction to Cryptography: The Art of Securing Information

Cryptography, also known as cryptology, derives its name from the Greek words "kryptós," meaning hidden or secret, and "graphein," meaning to write. It encompasses the art and science of safeguarding communication against potential adversaries. Broadly speaking, cryptography involves creating and analyzing protocols that prevent unauthorized parties or the public from accessing private messages. This field is situated at the intersection of various disciplines, including mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and more. Key principles in information security, such as data confidentiality, data integrity, authentication, and non-repudiation, are integral to cryptography. This discipline finds practical application in electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Historically, cryptography was primarily concerned with encryption, the process of converting readable information (plaintext) into unintelligible text (ciphertext). Decryption reverses this process, rendering the message readable. The sender of an encrypted message shares the decryption method only with the intended recipients to prevent unauthorized access. With the development of rotor cipher machines during World War I and the advent of computers in World War II, cryptographic methods grew in complexity and found diverse applications.

Modern cryptography is deeply rooted in mathematical theory and computer science. Cryptographic algorithms are designed based on computational hardness assumptions, making them resistant to practical attacks by adversaries. While theoretically breakable, breaking into well-designed systems is infeasible in practice. Such systems are referred to as "computationally secure." However, as technology advances, designs need constant reevaluation and adaptation to stay secure. Information-theoretically secure systems, like the one-time pad, which cannot be broken even with unlimited computing power, are less practical than the best theoretically breakable but computationally secure schemes.

The rise of cryptographic technology has given rise to legal issues in the Information Age. Some governments have classified cryptography as a weapon due to its potential for espionage and sedition, leading to restrictions and even prohibitions on its use and export. In jurisdictions where cryptography is legal, laws may empower investigators to demand encryption keys for relevant documents during investigations.
Cryptography also plays a significant role in digital rights management and copyright infringement disputes in the realm of digital media.
As technology advances, ciphers continue to evolve. Cryptographers work to develop stronger and more resilient ciphers to counter emerging threats and challenges, ensuring data security in an increasingly interconnected world.

Cipher : The Art of Secrecy and Security

Cryptography, an ancient and evolving science, encompasses a wide array of techniques to secure information. At its core, cryptography revolves around the concept of ciphers, which are algorithms used for encrypting and decrypting data.

Ciphers have played a pivotal role throughout history, from ancient civilizations to the modern digital age, where they are instrumental in ensuring data confidentiality and integrity.

Cryptography employs algorithms known as ciphers for the purpose of encrypting or decrypting data. These ciphers are sets of well-defined steps that dictate how to perform these operations. A less common term for this process is "encipherment," which signifies the conversion of information into a cipher.

Ciphers follow algorithmic processes, requiring that the input conform to the cipher's rules to be deciphered. Ciphers are commonly utilized for encrypting written information.

When using a cipher, the original information is referred to as plaintext, while the encrypted version is known as ciphertext. The ciphertext contains all the information present in the plaintext message but is presented in a format that is unreadable without the appropriate decryption method, whether for humans or computers.

The operation of a cipher typically relies on an additional piece of information called a key (or, traditionally in NSA terminology, a cryptovariable). The key affects the encryption process, modifying the algorithm's detailed operation. Before employing a cipher to encrypt a message, one must select a key. Without knowledge of the key, decrypting the resulting ciphertext into readable plaintext should be extremely difficult, if not practically impossible.

Most modern ciphers can be categorized in several ways:

- By whether they operate on fixed-size blocks of symbols (block ciphers) or on a continuous stream of symbols (stream ciphers).

- By whether the same key is used for both encryption and decryption (symmetric key algorithms) or if a distinct key is used for each (asymmetric key algorithms). In the case of symmetric algorithms, the key must be known to both the sender and the recipient and kept secret from all others. In asymmetric algorithms, the enciphering key is different from, but intricately related to, the deciphering key. If one key cannot be deduced from the other, the asymmetric algorithm exhibits the public/private key property, allowing one of the keys to be made public without compromising confidentiality.

Historical Significance

Ciphers have a rich history dating back thousands of years. The term "cipher" is derived from the Arabic word "sifr," meaning zero, highlighting its connection to numerical codes. Historically, ciphers were primarily associated with secret communication, espionage, and military strategy.

1. Ancient Ciphers

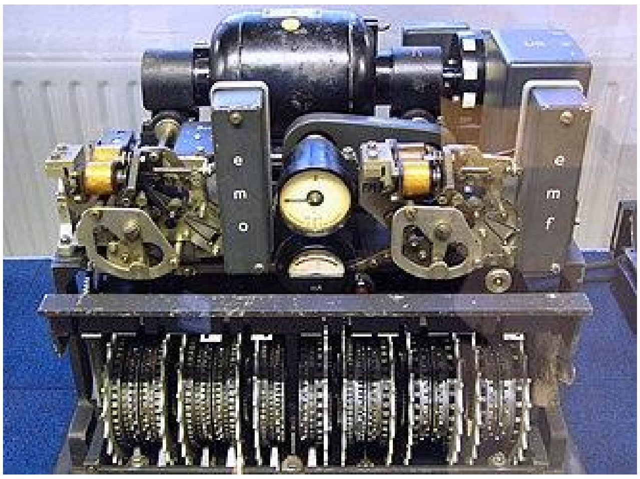
- The earliest ciphers were simple substitution ciphers used by the ancient Egyptians and Greeks to hide messages.
- Julius Caesar employed a famous cipher technique known as the Caesar cipher, shifting letters in the alphabet to encode messages.

2. Renaissance and Beyond

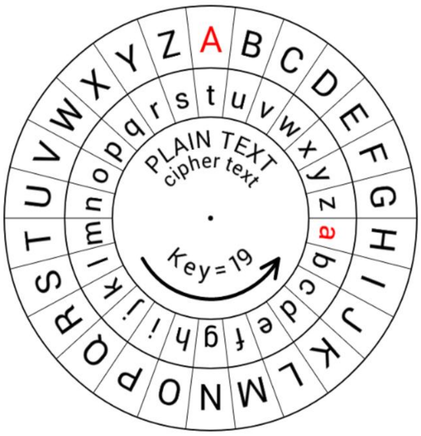
- The Renaissance saw the emergence of more complex ciphers like the Vigenère cipher, which used a keyword to determine the shifting pattern.
- The advent of the telegraph in the 19th century gave rise to the need for secure communication, leading to the development of more sophisticated ciphers.

3. World Wars and Cipher Machines

- World War I introduced rotor cipher machines like the Enigma, which played a pivotal role in military communication.
- World War II witnessed the advancement of computer-assisted decryption efforts, leading to the development of modern cryptography.



Lorenz cipher machine, used in World War II to encrypt communications of the German High Command.


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
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key = 19

Additive Cipher wheel with key 19.

Core Concepts

Ciphers are fundamental to the practice of cryptography, and they operate on well-defined principles:

1. Encryption and Decryption

- Encryption is the process of converting plaintext (unencrypted data) into ciphertext (encrypted data) using a cipher and a cryptographic key.

- Decryption is the reverse process of converting ciphertext back into plaintext, but only with the appropriate key.

2. Key

- A key is a crucial component in the operation of ciphers. It determines how the algorithm encrypts and decrypts data.

- Keys can be symmetric, where the same key is used for both encryption and decryption, or asymmetric, with separate keys for each process.

