**` 2020BTECS00085, MANJIRI CHANDURE**

**CRYPTOGRAPHY AND NETWORK SECURITY LAB**

**ASSIGNMENT 1**

**Aim: To Study and Implement Encryption and Decryption Using Caesar Cipher.**

**Theory:**

**CAESAR CIPHER:**

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

The number of positions a letter is shifted is determined by a key.

Easy to implement and use thus, making suitable for beginners to learn about encryption.

It is not secure against modern decryption methods. The small number of possible keys means that an attacker can easily try all possible keys until the correct one is found, making it vulnerable to a brute force attack. It is not suitable for long text encryption as it would be easy to crack. It is not suitable for secure communication as it is easily broken. Does not provide confidentiality, integrity, and authenticity in a message.

**Encryption:**

**In Encryption, input is a Plain text and output is a Cipher text.**

Step 1: Choose a secret key (a positive integer).

Step 2: Take the plaintext message you want to encrypt.

Step 3: Shift each letter in the message forward in the alphabet by the key positions.

Step 4: Non-alphabetical characters remain unchanged.

Step 5: The result is the ciphertext, the encrypted message.

**Decryption:**

**In Decryption, input is a Cipher text and output is a Plain text.**

Step 1: Have the same key used for encryption.

Step 2: Take the ciphertext (the encrypted message).

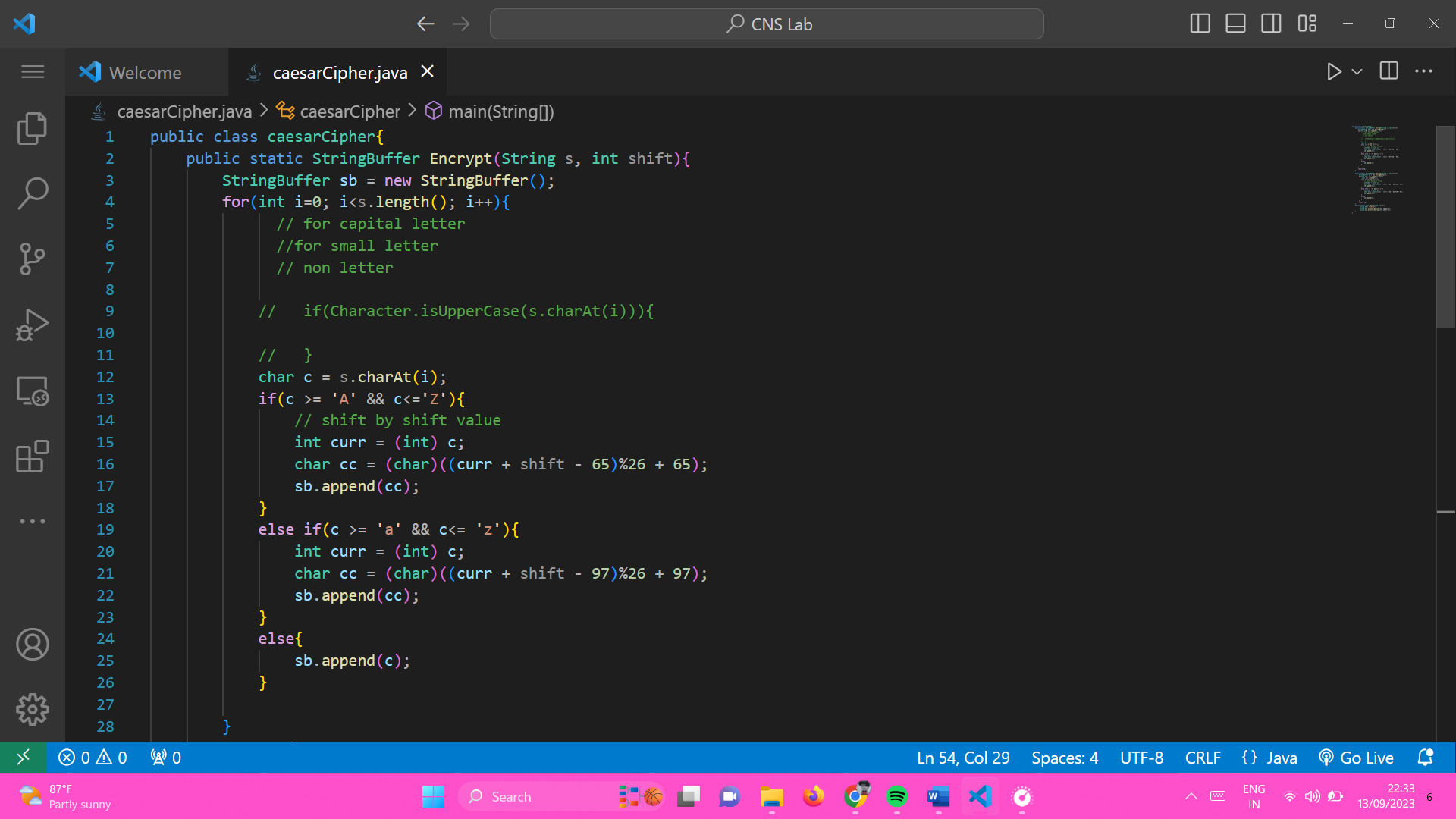
Step 3: Shift each letter in the ciphertext backward in the alphabet by the key positions.

