Excelssior Education Society's
K. C. College of Engineering & Management Studies & Research
Department of Computer Engineering

CAESAR CIPHER

(Secrete messaging,securing data)

GROUP MEMBERS

SAHIL A. SAWANT (B-17)

ADITYA P. SHINDE (B-25)

VINAYAK V. UTEKAR (B-42)

Under the Supervision of

Prof.POULAMI DAS

OVERVIEW

- Introduction
- Literature Survey
- Problem finding and Motivation to the work
- Hardware and Software Requirements
- Methodology
- Proposed Techniques
- Results and Discussions
- Conclusion
- References

Introduction

- In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.
- The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.
- Few common items that are encrypted include text files, images, e-mail messages, user data and directories. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. It may also be performed with a set of keys or passwords.
- Here we have used Caesar Cipher. Which is one of the most used technique for secret messaging and exchanging of confidential data

Literature Survey

The Caesar Cipher technique is one of the earliest and widely used method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after **Julius Caesar**, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

Problem Statement

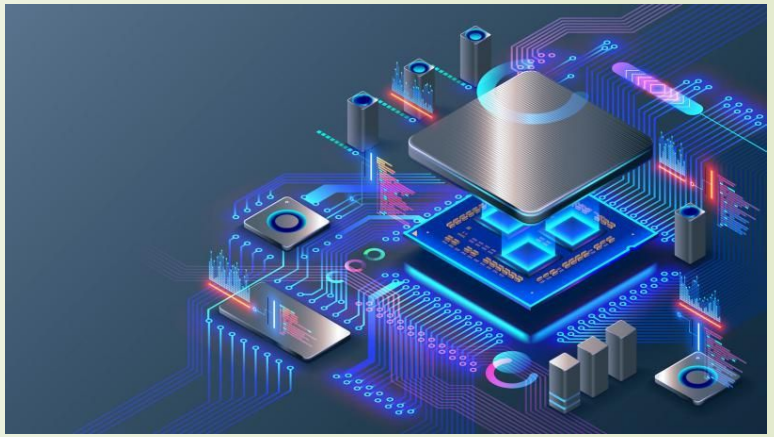
How to secure your information from unauthorized access?

Secure message/ data transfer.

Encoder-Decoder – Secures your Information by Encoding the messages.

Hardware Requirements

SYSTEM :- INTEL CORE I3 (Min)
HARD DISK :- 500 GB
MONITOR : STANDARD LED MONITOR
INPUT DEVICES :- KEYBOARD
RAM:- 4 GB



Software Requirements

OPERATING SYSTEM :- WINDOWS 7 (Min)
PROGRAMMING LANGUAGE :- PYTHON
CODE EDITOR :- VS CODE / ATOM
LIBRARIES USED :- TKINTER & BASE 64
ENCRYPTING METHOD :- CAESER CIPHER