Types of Ciphers

Ciphers come in various forms, each with its unique characteristics and applications. The two primary categories are:

1. Symmetric Ciphers

- Symmetric ciphers use the same key for both encryption and decryption.

- Notable examples include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES).

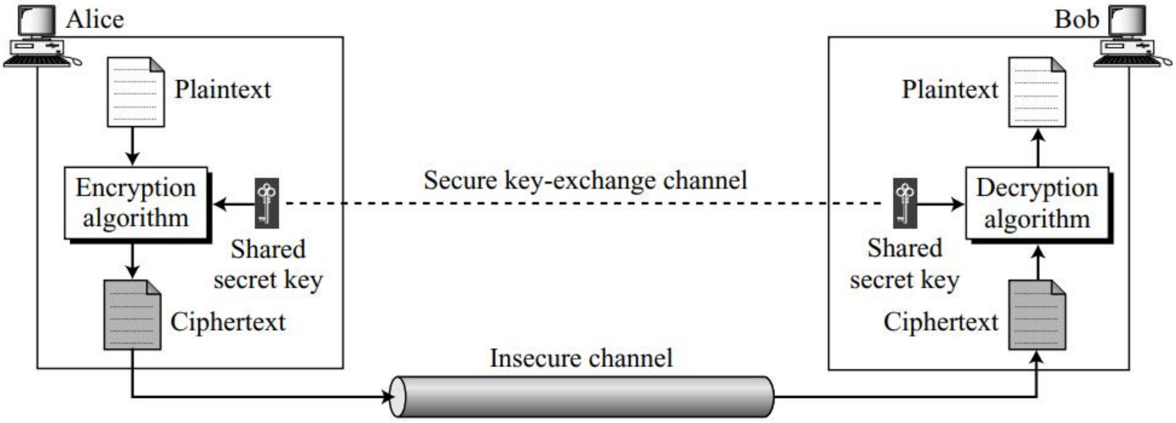
2. Asymmetric Ciphers

- Asymmetric ciphers use a pair of keys: a public key for encryption and a private key for decryption.
- Well-known asymmetric ciphers are RSA and Elliptic Curve Cryptography (ECC).

Symmetric-Key Cipher

Symmetric-key cipher, also known as symmetric-key encryption, are cryptographic techniques that employ the same cryptographic keys for both encrypting plaintext and decrypting ciphertext. These keys can either be identical or subject to a straightforward transformation, facilitating the transition between encryption and decryption operations.
In practice, these keys represent a shared secret held by two or more parties, allowing them to establish a private and secure channel for transmitting information.

General idea of symmetric-key cipher

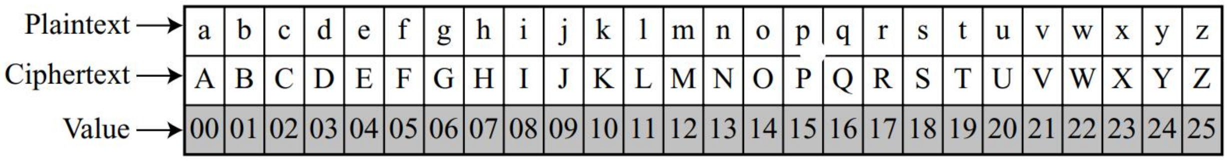


A **substitution cipher** replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.
In monoalphabetic substitution, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text. In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Additive Cipher

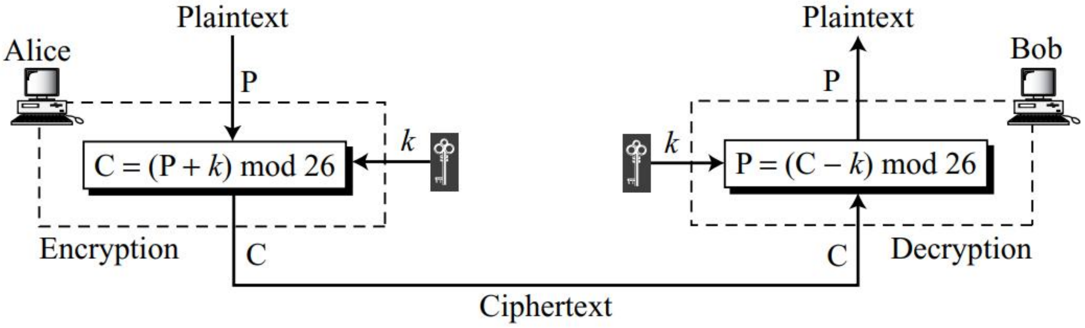
The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature. Assume that the plaintext consists of lowercase letters (a to z), and that the ciphertext consists of uppercase letters (A to Z). To be able to apply mathematical operations on the plaintext and ciphertext, we assign numerical values to each letter (lower- or uppercase), as shown in figure below.



Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The additive cipher is a type of substitution cipher, where each letter in the plaintext is shifted a fixed number of positions down or up the alphabet.
In the figure above each character (lowercase or uppercase) is assigned an integer in Z_{26}. The secret key between the sender and receiver is also an integer in Z_{26}.
The encryption algorithm adds the key to the plaintext character, the decryption algorithm subtracts the key from the ciphertext character. All operations are done in Z_{26}.

The flowchart of the implementation of additive cipher:



Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

Shift Cipher
Historically, additive ciphers are called shift ciphers. The reason is that the encryption algorithm can be interpreted as “shift key characters down” and the encryption algorithm can be interpreted as “shift key character up”.

Caesar Cipher

Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications.

Cryptanalysis

Additive ciphers are vulnerable to ciphertext-only attacks using exhaustive key searches (brute-force attacks). The key domain of the additive cipher is very small; there are only 26 keys. However, one of the keys, zero, is useless (the ciphertext is the same as the plaintext). This leaves only 25 possible keys.Attacker can easily launch a brute force attack on the ciphertext.

Additive Cipher Implementation

Encryption Process:

1. Key: The key for the additive cipher is an integer value representing the number of positions each letter is shifted in the alphabet. This key is typically a positive integer.

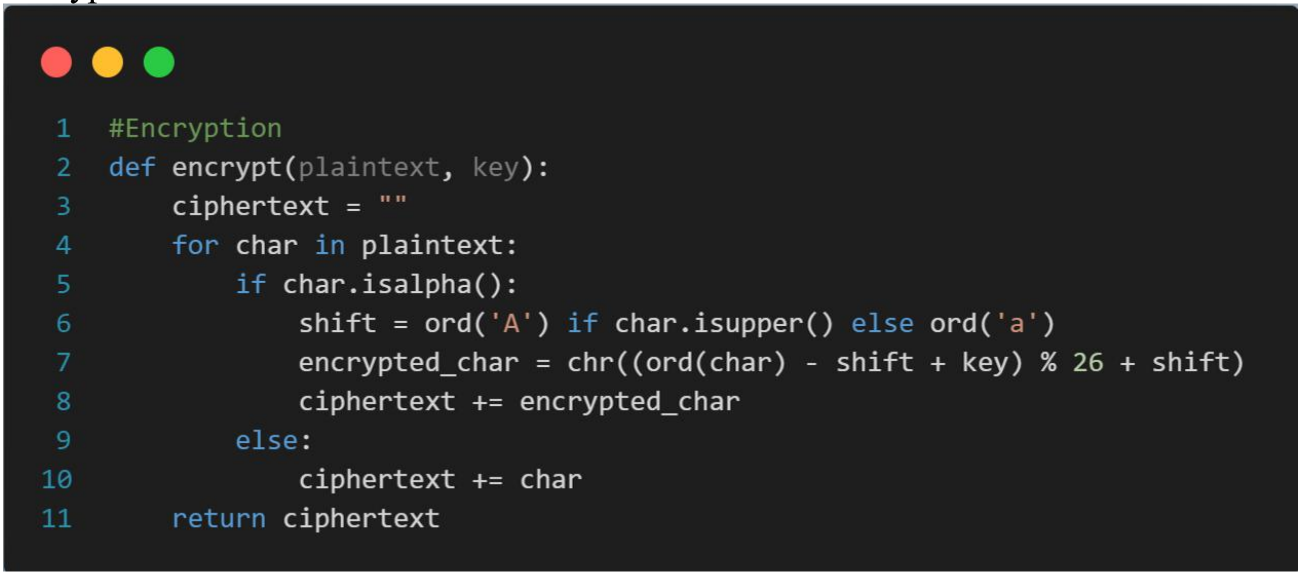
2. Alphabet: The additive cipher operates on the letters of the alphabet. It preserves the case of letters (usually lowercase).

