Name: Asmita Suresh Shinde

PRN: 21510012

Batch: B1

CNS LAB LA1

List of Experiments:

1. Perform encryption, decryption using the following substitution techniques

a. Ceaser Cipher,

b. Playfair Cipher

c. Hill Cipher

d. Vigenère Cipher

2. Perform encryption and decryption using following transposition techniques

a. Rail fence

b. row and Column Transformation

3. Implementation of Euclidean and Extended Euclidean Algorithm

4. Implementation of Chinese Remainder Theorem (CRT)

5. Apply DES algorithm for practical applications

6. Apply AES algorithm for practical applications

**Experiment 1: Perform encryption, decryption using the following substitution techniques.**

Ceaser Cipher:

Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: Julius
2. Choose a shift value. In this case, we will use a shift of 4.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

 J becomes N (shift 4 from J)

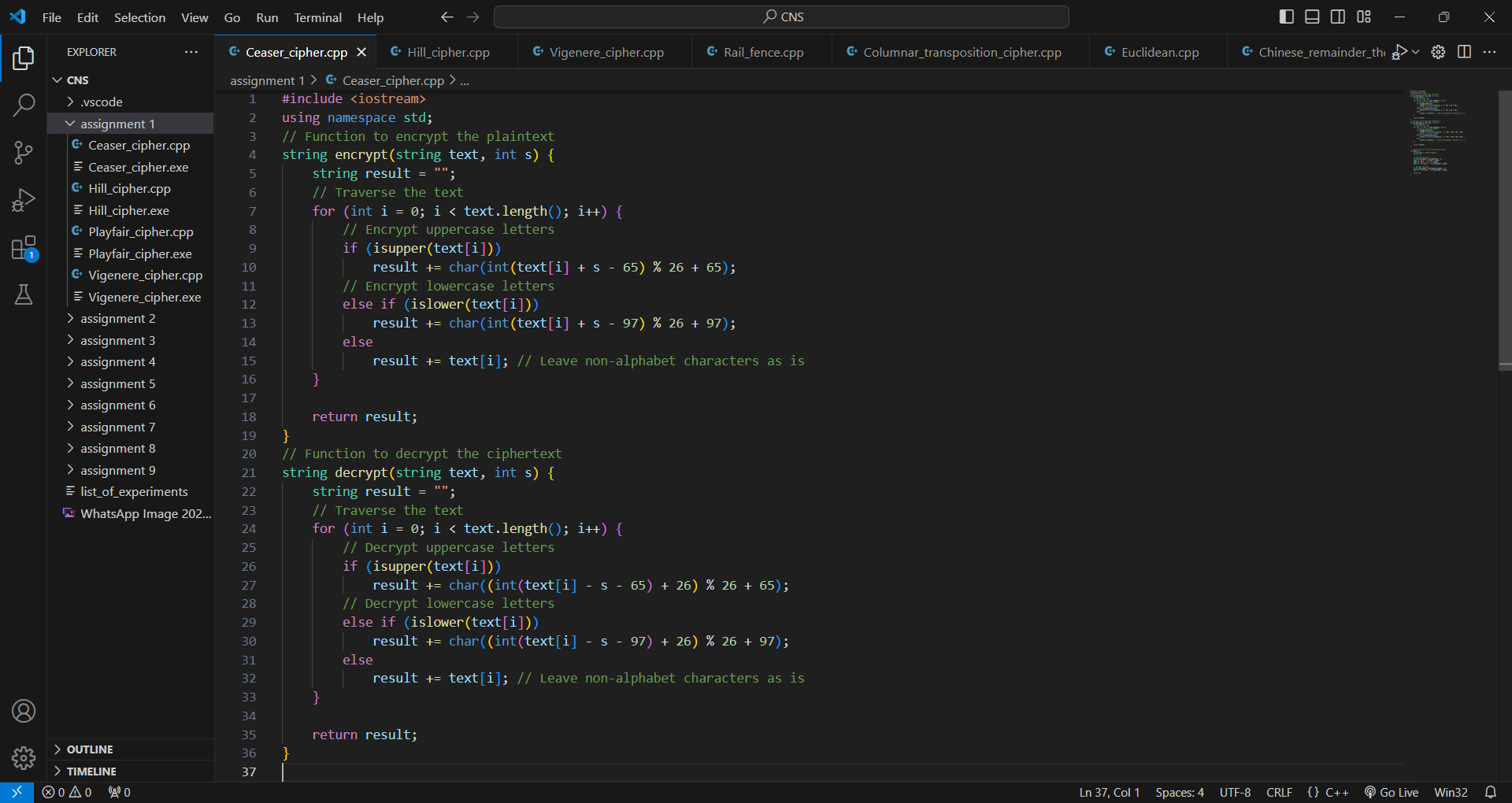
u becomes y (shift 4 from u)     
l becomes p (shift 4 from l)      
i becomes m (shift 4 from i)

u becomes y (shift 4 from u)

s becomes w (shift 4 from s)

The encrypted message is now “Nypmyw”.

To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “Nypmyw” back by 4 positions to get the original message, “Julius”.



A screenshot of a computer program

Description automatically generated

Playfair Cipher:

Generate the key Square(5×5):

The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Rules for Encryption:

