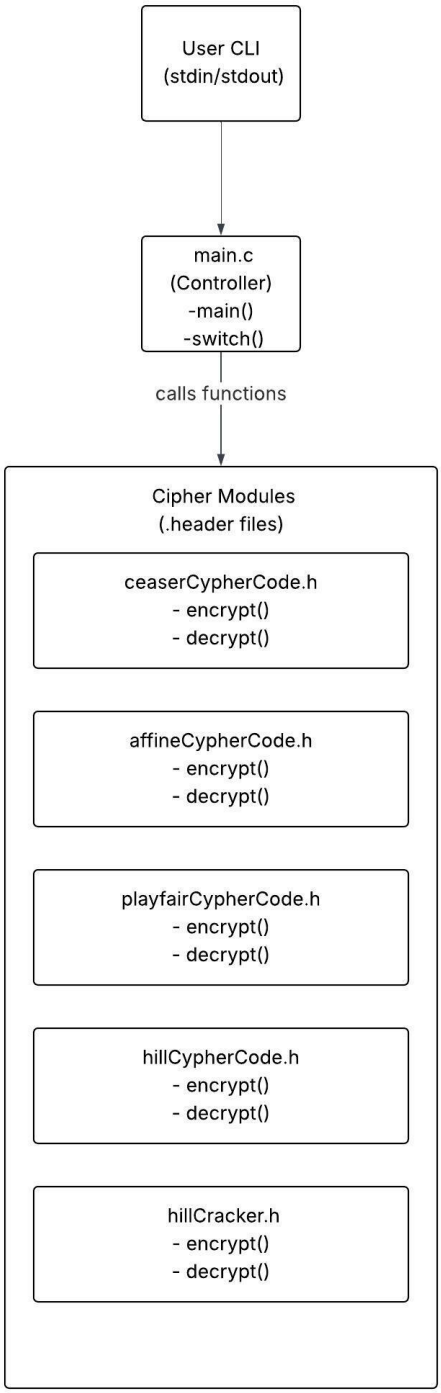
Report

Tool Architecture:



List of Libraries Used:

The program is built using the following standard C libraries, whose complete specifications can be found in the official C language documentation.

<stdio.h>	Standard Input/Output library. Handles all terminal I/O and file operations. [Documentation]
<stdlib.h>	Standard General Utilities library. Provides functions for memory management, process control, and conversions. [Documentation]
<ctype.h>	Character Type library. Contains functions for character classification and case conversion. [Documentation]
<string.h>	String library. Essential for string manipulation, including copying, concatenation, and comparison. [Documentation]
<math.h>	Mathematics library. Provides common mathematical functions. [Documentation]

Running the Tool

Launch the command-line application by double-clicking ***tool.exe***. This will open an interactive terminal where you can provide inputs and receive outputs as prompted.

Menu Navigation

Upon starting, you will see a menu listing available operations. Choose an option by entering a number from **1 to 9**. To exit the program at any time, enter **-1**.

Caesar Cipher

For encryption, the system prompts the user for a numeric key, adds this value to each character of the plaintext, and reduces the result modulo 26 to produce the ciphertext. During decryption, the same key is requested, subtracted from the ciphertext, and again taken modulo 26 to restore the original plaintext.

Encrypt (Option 1)

- **Input File:** Provide the path to a .txt file containing the plaintext
- **Output File:** Provide the path for a new .txt file where the ciphertext will be saved
- **Encryption Key:** Enter a numerical key (shift value) for the encryption

Output: The program will generate the ciphertext file plus an additional .txt file containing the encryption key.

Decrypt (Option 2)

- **Input File:** Provide the path to a .txt file containing the ciphertext
- **Decryption Key:** Enter the numerical key used to decrypt the message

Output: The program will restore the original plaintext from the ciphertext.

Affine Cipher

In the Affine Cipher, two integer keys, [**a**] and [**b**], are required. The key [**a**] must be coprime with 26, while [**b**] may be any integer from 0 to 25. Encryption is performed by applying the formula

```
E ( x ) = ( a x + b ) mod 26
```

where (x) represents the numerical value of the plaintext letter.

For decryption, the inverse of [**a**] modulo 26 is calculated, and the original plaintext is recovered using

```
D ( x ) = a^-1 ( x - b ) mod m
```

where (x) now denotes the ciphertext letter's numerical equivalent.

Encrypt (Option 3)

- **Input File:** Provide the path to a .txt file containing the plaintext
- **Output File:** Provide the path for a new .txt file for the ciphertext
- **Encryption Keys:** Enter two numerical keys, 'a' and 'b', which form the complete Affine cipher key

Note: The first key, **a**, must be a number between 1–25 that is **coprime with 26.** The second key, **b**, can be any integer between 0 and 25.

Output: The program generates the ciphertext file plus a key file containing both encryption keys.

Decrypt (Option 4)

- **Input File:** Provide the path to a .txt file containing the ciphertext
- **Output File:** Provide the path for a new .txt file for the decrypted text
- **Decryption Keys:** Enter the two numerical keys ('a' and 'b') required for decryption

Output: The program restores the original plaintext.

Playfair Cipher

The key matrix is first generated from a user-provided keyword. Before encryption, the plaintext is prepared by inserting 'X' between any double letters and appending an 'X' if the total character count is odd. The text is then split into digraphs (pairs of letters). For each pair, three rules apply based on their positions in the 5x5 matrix. If both letters are in the same column, each is replaced by the letter directly below it, wrapping to the top if the letter is at the bottom of the column. If they are in the same row, each shifts to the letter immediately to its right, wrapping to the leftmost position if at the end of the row. For letters forming a rectangle (different rows and columns), each letter is replaced by the letter in its own row that lies in the column of the other letter. Decryption follows the same logic but reverses the direction of the row and column shifts.

