CIS-7-Final

Project X - Vigenère Cipher Encryption Tool

Overview

Project X is a C++ application that implements a Vigenère cipher encryption system with additional hashing capabilities. The program allows users to encrypt messages and optionally save hashed versions of the encrypted text to their Documents directory.

Features

- Message encryption using the Vigenère cipher algorithm
- Simple hash generation for encrypted messages
- Cross-platform file handling for Windows and Unix-like systems
- Interactive command-line interface
- Automatic screen clearing for better user experience

Technical Architecture

Main Components

1. **Project_X.cpp** - Main application logic
   - Contains the core encryption and user interface functionality
   - Implements the Vigenère cipher algorithm
   - Handles user input and program flow
2. **file_utils.cpp/.h** - File handling utilities
   - Manages saving hashed messages to the user's Documents directory
   - Provides cross-platform compatibility for file operations
   - Handles environment variable access safely

Core Functions

Encryption and Hashing

- `vigenereEncrypt(const string& message, const string& key)`
  - Implements the Vigenère cipher encryption
  - Preserves case sensitivity and non-alphabetic characters

  - Uses a default key defined as "defaultkey"
- `hashMessage(const string& message)`
  - Implements a simple hash function
  - Uses a multiplication and modulo approach
  - Returns a string representation of the hash

User Interface

- `displayMenu()`
  - Shows the main program options
  - Provides a clean, formatted interface
- `getUserInput(const string& prompt, bool allowSpaces = true)`
  - Handles user input with validation
  - Supports both space-allowed and space-restricted input
  - Ensures non-empty input

File Operations

- `saveHashedMessageToFile(const string& hashedMessage)`
  - Saves hashed messages to the user's Documents directory
  - Handles platform-specific path differences
  - Implements error handling for file operations

Usage Flow

1. User starts the program
2. Program displays the main menu
3. User selects to encrypt a message
4. User enters the message
5. Program encrypts the message using the Vigenère cipher
6. User chooses whether to save the hashed version
7. If yes, program saves to Documents directory
8. Screen clears after 5 seconds
9. Process repeats or user exits

Technical Details

Security Considerations

- Uses a hardcoded encryption key (DEFAULT_KEY)
- Implements basic input validation
- File operations use platform-specific secure methods
- Simple hashing algorithm (not cryptographically secure)

Platform Compatibility

The program supports:

- Windows (using _WIN32 or _WIN64 macros)
- Unix-like systems (Linux, macOS)

Dependencies

- Standard C++ libraries only:
  - `<iostream>`
  - `<fstream>`
  - `<string>`
  - `<cctype>`
  - `<chrono>`
  - `<thread>`

Build and Compilation

Required Files

- Project_X.cpp
- file_utils.cpp
- file_utils.h

Compilation Notes

- Requires C++11 or later
- No external dependencies needed
- Standard build tools (g++, clang++, or MSVC) can be used

Limitations and Future Improvements

1. Fixed encryption key (could be made configurable)
2. Basic hashing algorithm (could be replaced with a cryptographic hash)
3. Limited error handling for file operations

4. No decryption functionality
5. No input file support (currently only handles direct text input)

Error Handling

- Input validation for menu choices
- File operation error checking
- Environment variable access validation
- Invalid input recovery mechanisms