If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

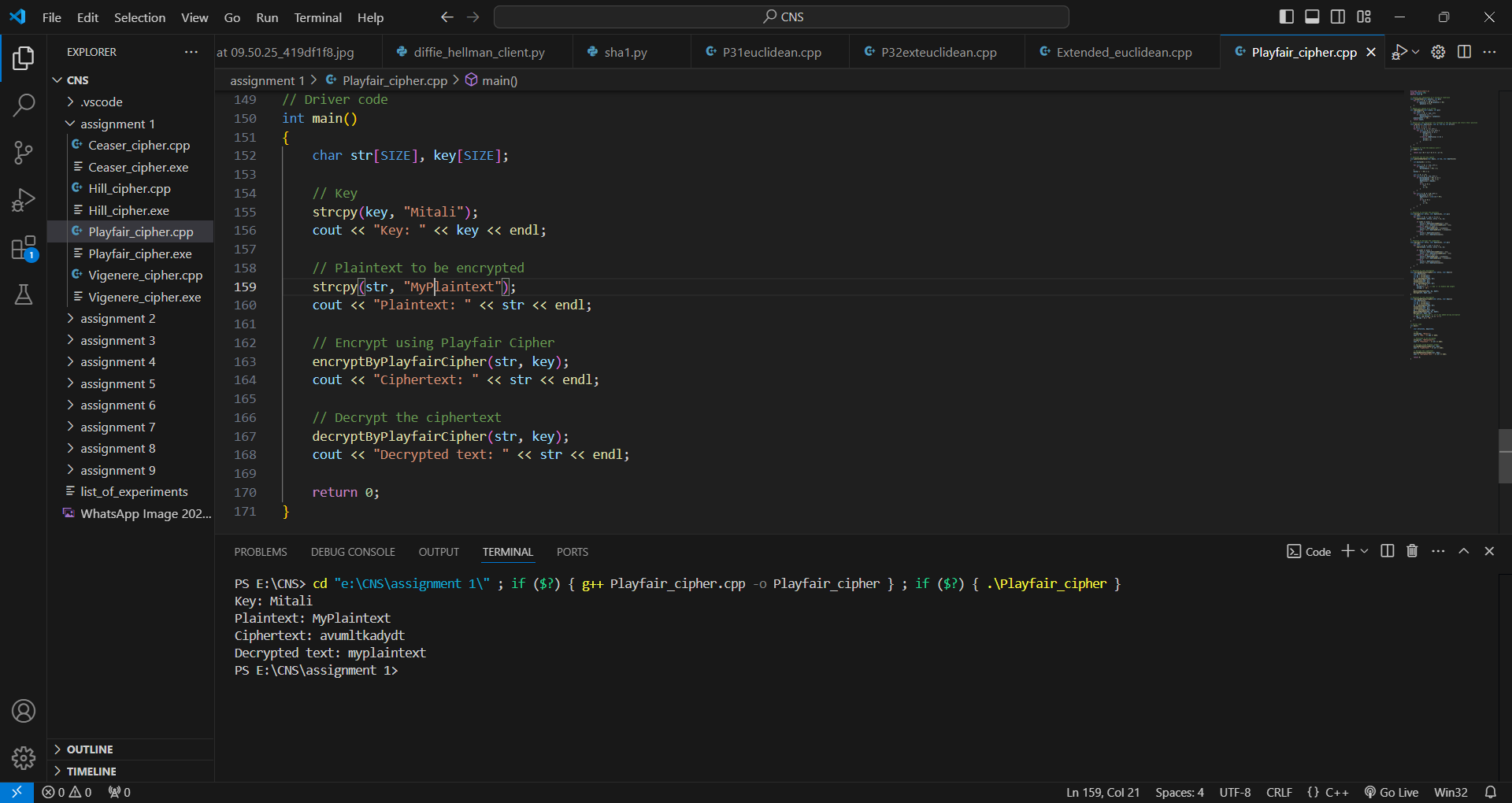
Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated



Hill Cipher:

The Hill cipher is a polygraphic substitution cipher that uses linear algebra to encrypt and decrypt messages.

**Encryption:**

1. **Convert Plaintext**: Break the message into blocks of letters (e.g., "ACT") and convert each letter to numbers (A=0, B=1, etc.).
2. **Key Matrix**: Use an invertible square matrix (e.g., 3x3) as the key, where each letter of the key is also converted to numbers.
3. **Matrix Multiplication**: Multiply the message block (as a vector) by the key matrix and take the result modulo 26.
4. **Ciphertext**: Convert the resulting numbers back into letters to get the encrypted message.

**Decryption:**

1. **Convert Ciphertext**: Convert the encrypted message back to numbers.
2. **Inverse Matrix**: Use the inverse of the key matrix for decryption.
3. **Matrix Multiplication**: Multiply the ciphertext vector by the inverse matrix and take the result modulo 26.
4. **Plaintext**: Convert the numbers back to letters to retrieve the original message.

Example:

* **Plaintext**: "ACT"
* **Key**: "GYBNQKURP" (3x3 matrix)
* **Ciphertext**: "POH"

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

Vigenère Cipher:

The Vigenère Cipher is a polyalphabetic substitution cipher that encrypts alphabetic text using multiple Caesar ciphers, depending on a repeating keyword.

**Encryption:**

1. **Vigenère Square**: A table with 26 rows, each shifted alphabetically, representing 26 Caesar ciphers.
2. **Key Generation**: The keyword is repeated to match the length of the plaintext. For example:
   * Plaintext: "PLAINTEXT"
   * Keyword: "MITALI" becomes "MITALIMITA" (repeated).
3. **Encryption Process**: For each letter of the plaintext, use the row corresponding to the plaintext letter and the column for the key letter. The intersecting letter is the ciphertext.

Example:

* Plaintext: "PLAINTEXT"
* Key: "MITALIMITA"
* Ciphertext: "BYIALSKWW"

