FACULTY OF COMPUTING & INFORMATION TECHNOLOGY
KING ABDULAZIZ UNIVERSITY

FCIT
KAU

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز

Cipher Application Project

Information Security - CPCS 425

Course Instructor: Dr. Reemah Alhebshi

Table of Contents

Abstract:

This report presents the pseudocode and Flowchart of the Cipher Application and the screenshots for the encryption & decryption processes.

The pseudocode of Cipher Application methods (Encryption & Decryption):

```
Class Cipher:
// Method: Encryption
// Input: line (string)
// Output: encrypted Line (string)

1. Remove any leading or trailing whitespace from the line.
   line → line.trim()

2. Convert all letters in the string to UPPERCASE.
   line → line.toUpperCase()

3. Move the first half of the string to be the last half.
   mid → length(line) / 2
   first_half → substring(line, 0, mid)
   last_half → substring(line, mid + length(line) % 2)
   line → last_half + first_half

4. Swap the first 2 characters of the line with the last two
characters.
   first_two → substring(line, 0, 2)
   last_two → substring(line, length(line) - 2)
   middle → substring(line, 2, length(line) - 2)
   line → last_two + middle + first_two
```

5. Swap the two characters immediately to the left of the middle of the string with the two characters that immediately follow them.

```
mid → length(line) / 2
left → substring(line, mid - 2, 2)
right → substring(line, mid + 2, 2)
middle → substring(line, mid - 2, 4)
line → substring(line, 0, mid - 2) + right + middle + left + substring(line, mid + 4)
```

6. Perform the following character substitutions:

```
replacements → {
    'A' → '@'
    'E' → '='
    'I' → '!'
    'J' → '?'
    'O' → '*'
    'P' → '#'
    'R' → '&'
    'S' → '$'
    'T' → '+'
    'V' → '^'
    'X' → '%'
    ' ' → '_'
}
for each character in line:
    if character is in replacements:
        replace character with replacements[character]
```

7. The result line is the encrypted output.

```
// Method: Decryption
// Input: line (string)
// Output: decrypted Line (string)
1. Perform the following character substitutions:
   replacements → {
      '@' → 'A'
      '=' → 'E'
      '!' → 'I'
      '?' → 'J'
      '*' → 'O'
      '#' → 'P'
      '&' → 'R'
      '$'→ 'S'
      '+' → 'T'
      '^' → 'V'
      '%' →'X',
      '_' → ' ‘ // (space)
   }
   for each character in line:
      if character is in replacements:
         replace character with replacements[character]

2. Remove any leading or trailing whitespace from the line.
   line → line.trim()

3. Swap the two characters immediately to the right of the middle of
the string with the two characters that immediately precede them.
```

```
   mid → length(line) / 2

   left → substring(line, mid - 2, 2)

   right → substring(line, mid, 2)

   middle → substring(line, mid - 2, 2)

   line → substring(line, 0, mid - 2) + right + middle + left +
substring(line, mid + 2)
```

4. Swap the first 2 characters of the line with the last two characters.

```
   first_two → substring(line, 0, 2)

   last_two → substring(line, length(line) - 2)

   middle → substring(line, 2, length(line) - 2)

   line → last_two + middle + first_two
```

