**2020BTECS00085, MANJIRI CHANDURE**

**CRYPTOGRAPHY AND NETWORK SECURITY LAB**

**ASSIGNMENT 3**

**Aim : Encryption and Decryption using Playfair Cipher Technique.**

The Playfair Cipher Technique is a substitution cipher that encrypts pairs of characters (digraphs) from the plaintext using a 5x5 key square matrix.

The matrix is constructed from a keyword, with duplicate letters removed and the keyword letters placed at the beginning.

Encryption involves applying rules based on the positions of the letters within the key square.

If the letters are in the same row, column, or form a rectangle, they are replaced by specific neighboring letters.

**Encryption:**

**1.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. 

**2.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.

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

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.

**Decryption**:

* Divide the ciphertext into digraphs.
* Apply the rules in reverse to each digraph to retrieve the original plaintext.

**Advantages**:

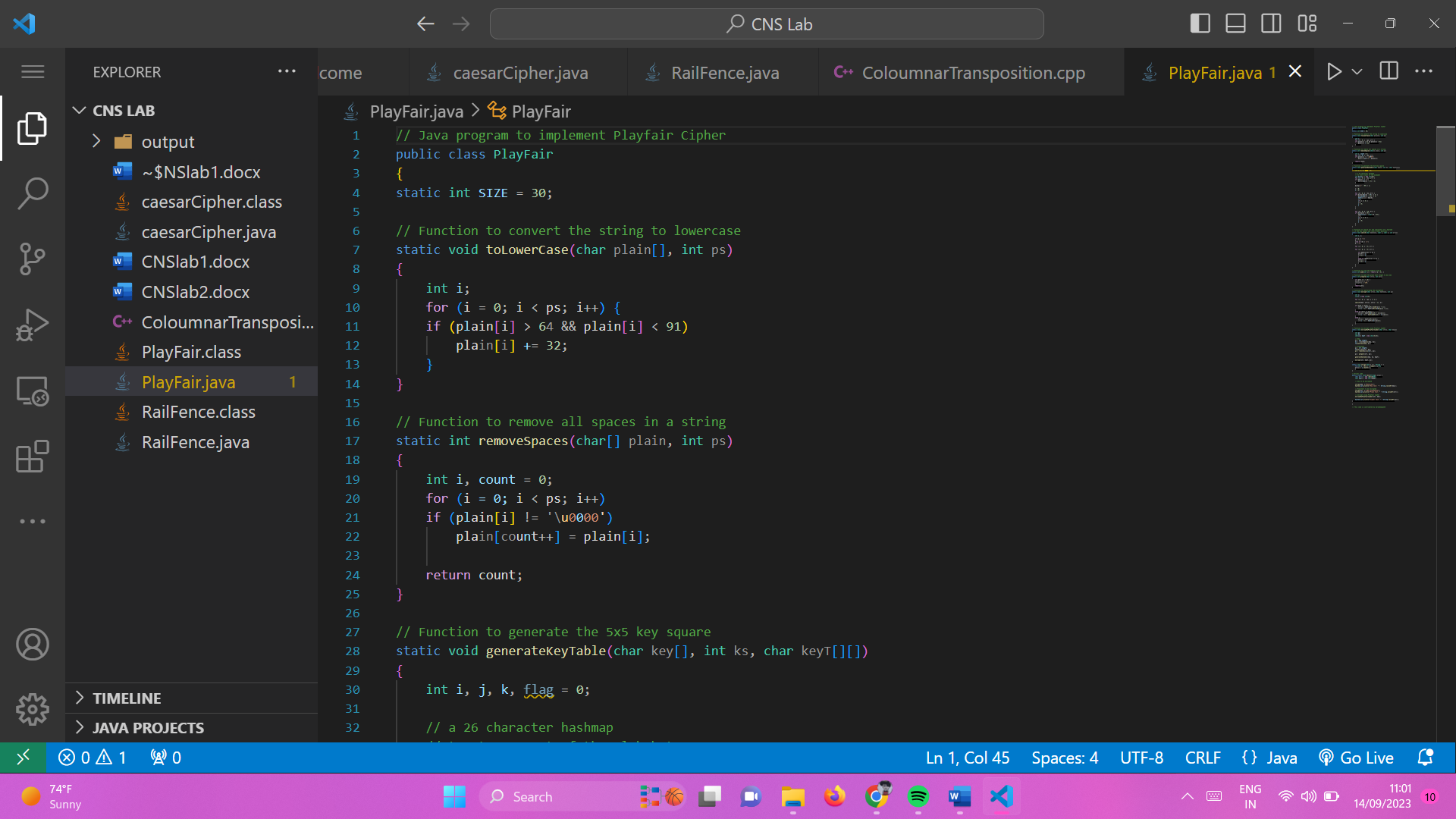
* Enhanced security due to digraphs and key square usage.
* Reduces susceptibility to frequency analysis.
* Key square generation is straightforward using a keyword.