Encrypt (Option 5)

- **Input File:** Provide the path to a .txt file containing the plaintext
- **Output File:** Provide the path for a new .txt file for the ciphertext
- **Encryption Key:** Enter the keyword or phrase used to generate the Playfair cipher's encryption matrix

Output: The program generates the ciphertext file plus a key file containing the encryption keyword.

Decrypt (Option 6)

- **Input File:** Provide the path to a .txt file containing the ciphertext
- **Output File:** Provide the path for a new .txt file for the decrypted text
- **Decryption Key:** Enter the exact keyword or phrase used to encrypt the message

Output: The program restores the original plaintext.

Hill Cipher

The Hill Cipher encrypts blocks of three letters using a 3×3 numeric key matrix. The plaintext is prepared by converting letters to numbers and padding with 'X' to ensure length is a multiple of three. During encryption, each block is multiplied by the key matrix, and the result is taken modulo 26 to produce ciphertext. For decryption, the same key matrix must be invertible modulo 26. The decryption key is its modular inverse. This inverse matrix is multiplied by the ciphertext blocks to recover the original numeric values. Finally, the numbers are converted back to letters, and padding 'X' characters are removed to restore the original message.

Encrypt (Option 7)

- **Input File:** Provide the path to a .txt file containing the plaintext
- **Output File:** Provide the path for a new .txt file for the ciphertext
- **Encryption Key Matrix:** Enter the numerical 3x3 matrix key (must be square and invertible modulo 26)

Output: The program generates the ciphertext file plus a key file containing the encryption matrix.

Decrypt (Option 8)

- **Input File:** Provide the path to a .txt file containing the ciphertext
- **Output File:** Provide the path for a new .txt file for the decrypted text
- **Decryption Key Matrix:** Enter the exact numerical matrix key used for encryption

Output: The program restores the original plaintext.

Note: The Hill cipher requires square, invertible matrices modulo 26.

Hill Cipher Cracker (Option 9)

Launches an interactive tool to recover the 2×2 key matrix using a known-plaintext attack. It takes two plaintext-ciphertext letter pairs as input and converts them to numerical matrices. The encryption key matrix is recovered by computing $\mathbf{K = C \times P^{-1} \pmod{26}}$, where C is the ciphertext matrix and P^{-1} is the modular inverse of the plaintext matrix. The recovered 2×2 key matrix is then output in both numeric and letter form.

How to Use: The program prompts for two known plaintext-ciphertext pairs:

1. For each pair, enter:
    a. **Plaintext:** 2 letters from the original message
    b. **Ciphertext:** Corresponding 2 encrypted letters

Requirements:

- Each pair must be exactly 2 letters
- Plaintext and ciphertext must correctly correspond
- The two plaintext pairs must form an invertible 2×2 matrix modulo 26

Output: Displays the recovered encryption key matrix in numerical and letter forms.

Note: This tool only works for 2×2 Hill ciphers. If the plaintext matrix is not invertible modulo 26, try different pairs.

Important Notes for All Ciphers

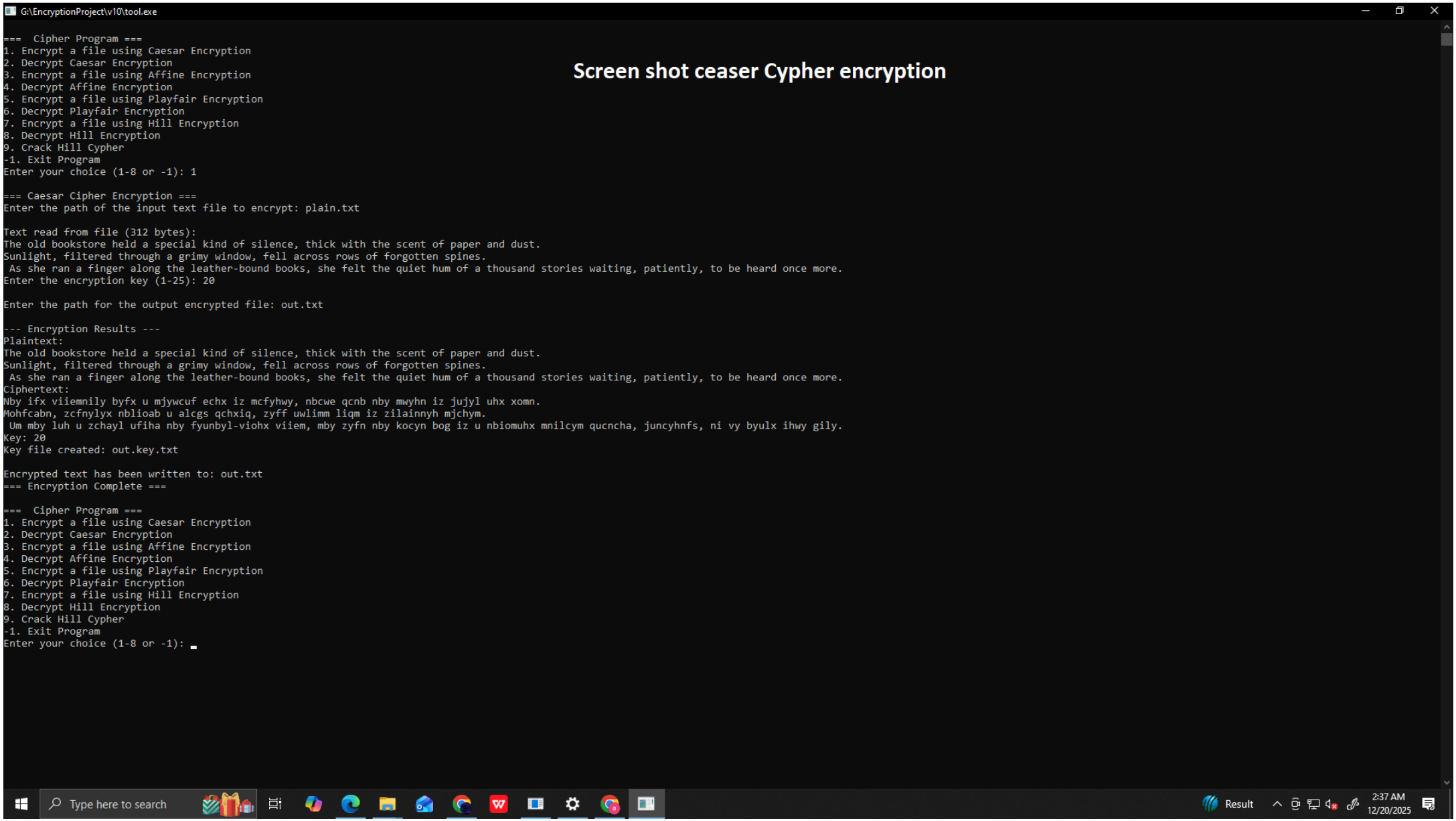
- All input and output files must use the **.txt file extension**
- For successful decryption, you must provide the **exact same key** used during encryption
- Ensure file paths are correctly specified and files exist before proceeding

