

# 1 About project

This project implements several classical encryption algorithms (Playfair, Winston, Vigenère) using a modular and extensible architecture based on well-established software design patterns.

## 2 Cipher Logic Overview

### 2.1 Playfair Cipher

- The message is split into bigrams (letter pairs).
- If a pair contains identical letters, the second is replaced with Z.
- If the total length is odd, an X is added at the end.
- A 5×5 matrix is built using the first key ( $I = J$ ).
- Each pair is processed as follows:
  - Same row → letters shift right
  - Same column → letters shift down
  - Rectangle → letters are swapped to opposite corners in the same row

### 2.2 Winston Cipher

- The message is split into bigrams (letter pairs).
- If a pair contains identical letters, the second is replaced with Z.
- If the total length is odd, an X is added at the end.
- A 5×5 matrix is built using the first key ( $I = J$ ).
- A 5×5 matrix is built using the second key ( $I = J$ ).
- Find the first bigram's letter in at the first table[ $row1$ ][ $col1$ ]
- Find the second bigram's letter in at the second table[ $row2$ ][ $col2$ ]
- Find result at the first table [ $row1$ ][ $col2$ ]
- Find result at the first table [ $row2$ ][ $col1$ ]

### 2.3 Vigenère Cipher

- If two identical letters appear in a row, the second is replaced with Z.
- If the message has an odd number of letters, add X at the end.
- The key is repeated to match the length of the message.
- Each letter is shifted forward in the alphabet by the alphabetical index of the corresponding key letter.

## 3 Project structure

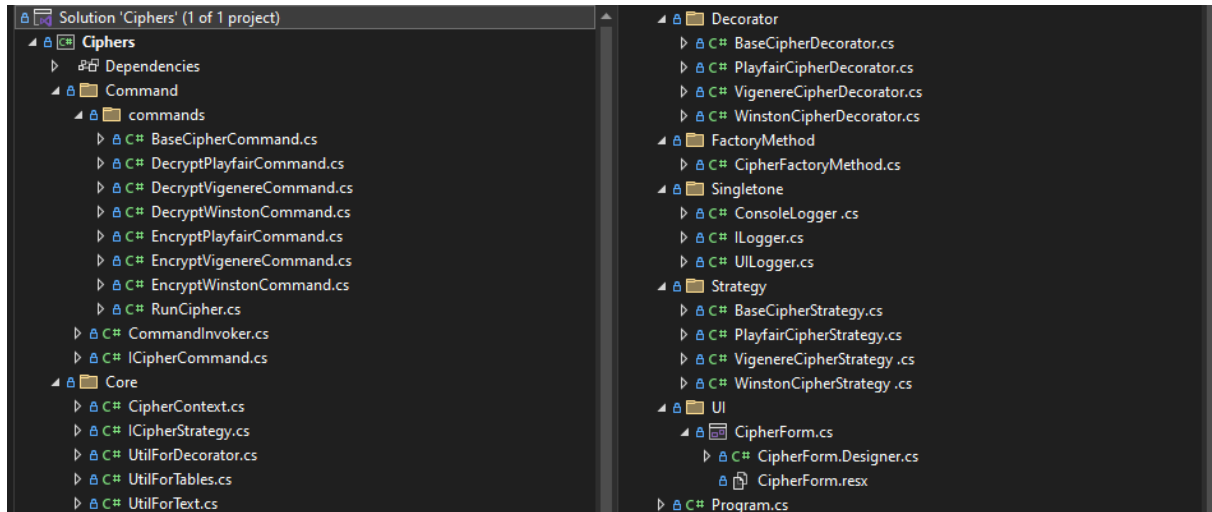


Figure 1: Project structure

### 3.1 Folder - Strategy

**Used in:** ICipherStrategy, concrete strategy classes.

**Purpose:** Make ciphers interchangeable.

### 3.2 Folder - Decorator

**Used in:** BaseCipherDecorator, adds logging.

**Purpose:** Extend cipher without modifying original.

### 3.3 Folder - Factory Method

**Used in:** CipherFactoryMethod.Create().

**Purpose:** Centralized object creation based on user input.

### 3.4 Folder - Command

**Used in:** ICipherCommand, RunCipher, CommandInvoker.

**Purpose:** Encapsulate cipher action logic.

### 3.5 Folder - Singleton

**Used in:** ConsoleLogger, UILogger.

**Purpose:** Share a single logger across app.

**Note:** UILogger requires explicit initialization with a form.

## 3.6 Folder - Core

**ICipherStrategy** – interface shared by all cipher strategies.

**CipherContext** – structural holder for strategy and mode (not actively used but supports Strategy-compliant architecture).

