# 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 plaintext using the Vigenère Cipher.
2. Utilizing a table of alphabets arranged in a specific order for encryption and decryption.
3. Ensuring the program is efficient and able to handle various input sizes.

## Tools to be used:

* VSCode
* MASM
* Irvine

## 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 keyword. 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.

## What is Vigenère Cipher.

The Vigenère Cipher is a method of encrypting alphabetic text using a simple form of polyalphabetic substitution. It employs a keyword or keyphrase to determine the shifting of letters in the plaintext. The key is repeated to match the length of the plaintext, ensuring each letter in the plaintext is encrypted using a different shift.

## 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>