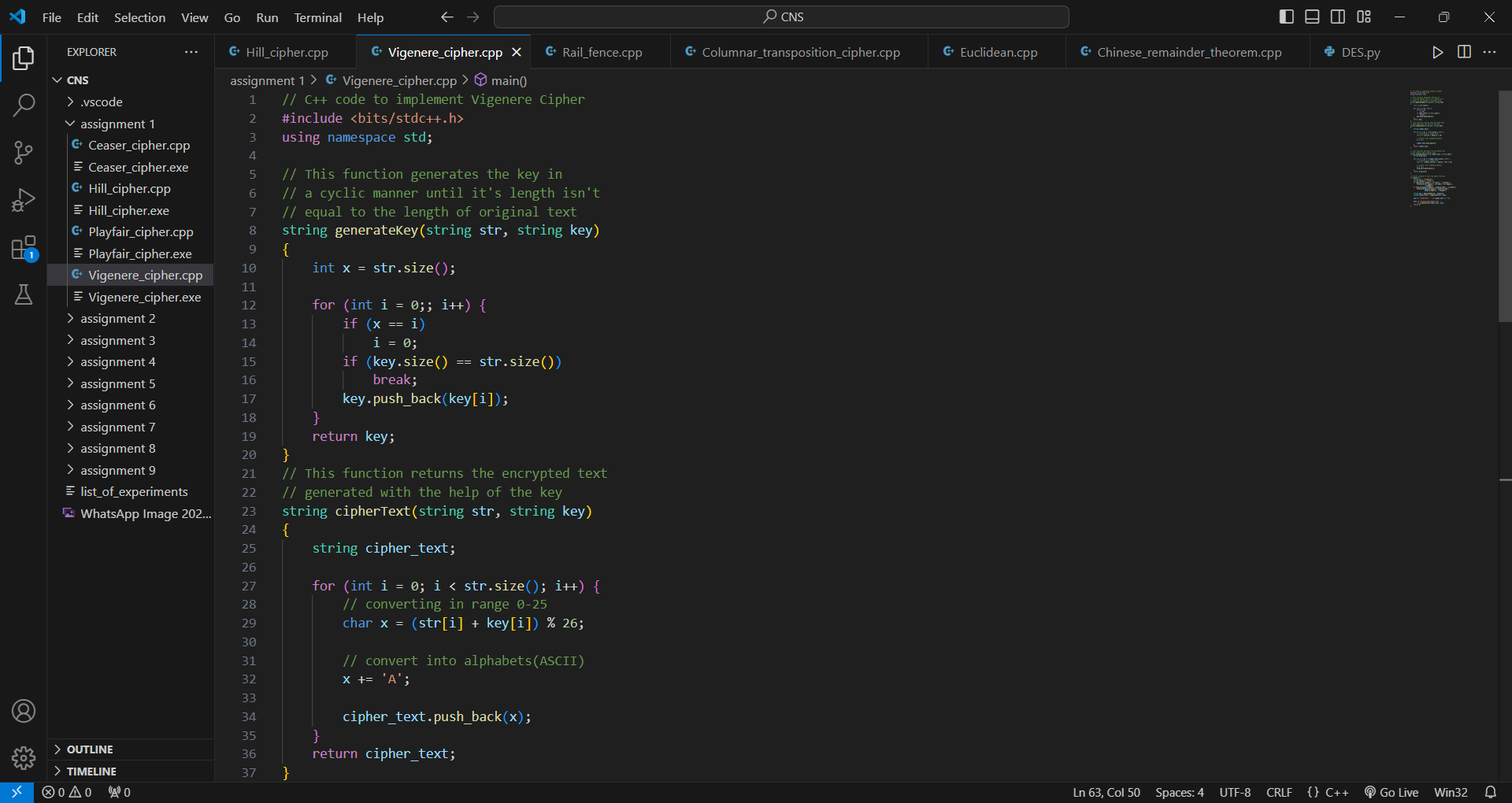
**Decryption:**

To decrypt, use the key to find the corresponding row in the Vigenère table. Then locate the ciphertext letter in that row and find its column label, which gives the plaintext letter.

Alternatively, you can use a mathematical approach:

* **Encryption**: Ei=(Pi+Ki)mod  26E\_i = (Pi + Ki) \mod 26Ei​=(Pi​+Ki​)mod26
* **Decryption**: Di=(Ei−Ki)mod  26D\_i = (Ei - Ki) \mod 26Di​=(Ei​−Ki​)mod26

This converts letters [A-Z] to numbers [0–25], performs modulo operations, and converts back to letters.