3. Shift: Each letter in the plaintext is shifted by the key value (k).

4. Modulo Operation: To ensure that the shifted letter remains within the bounds of the alphabet, a modulo operation is applied. For example, in English, there are 26 letters, so (26 + k) % 26 equals number from 0 to 25, ensuring that the alphabets are from A to Z.

5. Spaces and Other Characters: Spaces and characters that are not part of the alphabet remain unchanged in the ciphertext.

Encryption Function

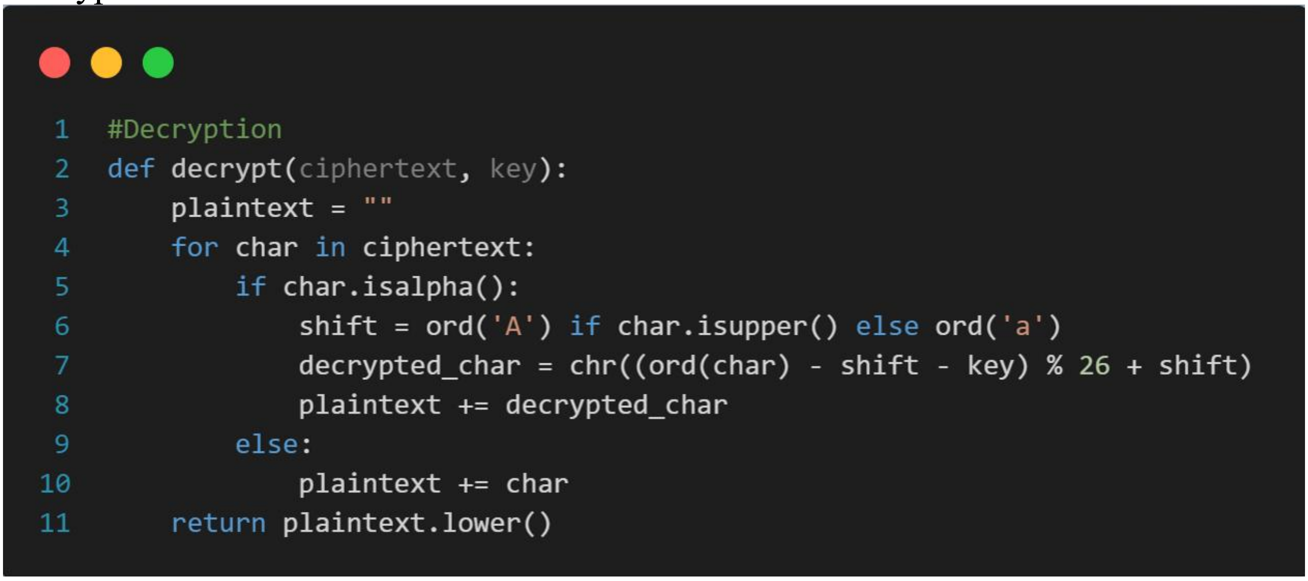


```python
#Encryption
def encrypt(plaintext, key):
    ciphertext = ""
    for char in plaintext:
        if char.isalpha():
            shift = ord('A') if char.isupper() else ord('a')
            encrypted_char = chr((ord(char) - shift + key) % 26 + shift)
            ciphertext += encrypted_char
        else:
            ciphertext += char
    return ciphertext
```

Decryption Process:

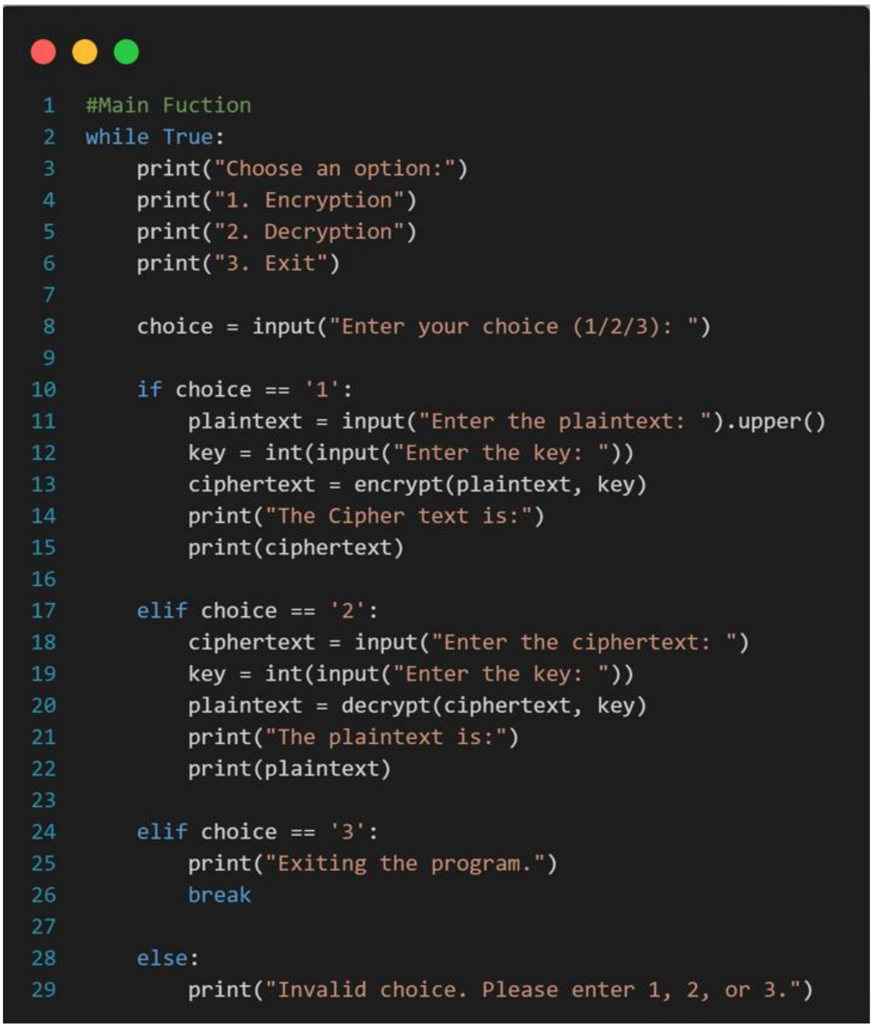
The decryption process is the reverse of encryption. To decrypt a message, one needs to know the key used for encryption and shift each letter in the ciphertext in the opposite direction.