**UtilForText** – provides text preprocessing:

- filters input
- generates bigrams
- repeats key for Vigenère

**UtilForTables** – table generation and lookup used in Playfair and Winston.

**UtilForDecorator** – printing tables and debug-formatting for decorators.

## 3.7 Folder - UI

**CipherForm** – main Windows Forms class that builds the user interface.

**Purpose:** collect user input and trigger cipher execution.

**Includes:**

- ComboBox for selecting cipher type and mode (Encrypt/Decrypt)
- TextBox inputs for first key, second key, and message
- Button to run the cipher process
- textBoxLog and textBoxResults to display logs and results

**Works with:** CipherFactoryMethod, RunCipher, and UILogger

# 4 Ciphers in action

## 4.1 Playfair

```
[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 1
[REQUIREMENT] Write message: hello world
[REQUIREMENT] Write key: key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 1
[CHAPTER] Cipher Debug Info:
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Message : HELLOWORLD
Key1 : KEY
Bigrams: H E | L X | O W | O R | L D |
[CHAPTER] Table for key 'key':
k e y a b
c d f g h
i l m n o
p q r s t
u v w x z
[INFO] Encryption started...
[h, e] => [d, b]
[l, x] => [n, v]
[o, w] => [m, z]
[o, r] => [m, t]
[l, d] => [q, l]
[RESULT] Encrypted: dbnmvzmtql
[SUCCESS] Playfair cipher completed successfully.
[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 1
[REQUIREMENT] Write message: dbnmvzmtql
[REQUIREMENT] Write key: key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 2
[CHAPTER] Cipher Debug Info:
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Message : DBNMVZMTQL
Key1 : KEY
Bigrams: D B | N V | M Z | M T | Q L |
[CHAPTER] Table for key 'key':
k e y a b
c d f g h
i l m n o
p q r s t
u v w x z
[INFO] Decryption started...
[d, b] => [h, e]
[n, v] => [l, x]
[m, z] => [o, w]
[m, t] => [o, r]
[q, l] => [l, d]
[RESULT] Decrypted: helloworld
[INFO] Clean Decryption started...
[RESULT] Clean Decrypted: helloworld
[SUCCESS] Playfair cipher completed successfully.
[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number:
```