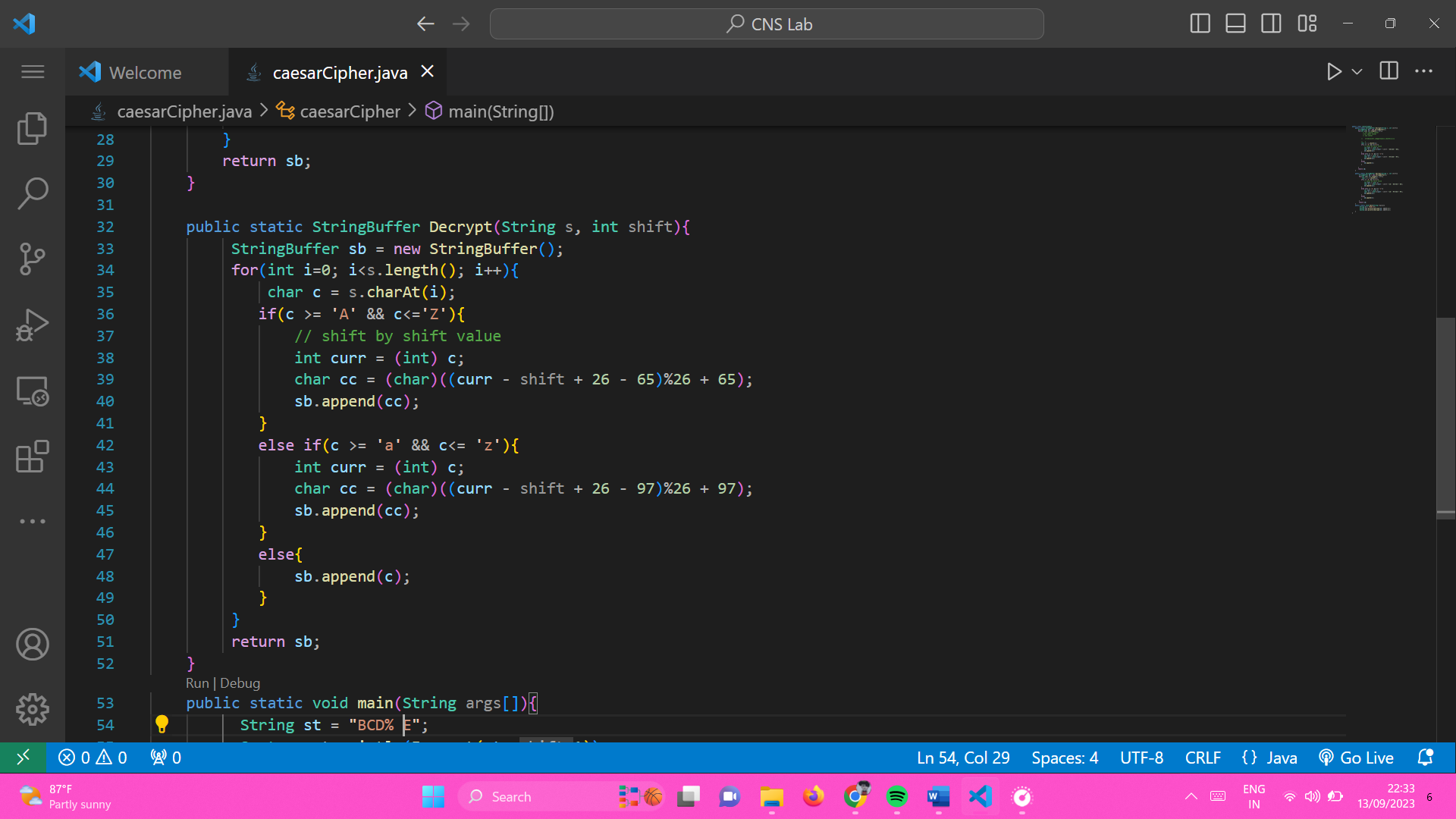
Step 4: Non-alphabetical characters remain unchanged.