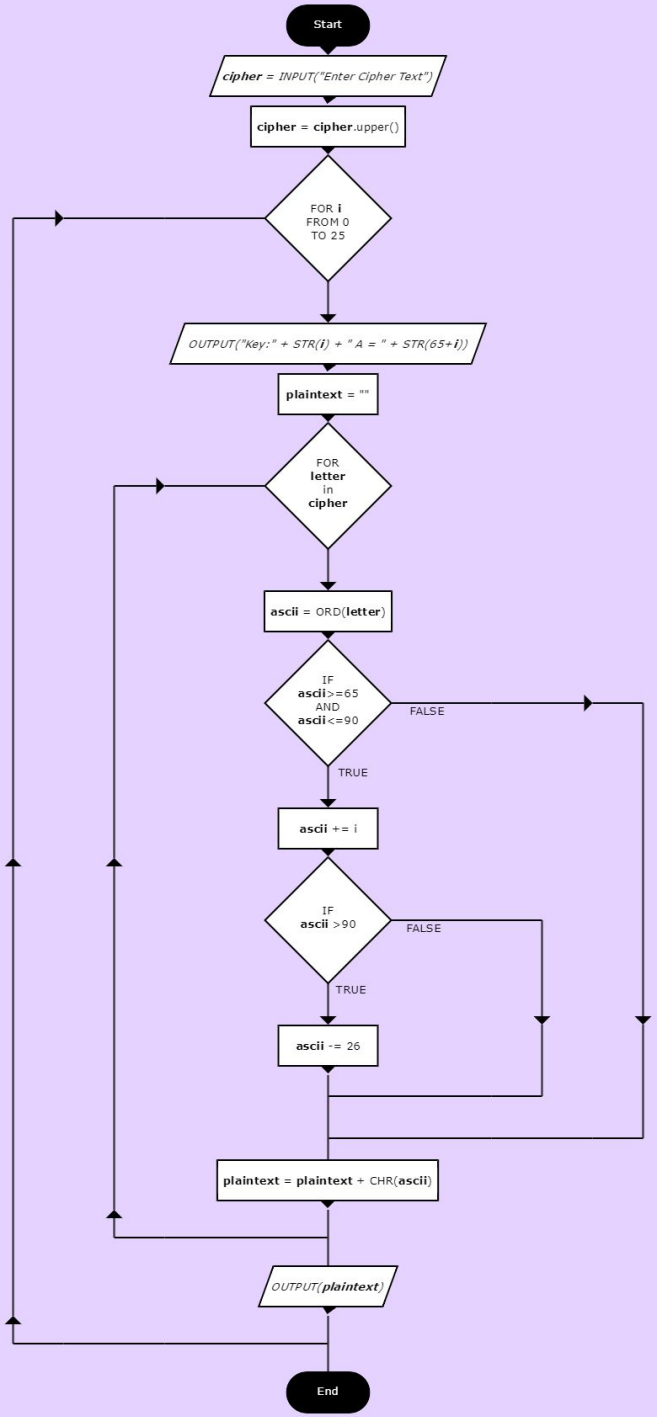
Methodology

- Import tkinter, numpy libraries.
- Initialized window to cover the whole screen.
- Added labels, input fields and buttons.
- Created a function **encrypt()** to encode the input string entered by user.
- Ask the user to provide a **key** which will help to decode the text while decrypting.
- Created a function **decrypt()** to decode the the encrypted text.
- If the user will enter same key used while encrypting text, it will show the decoded text.
- Press "**Show Result**" button to get the decoded text.