Figure 2: Playfair in console mode

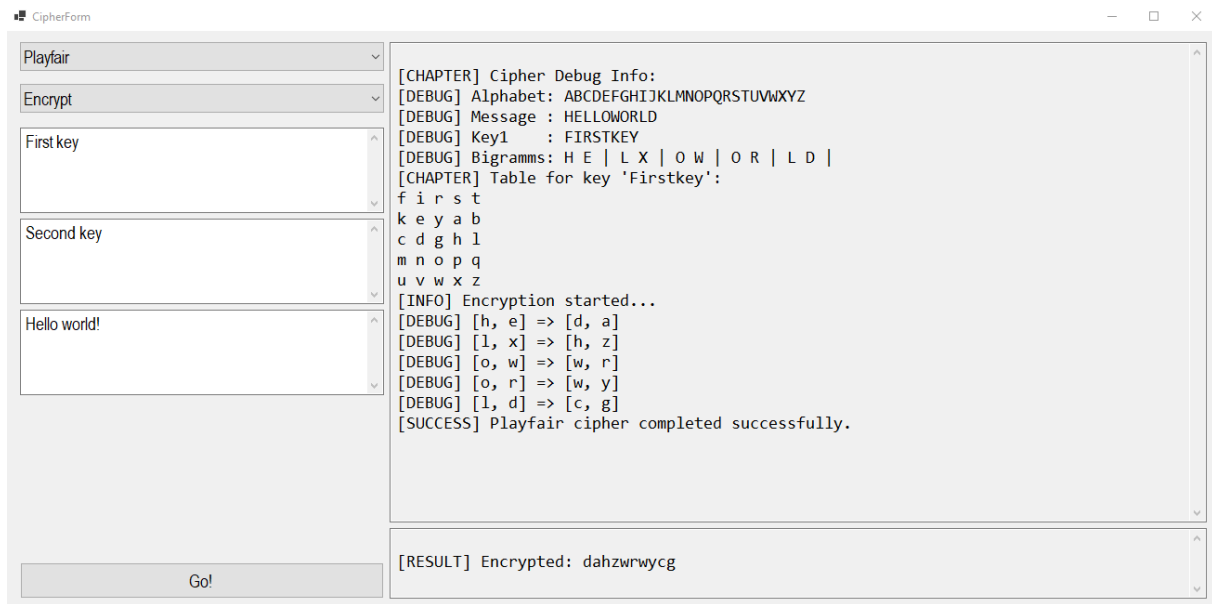


Figure 3: Playfair encrypt in WinForms mode

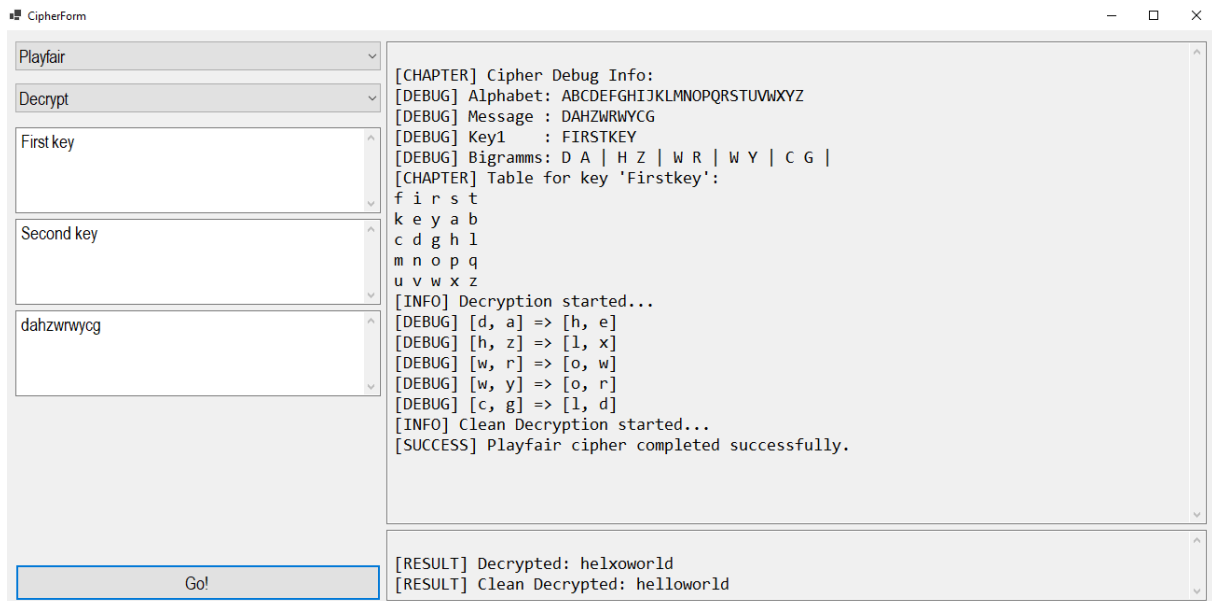


Figure 4: Playfair decrypt in WinForms mode

## 4.2 Winston

```
[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 2
[REQUIREMENT] Write message: hello world
[REQUIREMENT] Write key: first key
[REQUIREMENT] Write second key: second key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 1
[CHAPTER] Cipher Debug Info:
Alphabet: abcdefghijklmnopqrstuvwxyz
Message : HELLOWORLD
Key1 : FIRSTKEY
Key2 : SECONDKEY
Bigrams: H E | L X | O W | O R | L D |
[CHAPTER] Table for key 'firstkey':
f i r s t
k e y a b
c d g h l
m n o p q
u v w x z
[CHAPTER] Table for key 'secondkey':
s e c o n
d k y a b
f g h i l
m p q r t
u v w x z
[INFO] Encryption started...
Bigram: h, in Table1 (2, 3) -> Result: d, in Table1 - (2, 1)
Bigram: e, in Table2 (0, 1) -> Result: o, in Table2 - (0, 3)
Bigram: l, in Table1 (2, 4) -> Result: h, in Table1 - (2, 3)
Bigram: x, in Table2 (4, 3) -> Result: z, in Table2 - (4, 4)
Bigram: o, in Table1 (3, 2) -> Result: o, in Table1 - (3, 2)
Bigram: w, in Table2 (4, 2) -> Result: w, in Table2 - (4, 2)
Bigram: o, in Table1 (3, 2) -> Result: p, in Table1 - (3, 3)
Bigram: r, in Table2 (3, 3) -> Result: q, in Table2 - (3, 2)
Bigram: l, in Table1 (2, 4) -> Result: c, in Table1 - (2, 0)
Bigram: d, in Table2 (1, 0) -> Result: b, in Table2 - (1, 4)
[RESULT] Encrypted: dohzowpqcb

[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 2
[REQUIREMENT] Write message: dohzowpqcb
[REQUIREMENT] Write key: first key