Decryption Function



```
#Decryption
def decrypt(ciphertext, key):
    plaintext = ""
    for char in ciphertext:
        if char.isalpha():
            shift = ord('A') if char.isupper() else ord('a')
            decrypted_char = chr((ord(char) - shift - key) % 26 + shift)
            plaintext += decrypted_char
        else:
            plaintext += char
    return plaintext.lower()
```

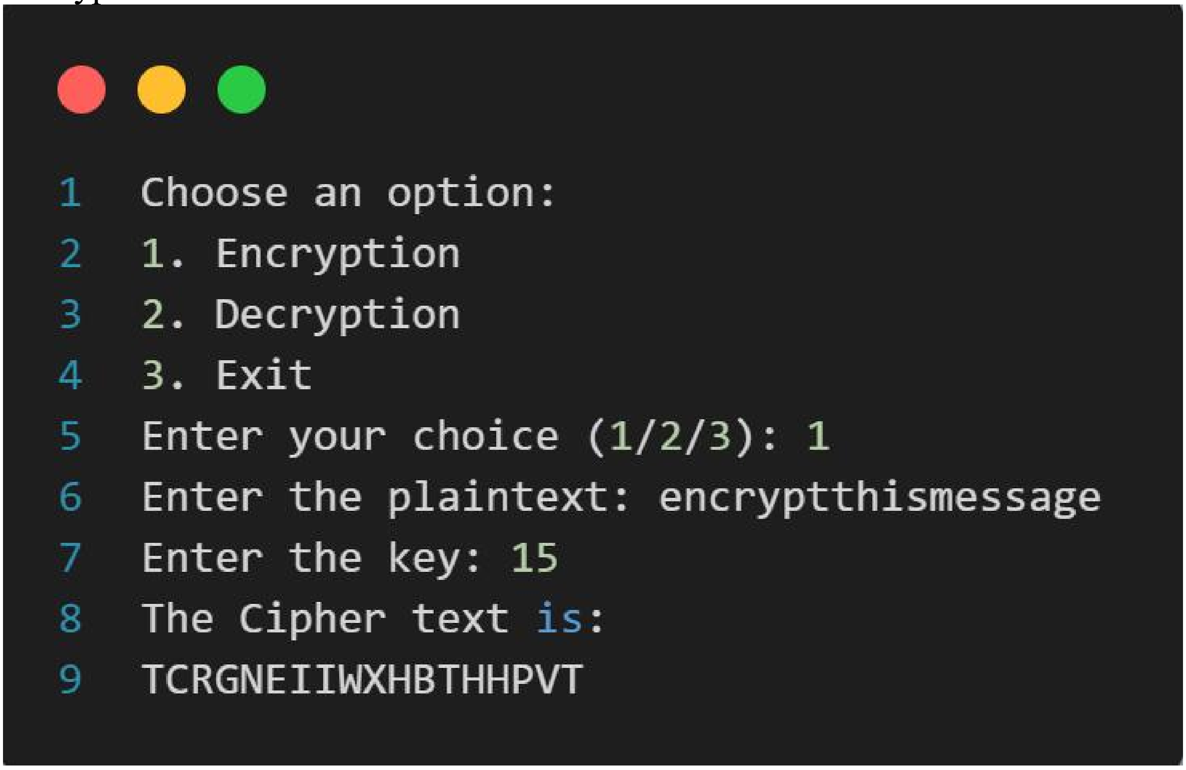
Main Function



```
#Main Fuction
while True:
    print("Choose an option:")
    print("1. Encryption")
    print("2. Decryption")
    print("3. Exit")

    choice = input("Enter your choice (1/2/3): ")

    if choice == '1':
        plaintext = input("Enter the plaintext: ").upper()
        key = int(input("Enter the key: "))
        ciphertext = encrypt(plaintext, key)
        print("The Cipher text is:")
        print(ciphertext)

    elif choice == '2':
        ciphertext = input("Enter the ciphertext: ")
        key = int(input("Enter the key: "))
        plaintext = decrypt(ciphertext, key)
        print("The plaintext is:")
        print(plaintext)

    elif choice == '3':
        print("Exiting the program.")
        break

    else:
        print("Invalid choice. Please enter 1, 2, or 3.")
```

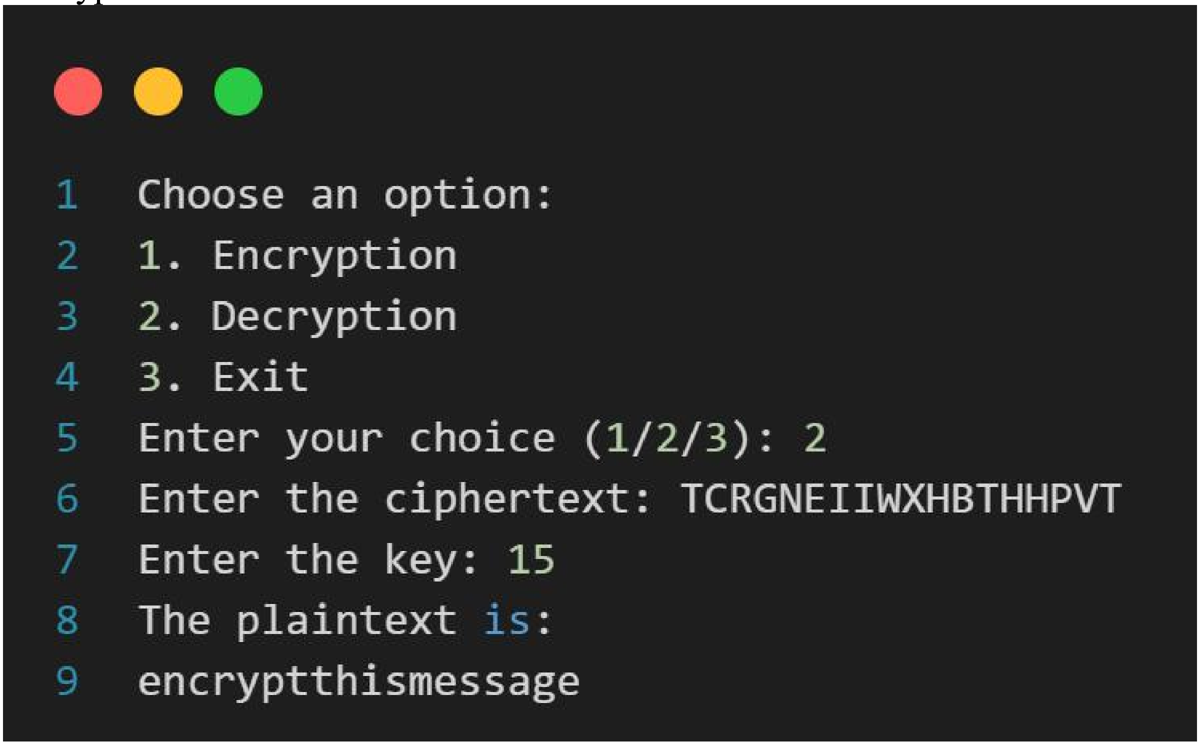
Snapshots of Implementation

Encryption:



```
Choose an option:
1. Encryption
2. Decryption
3. Exit
Enter your choice (1/2/3): 1
Enter the plaintext: encryptthismessage
Enter the key: 15
The Cipher text is:
TCRGNEIIWXHBTHHPVT
```

Decryption:



```
Choose an option:
1. Encryption
2. Decryption
3. Exit
Enter your choice (1/2/3): 2
Enter the ciphertext: TCRGNEIIWXHBTHHPVT
Enter the key: 15
The plaintext is:
encryptthismessage
```

Advantages and Disadvantages of Additive Cipher:

Advantages:

1. Simplicity: The Additive Cipher is one of the simplest encryption methods to understand and implement. It is a straightforward introduction to the concept of encryption.