Step 5: The result is the plaintext, the original message.

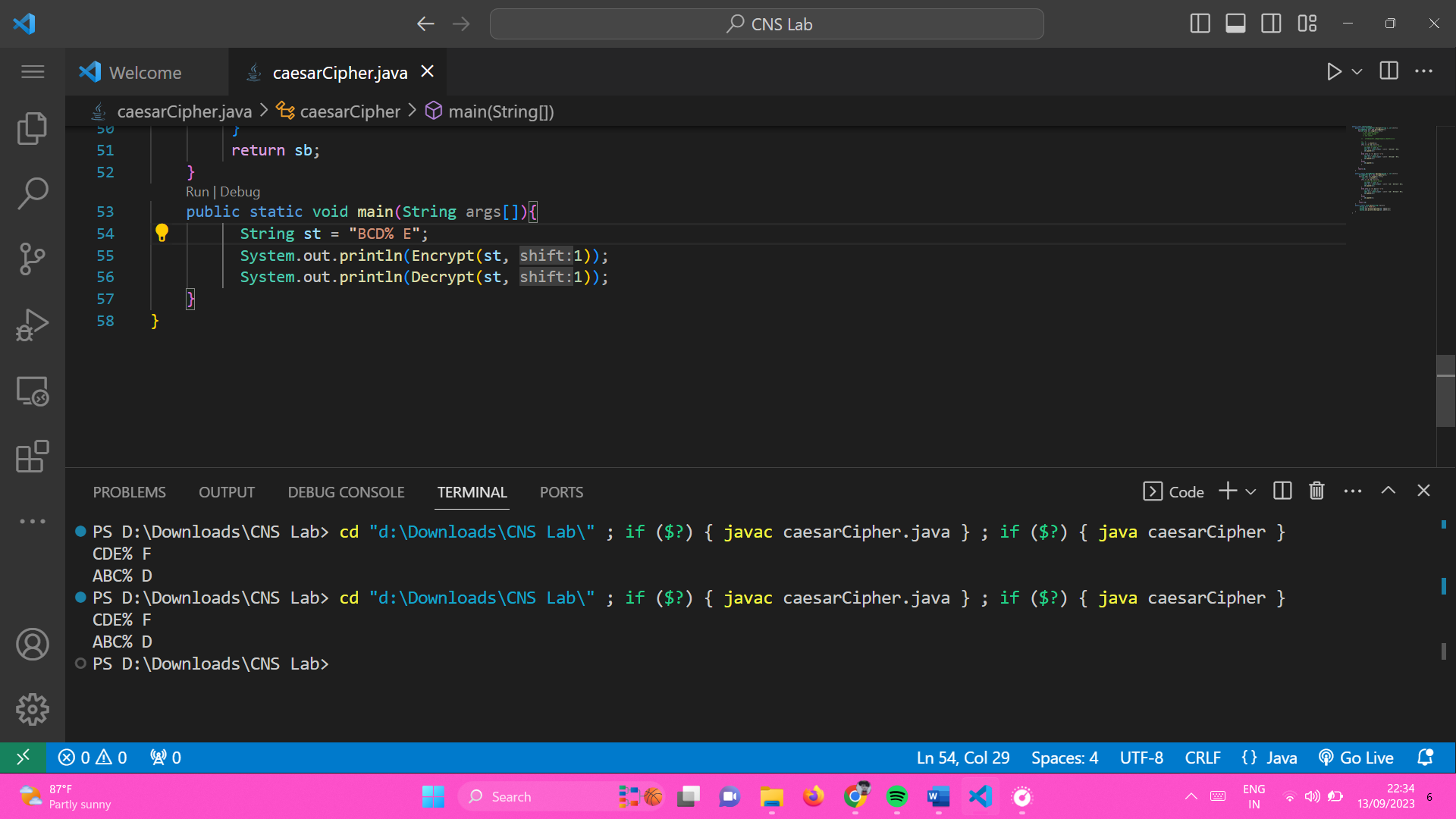
**Code:**

Caesar Cipher implementation in java:





**Output:**



**Limitations:**

1. It is not secure against modern decryption method.
2. Key space is small, so that attacker can try all possible keys.
3. It is vulnerable to brute force attack.
4. Not suitable for long size plaintext.
5. Does not provide confidentiality, integrity.
6. Not secure beacause it get easily broken.

