KINGDOM OF SAUDI ARABIA
MINISTRY OF EDUCATION
TAIBAH UNIVERSITY
COLLEGE OF COMPUTER SCEIENCE

المملكة العربية السعودية
وزارة التعـــــليم
جامعة طيبة / كلية علوم الحاسب

Security in Computing

CS433

Text Encryption & Decryption Tool

Section: M5

Students Work:
Mohammad Gumgumji
Waseem aljumah
Ayman Aljuhani

IDs:
4100072
4206111
4104570

Supervised by:
Talal Noor

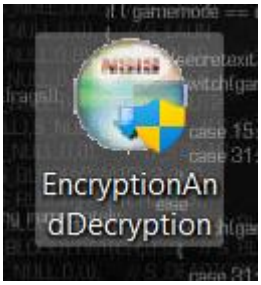
Introduction:

This project mainly focuses on creating an algorithm that allows the user to encrypt and decrypt encrypted text using the **Caesar cipher** and the **Vigenère cipher**.
With digital development, hacks have become more frequent, and we must protect our data and increase security. The project will be to create a simple tool to encrypt and decrypt text that ensures that only authorized individuals who have the encryption key can decrypt the text and access the original text, maintaining the confidentiality of the data.

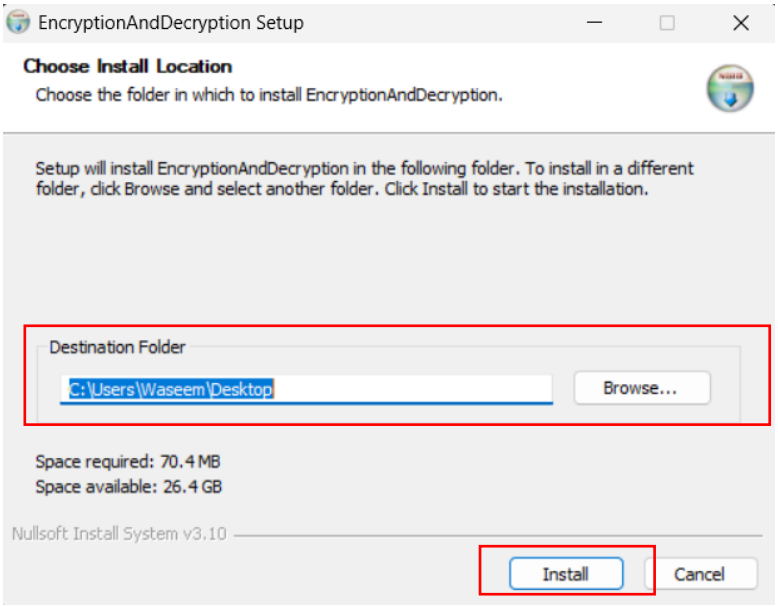
Steps to install the tool:

1- Download the file "**EncryptionAndDecryption.exe**"

2- Double-click "**EncryptionAndDecryption.exe**" on the file after installation

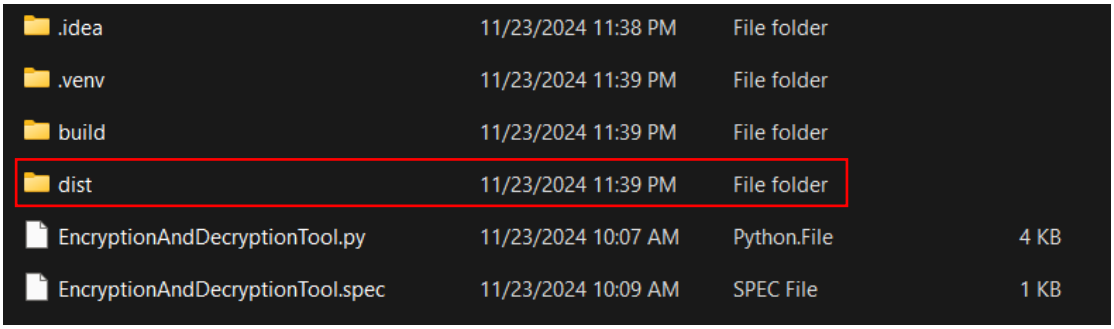


3- Choose the location where you want to install the program and click install



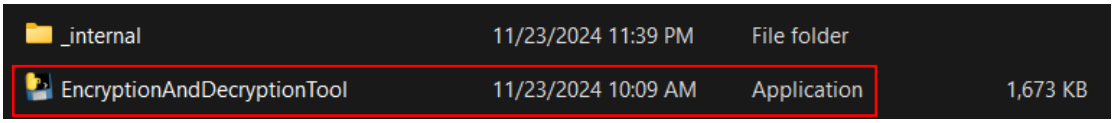
4- Open the new "**EncryptionAndDecryptionl**" installed file