5. Move the first half of the string to be the last half.

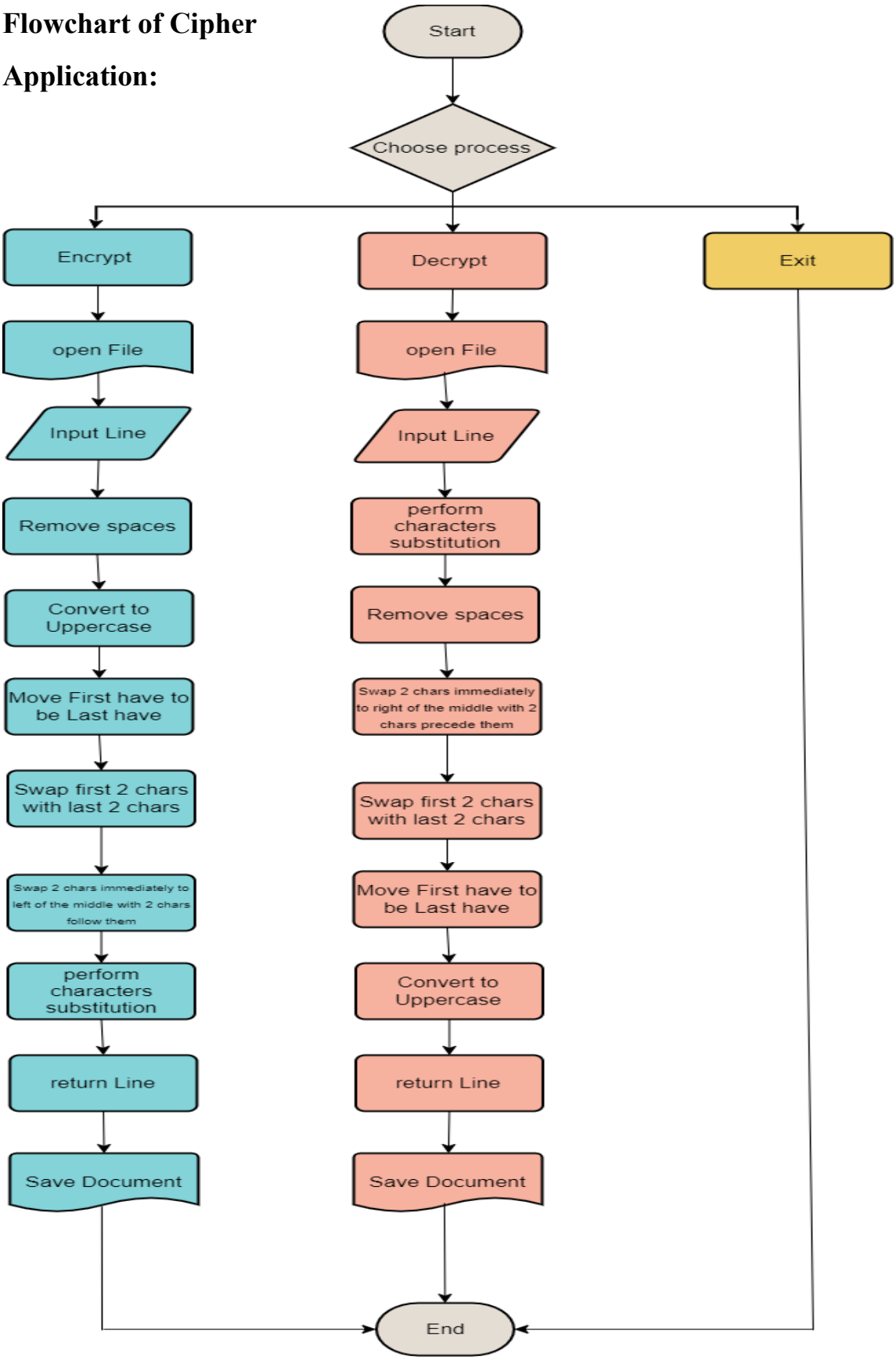
```
   mid → length(line) / 2

   first_half → substring(line, 0, mid - length(line) % 2)

   last_half → substring(line, mid - length(line) % 2)

   line = last_half + first_half
```

6. Convert all letters in the string to lowercase.

```
   line → line.toLowerCase()
```

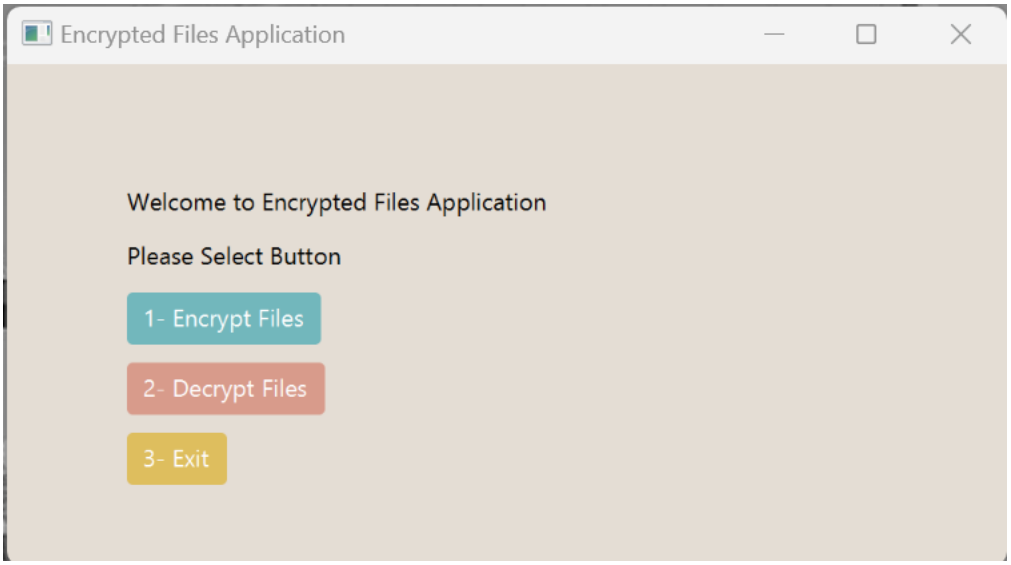
7. The result line is the encrypted output.