2. Educational Value: It is often used as a teaching tool to introduce basic cryptographic principles. Students can easily grasp the concept of letter shifting to encode and decode messages.

3. Speed: Both encryption and decryption using the Additive Cipher are very fast. It involves simple arithmetic operations, making it efficient for small-scale applications.

4. Customizable Security: Users can choose the key value, which allows for some level of customization in terms of security. By selecting a larger key, the cipher becomes slightly more resistant to casual attacks.

Disadvantages:

1. Weak Security: The most significant disadvantage of the Additive Cipher is its weak security. The key space is very small, with only 25 possible keys for English alphabets (assuming a key of 0 is not used). This makes it highly vulnerable to brute force attacks.

2. Known-Plaintext Attack: If an attacker has access to both the plaintext and the corresponding ciphertext, they can easily determine the key and decrypt the entire message. This is known as a known-plaintext attack.

3. Frequency Analysis: The Additive Cipher is susceptible to frequency analysis. An attacker can analyze the frequency of letters in the ciphertext to make educated guesses about the key and potentially decrypt the message.

4. Limited Applicability: Due to its security vulnerabilities, the Additive Cipher is not suitable for securing sensitive or important data in the modern digital world. It may be appropriate for informal communication or educational purposes but is not practical for secure data protection.

5. Lack of Authentication: The Additive Cipher only focuses on confidentiality and does not provide any form of message authentication or integrity. This means that it does not protect against tampering or the insertion of false data.

In summary, the Additive Cipher is a simple and educational encryption method, but its limited key space and vulnerability to known-plaintext attacks and frequency analysis make it unsuitable for securing sensitive information in most practical applications. It is more of a historical curiosity than a modern encryption technique.

Application of Additive Cipher:

The Additive Cipher, also known as the Caesar Cipher, while not suitable for securing sensitive or critical information due to its security weaknesses, has found some limited applications and use cases:

1. Educational Tool: The Additive Cipher is commonly used as an educational tool to introduce basic concepts of cryptography and encryption. It helps students understand the fundamental idea of letter shifting for encoding and decoding messages.

2. Puzzles and Games: Caesar Cipher puzzles are often used in recreational settings, such as crossword puzzles and brain-teasers. Solving these puzzles involves decrypting a message encoded with the Caesar Cipher.

3. Historical Reference: The Caesar Cipher is historically significant, as it is believed to have been used by Julius Caesar to protect the confidentiality of his messages. It serves as a reference point for the evolution of cryptographic techniques.

4. Steganography: In some modern applications of steganography (the practice of hiding messages within other content), the Caesar Cipher might be used as a simple means to encode hidden messages. However, this is more for the sake of concealing information rather than ensuring strong security.

5. Basic Encryption for Non-Sensitive Data: While not recommended for securing sensitive data, the Caesar Cipher can be used to obscure non-sensitive information in casual contexts. For example, individuals might use it to encode messages in games, informal communication, or playful exchanges.

6. Cryptography Courses and Challenges: Cryptography enthusiasts and security professionals may encounter Caesar Cipher challenges in educational or recreational settings, where solving encoded messages is part of a learning experience or competition.

7. Introduction to Programming: Programmers and software developers often implement the Caesar Cipher as one of the first encryption algorithms they learn to code. It serves as a stepping stone to understanding more complex encryption techniques.

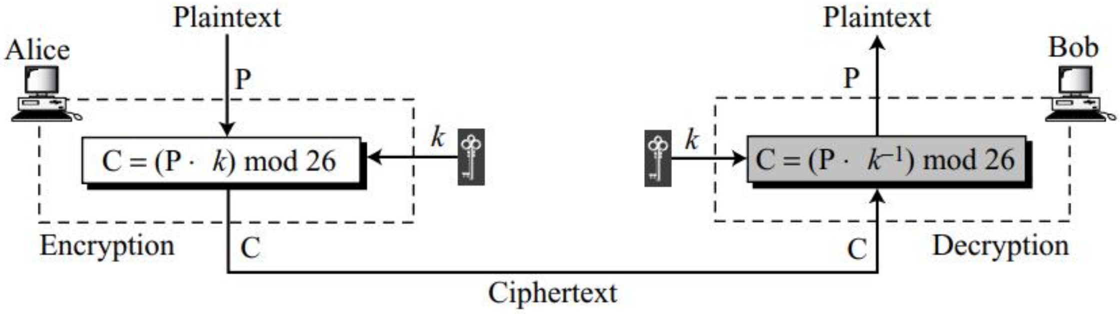
8. Simple Encryption for Fun or Nostalgia: Some individuals might use the Caesar Cipher for nostalgic or fun purposes, such as creating secret codes or messages within a group of friends or family.

It's important to emphasize that while the Additive Cipher has these applications, it is not suitable for securing important or confidential information in the digital age. It lacks the security strength needed to protect data from modern cryptographic attacks. For secure communication and data protection, more advanced encryption methods are necessary.

Multiplicative Cipher

The multiplicative cipher, is a classical encryption technique that falls under the category of substitution ciphers. It is a simple yet slightly more secure alternative to the Additive Cipher (Caesar Cipher). The multiplicative cipher involves multiplying each letter's position in the alphabet by a fixed key value and then taking the result modulo the alphabet size. This operation is applied to each letter in the plaintext to produce the ciphertext.

In a multiplicative cipher, the encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the ciphertext by the key as shown in figure . However, since operations are in Z_{26}, decryption here means multiplying by the multiplicative inverse of the key. Note that the key needs to belong to the set Z_{26}* to guarantee that the encryption and decryption are inverses of each other.



In a multiplicative cipher, the plaintext and ciphertext are integers in Z26; the key is an integer in Z_{26}*.