5- Open the "**dist**" file



6- Open the "**EncryptionAndDecryptionTool**" file

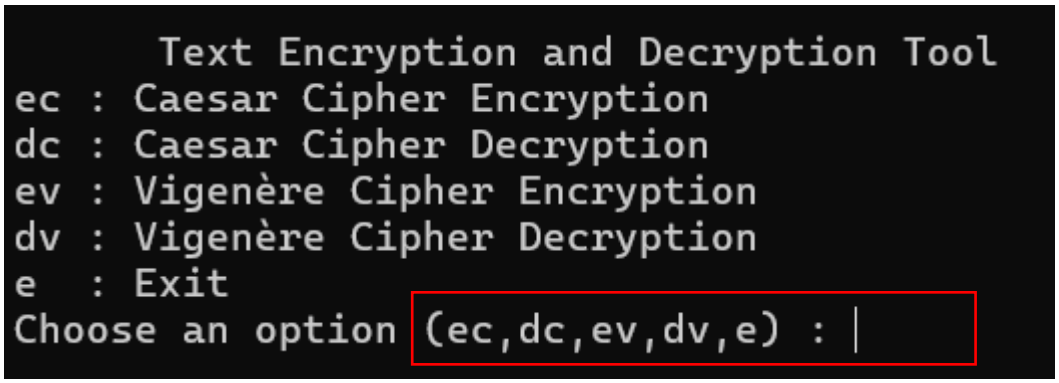
7- Open the program "**EncryptionAndDecryptionTool**"



How to Use:

First step:

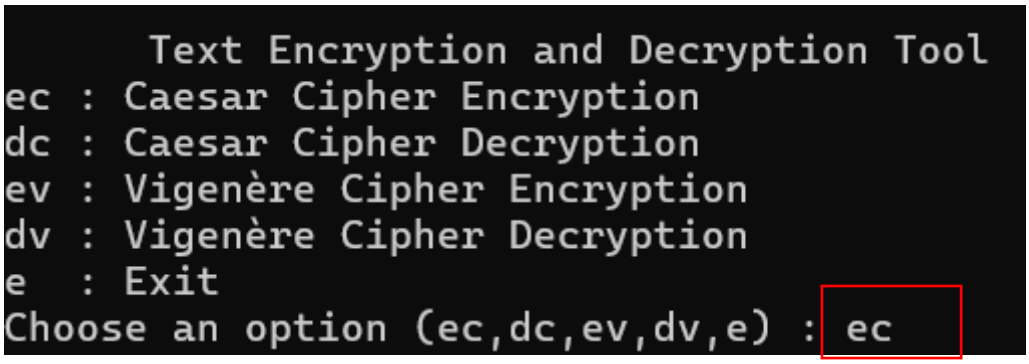
Select a symbol from the five available symbols



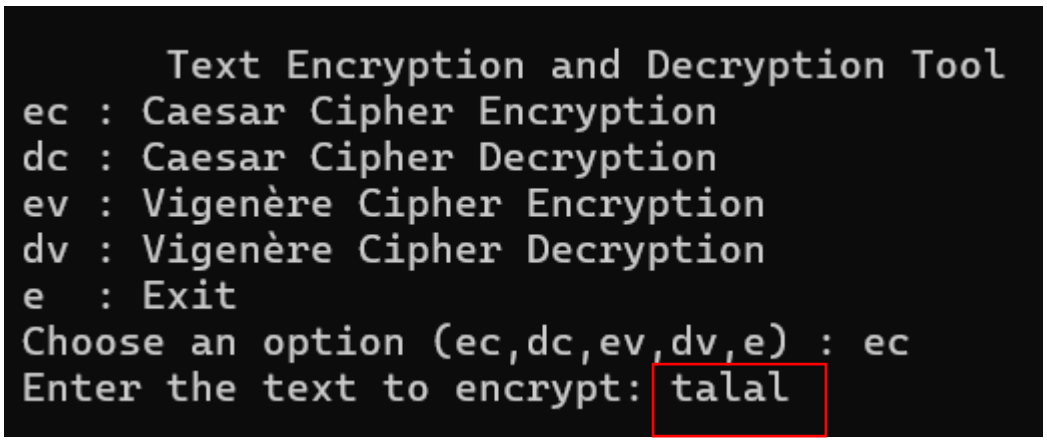
Second step:

- If you want to **encrypt** text using **Caesar cipher**,

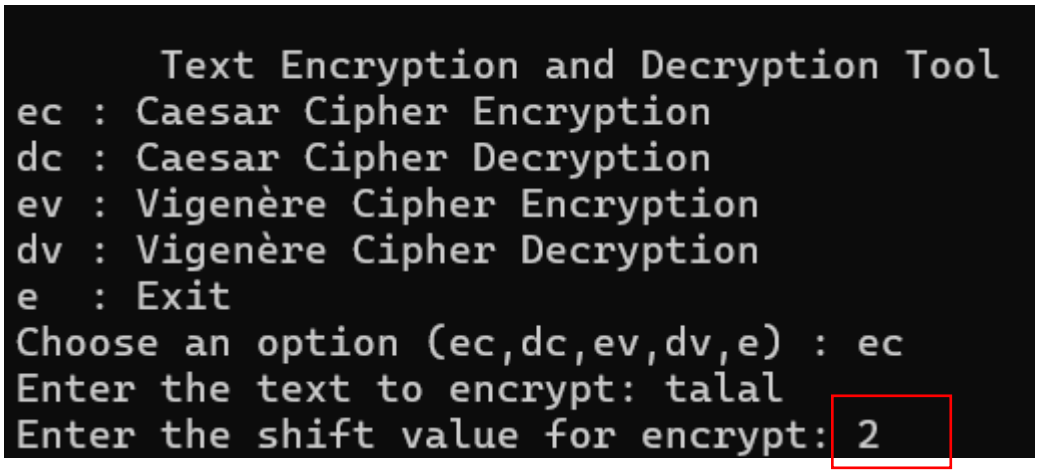
1- choose ec



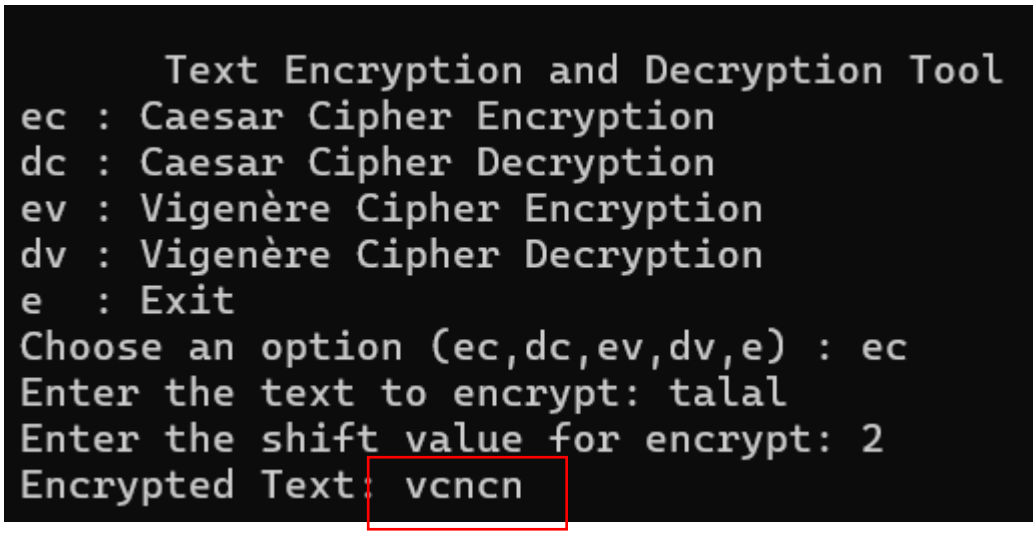
2- Enter the text to be encrypted



3- Enter the amount of shift you want to have and it will be the encryption key to decrypt the text.