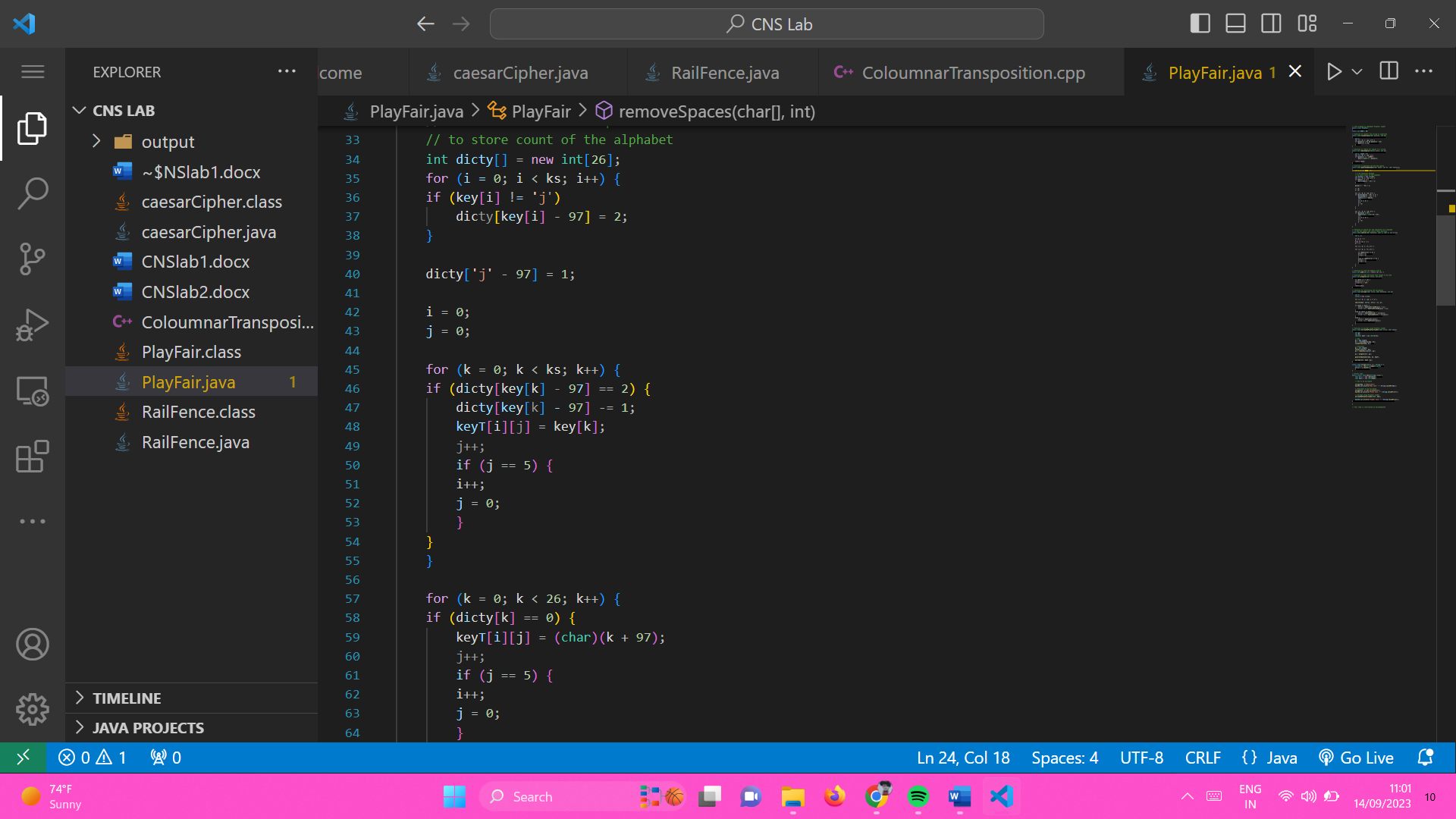
**Disadvantages**:

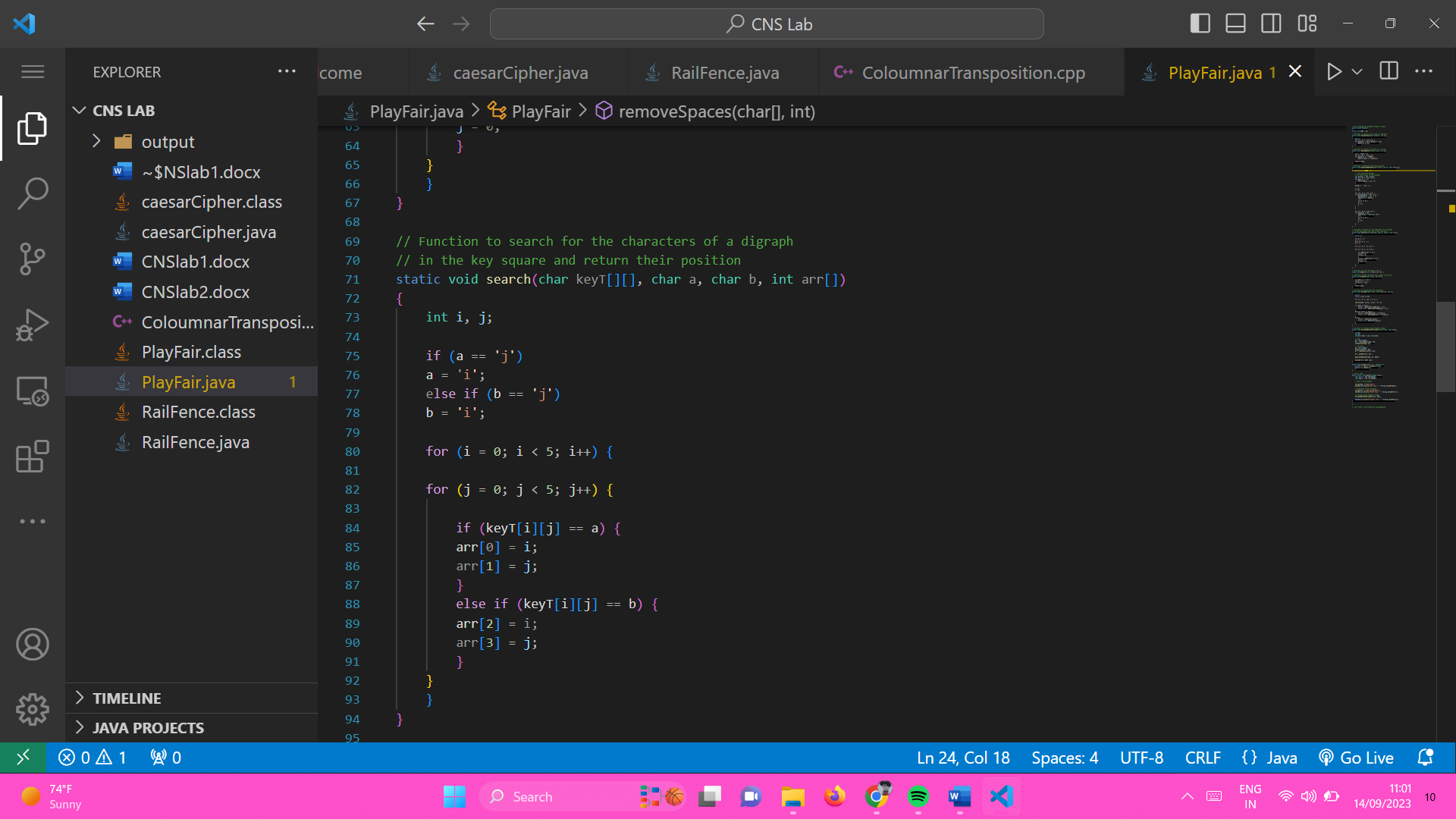
* Complexity increases with handling various cases (same row, column, rectangle).
* Security depends on the keyword and arrangement of the key square.