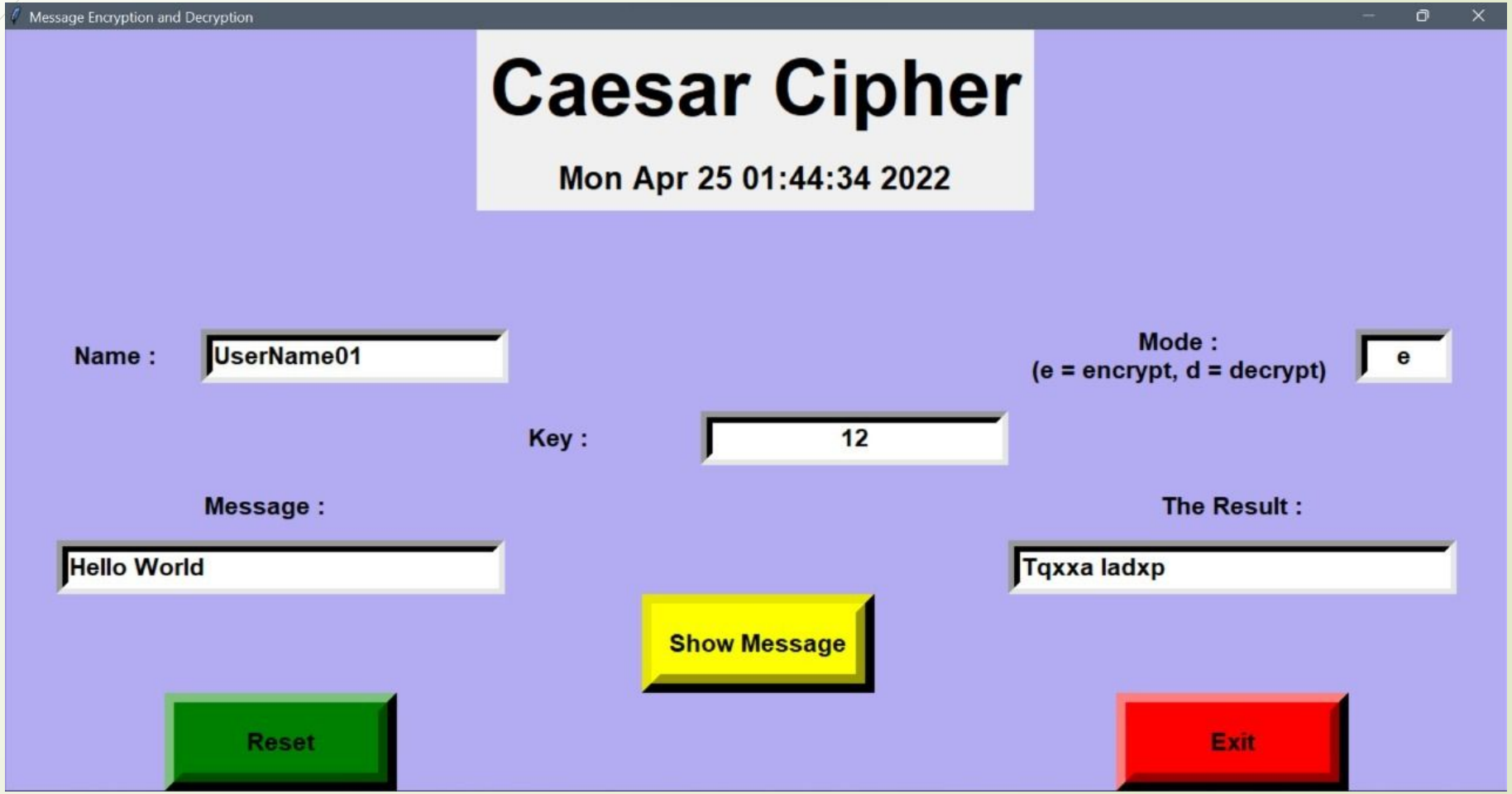
ALGORITHM

STEP 1 : START
STEP 2 : Initialize window.
STEP 3 : Enter name, key and message.
STEP 4 : Type ‘e’ to encrypt code in mode input field.
STEP 5 : Click on “Show Message” button for result.
STEP 6 : Copy the encrypted message.
STEP 7 : Click on “Reset” button.
STEP 8 : Now, Enter name, key, message and type ‘d’ to decrypt code.
STEP 9 : Click on “Show Message” button for result.
STEP 10 : Click on “Exit” button to exit program.
STEP 11 : STOP