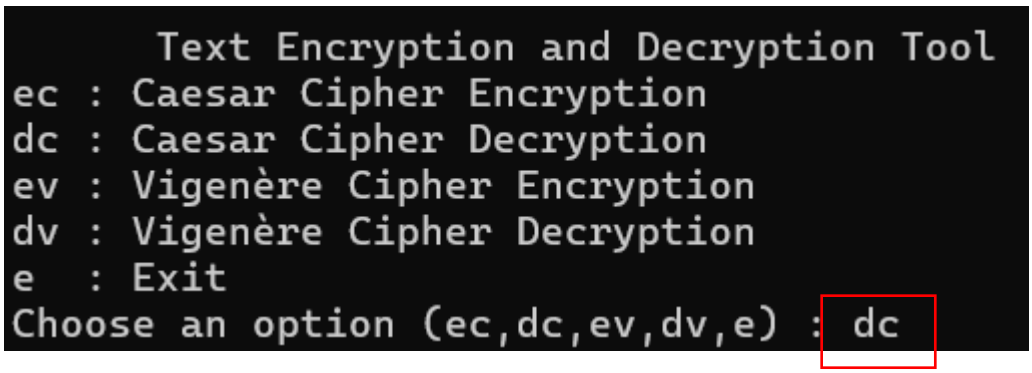


4- The encrypted text will be displayed to you



- If you want to **decrypt** a text that was encrypted with **Caesar cipher**

1- choose dc



2- Enter the text to be decrypted

```
      Text Encryption and Decryption Tool
ec : Caesar Cipher Encryption
dc : Caesar Cipher Decryption
ev : Vigenère Cipher Encryption
dv : Vigenère Cipher Decryption
e  : Exit
Choose an option (ec,dc,ev,dv,e) : dc
Enter the text to decrypt: vcncn
```

3- Enter the encryption key to decrypt the text, which is the amount of shift that was made for the encryption

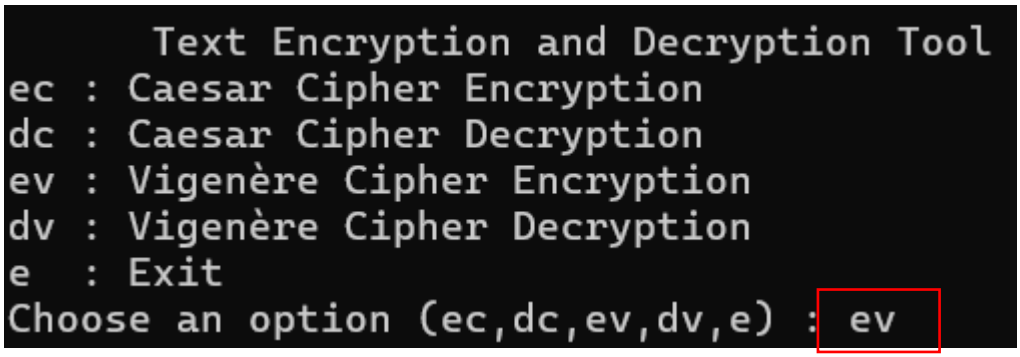
```
      Text Encryption and Decryption Tool
ec : Caesar Cipher Encryption
dc : Caesar Cipher Decryption
ev : Vigenère Cipher Encryption
dv : Vigenère Cipher Decryption
e  : Exit
Choose an option (ec,dc,ev,dv,e) : dc
Enter the text to decrypt: vcncn
Enter the shift value for decrypt: 2
```

4- The decrypted text will be displayed to you

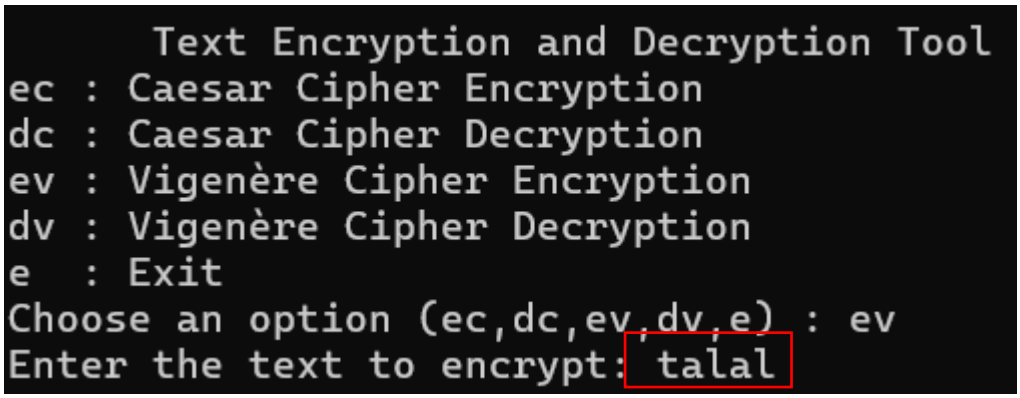
```
      Text Encryption and Decryption Tool
ec : Caesar Cipher Encryption
dc : Caesar Cipher Decryption
ev : Vigenère Cipher Encryption
dv : Vigenère Cipher Decryption
e  : Exit
Choose an option (ec,dc,ev,dv,e) : dc
Enter the text to decrypt: vcncn
Enter the shift value for decrypt: 2
Decrypted Text: talal
```