[REQUIREMENT] Write second key: second key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 2
[CHAPTER] Cipher Debug Info:
Alphabet: abcdefghijklmnopqrstuvwxyz
Message : DOHZOWPQCB
Key1 : FIRSTKEY
Key2 : SECONDKEY
Bigrams: D O | H Z | O W | P Q | C B |
[CHAPTER] Table for key 'firstkey':
f i r s t
k e y a b
c d g h l
m n o p q
u v w x z
[CHAPTER] Table for key 'secondkey':
s e c o n
d k y a b
f g h i l
m p q r t
u v w x z
[INFO] Decryption started...
Bigram: d, in Table1 (2, 1) -> Result: h, in Table1 - (2, 3)
Bigram: o, in Table2 (0, 3) -> Result: e, in Table2 - (0, 1)
Bigram: h, in Table1 (2, 3) -> Result: l, in Table1 - (2, 4)
Bigram: z, in Table2 (4, 4) -> Result: x, in Table2 - (4, 3)
Bigram: o, in Table1 (3, 2) -> Result: o, in Table1 - (3, 2)
Bigram: w, in Table2 (4, 2) -> Result: w, in Table2 - (4, 2)
Bigram: p, in Table1 (3, 3) -> Result: o, in Table1 - (3, 2)
Bigram: q, in Table2 (3, 2) -> Result: r, in Table2 - (3, 3)
Bigram: c, in Table1 (2, 0) -> Result: l, in Table1 - (2, 4)
Bigram: b, in Table2 (1, 4) -> Result: d, in Table2 - (1, 0)
[RESULT] Decrypted: helloworld
```

Figure 5: Winston in console mode

The screenshot shows a WinForms application window titled 'CipherForm'. On the left, there's a sidebar with a 'Winston' dropdown menu and an 'Encrypt' button. Below these are input fields for 'First key', 'Second key', and a text area containing 'hello world'. At the bottom left is a 'Go!' button. The main area on the right displays the application's output, which includes chapter headers, requirements, and a detailed debug log of the encryption process, ending with the encrypted message 'dohzowpqcb'.