GitHub Link

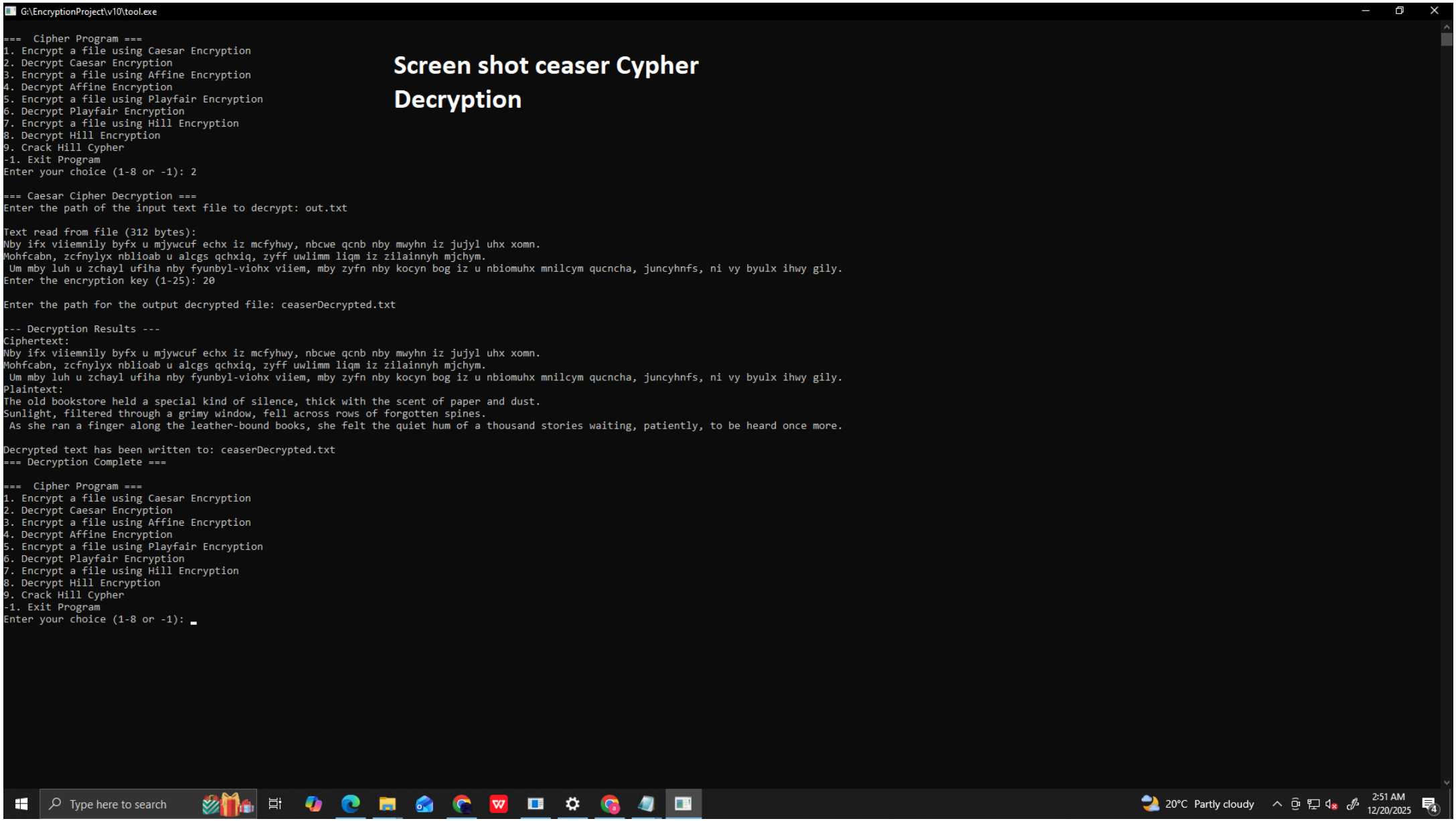
https://github.com/Glitch1258/MyCode-LegacyEncryptionMethodsImplemented.git