- If you want to **encrypt** text using **Vigenère cipher**

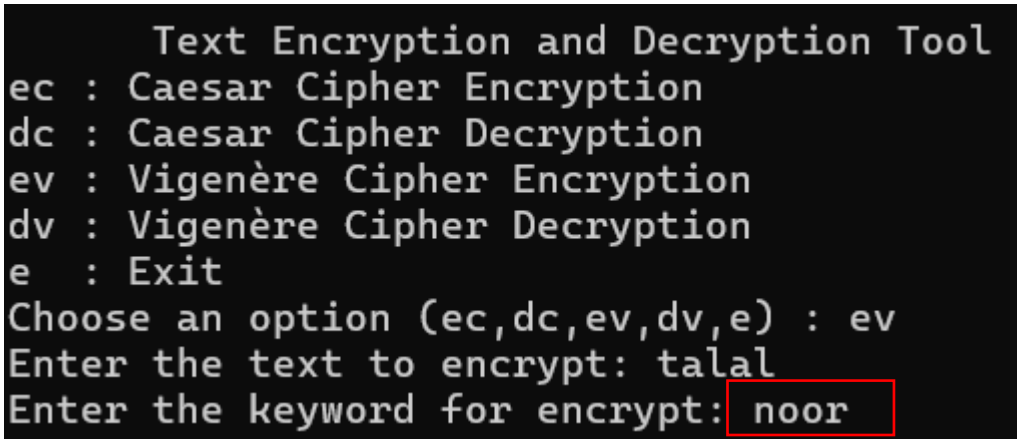
1- choose ev



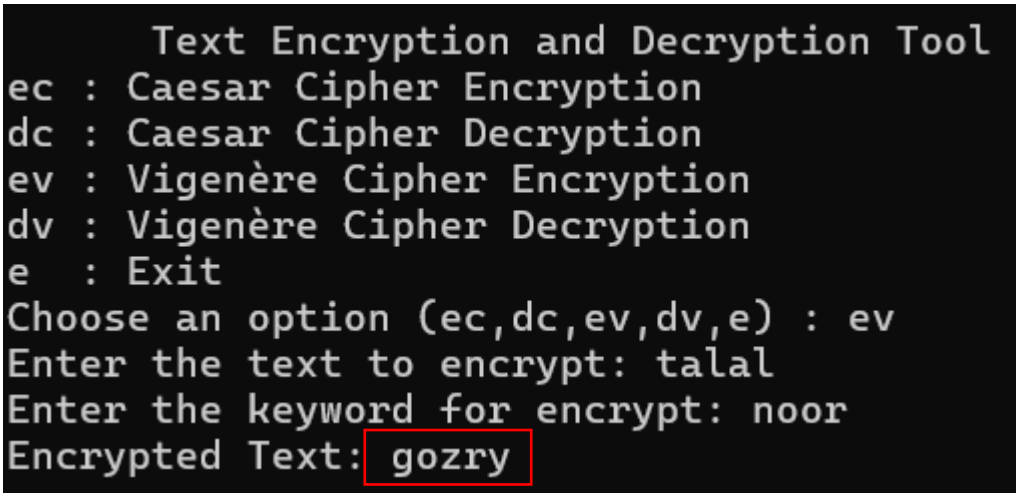
2- Enter the text to be encrypted



3- Enter a key word to encrypt the text and let it be the encryption key

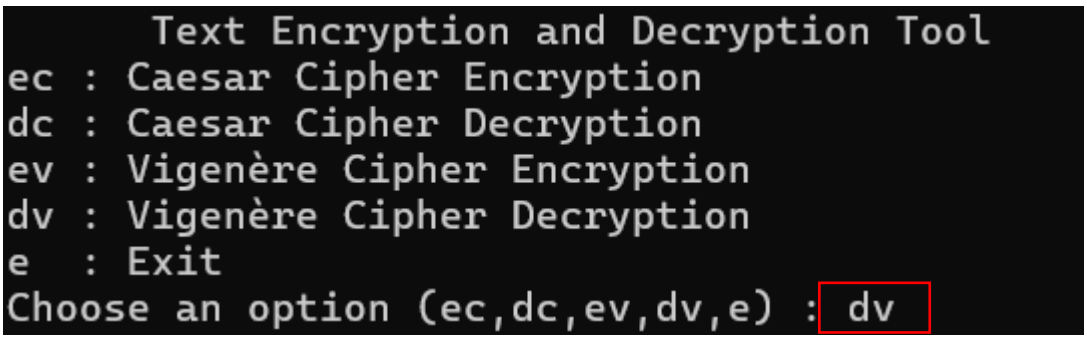


4- The encrypted text will be displayed to you

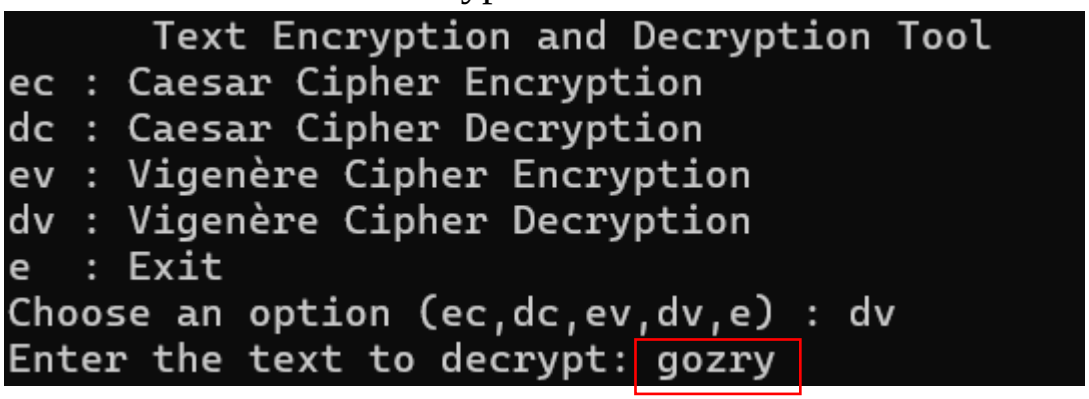


- If you want to **decrypt** a text that was encrypted with **Vigenère cipher**

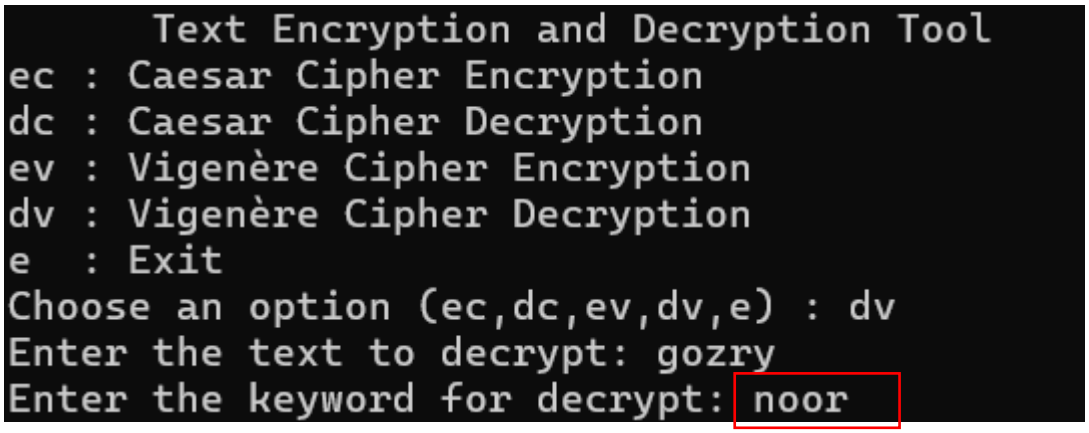
1- choose dv



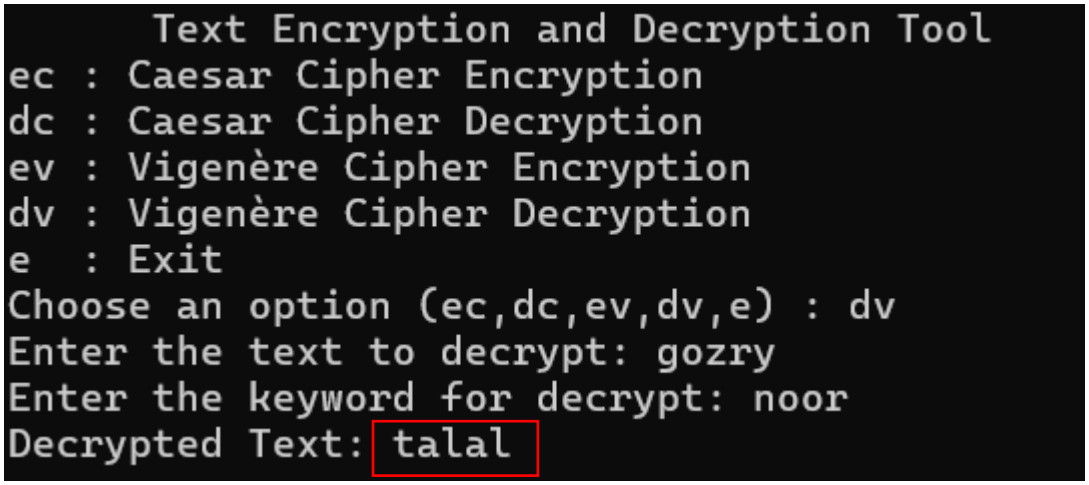
2- Enter the text to be decrypted