Figure 6: Winston encrypt in WinForms mode

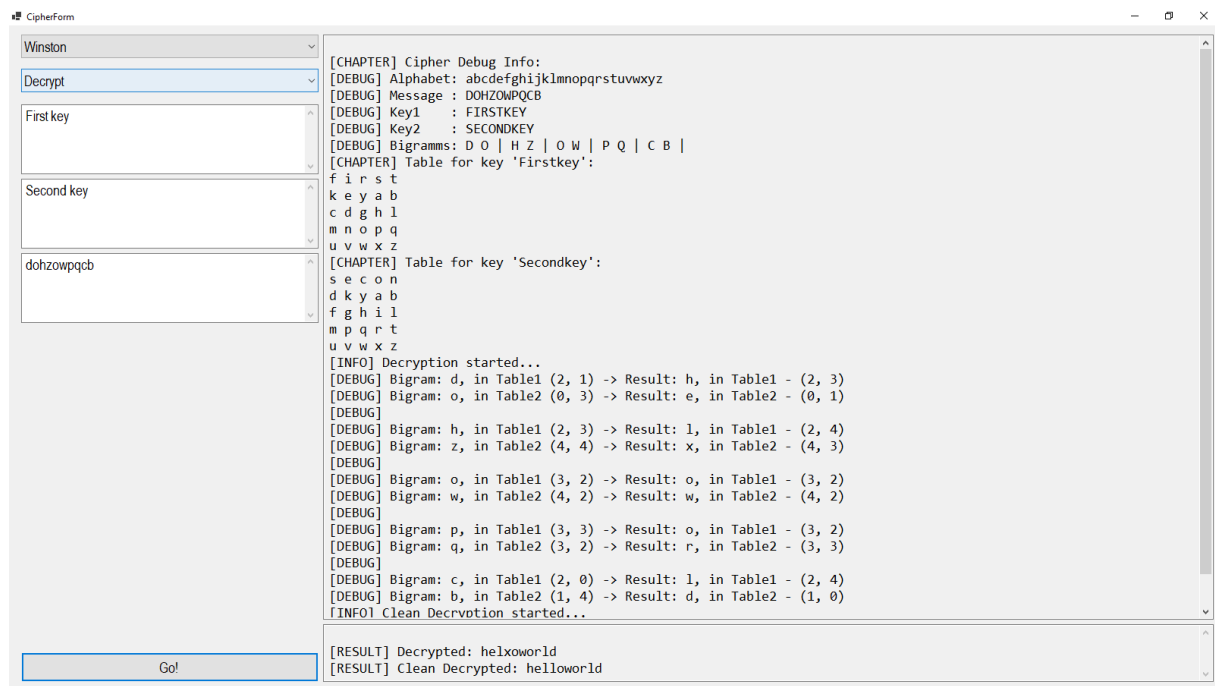


Figure 7: Winston decrypt in WinForms mode

## 4.3 Vigenere

```
[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 3
[REQUIREMENT] Write message: helloworld
[REQUIREMENT] Write key: first key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 1
[CHAPTER] Cipher Debug Info:
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Message : HELLOWORLD
Key : FIRSTKEYFI
[CHAPTER] The Vigenere's table:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B c d e f g h i j k l m n o p q r s t u v w x y z a
C d e f g h i j k l m n o p q r s t u v w x y z a b
D e f g h i j k l m n o p q r s t u v w x y z a b c
E f g h i j k l m n o p q r s t u v w x y z a b c d
F g h i j k l m n o p q r s t u v w x y z a b c d e
G h i j k l m n o p q r s t u v w x y z a b c d e f
H i j k l m n o p q r s t u v w x y z a b c d e f g
I j k l m n o p q r s t u v w x y z a b c d e f g h
J k l m n o p q r s t u v w x y z a b c d e f g h i
K l m n o p q r s t u v w x y z a b c d e f g h i j
L m n o p q r s t u v w x y z a b c d e f g h i j k
M n o p q r s t u v w x y z a b c d e f g h i j k l
N o p q r s t u v w x y z a b c d e f g h i j k l m
O p q r s t u v w x y z a b c d e f g h i j k l m n
P q r s t u v w x y z a b c d e f g h i j k l m n o
Q r s t u v w x y z a b c d e f g h i j k l m n o p
R s t u v w x y z a b c d e f g h i j k l m n o p q
S t u v w x y z a b c d e f g h i j k l m n o p q r
T u v w x y z a b c d e f g h i j k l m n o p q r s
U v w x y z a b c d e f g h i j k l m n o p q r s t
V w x y z a b c d e f g h i j k l m n o p q r s t u
W x y z a b c d e f g h i j k l m n o p q r s t u v
X y z a b c d e f g h i j k l m n o p q r s t u v w
Y z a b c d e f g h i j k l m n o p q r s t u v w x
Z a b c d e f g h i j k l m n o p q r s t u v w x y
[INFO] Encryption started...
[h, f] -> [m]
[e, i] -> [a]
[l, r] -> [c]
[l, s] -> [d]
[o, t] -> [h]
[w, k] -> [g]
[o, e] -> [s]
[r, y] -> [p]
[l, f] -> [q]
[d, i] -> [l]
[RESULT] Encrypted: mmcdhgspql
[SUCCESS] Vigenere cipher completed successfully.

[CHAPTER] Select UI mode:
1. Console
2. WinForms