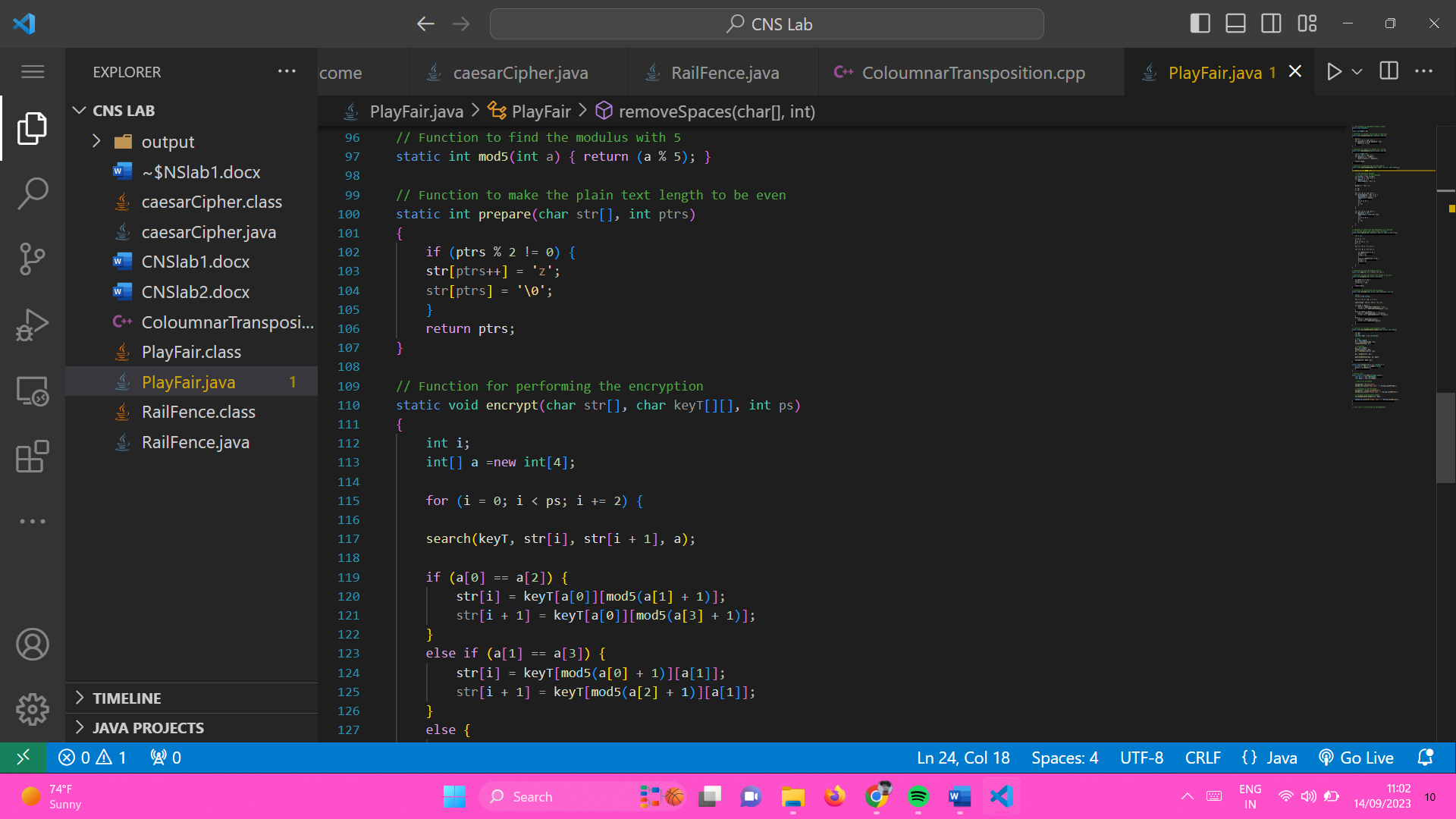
**Code:**