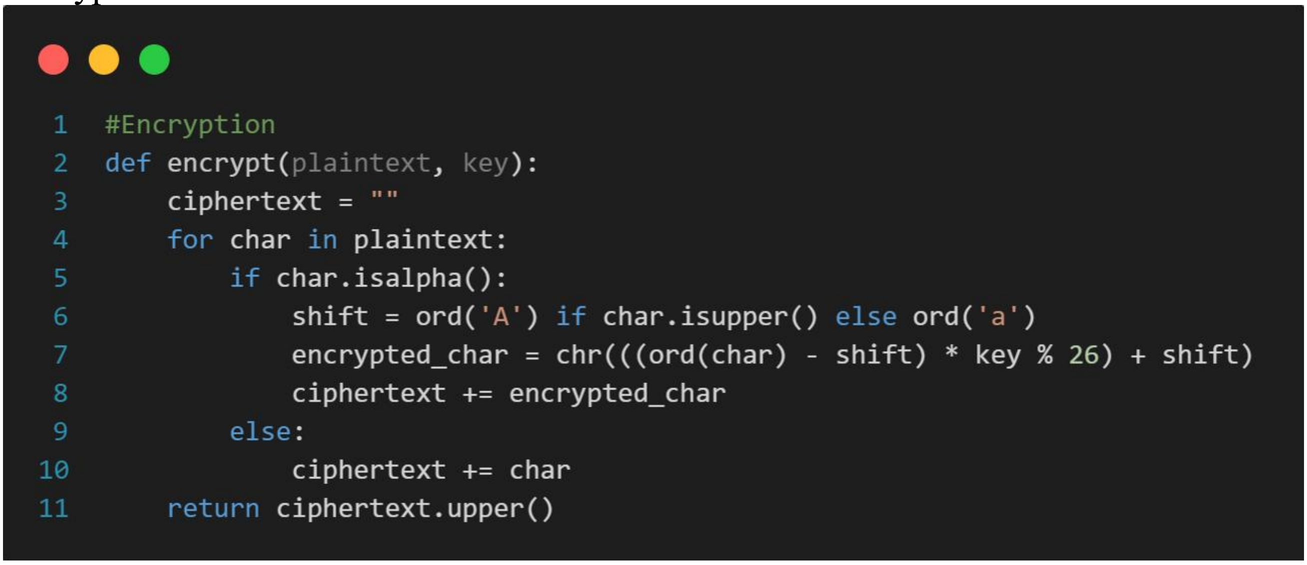
Multiplicative Cipher Implementation

1. Key: The key for the multiplicative cipher is a positive integer that represents the multiplier. The key must be coprime to the size of the alphabet (typically 26 for English letters).

2. Alphabet: The cipher operates on letters of the alphabet. It can be used with both uppercase and lowercase letters.

3. Encryption: To encrypt a letter, it is represented as its position in the alphabet. The letter is then multiplied by the key, and the result is taken modulo the alphabet size. The result is converted back to a letter.

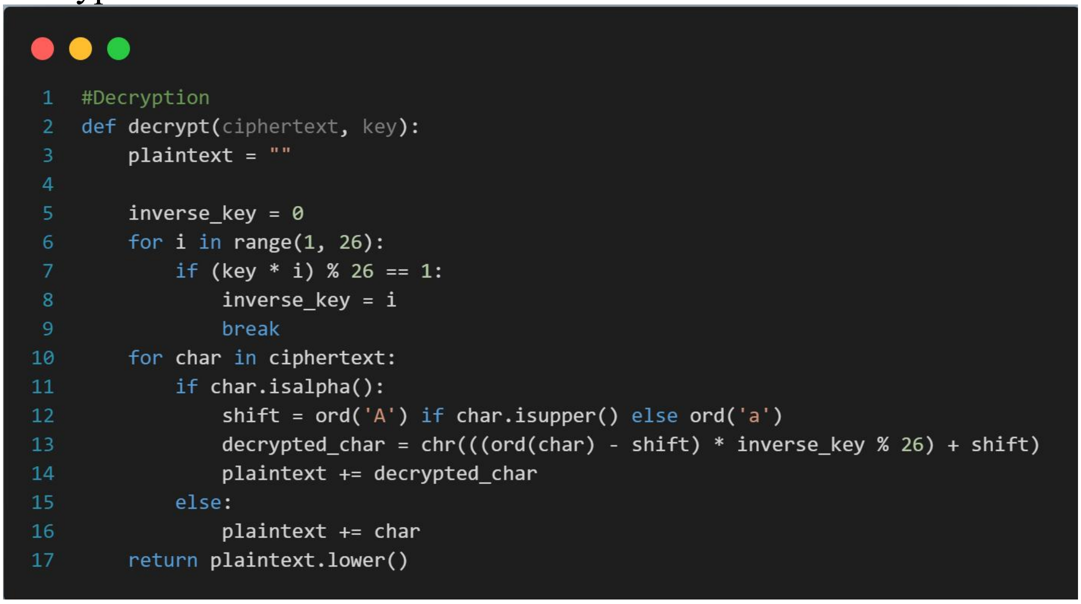
Encryption Function



```python
#Encryption
def encrypt(plaintext, key):
    ciphertext = ""
    for char in plaintext:
        if char.isalpha():
            shift = ord('A') if char.isupper() else ord('a')
            encrypted_char = chr(((ord(char) - shift) * key % 26) + shift)
            ciphertext += encrypted_char
        else:
            ciphertext += char
    return ciphertext.upper()
```

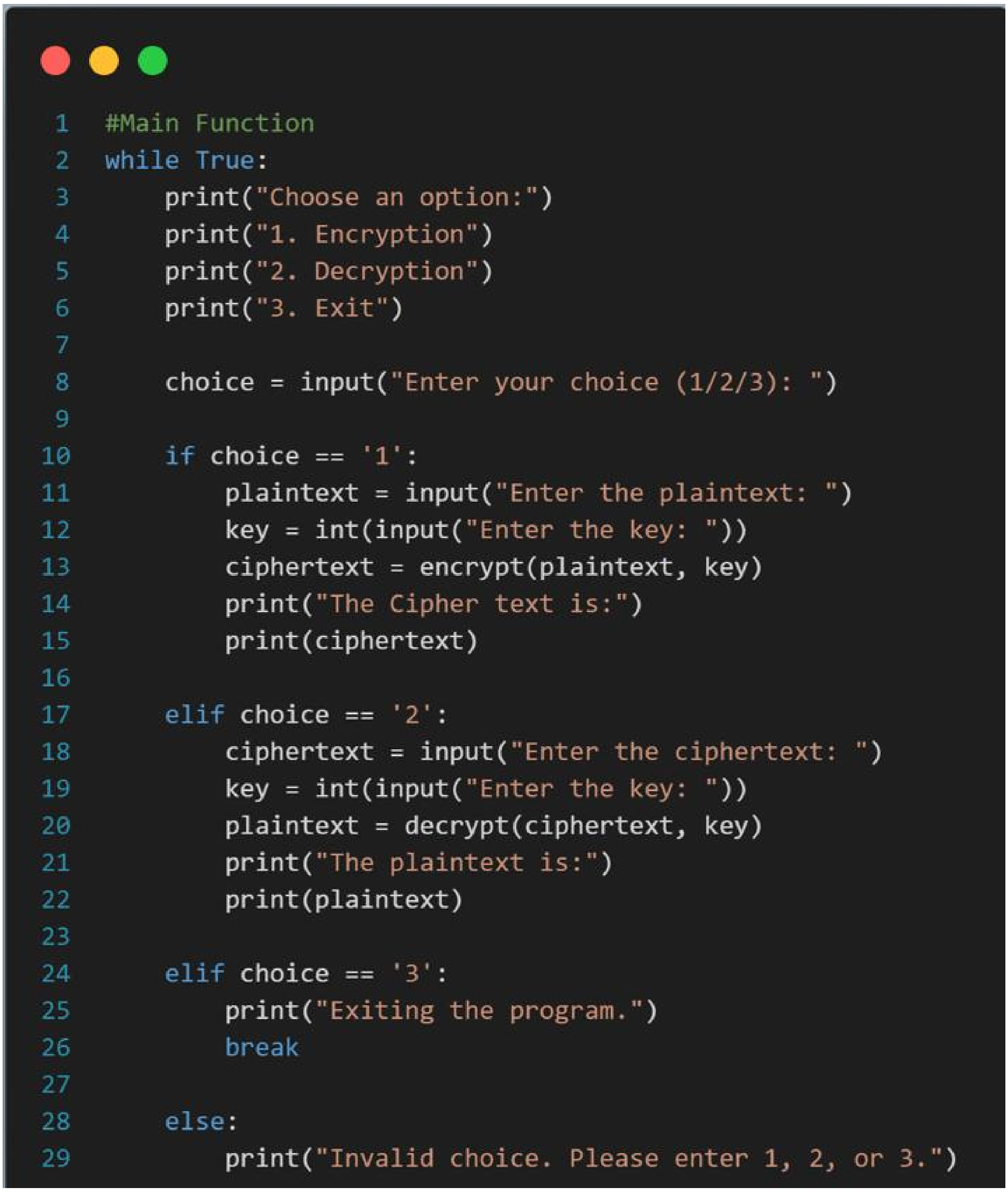
4. Decryption: Decryption is the reverse process. The letter's position in the alphabet is multiplied by the multiplicative inverse of the key (found modulo the alphabet size) to obtain the original letter.