3- Enter the key word that was used to encrypt the text and the text was decrypted

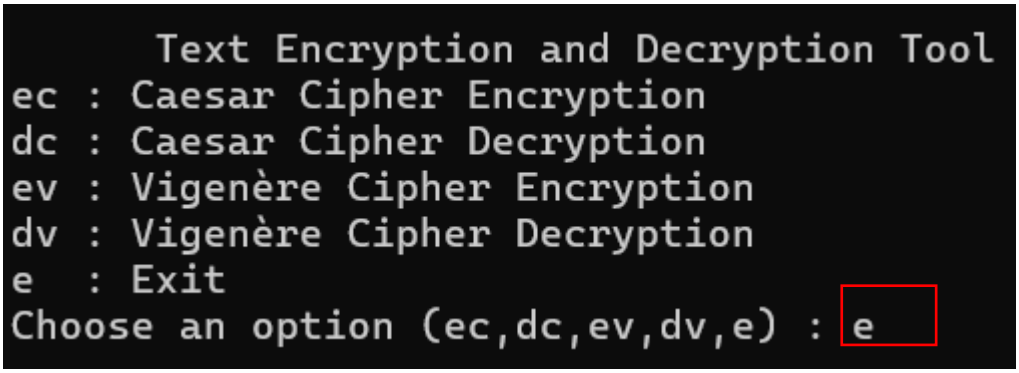


4- The decrypted text will be displayed to you



• If you want to exit

1- Choose e



Encryption Techniques:

1- Caesar cipher

Caesar cipher is an encryption technique that shifts each letter in plain text a fixed number of positions in the alphabet, the amount of shift is chosen to encrypt the word. The shift amount is chosen and each letter in the word is shifted by the specified shift amount.

Example of encryption:
The text is: TALAL, shift=2

The letter T will be replaced by the letter V because T then U then V, and shift 2 if it will be V
The letter A will be replaced by the letter C because A then B then C, and shift 2 if it will be C
The letter L will be replaced by the letter N because L then M then N, and shift 2 if it will be N
The letter A will be replaced by the letter C because A then B then C, and shift 2 if it will be C
The letter L will be replaced by the letter N because L then M then N, and shift 2 if it will be N
So the encrypted word is "VCNCN"

Another example of encryption:
The text is: Welcome to Computer Security Lectures, shift=3
The Encrypted text is: Zhofrph wr Frpsxwhu Vhfxulwb Ohfwxuhv

To decrypt the text, the process is reversed by moving each letter back the same amount of shift.