A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

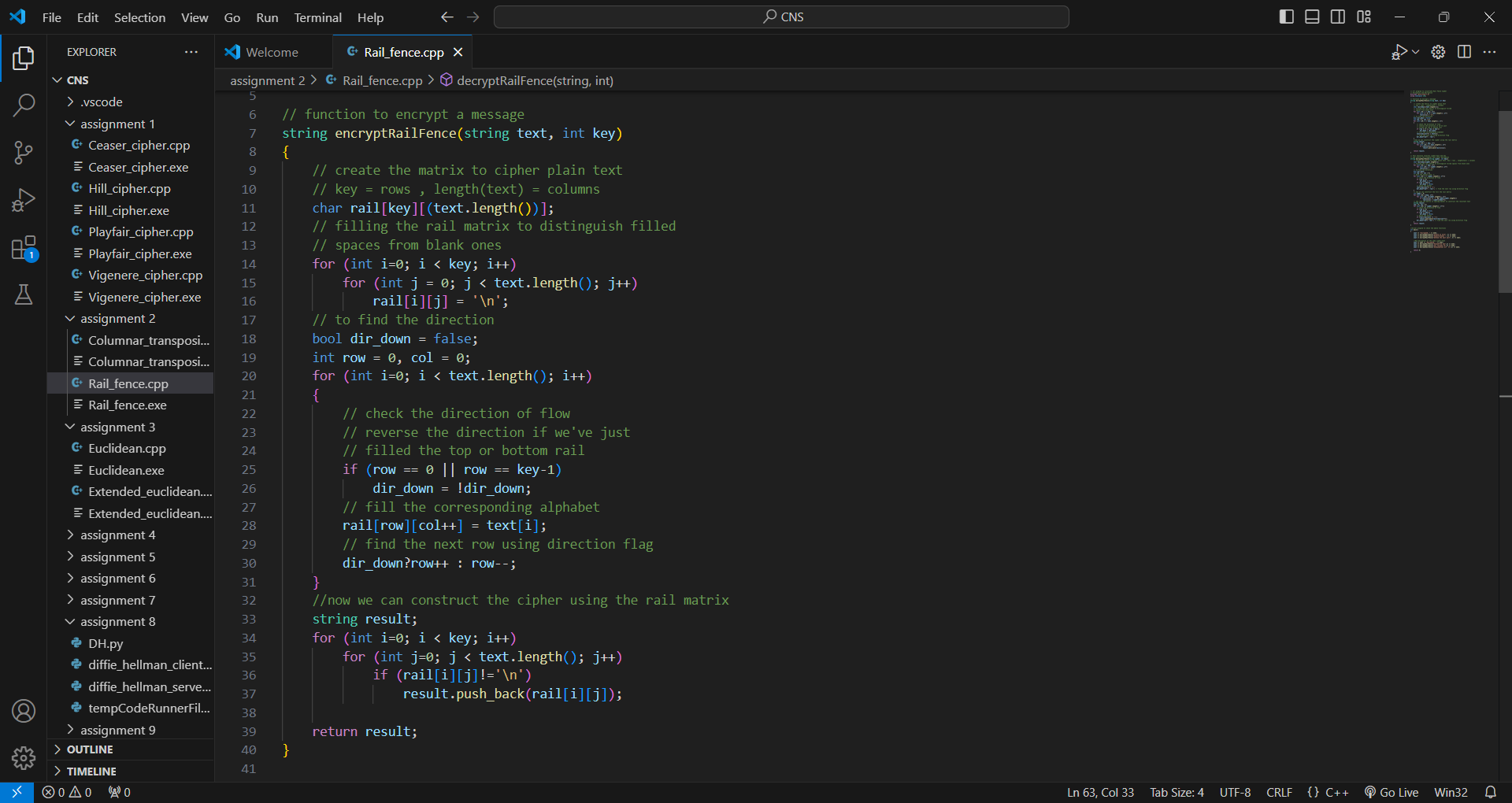
Description automatically generated

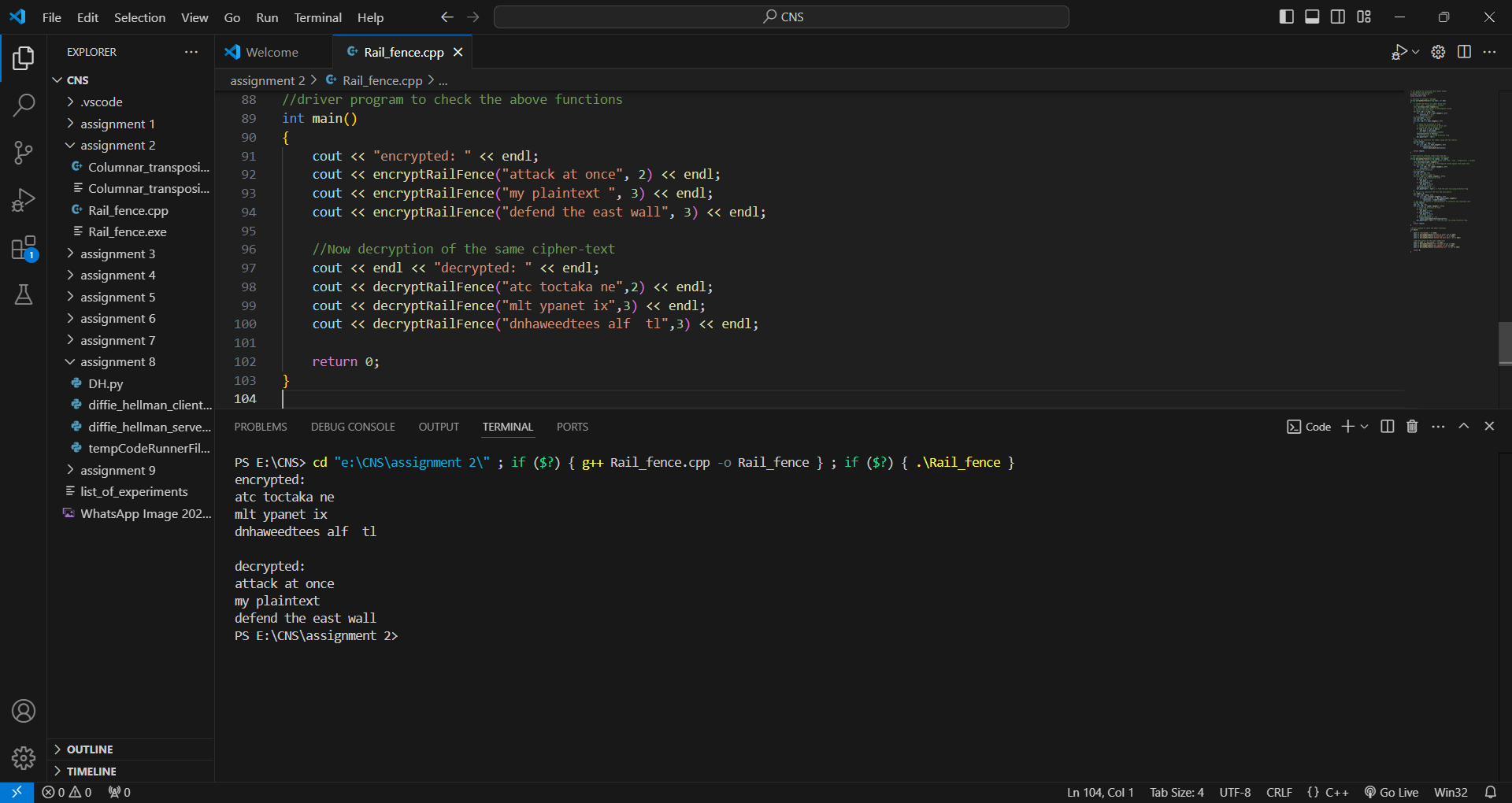
**Experiment 2:** **Perform encryption and decryption using following transposition techniques**

Rail fence:

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

* In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
* When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner.
* After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