Screen shots:

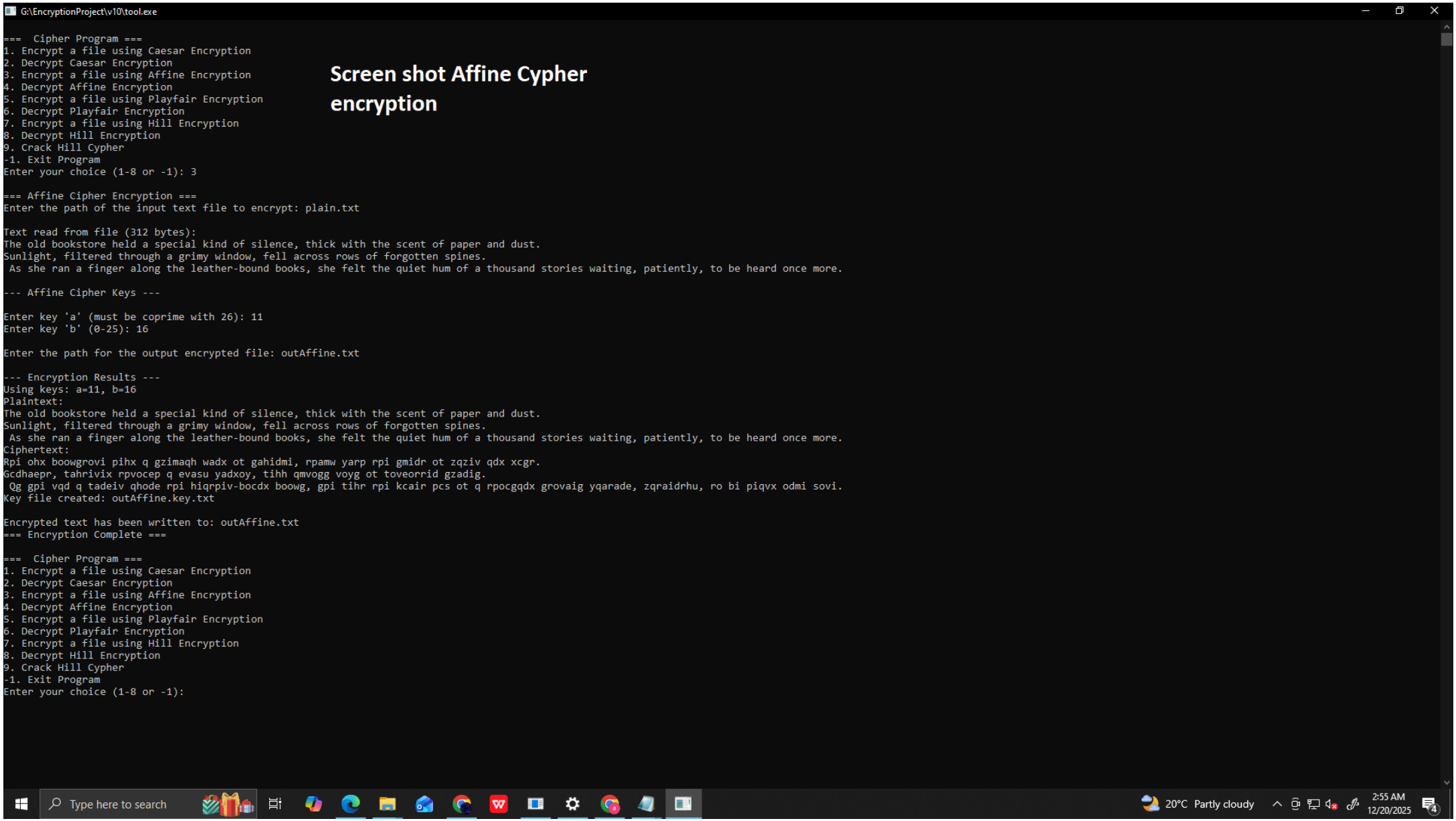
Screen shot ceaser Cypher encryption

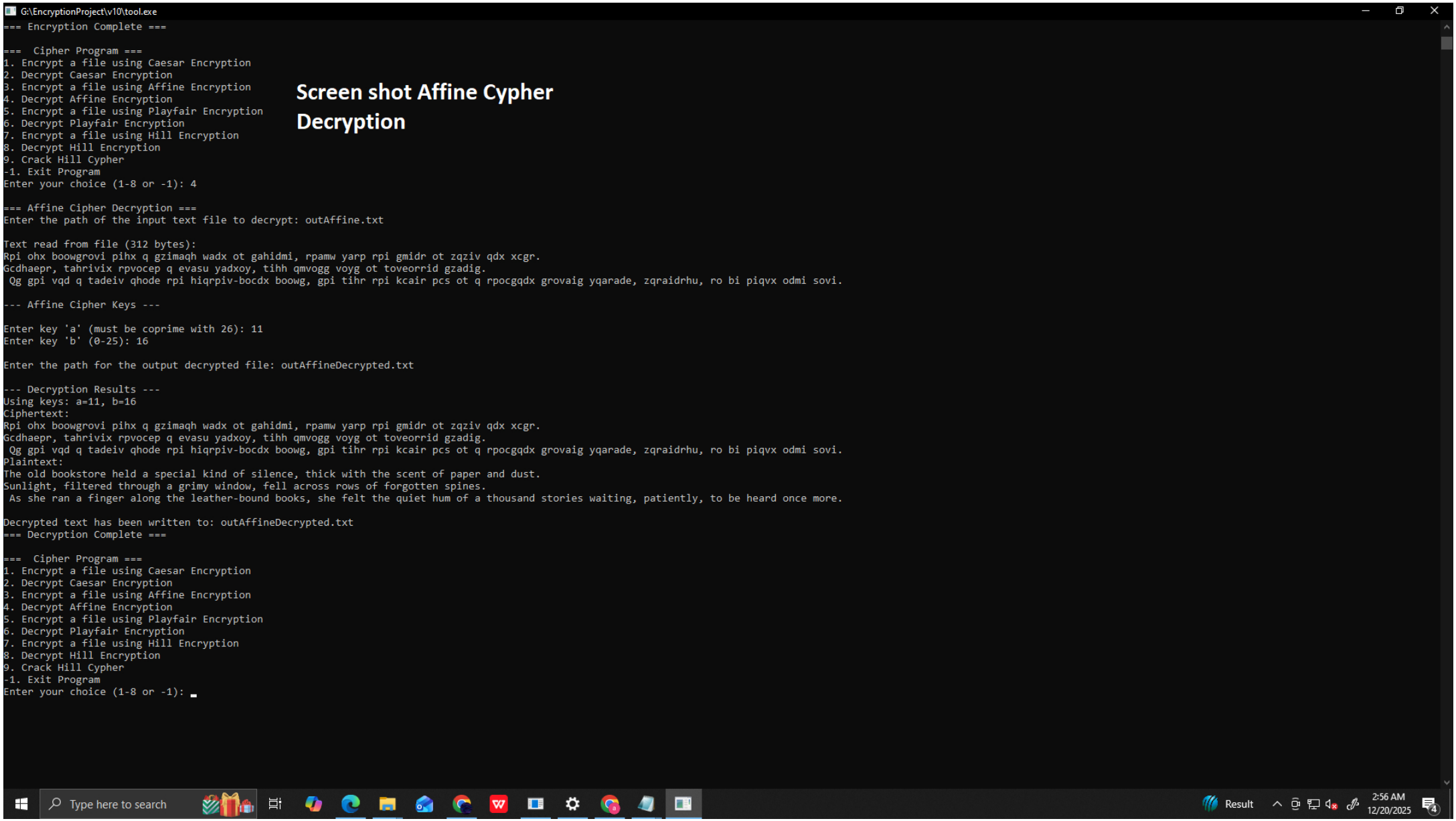


Screen shot ceaser Cypher Decryption



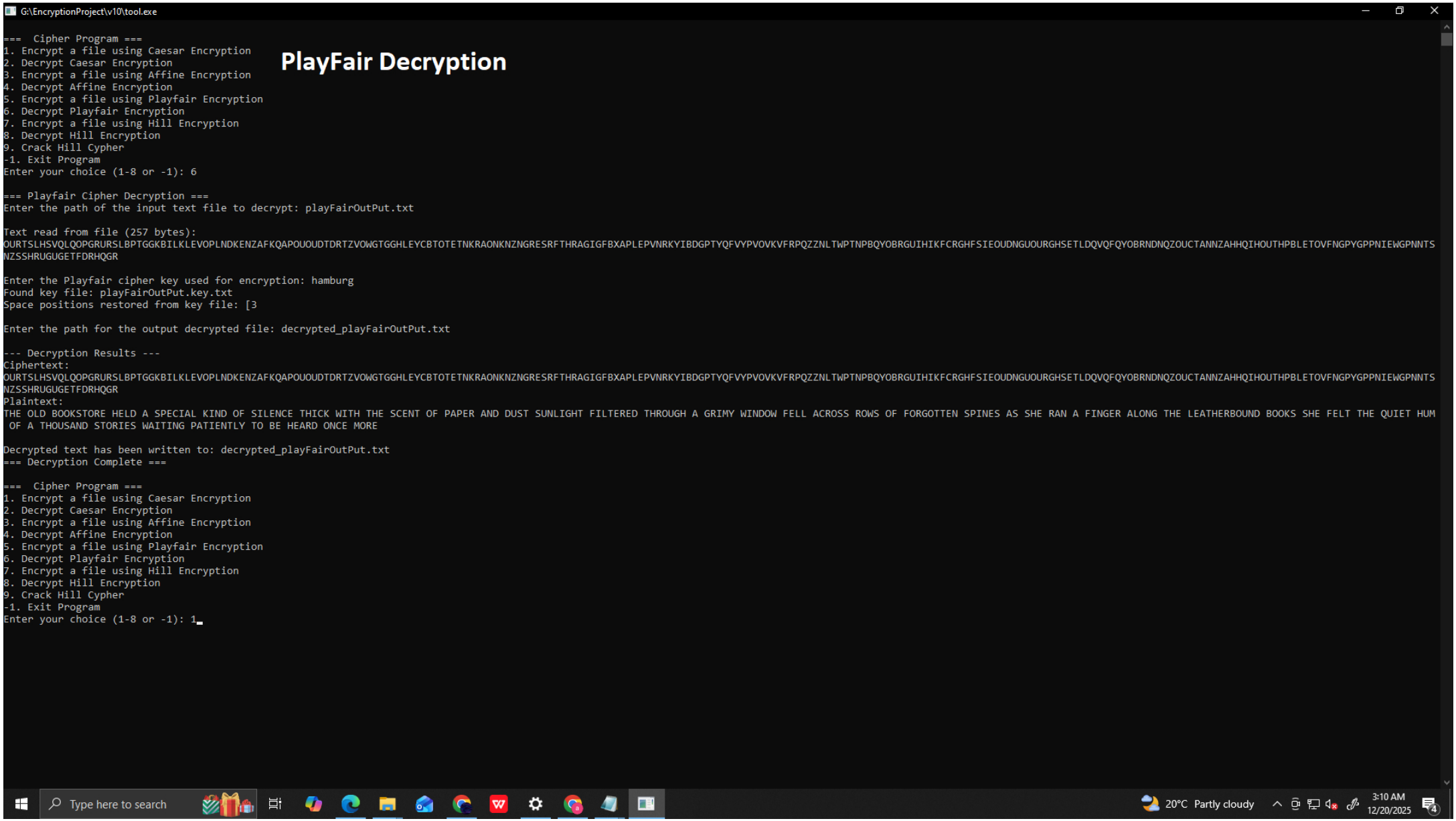
Screen shot Affine Cypher encryption



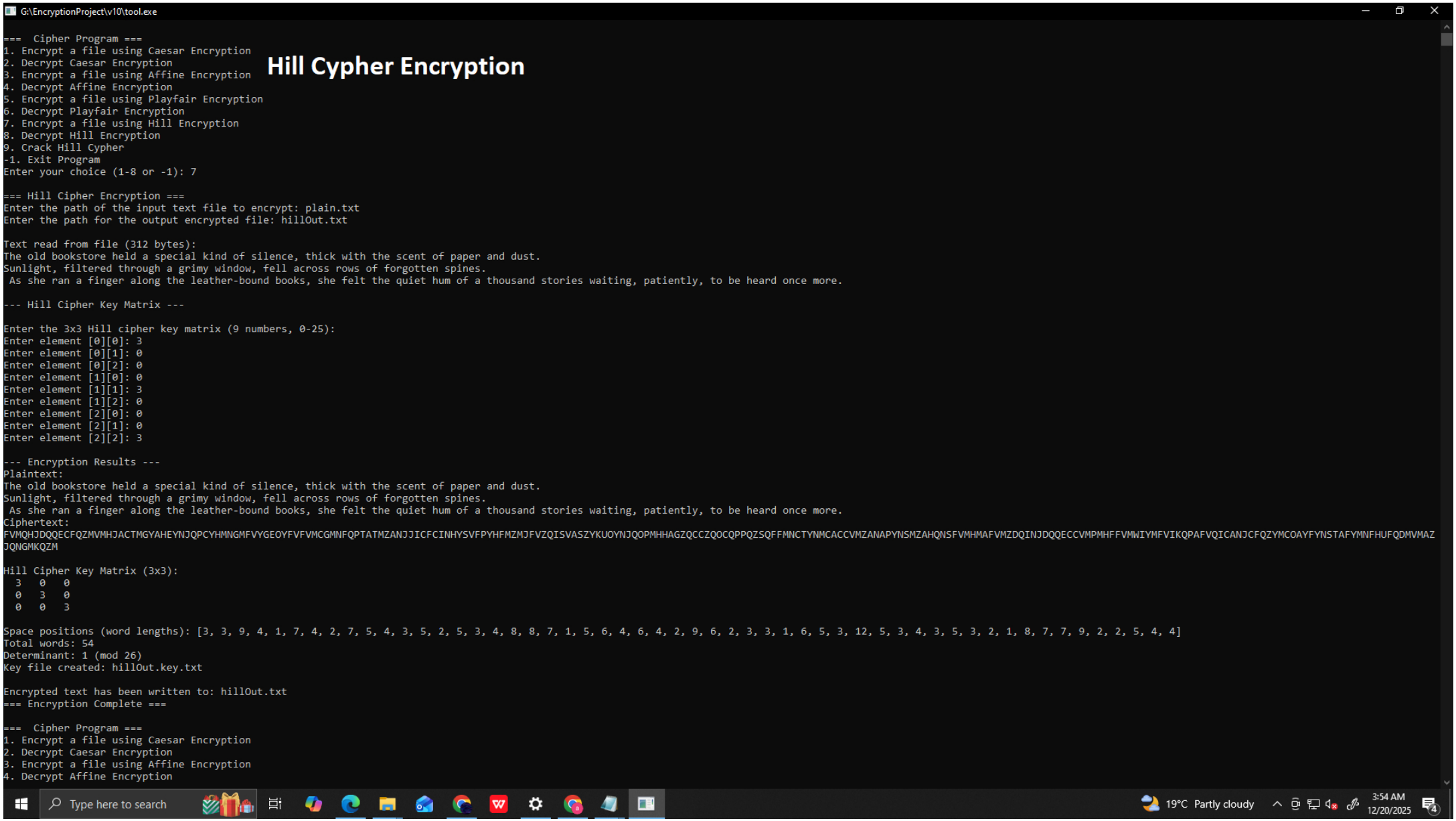

G:\EncryptionProject\v10\tool.exe
=== Encryption Complete ===
=== Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 4
=== Affine Cipher Decryption ===
Enter the path of the input text file to decrypt: outAffine.txt
Text read from file (312 bytes):
Rpi ohx boowgrovi pihx q gzimaqh wadx ot gahidmi, rpamw yarp rpi gmidr ot zqziv qdx xcgr.
Gcdhaepr, tahrivix rpvocep q evasu yadxoy, tihh qmvogg voyg ot toveorrid gzadig.
Qg gpi vqd q tadeiv qhode rpi hiqrpiv-bocdx boowg, gpi tihr rpi kcair pcs ot q rpocgqdx grovaig yqarade, zqraidrhu, ro bi piqvx odmi sovi.
--- Affine Cipher Keys ---
Enter key 'a' (must be coprime with 26): 11
Enter key 'b' (0-25): 16
Enter the path for the output decrypted file: outAffineDecrypted.txt
--- Decryption Results ---
Using keys: a=11, b=16
Ciphertext:
Rpi ohx boowgrovi pihx q gzimaqh wadx ot gahidmi, rpamw yarp rpi gmidr ot zqziv qdx xcgr.
Gcdhaepr, tahrivix rpvocep q evasu yadxoy, tihh qmvogg voyg ot toveorrid gzadig.