Decryption Function



```python
#Decryption
def decrypt(ciphertext, key):
    plaintext = ""

    inverse_key = 0
    for i in range(1, 26):
        if (key * i) % 26 == 1:
            inverse_key = i
            break
    for char in ciphertext:
        if char.isalpha():
            shift = ord('A') if char.isupper() else ord('a')
            decrypted_char = chr(((ord(char) - shift) * inverse_key % 26) + shift)
            plaintext += decrypted_char
        else:
            plaintext += char
    return plaintext.lower()
```

Main Function

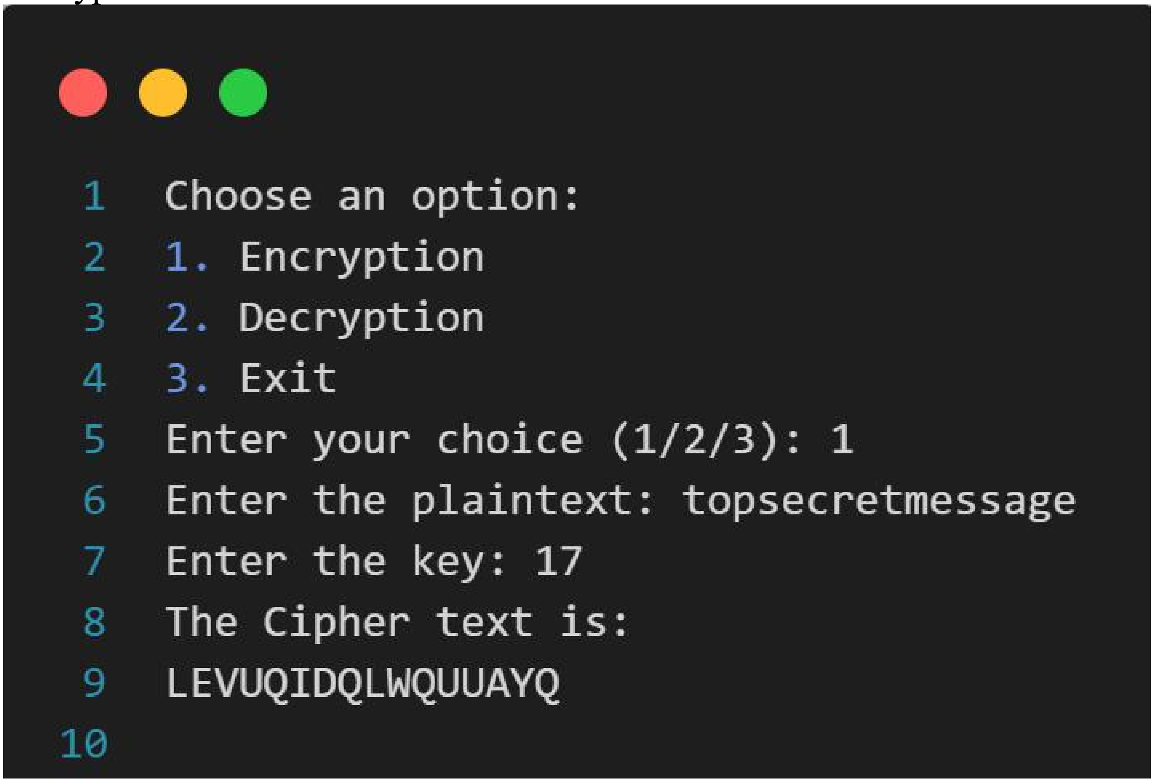


```python
#Main Function
while True:
    print("Choose an option:")
    print("1. Encryption")
    print("2. Decryption")
    print("3. Exit")

    choice = input("Enter your choice (1/2/3): ")

    if choice == '1':
        plaintext = input("Enter the plaintext: ")
        key = int(input("Enter the key: "))
        ciphertext = encrypt(plaintext, key)
        print("The Cipher text is:")
        print(ciphertext)

    elif choice == '2':
        ciphertext = input("Enter the ciphertext: ")
        key = int(input("Enter the key: "))
        plaintext = decrypt(ciphertext, key)
        print("The plaintext is:")
        print(plaintext)

    elif choice == '3':
        print("Exiting the program.")
        break

    else:
        print("Invalid choice. Please enter 1, 2, or 3.")
```

The implementation of a multiplicative cipher begins with selecting a key, which is a positive integer that serves as the encryption parameter. To encrypt a message, each letter in the plaintext is first assigned a numerical value based on its position in the alphabet (e.g., 'A' is 0, 'B' is 1, and so on). Then, for each letter, the numerical value is multiplied by the chosen key, and the result is taken modulo 26 to ensure the result remains within the bounds of the alphabet. The encrypted message is formed by converting these numerical values back to letters. To decrypt the message, the recipient uses the multiplicative inverse of the key modulo 26, then multiplies this inverse by the numerical values of the ciphertext, again applying modulo 26, and finally converting the results back to their corresponding letters. This process ensures the confidentiality of the message using a simple and reversible mathematical operation.