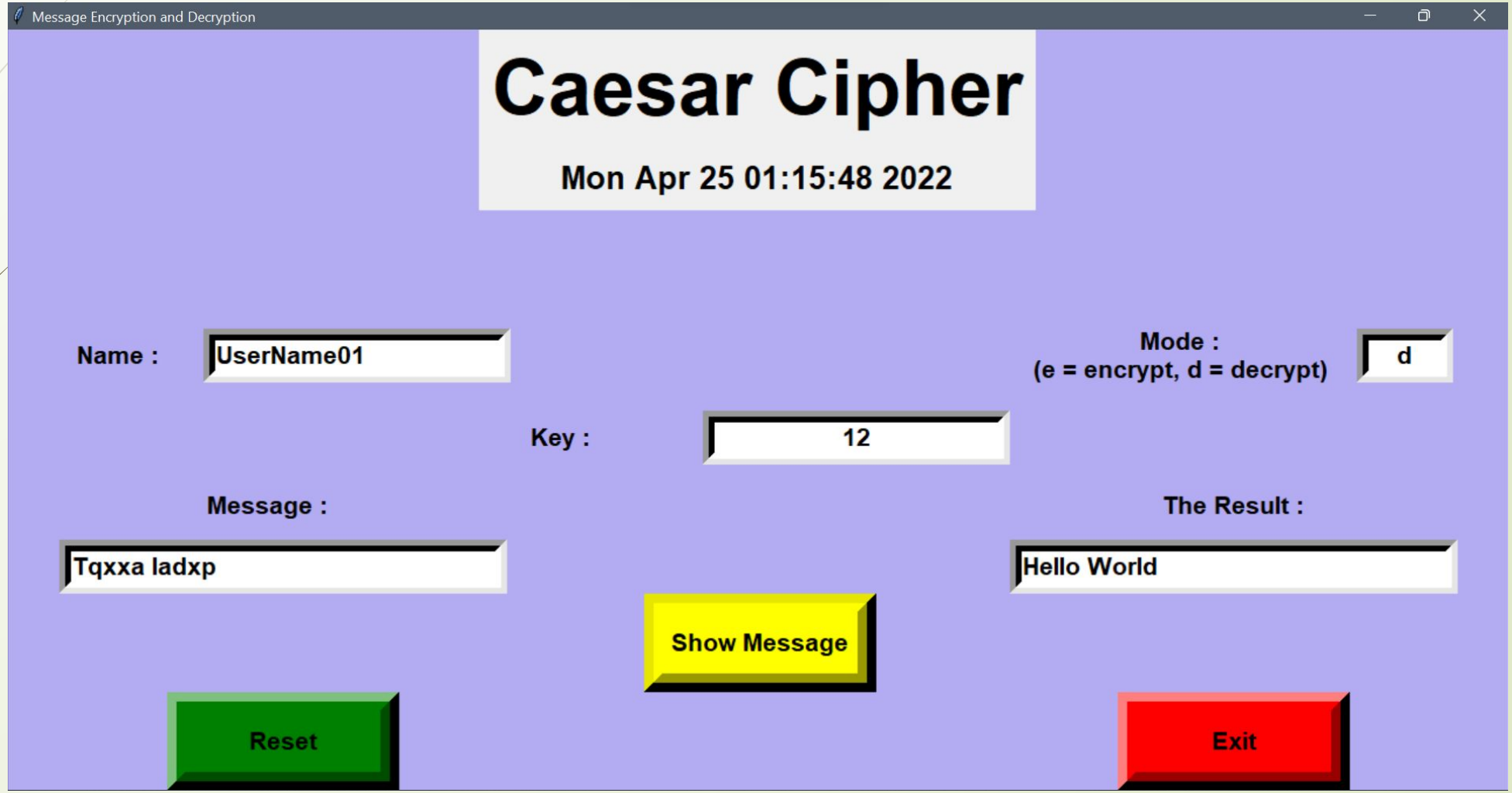
FLOWCHART


Start
cipher = INPUT("Enter Cipher Text")
cipher = cipher.upper()
FOR i FROM 0 TO 25
OUTPUT("Key:" + STR(i) + " A = " + STR(65+i))
plaintext = ""
FOR letter in cipher
ascii = ORD(letter)
IF ascii>=65 AND ascii<=90
FALSE
TRUE
ascii += i
IF ascii >90
FALSE
TRUE
ascii -= 26
plaintext = plaintext + CHR(ascii)
OUTPUT(plaintext)
End

Results


Message Encryption and Decryption
Caesar Cipher
Mon Apr 25 01:44:34 2022
Name :
UserName01
Mode :
(e = encrypt, d = decrypt)
e
Key :
12
Message :
Hello World
The Result :
Tqxxa ladxp
Show Message
Reset
Exit

Results


Message Encryption and Decryption
Caesar Cipher
Mon Apr 25 01:15:48 2022
Name :
UserName01
Mode :
(e = encrypt, d = decrypt)
d
Key :
12
Message :
Tqxxa ladxp
The Result :
Hello World
Show Message
Reset
Exit

Advantages

Encryption Provides Security for Data at All Times:

Generally, data is most vulnerable when it is being moved from one location to another. Encryption works during data transport or at rest, making it an ideal solution no matter where data is stored or how it is used.

Encryption Protects Privacy:

Encryption is used to protect sensitive data, including personal information for individuals. This helps to ensure anonymity and privacy, reducing opportunities for surveillance by both criminals and government agencies. Encryption technology is so powerful that some governments are attempting to put limits on the effectiveness of encryption—which does not ensure privacy for companies or individuals.

Encrypted Data Maintains Integrity:

Hackers don't just steal information, they also can benefit from altering data to commit fraud. While it is possible for skilled individuals to alter encrypted data, recipients of the data will be able to detect the corruption, which allows for a quick response to the cyber-attack.