Flowchart of Cipher Application:

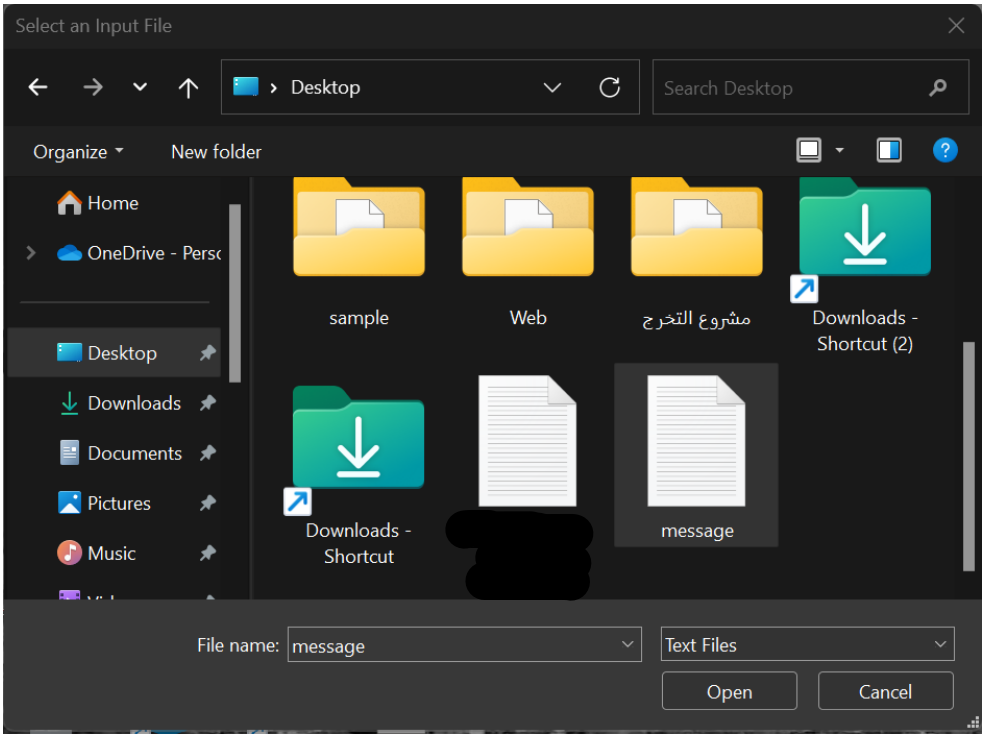


Cipher application screenshots:

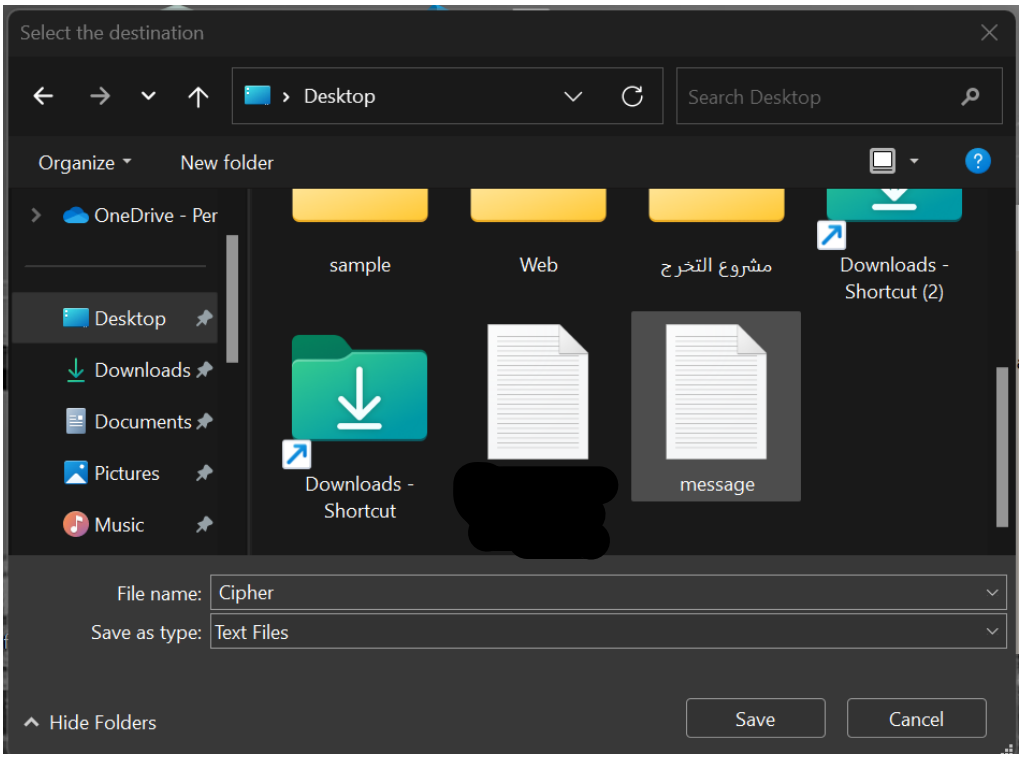
The application's main GUI



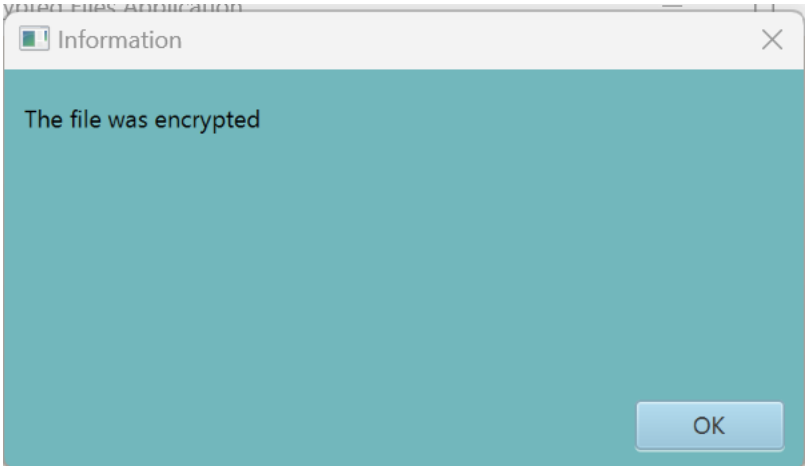
1- The user selects Encrypt file: >> select an input file



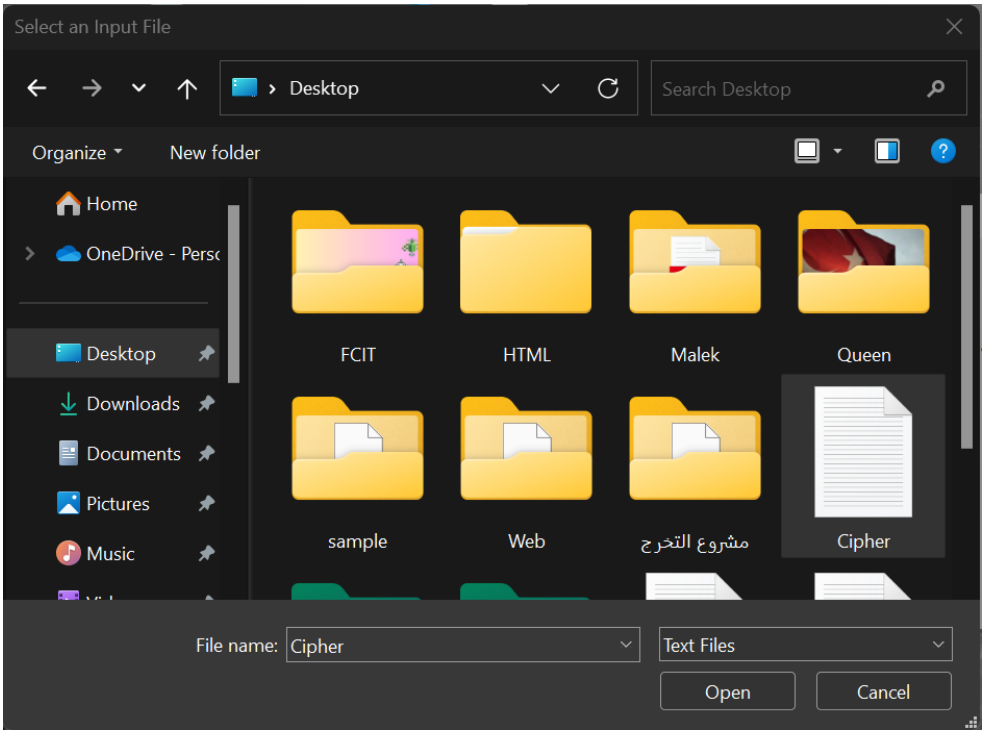
Select the destination (with a default (Cipher) name of the output file)