Example of decryption:
The Encrypted text is: VCNCN, shift=2
-The letter V will be changed to the letter T because the letter V is preceded by U and before it is T, and the shift 2 if it will be T
-The letter C will be changed to the letter A because the letter C is preceded by B and before it is A, and the shift 2 if it will be A
-The letter N will be changed to the letter L because the letter N is preceded by M and before it is L, and the shift 2 if it will be L
-The letter C will be changed to the letter A because the letter C is preceded by B and before it is A, and the shift 2 if it will be A
-The letter N will be changed to the letter L because the letter N is preceded by M and before it is L, and the shift 2 if it will be L
So the plaintext is "TALAL"

Another example of decryption:
The Encrypted text is: Pxevhfx mh Mtbuta Ngboxklbmr, shift=45
The plaintext text is: Welcome to Taibah University

2- Vigenère cipher

The Vigenère cipher is a method of encrypting text using a series of different Caesar ciphers based on the letters of a keyword. Unlike the Caesar cipher, which uses a fixed transformation for each letter, the Vigenère cipher uses multiple transformations, making it more secure.

1- Choose a keyword: A keyword is selected (for example, "NOOR"). This keyword is repeated to match the length of the plaintext message. For example, if the plaintext is "TALAL", the keyword "NOOR" will be repeated as "NOORN".

2- The position of each letter of the keyword is calculated starting from 0, where A is 0, B is 1 ... And Z is 25
Based on the number, the base letter is shifted until we reach the new letter, and it is applied to each letter of the text to be encrypted with its corresponding base word.

Example of encryption:
The text is: TALAL, the Keyword is NOOR

T A L A L
N OOR N

-The letter T corresponds to the letter N in the Keyword, and the position of the letter N is 13, so it will be shifted 13 from the letter T and replaced with the letter G
-The letter A corresponds to the letter O in the Keyword, and the position of the letter O is 14, so it will be shifted 14 from the letter A and replaced with the letter W
-The letter L corresponds to the letter O in the Keyword, and the position of the letter O is 14, so it will be shifted 14 from the letter L and replaced with the letter Z
-The letter A corresponds to the letter R in the Keyword, and the position of the letter R is 17, so it will be shifted 17 from the letter A and replaced with the letter R
-The letter L corresponds to the letter N in the Keyword, and the position of the letter N is 13, so it will be shifted 13 from the letter L and replaced with the letter Y
So the encrypted word is "GOZRY"

Another example of encryption:
The text is: Welcome to Medina, the Keyword is Taibah
The Encrypted text is: Petdotx tw Nekbni

To decrypt the text, the process is reversed by moving each letter back the same amount of displacement that was extracted from the key word.

Example of decryption:
The Encrypted text is: GOZRY, the Keyword is NOOR

G O Z R Y
N OOR N
- The letter G corresponds to the letter N in the Keyword, and the position of the letter N is 13, so it is shifted back 13 from the letter G and replaced with the letter T
- The letter O corresponds to the letter O in the Keyword, and the position of the letter O is 14, so it is shifted back 14 from the letter O and replaced with the letter A
- The letter Z corresponds to the letter O in the Keyword, and the position of the letter O is 14, so it is shifted back 14 from the letter Z and replaced with the letter L
- The letter R corresponds to the letter R in the Keyword, and the position of the letter R is 17, so it is shifted back 17 from the letter R and replaced with the letter A
- The letter Y corresponds to the letter N in the Keyword, and the position of the letter N is 13, so it is shifted 13 from the letter Y and replaced with the letter L

So the plaintext is "TALAL"

Another example of decryption:
The Encrypted text is: Lvzqtzx tz tsr tfsri tcauhmec snvrbqv brxcw, the Keyword is: proof talal noor
The plaintext text is: Welcome to the great computer science major

Troubleshooting

1- When entering letters other than those in the options or entering numbers to choose the encryption or decryption method, an error will appear, and only one of the existing symbols must be entered.

2- In the caesar cipher, it is not acceptable to enter a decimal number or letters in the shift, and it must be an integer only.

3- In the vigenère cipher, it is not acceptable to enter numbers in the encryption key word, it must be letters only.

Additional Resources:

1- GitHub

2- https://cryptii.com/pipes/caesar-cipher

3- https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

4- https://cryptii.com/pipes/vigenere-cipher

5- https://www.geeksforgeeks.org/vigenere-cipher/

Conclusion:

This project achieves increased security and protection when sending messages between users. Currently, there are many ways to hack and access the sent data, and algorithms have emerged to encrypt data and increase security, privacy, and the difficulty of accessing basic data before encryption.
It makes it easy for users to access some of the algorithms that have been placed in this program and encrypt texts easily and quickly.