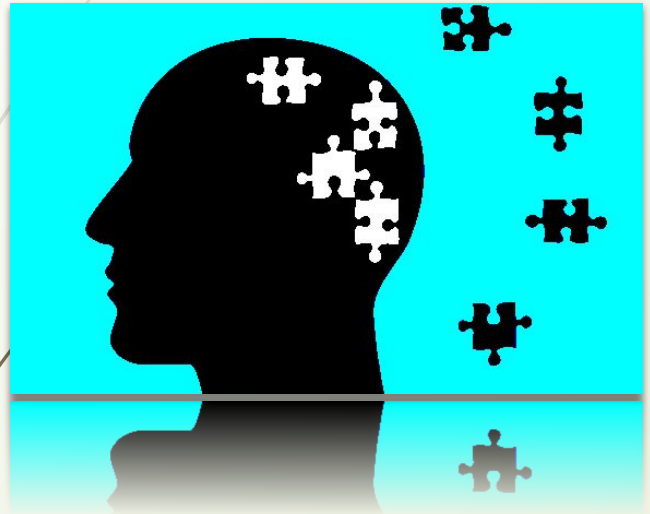
Time complexity of the cipher is O(n):

Which means that running time increases at most linearly with the size of input.

Limitations

Forgetting Passwords/Key:

General most of the people forget the password/keys so they find difficulties to access the message or data.



Requiring Cooperation:

Using encrypted files that are designed to be opened and shared by two or more people can be disadvantageous when one or more participants finds it a burden to use encryption.

Developing a False Sense of Security:

A disadvantage of encrypted files is that relying on them to keep things secret could lull you into a false sense of security. A determined person may marshal overwhelming computer resources to decrypt your secret files.

Applications

1)**Encryption/Decryption in emai**l: Email encryption is a method of securing the content of emails from anyone outside of the email conversation looking to obtain a participant's information. In its encrypted form, an email is no longer readable by a human. Only with your private email key can your emails be unlocked and decrypted back into the original message.

2) **Defense Government Organizations**- to facilitate secret communication

3) **For sending highly confidential message or details on Social Media like Card details or Bank Information**.

4) **Encryption is also used to protect data in transi**t, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years.

Applications

5)**Encryption can be used to protect data "at rest"**, such as information stored on computers and storage devices (e.g. USB flash drives). In recent years, there have been numerous reports of confidential data, such as customers' personal records, being exposed through loss or theft of laptops or backup drives; encrypting such files at rest helps protect them if physical security measures fail

6) **Digital rights management systems**, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection), is another somewhat different example of using encryption on data at rest.

Future Scope

1. More encoding cipher options could be added such as STEGANOGRAPHY ,
   ADVANCED ENCRYPTION STANDARD (AES),
   TRIPLE DES (DATA ENCRYPTION STANDARD).

2. More secure and user oriented encryption can be done

3. It will be used in all purpose such as Internet banking, Sharing Personal details, Military & Defence connections and also identifing Terrorist threats , Securing your data in own devices more safely,

Conclusion

- Today, encryption is used in the transfer of communication over the Internet for security and commerce. As computing power continues to increase, computer encryption is constantly evolving to prevent attacks. Encryption serves as a mechanism to ensure confidentiality. Since data may be visible on the Internet, sensitive information such as passwords and personal communication may be exposed to potential interceptors

- Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing.Modern encryption schemes utilize the concepts of public-key and symmetric-key.Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

- We have successfully developed Encoder-Decoder project in Python. We used the popular tkinter library for rendering graphics on a display window to encode & decode using the Ceaser Cipher method for encrypting. In this way, we can encode our message and decode the encoded message in a secure way by using the Password key

References

1) Tkinter library:
https://docs.python.org/3/library/tkinter.html

https://www.tutorialspoint.com/python/python_gui_programming.htm#%20:~:text=Tkinter%20is%20the%20standard%20GUI,to%20the%20Tk%%2020GUI%20toolkit.&text=Import%20the%20Tkinter%20module.

3)Cesar Cipher:
https://en.wikipedia.org/wiki/Caesar_cipher

https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

THANK YOU