Qg gpi vqd q tadeiv qhode rpi hiqrpiv-bocdx boowg, gpi tihr rpi kcair pcs ot q rpocgqdx grovaig yqarade, zqraidrhu, ro bi piqvx odmi sovi.
Plaintext:
The old bookstore held a special kind of silence, thick with the scent of paper and dust.
Sunlight, filtered through a grimy window, fell across rows of forgotten spines.
As she ran a finger along the leather-bound books, she felt the quiet hum of a thousand stories waiting, patiently, to be heard once more.
Decrypted text has been written to: outAffineDecrypted.txt
=== Decryption Complete ===
=== Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1):
Screen shot Affine Cypher Decryption
Type here to search
Result
2:56 AM
12/20/2025

PlayFair Encryption

```
G:\EncryptionProject\v10\tool.exe

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 5

=== Playfair Cipher Encryption ===
Enter the path of the input text file to encrypt: plain.txt

Text read from file (312 bytes):
The old bookstore held a special kind of silence, thick with the scent of paper and dust.
Sunlight, filtered through a grimy window, fell across rows of forgotten spines.
 As she ran a finger along the leather-bound books, she felt the quiet hum of a thousand stories waiting, patiently, to be heard once more.

Enter the Playfair cipher key (letters only): hamburg

Enter the path for the output encrypted file: playFairOutput.txt

--- Encryption Results ---
Plaintext:
The old bookstore held a special kind of silence, thick with the scent of paper and dust.
Sunlight, filtered through a grimy window, fell across rows of forgotten spines.
 As she ran a finger along the leather-bound books, she felt the quiet hum of a thousand stories waiting, patiently, to be heard once more.
Ciphertext:
OURTSLHSVQLQOPGRURSLBPTGGKBILKLEVOPLNDKENZAFKQAPOUOUDTDRTZVOWGTGGHLEYCBTOTETNKRAONKNZNGRESRFTHRAGIGFBXAPLEPVNRKYIBDGPTYQFVYPVOVKVFRPQZZNLTWPTNPBQYOBRGUIHIKFCRGHFSIEOUDNGUOURGHSETLDQVQFQYOBRNDNQZOUCTANNZAHHQIHOUTHPBLETOVFNGPYGPPNIEWGPNNTSNZSSHRUGUGETFDRHQGR
Key: hamburg
Space positions: [3,3,9,4,1,7,4,2,7,5,4,3,5,2,5,3,4,8,8,7,1,5,6,4,6,4,2,9,6,2,3,3,1,6,5,3,12,5,3,4,3,5,3,2,1,8,7,7,9,2,2,5,4,4]

Playfair Matrix:
H A M B U
R G C D E
F I K L N
O P Q S T
V W X Y Z
Key file created: playFairOutput.key.txt

Encrypted text has been written to: playFairOutput.txt
=== Encryption Complete ===

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): _
```


G:\EncryptionProject\v10\tool.exe
PlayFair Decryption
=== Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 6
=== Playfair Cipher Decryption ===
Enter the path of the input text file to decrypt: playFairOutPut.txt
Text read from file (257 bytes):