**2)**

**Aim: To Decrypt the cipher text without knowing the key**

**Theory:**

Decrypting the cipher text which get encrypt by Caesar cipher is easy because its key space(number of possible key to this technique.

It is vulnerable to brute force attack. Attacker can try all possible 26 key and get defiantly plaintext from it.

It is not supporting the modern decryption technique.

Algorithm:

Step 1) input as Cipher text.

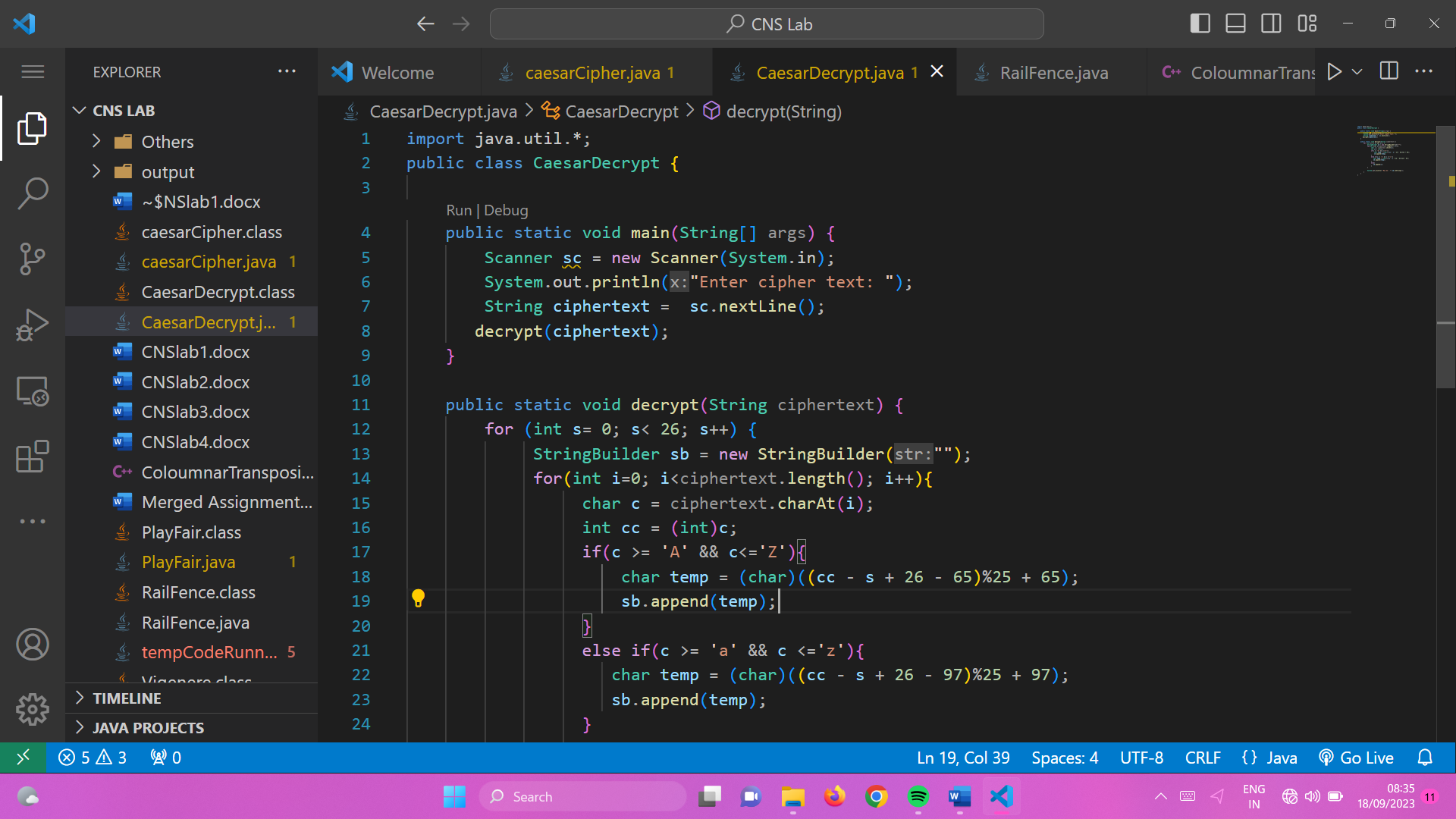
Step 2) For loop for 26 time.