[REQUIREMENT] Write mode number: 1
[CHAPTER] Change the cipher's number (1 - Playfair, 2 - Winston, 3 - Vigenere):
[REQUIREMENT] Write cipher's number: 3
[REQUIREMENT] Write message: mmcdhgspql
[REQUIREMENT] Write key: first key
[CHAPTER] Change the operation (1 - Encrypt, 2 - Decrypt):
[REQUIREMENT] Write operation: 2
[CHAPTER] Cipher Debug Info:
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Message : MMCDHGSPQL
Key : FIRSTKEYFI
[CHAPTER] The Vigenere's table:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B c d e f g h i j k l m n o p q r s t u v w x y z a
C d e f g h i j k l m n o p q r s t u v w x y z a b
D e f g h i j k l m n o p q r s t u v w x y z a b c
E f g h i j k l m n o p q r s t u v w x y z a b c d
F g h i j k l m n o p q r s t u v w x y z a b c d e
G h i j k l m n o p q r s t u v w x y z a b c d e f
H i j k l m n o p q r s t u v w x y z a b c d e f g
I j k l m n o p q r s t u v w x y z a b c d e f g h
J k l m n o p q r s t u v w x y z a b c d e f g h i
K l m n o p q r s t u v w x y z a b c d e f g h i j
L m n o p q r s t u v w x y z a b c d e f g h i j k
M n o p q r s t u v w x y z a b c d e f g h i j k l
N o p q r s t u v w x y z a b c d e f g h i j k l m
O p q r s t u v w x y z a b c d e f g h i j k l m n
P q r s t u v w x y z a b c d e f g h i j k l m n o
Q r s t u v w x y z a b c d e f g h i j k l m n o p
R s t u v w x y z a b c d e f g h i j k l m n o p q
S t u v w x y z a b c d e f g h i j k l m n o p q r
T u v w x y z a b c d e f g h i j k l m n o p q r s
U v w x y z a b c d e f g h i j k l m n o p q r s t
V w x y z a b c d e f g h i j k l m n o p q r s t u
W x y z a b c d e f g h i j k l m n o p q r s t u v
X y z a b c d e f g h i j k l m n o p q r s t u v w
Y z a b c d e f g h i j k l m n o p q r s t u v w x
Z a b c d e f g h i j k l m n o p q r s t u v w x y
[INFO] Decryption started...
[m, f] -> [h]
[m, i] -> [e]
[c, r] -> [l]
[d, s] -> [l]
[h, t] -> [o]
[g, k] -> [w]
[s, e] -> [o]
[p, y] -> [r]
[q, f] -> [l]
[l, i] -> [d]
[RESULT] Decrypted: helloworld
[INFO] Clean Decryption started...
[RESULT] Clean Decrypted: helloworld
[SUCCESS] Vigenere cipher completed successfully.
```

