KAKINADA INSTITUTION OF ENGINEERING AND TECHNOLOGY

2025-2029

CAESAR CIPHER

CSC (CYBER SECURITY)

DAYSCHOLAR

TEAM-2

TEAM MEMBERS

| NAMES	ROLL NO
P.BHAVITHA	25B21A4613
K.SAI PRASANNNA	25B21A4601
V.LAVANYA	25B21A4638
P.MAHA LAXMI	25B21A4635

Problem Statement:

In today's digital world, data security and confidentiality are critical. Even simple systems need basic encryption techniques to protect data from unauthorized access. The Caesar Cipher is a foundational encryption method that demonstrates how substitution ciphers work to scramble data.
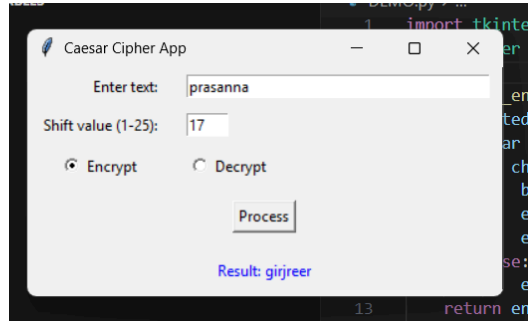
Our project aims to show how a Caesar Cipher can be used for basic text encryption and decryption, ideal for educational purposes or small-scale secure communication.

How You Do It (What You Used to Achieve It):

We created a program that allows users to input plain text and a key (number of shifts). The Caesar Cipher algorithm then shifts each letter of the text by the key's value to produce encrypted output. It also allows for decryption by reversing the shift.

Tools & Technologies Used:

- **Programming Language:** Python *(can also be implemented in C/C++/JavaScript)*
- **IDE:** VS Code / PyCharm
- **Concepts Used:**
    - ASCII values
    - Modulus operation
    - String manipulation
    - Loops and conditionals

📑 Page 3: Conclusion

The Caesar Cipher project successfully demonstrates how classical encryption works using simple shift logic. While not secure for modern applications, it's an excellent educational tool to understand the basics of cryptography.

Through this project, we learned about the importance of:

- Encrypting sensitive information
- Algorithmic thinking and logic design
- User-friendly implementation of cryptographic techniques

In the future, this can be expanded to include:

- Brute-force decryption
- Frequency analysis attacks
- Other ciphers like Vigenère or RSA for stronger encryption