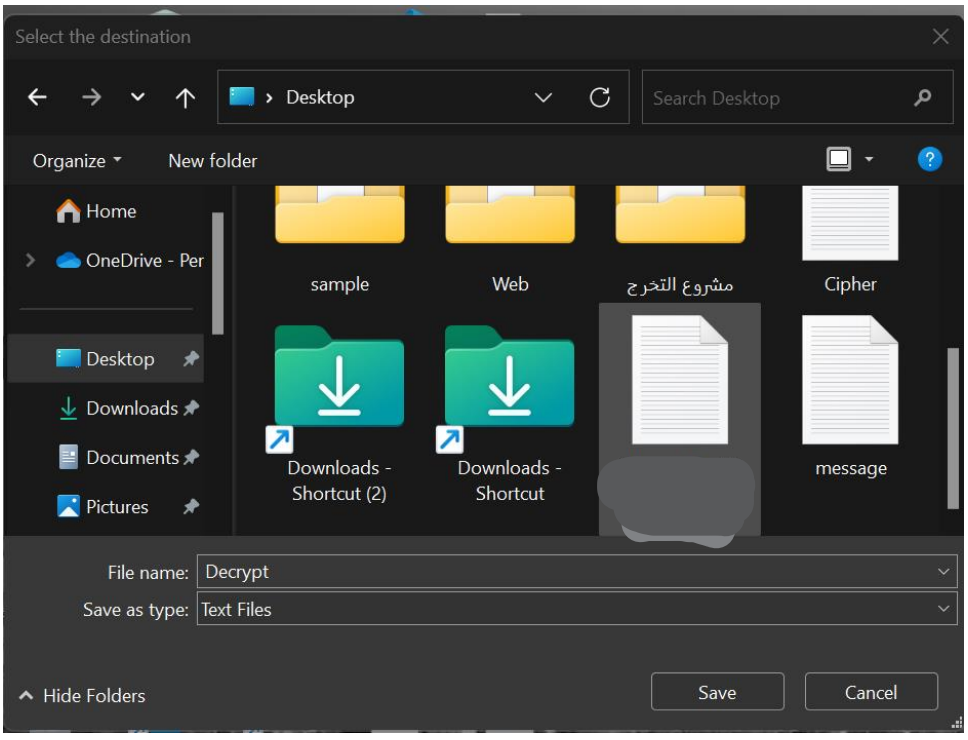
The file is encrypted.



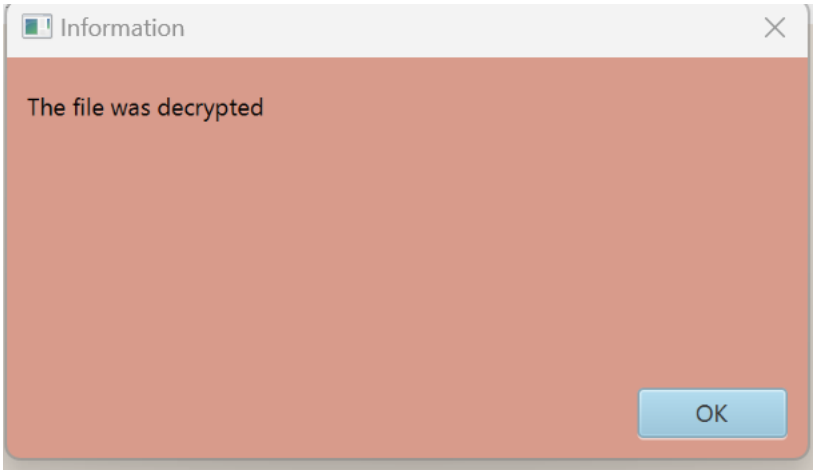
2- The user selects Decrypt file:>> select an input file