Figure 8: Vigenere in console mode

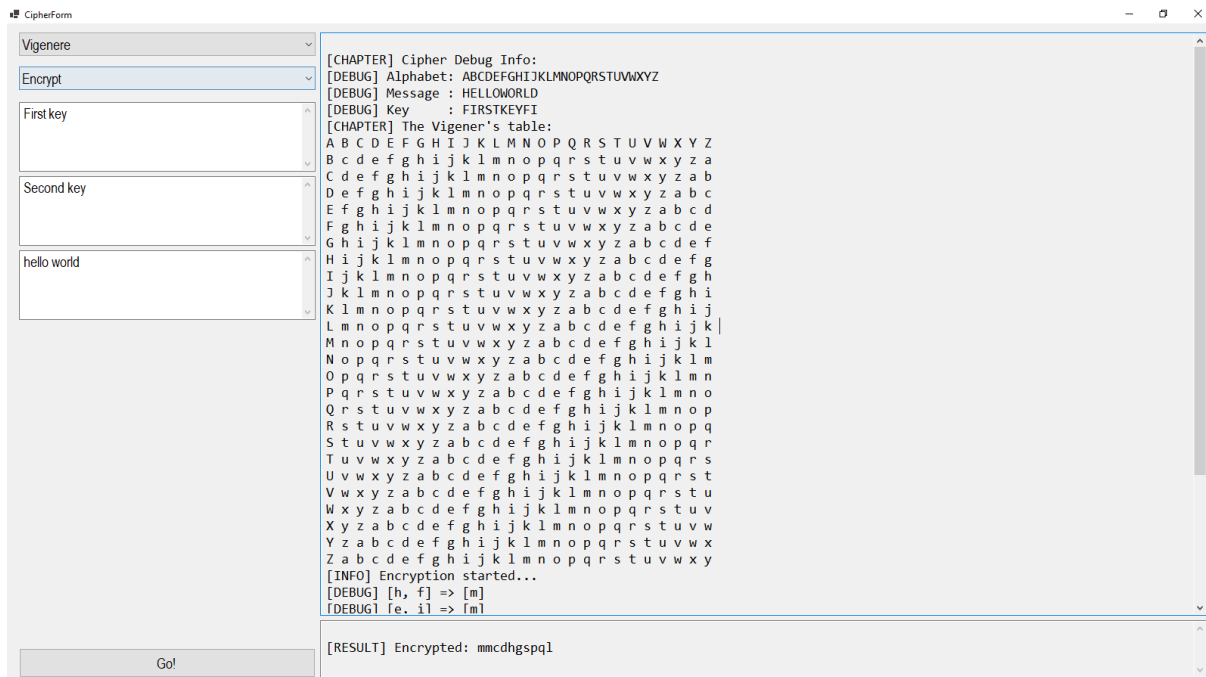


Figure 9: Vigenere encrypt part 1 in WinForms mode

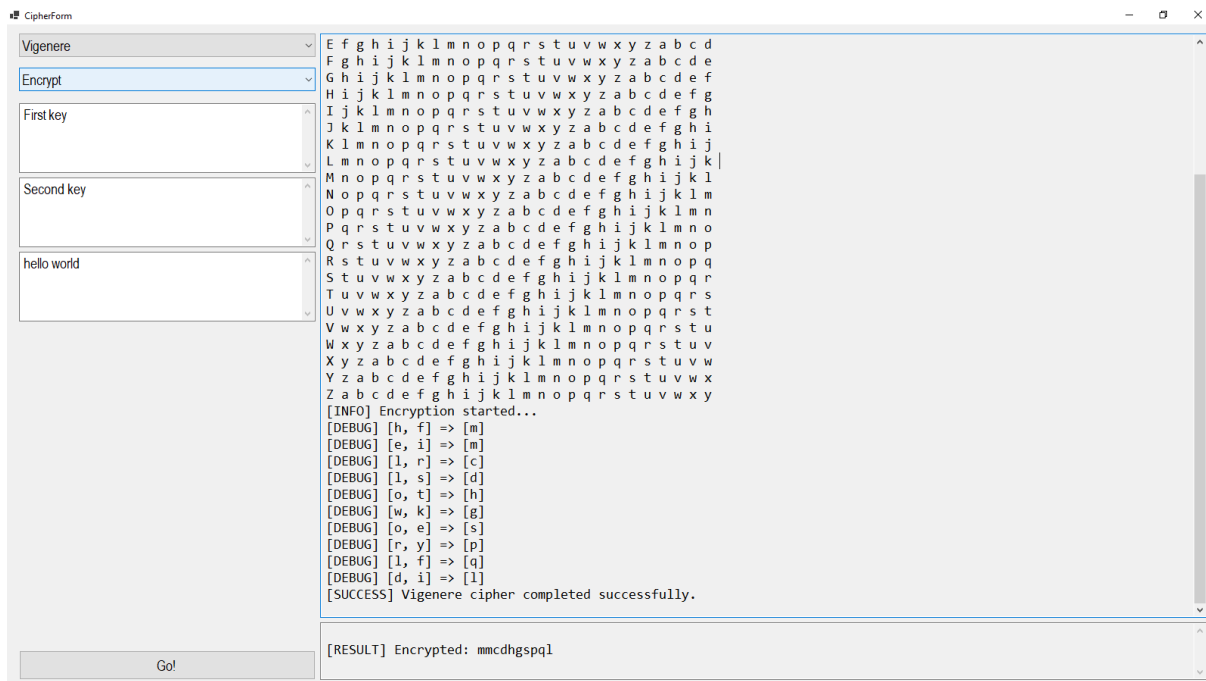


Figure 10: Vigenere encrypt part 2 in WinForms mode