 A screenshot of a computer program

Description automatically generated 

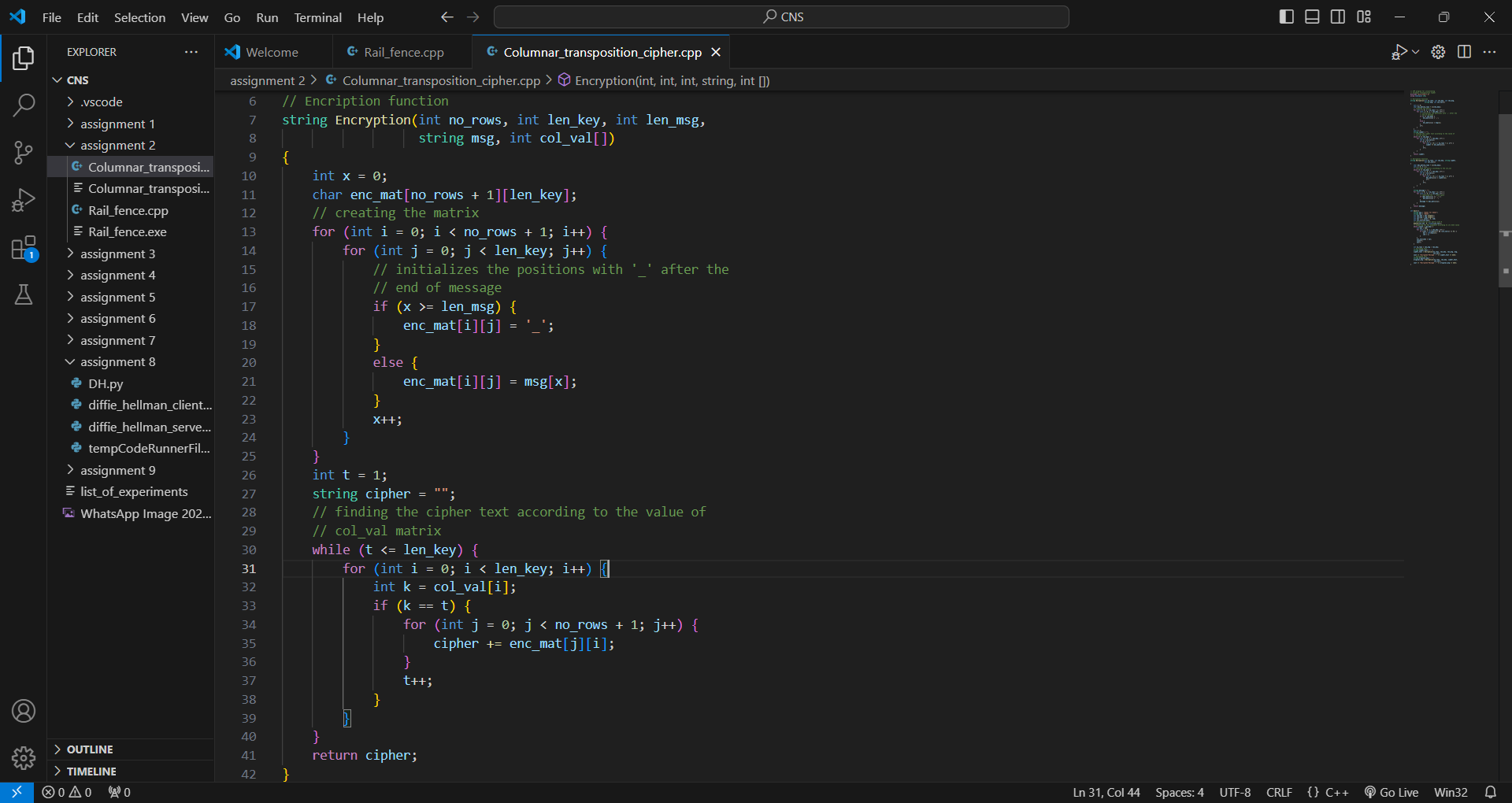
Row and Column Transformation:

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

1. The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
2. Width of the rows and the permutation of the columns are usually defined by a keyword.
3. For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: \_).
5. Finally, the message is read off in columns, in the order specified by the keyword.