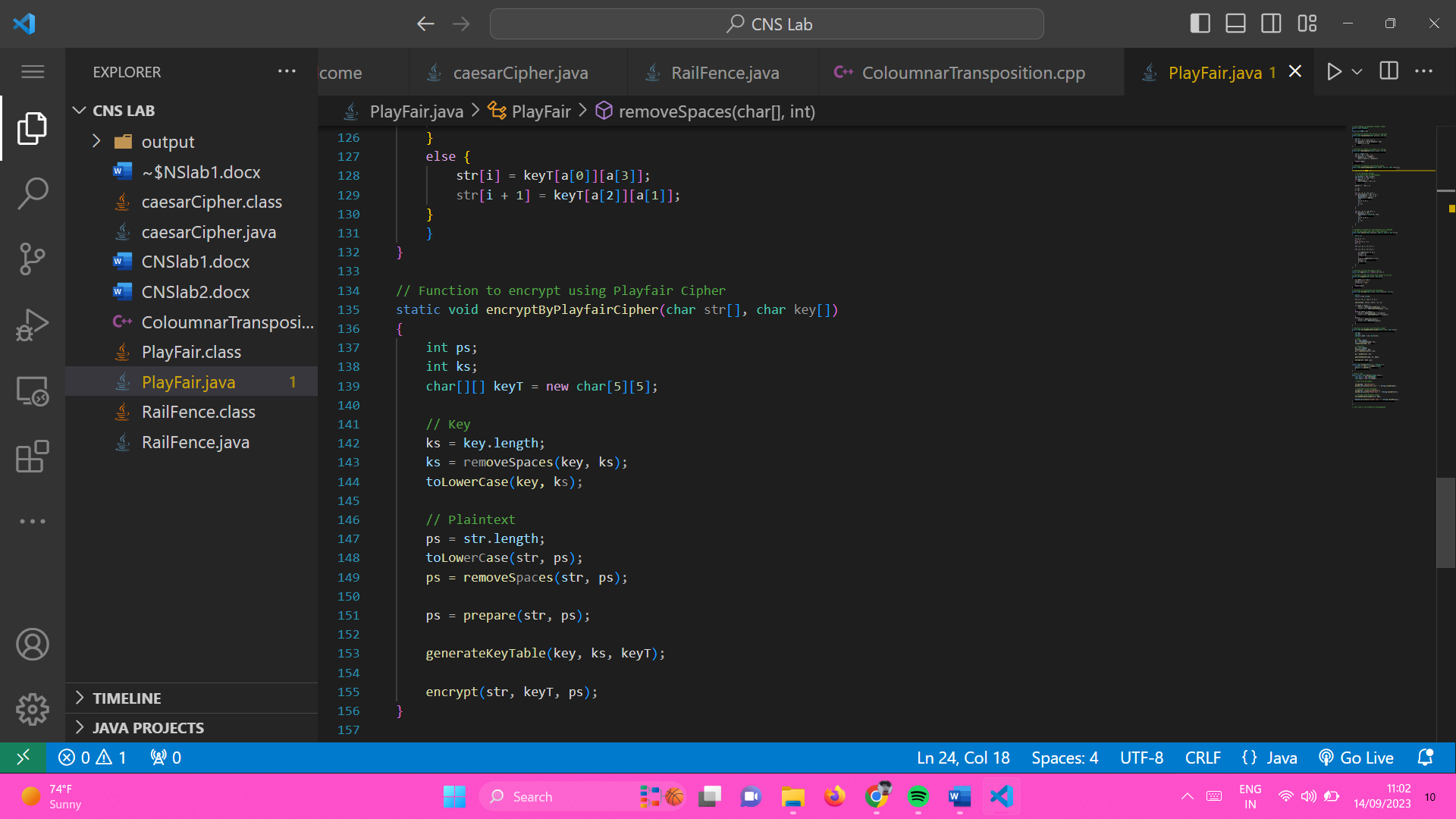
Implementation In Java:

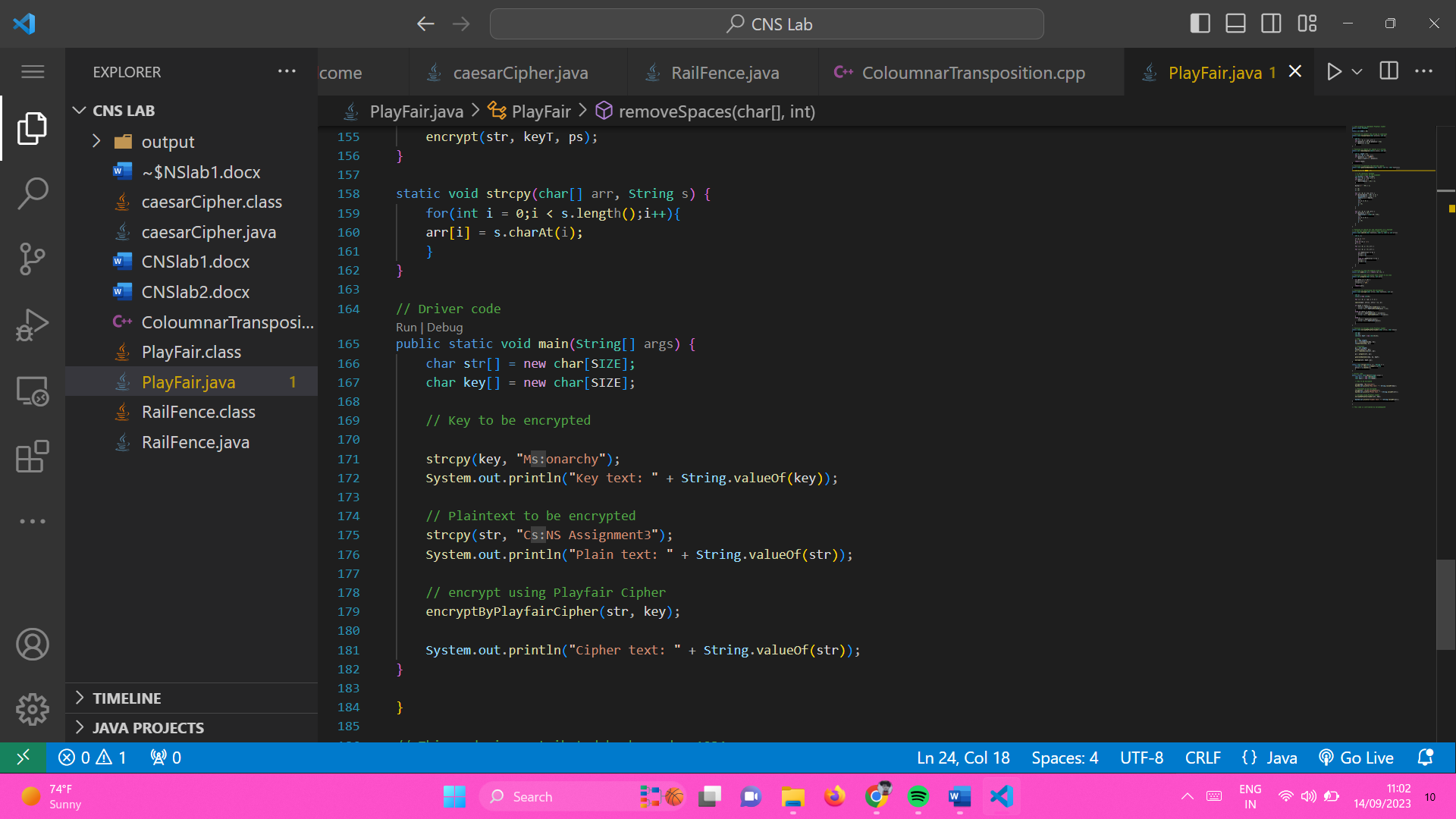




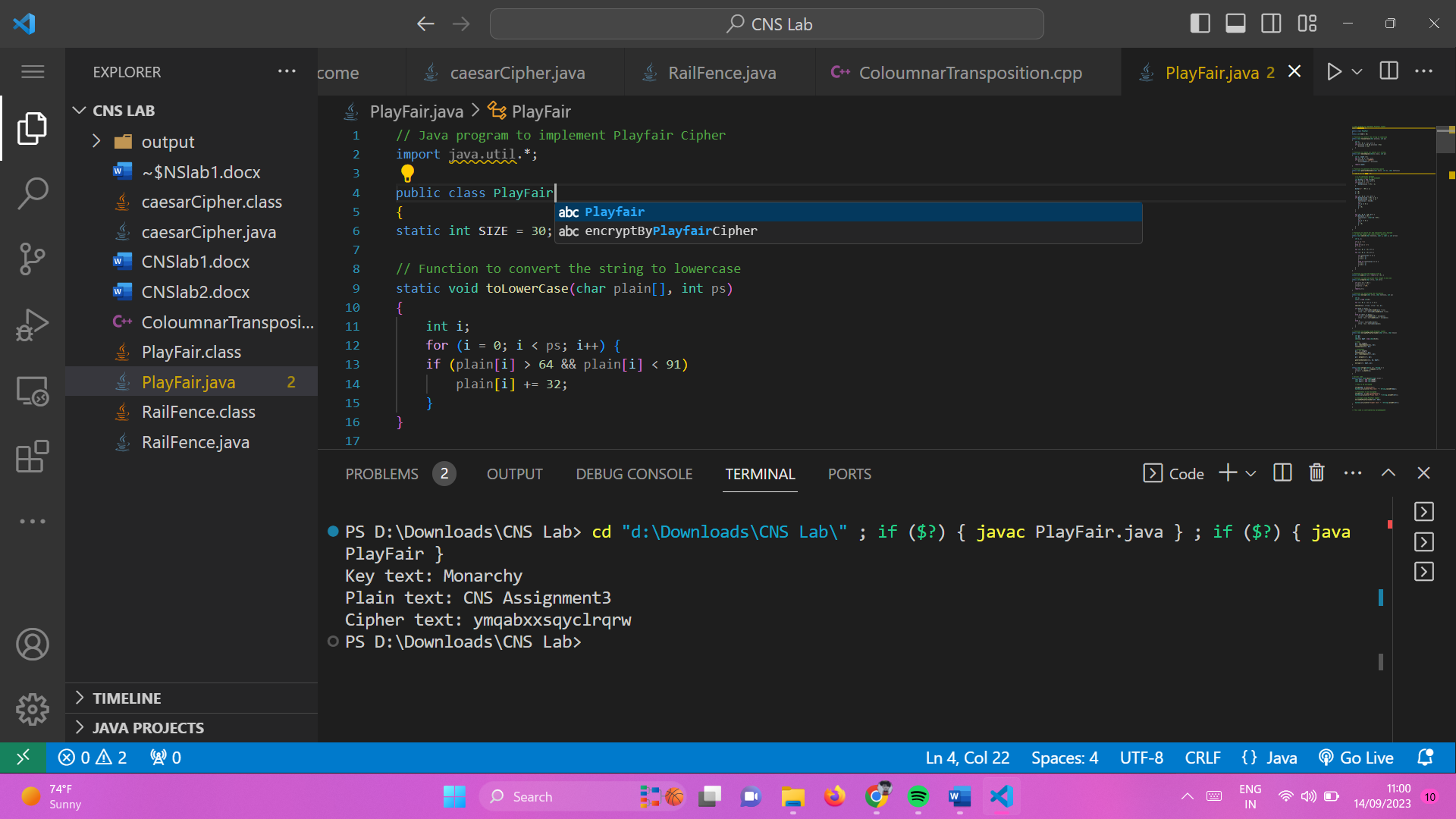








**Output:**

