# Computer Organization and Assembly Language

Project: Vigenère Cipher



**Group Members**

|  |  |
| --- | --- |
| Muhammad Hamza | 01-134231-051 |
| Mubarak Andrabi | 01-134231-088 |
| Humayun Tariq | 01-134231-028 |

## Objectives

The objective of this project is to implement the Vigenère Cipher in assembly language. The key objectives include:

1. Developing a program capable of encrypting and decrypting using the Vigenère Cipher.
2. Ensuring the program is efficient and able to handle both words and sentences.

## Tools to be used:

* Visual Studio Code
* MASM
* Irvine32
* Git

## Problem Statement

The Vigenère Cipher is a classical encryption technique that operates by shifting each letter of the plaintext by a corresponding letter in the key. This provides a form of polyalphabetic substitution, making it more secure than simpler substitution ciphers. The objective of this project is to create a program that can both encrypt and decrypt plaintext using this cipher. It would be able to handle encrypt and decrypt both single word and sentences.

## Timeline

Timeline link: <https://github.com/users/humayyuntariq/projects/3/>

## Conclusion

In conclusion, the implementation of the Vigenère Cipher in assembly language will provide a practical exercise in understanding both cryptographic principles and low-level programming concepts. By completing this project, we aim to deepen our understanding of computer organization, assembly language programming, and classical encryption techniques.

## Resources:

Resources Online: <https://www.geeksforgeeks.org/vigenere-cipher/> <https://cryptii.com/pipes/vigenere-cipher>