**Decryption**

1. To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.
2. Then, write the message out in columns again, then re-order the columns by reforming the key word.

 A screenshot of a computer

Description automatically generated A screen shot of a computer

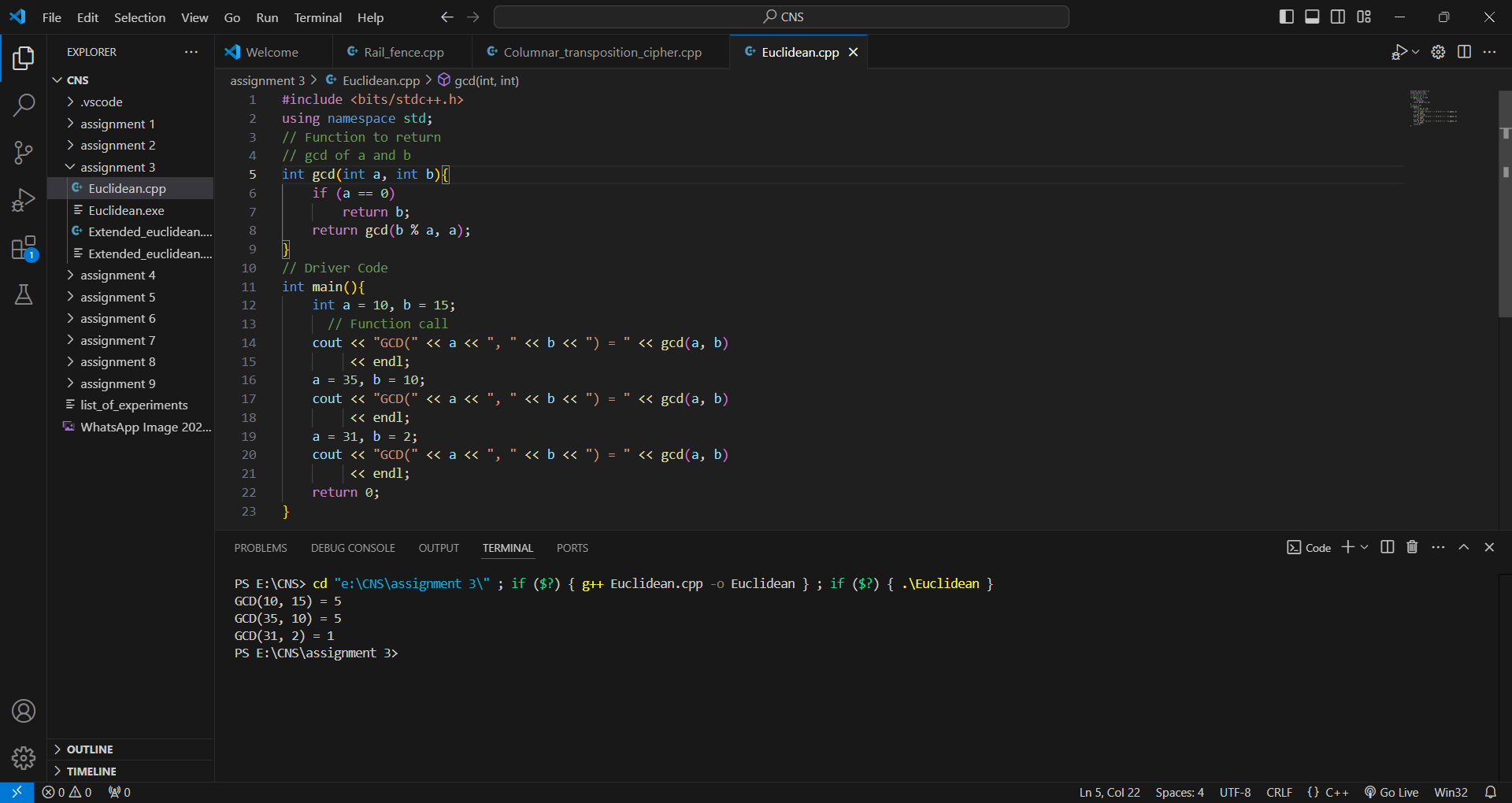
Description automatically generated

A screenshot of a computer program

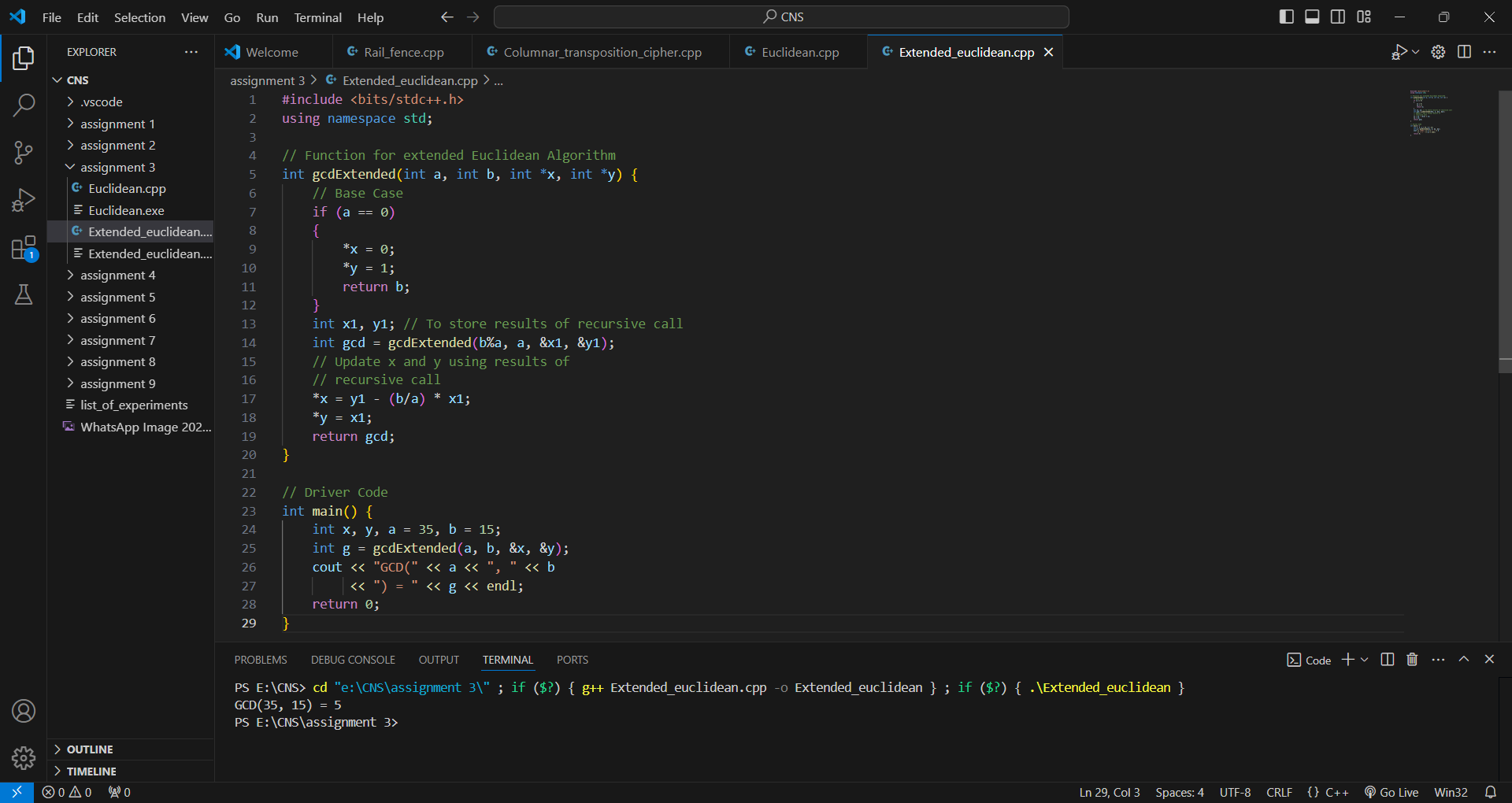
Description automatically generated

**Experiment 3:** **Implementation of Euclidean and Extended Euclidean Algorithm**

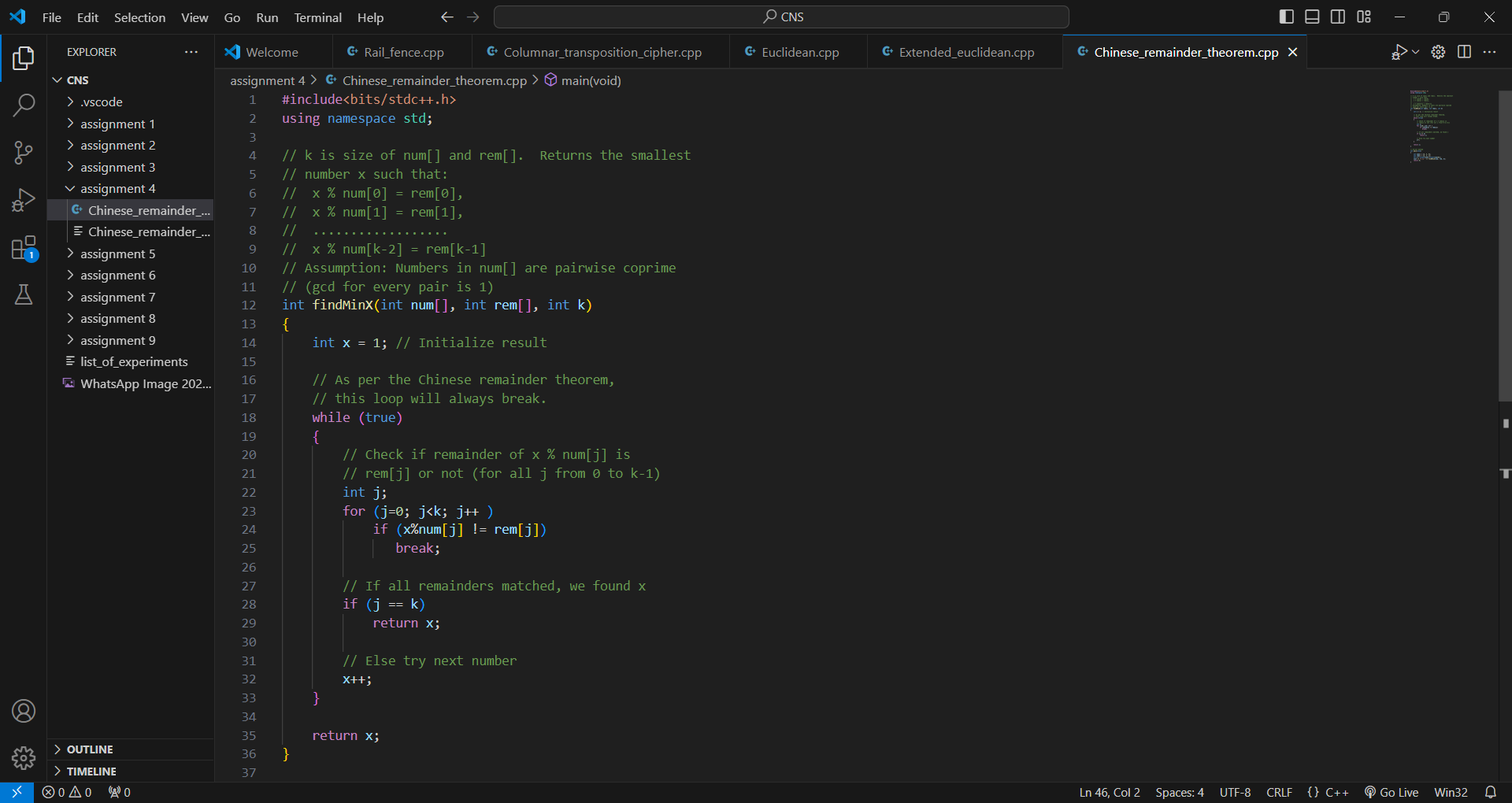
Euclidean:



Extended Euclidean:



**Experiment 4:** **Implementation of Chinese Remainder Theorem (CRT)**

****

**A screenshot of a computer

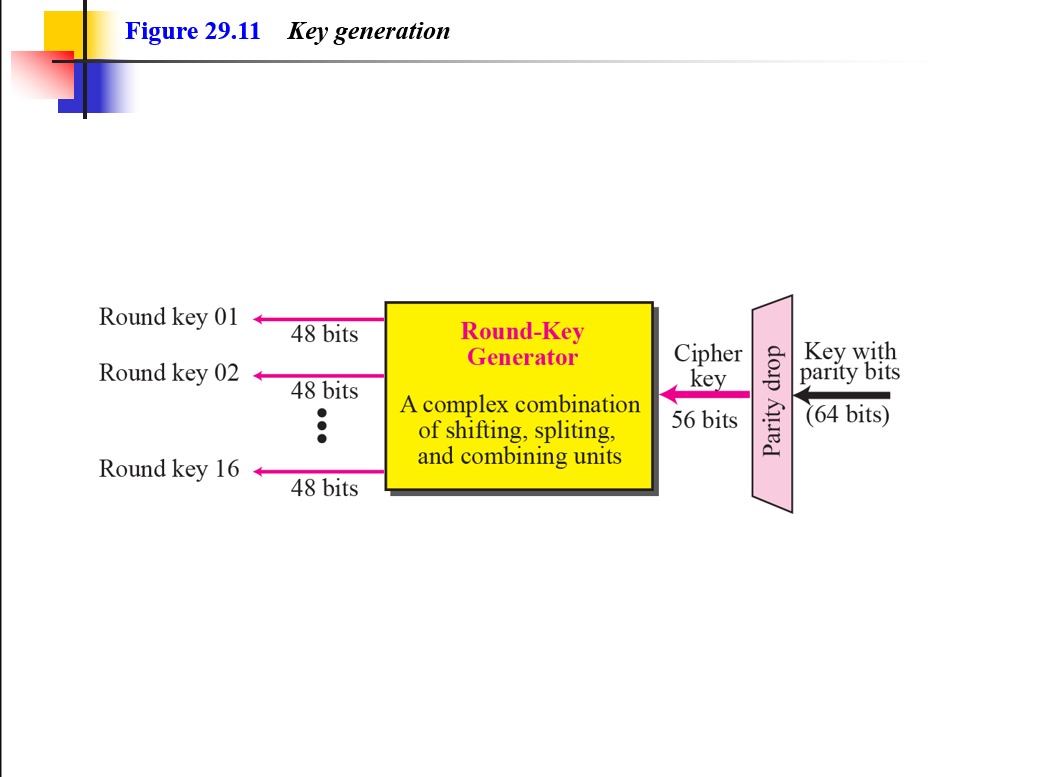
Description automatically generated**

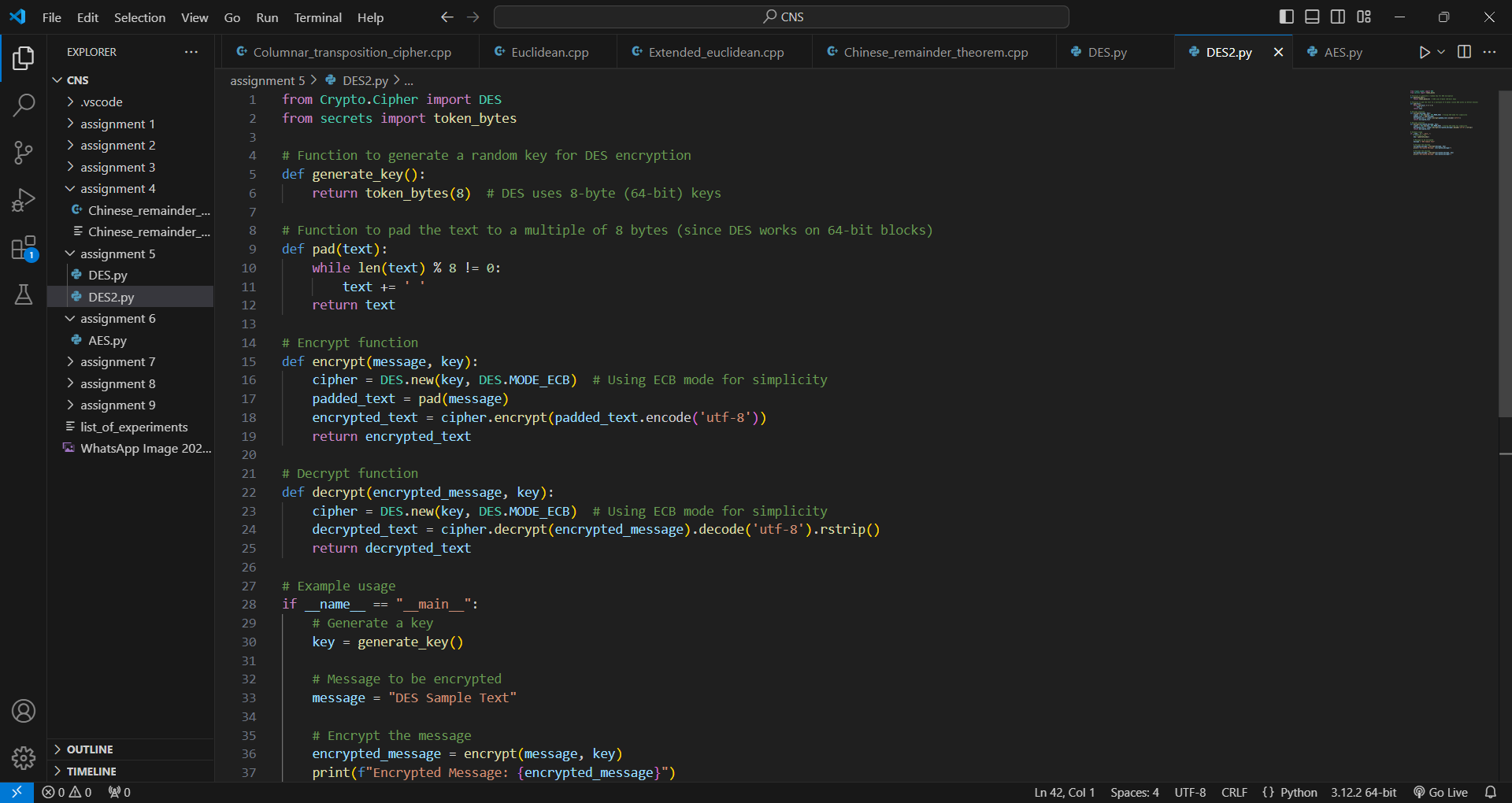
**Experiment 5:** **Apply DES algorithm for practical applications**