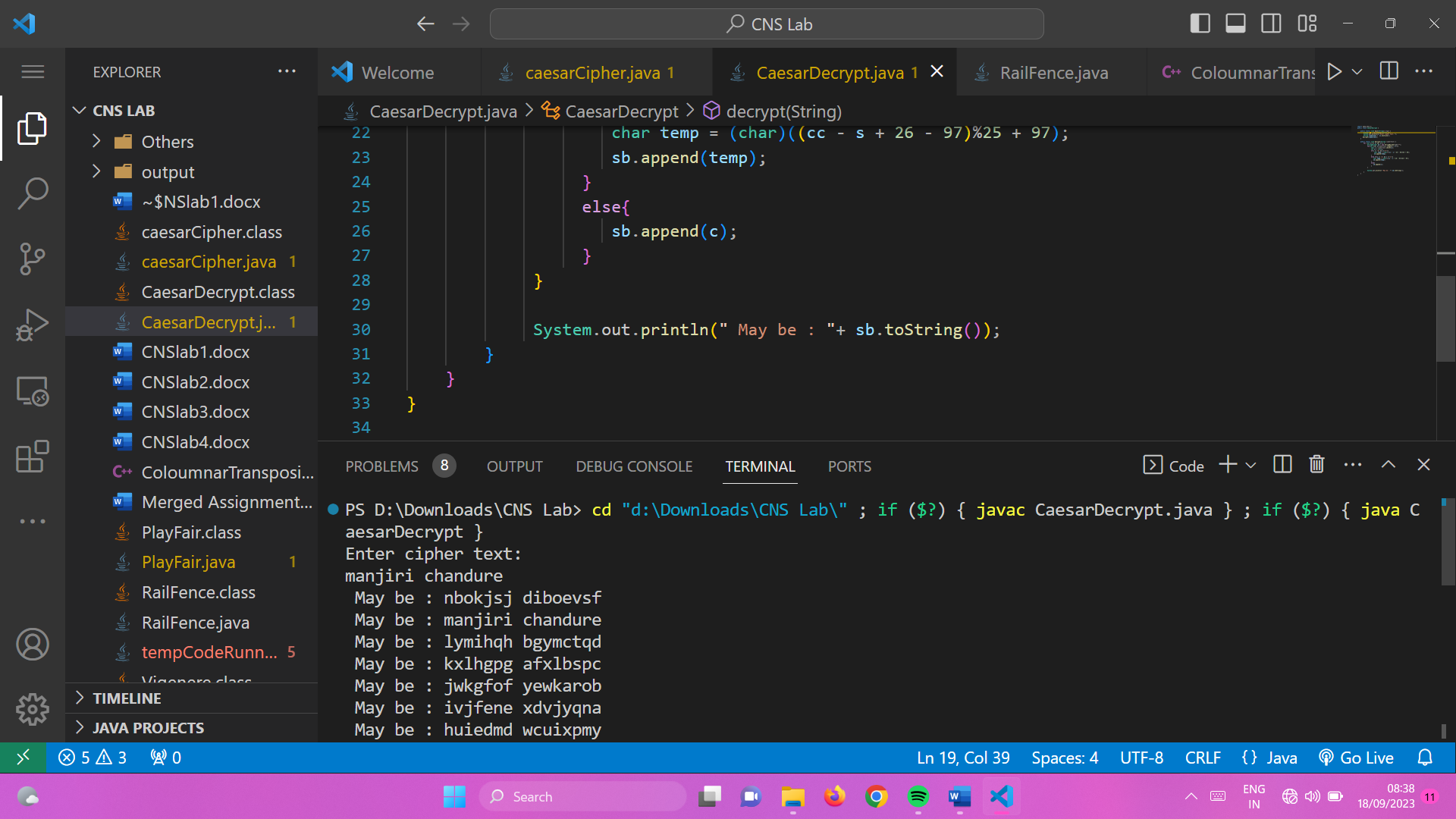
Step 3) try to shift each character of cipher text left, means decrypting. Done by converting char to int, and subtract shift value for each value in each iteration.

Step 4) convert again to char. Create string from it.

Step 5) Print all possible plaintext from given shift value.

**Code:**





**Output:**