OURTSLHSVQLQOPGRURSLBPTGGKBILKLEVOPLNDKENZAFKQAPOUOUDTDRTZVOWGTGGHLEYCBTOTETNKRAONKNZNGRESRFTHRAGIGFBXAPLEPVNRKYIBDGPTYQFVYPVOVKVFRPQZZNLTWPTNPBQYOBRGUIHIKFCRGHFSIEOUDNGUOURGHSETLDQVQFQYOBRNDNQZOUCTANNZAHHQIHOUTHPBLETOVFNGPYGPPNIEWGPNNTS
NZSSHRUGUGETFDRHQGR
Enter the Playfair cipher key used for encryption: hamburg
Found key file: playFairOutPut.key.txt
Space positions restored from key file: [3
Enter the path for the output decrypted file: decrypted_playFairOutPut.txt
--- Decryption Results ---
Ciphertext:
OURTSLHSVQLQOPGRURSLBPTGGKBILKLEVOPLNDKENZAFKQAPOUOUDTDRTZVOWGTGGHLEYCBTOTETNKRAONKNZNGRESRFTHRAGIGFBXAPLEPVNRKYIBDGPTYQFVYPVOVKVFRPQZZNLTWPTNPBQYOBRGUIHIKFCRGHFSIEOUDNGUOURGHSETLDQVQFQYOBRNDNQZOUCTANNZAHHQIHOUTHPBLETOVFNGPYGPPNIEWGPNNTS
NZSSHRUGUGETFDRHQGR
Plaintext:
THE OLD BOOKSTORE HELD A SPECIAL KIND OF SILENCE THICK WITH THE SCENT OF PAPER AND DUST SUNLIGHT FILTERED THROUGH A GRIMY WINDOW FELL ACROSS ROWS OF FORGOTTEN SPINES AS SHE RAN A FINGER ALONG THE LEATHERBOUND BOOKS SHE FELT THE QUIET HUM
OF A THOUSAND STORIES WAITING PATIENTLY TO BE HEARD ONCE MORE
Decrypted text has been written to: decrypted_playFairOutPut.txt
=== Decryption Complete ===
=== Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 1
Type here to search
20°C Partly cloudy
3:10 AM
12/20/2025

Hill Cypher Encryption



Hill Cypher Decryption

```
G:\EncryptionProject\v10\tool.exe

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 8

=== Hill Cipher Decryption ===
Enter the path of the input text file to decrypt: hillOut.txt
Enter the path for the output decrypted file: decrypt_hillOut.txt
Found key file: hillOut.key.txt
Read space positions from key file: [3, 3, 9, 4, 1, 7, 4, 2, 7, 5, 4, 3, 5, 2, 5, 3, 4, 8, 8, 7, 1, 5, 6, 4, 6, 4, 2, 9, 6, 2, 3, 3, 1, 6, 5, 3, 12, 5, 3, 4, 3, 5, 3, 2, 1, 8, 7, 7, 9, 2, 2, 5, 4, 4]

Text read from file (247 bytes):
FVMQHJDQQECFQZMVMHJACTMGYAHEYNJQPCYHMNGMFVYGEOYFVFVMCGMNFQPTATMZANJJICFCINHYSVFPYHFMZMJFVZQISVASZYKUOYNJQOPMHHAGZQCCZQOCQPPQZSQFFMNCTYNMCACCVMZANAPYNSMZAHQNSFVMHMAFVMZDQINJDQQECCVMPMHFFVMWIYMFVIKQPAFVQICANJCFQZYMCOAYFYNSTAFYMNFHUFQDMVMAZ
JQNGMKQZM

--- Hill Cipher Key Matrix ---

Enter the 3x3 Hill cipher key matrix (9 numbers, 0-25):
Enter element [0][0]: 3
Enter element [0][1]: 0
Enter element [0][2]: 0
Enter element [1][0]: 0
Enter element [1][1]: 3
Enter element [1][2]: 0
Enter element [2][0]: 0
Enter element [2][1]: 0
Enter element [2][2]: 3

--- Decryption Results ---
Ciphertext:
FVMQHJDQQECFQZMVMHJACTMGYAHEYNJQPCYHMNGMFVYGEOYFVFVMCGMNFQPTATMZANJJICFCINHYSVFPYHFMZMJFVZQISVASZYKUOYNJQOPMHHAGZQCCZQOCQPPQZSQFFMNCTYNMCACCVMZANAPYNSMZAHQNSFVMHMAFVMZDQINJDQQECCVMPMHFFVMWIYMFVIKQPAFVQICANJCFQZYMCOAYFYNSTAFYMNFHUFQDMVMAZ
JQNGMKQZM
Plaintext:
THE OLD BOOKSTORE HELD A SPECIAL KIND OF SILENCE THICK WITH THE SCENT OF PAPER AND DUST SUNLIGHT FILTERED THROUGH A GRIMY WINDOW FELL ACROSS ROWS OF FORGOTTEN SPINES AS SHE RAN A FINGER ALONG THE LEATHERBOUND BOOKS SHE FELT THE QUIET HUM
 OF A THOUSAND STORIES WAITING PATIENTLY TO BE HEARD ONCE MORE

Decrypted text has been written to: decrypt_hillOut.txt
=== Decryption Complete ===

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): -1
```

Hill Cypher Cracker

```
G:\EncryptionProject\v10\tool.exe

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): 9
=== Hill Cipher Key Recovery Attack ===
We need 2 known plaintext-ciphertext pairs (2 letters each).

Pair 1:
Plaintext (2 letters): hi
Ciphertext (2 letters): hc

Pair 2:
Plaintext (2 letters): ll
Ciphertext (2 letters): rz

Plaintext matrix P:
[ 7  8]
[11 11]

Ciphertext matrix C:
[ 7  2]
[17 25]

Inverse of plaintext matrix P^-1:
[25 22]
[ 1 23]

Recovered encryption matrix K:
[ 3  2]
[ 8  5]

In letter form:
DC  IF

===  Cipher Program ===
1. Encrypt a file using Caesar Encryption
2. Decrypt Caesar Encryption
3. Encrypt a file using Affine Encryption
4. Decrypt Affine Encryption
5. Encrypt a file using Playfair Encryption
6. Decrypt Playfair Encryption
7. Encrypt a file using Hill Encryption
8. Decrypt Hill Encryption
9. Crack Hill Cypher
-1. Exit Program
Enter your choice (1-8 or -1): _
```