A diagram of a diagram

Description automatically generated A diagram of a computer component

Description automatically generated



****

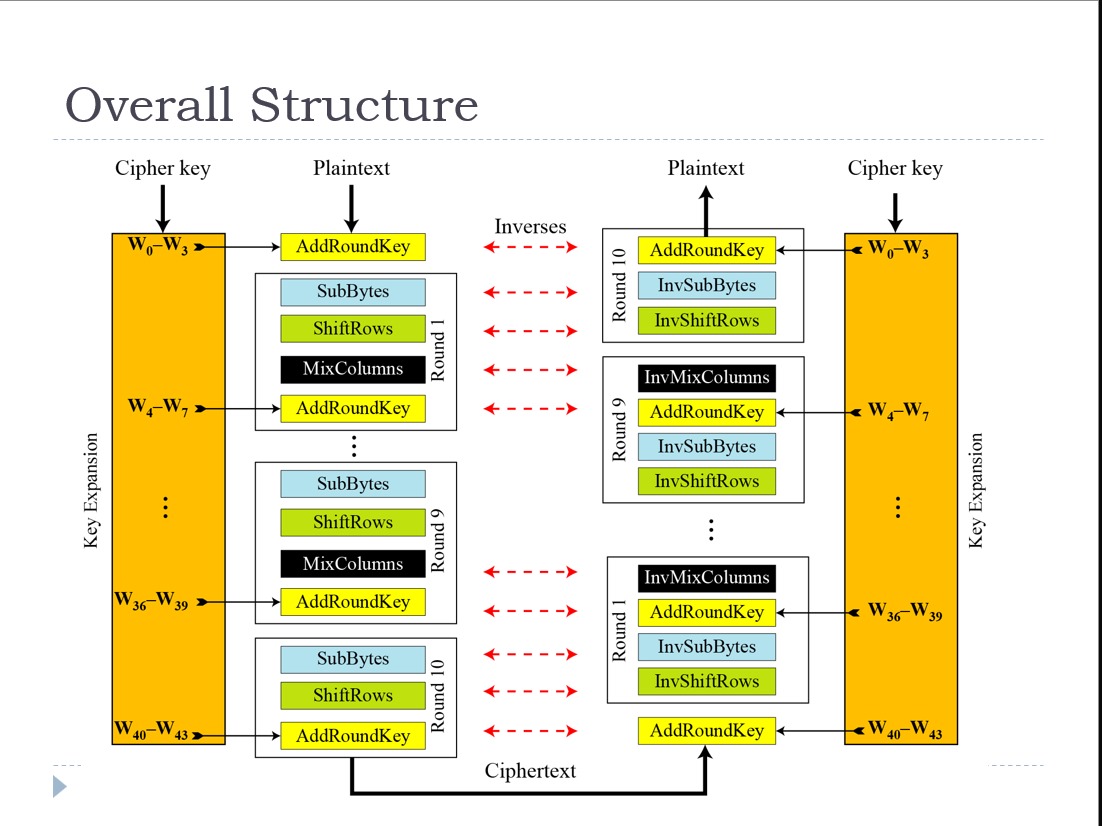
**A screenshot of a computer

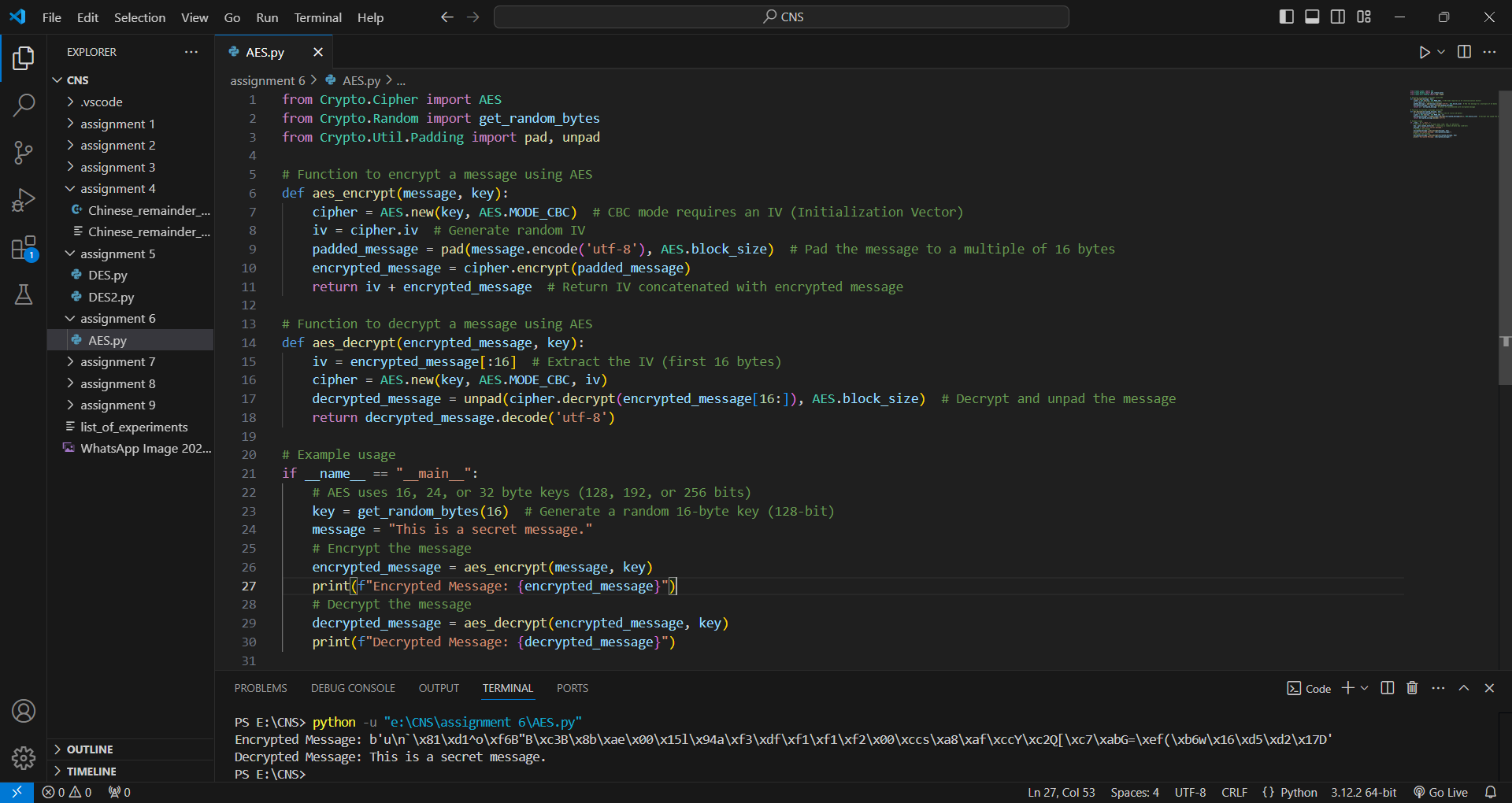
Description automatically generated**

**Experiment 6: Apply AES algorithm for practical applications**

A diagram of a number of round rounds

Description automatically generated



****