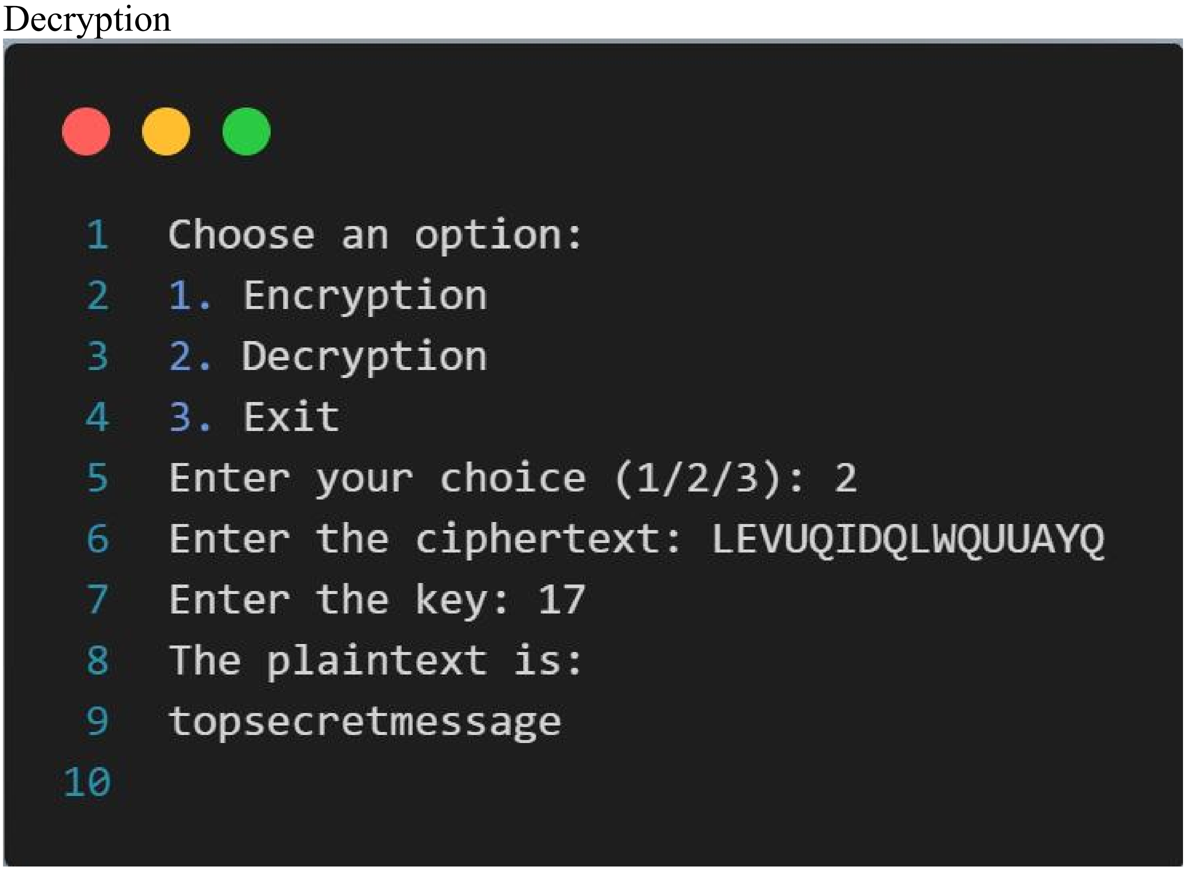
Snapshots of Implementation

Encryption



```
Choose an option:
1. Encryption
2. Decryption
3. Exit
Enter your choice (1/2/3): 1
Enter the plaintext: topsecretmessage
Enter the key: 17
The Cipher text is:
LEVUQIDQLWQUUAYQ

```

Decryption



```
Choose an option:
1. Encryption
2. Decryption
3. Exit
Enter your choice (1/2/3): 2
Enter the ciphertext: LEVUQIDQLWQUUAYQ
Enter the key: 17
The plaintext is:
topsecretmessage

```

Advantages and Disadvantages if Multiplicative Cipher:

Advantages:

1. Larger Key Space: The multiplicative cipher offers a larger key space compared to simpler ciphers like the Caesar Cipher. This means there are more possible keys, making it somewhat more resistant to brute force attacks.

2. Resistance to Frequency Analysis: While not immune to frequency analysis, the multiplicative cipher is more resistant to this form of attack than additive ciphers like the Caesar Cipher. Frequency analysis involves analyzing the frequency of letters in the ciphertext to deduce the key, and the multiplicative cipher's operation makes this process less straightforward.

3. Customization: Users can choose from a variety of key values, offering a degree of customization in terms of security. The key can be a positive integer that is coprime to the size of the alphabet.

4. Educational Value: The multiplicative cipher serves as an educational tool for teaching cryptographic concepts and introduces the idea of modular arithmetic, inverses, and the concept of an affine transformation.

Disadvantages:

1. Weak Security: While offering some advantages over simpler ciphers, the multiplicative cipher is still relatively weak in terms of security. The key space, while larger than that of the Caesar Cipher, is not sufficient to withstand modern cryptographic attacks.

2. Known-Plaintext Attack: If an attacker has access to both the plaintext and the corresponding ciphertext, they can determine the key and decrypt the entire message. This is known as a known-plaintext attack.

3. Limited Applicability: The multiplicative cipher is not suitable for securing sensitive or important data in the digital age. It may be used for casual communication or educational purposes but is not practical for strong data protection.

4. Lack of Authentication: Like other classical ciphers, the multiplicative cipher focuses solely on confidentiality and does not provide any form of message authentication or integrity. It does not protect against tampering or the insertion of false data.

Applications of Multiplicative Cipher:

Applications of the multiplicative cipher are limited due to its simplicity and vulnerability to various cryptographic attacks. However, it can still be used for educational purposes, puzzles, and situations where basic encryption is sufficient. Here are a few potential applications:

1. Educational Purposes: Multiplicative cipher is often used in educational settings to teach the basics of encryption and modular arithmetic. It helps students understand the fundamental concepts of cryptography.

2. Puzzles and Games:Multiplicative ciphers can be used in puzzles, riddles, and games where participants need to solve encrypted messages. These can be part of escape rooms, treasure hunts, or interactive storytelling experiences.

3. Basic Security: While not suitable for serious security applications, the multiplicative cipher can be used for very basic security measures where the threat level is low, and simplicity is more important than strong encryption. For example, it might be used in some home automation systems or IoT devices where a minimal level of security is required.

4. Historical Reenactments:Multiplicative ciphers were historically used by ancient civilizations like the Romans and Greeks. Enthusiasts and reenactors might use this cipher to exchange messages as part of historical demonstrations or events.

5. Cryptography Learning Tools:Online platforms and courses that teach cryptography often use multiplicative ciphers as exercises for learners to practice encryption and decryption techniques.

Remember that the multiplicative cipher is not secure for protecting sensitive information, as it can be easily broken using techniques like frequency analysis and brute-force attacks. Modern encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) are much more secure and widely used for protecting sensitive data.

CONCLUSION :

In conclusion, the report has explored two classical encryption techniques: the Additive Cipher (Caesar Cipher) and the Multiplicative Cipher. These ciphers, although simple and historically significant, serve as foundational concepts in the field of cryptography.

The Additive Cipher, which involves shifting each letter of the alphabet by a fixed number of positions, is a basic introduction to the concept of encryption. Its strengths lie in its simplicity, educational value, and speed, while its weaknesses are evident in its weak security, vulnerability to known-plaintext attacks, and susceptibility to frequency analysis.

The Multiplicative Cipher, which extends the concept by multiplying letter positions by a key value and applying modulo operations, offers a larger key space and resistance to certain attacks. While it provides more security compared to the Additive Cipher, it remains relatively weak in the context of modern cryptography, with limitations such as vulnerability to known-plaintext attacks.

Both ciphers have their respective advantages, including their roles as educational tools and references to historical cryptographic methods. They find applications in recreational settings, cryptographic challenges, and informal communication. However, they are not suitable for securing sensitive or critical data in the digital age.

As we conclude, it is important to recognize that the field of cryptography has advanced significantly since the development of these classical ciphers. Modern cryptographic techniques, including strong symmetric and asymmetric algorithms, offer the robust security required to protect data in an increasingly connected and digital world. While the Additive and Multiplicative Ciphers contribute to our understanding of cryptography, they represent only the starting point in a vast and evolving landscape of encryption and data security.

REFERENCES :

- Cryptography and Network Security By Behrouz A Forouzan
- https://www.geeksforgeeks.org
- https://en.wikipedia.org/wiki/Cryptography
- https://www.techtarget.com/searchsecurity/definition/cryptography
- https://www.khanacademy.org/computing/computer-science/cryptography
- https://brilliant.org/wiki/caesar-cipher/