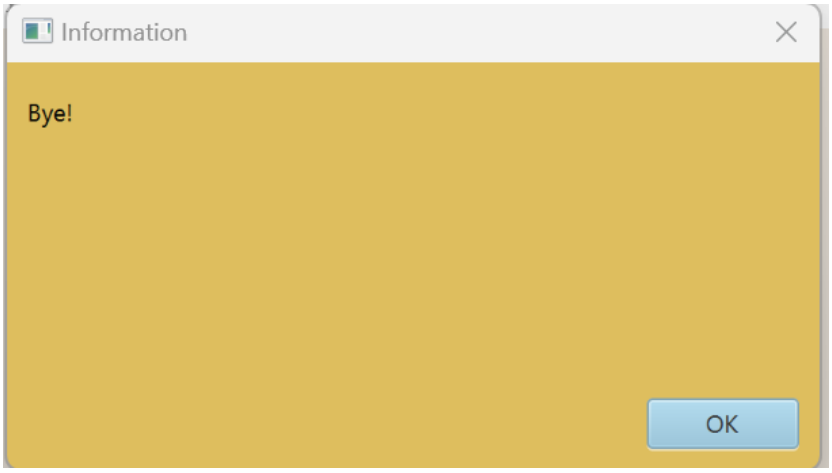
Select the destination (with a default name (Decrypt) of the output file)



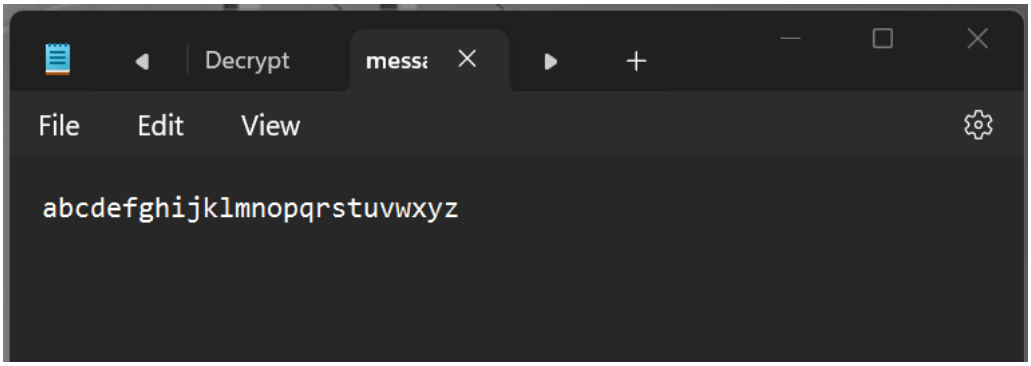
The file is decrypted.



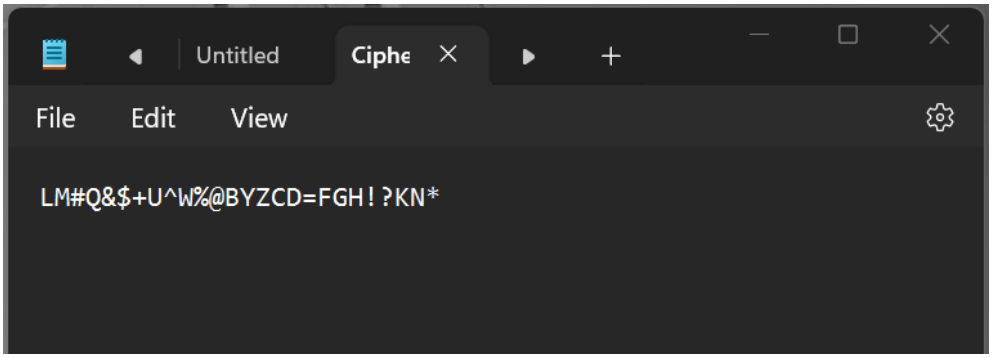
3- The user selects Exit:



The message (input file for Encryption method):



The cipher (output file from Encryption method and input file for Decryption method):



The Decrypt (output file from Decryption method):