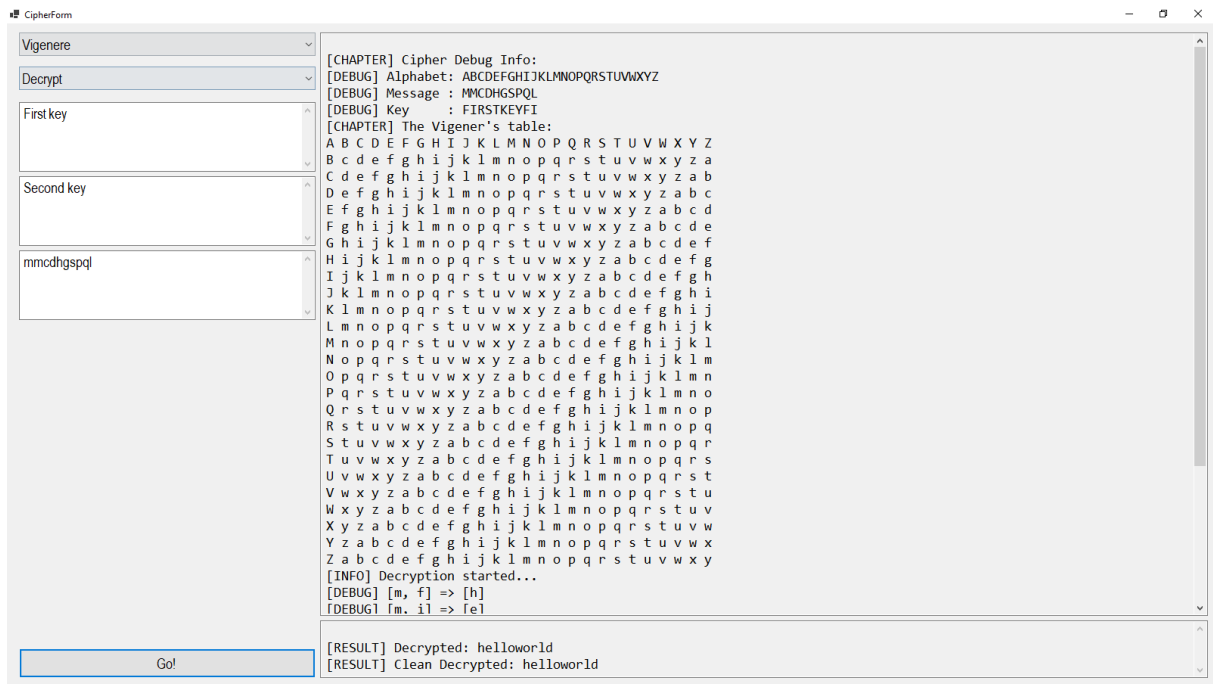


Figure 11: Vigenere decrypt part 1 in WinForms mode

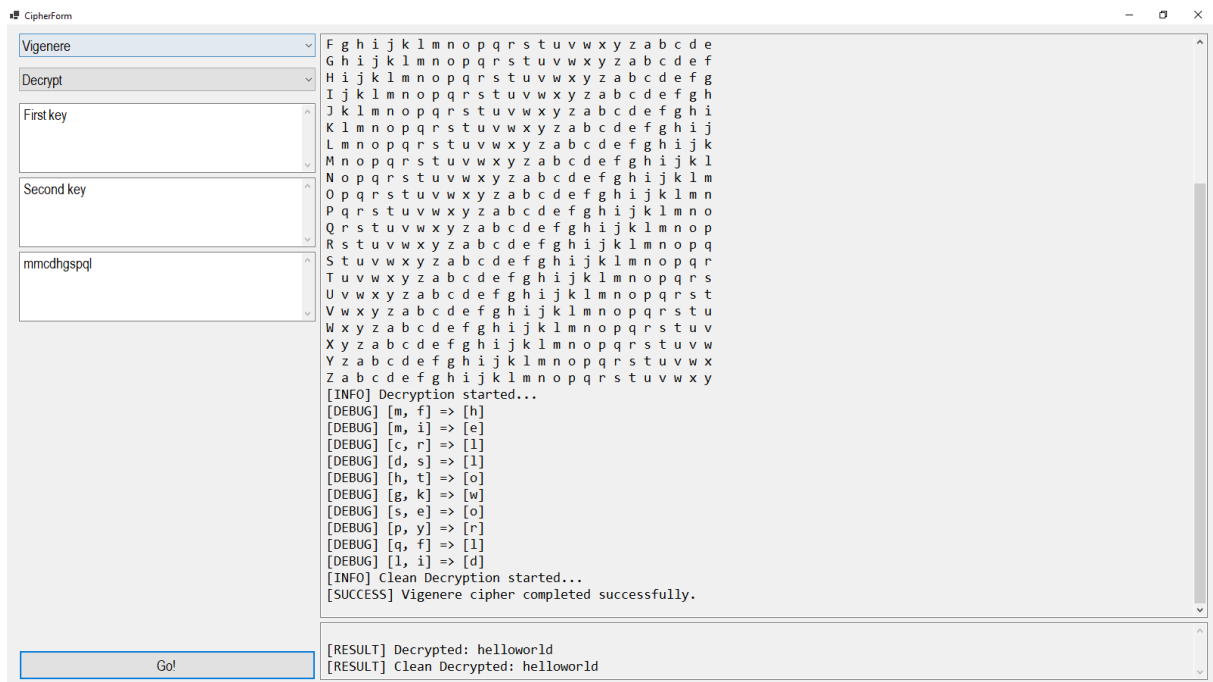


Figure 12: Vigenere decrypt part 2 in WinForms mode