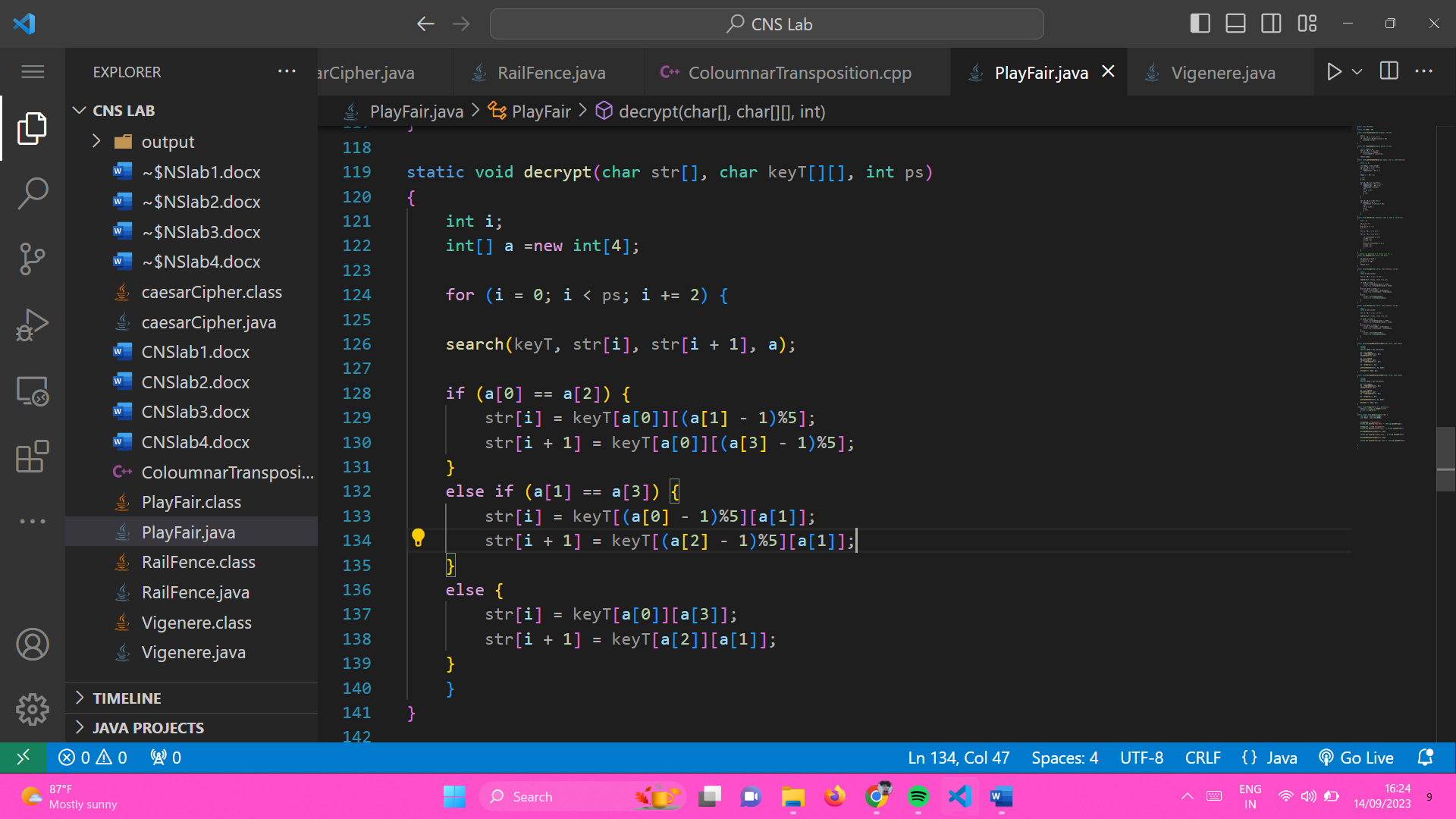


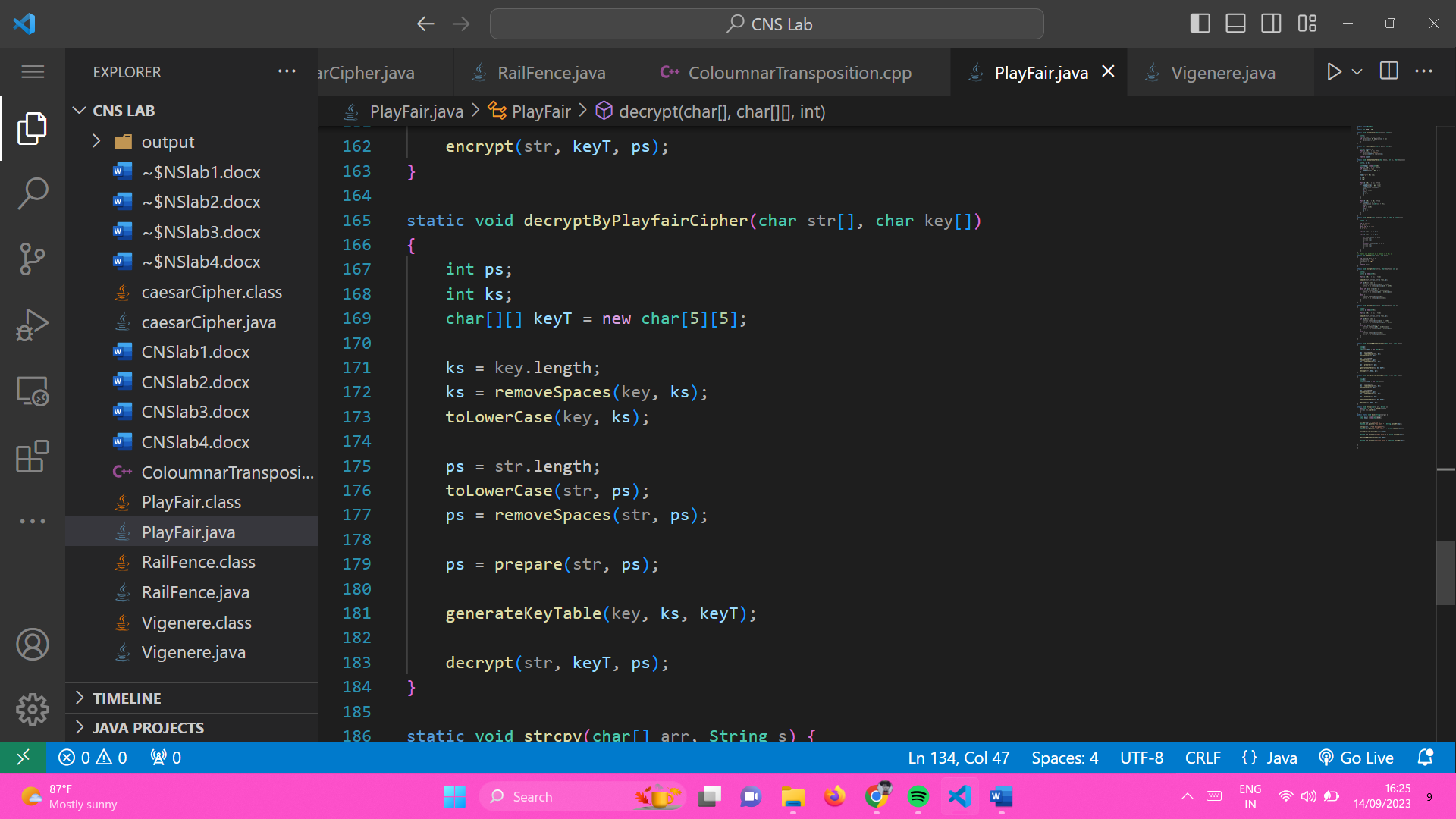
**Rules for Decryption:**

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

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





Output:

