**2020BTECS00085, MANJIRI CHANDURE**

**CRYPTOGRAPHY AND NETWORK SECURITY LAB**

**ASSIGNMENT 4**

**Aim: To encrypt and decrypt of plaintext by Vigenère Cipher Technique**

**Theory:**

The Vigenère Cipher Technique is a polyalphabetic substitution cipher that adds an extra layer of complexity to encryption by using a keyword or key phrase to determine the shifts applied to the plaintext letters.

Unlike monoalphabetic ciphers, where each letter is replaced with a fixed substitution, the Vigenère Cipher employs multiple alphabets with different shifts, making it more secure against frequency analysis.

**Key Setup:**

* Choose a keyword or key phrase.
* Replicate the keyword to match the length of the plaintext, repeating it as needed.
* Convert the keyword letters to their corresponding numerical values (A=0, B=1, ..., Z=25).

**Encryption:**

* Divide the plaintext into individual letters and convert them to numerical values.
* For each letter, determine the shift value using the corresponding keyword letter.
* Shift the plaintext letter by the calculated shift value (mod 26).
* Convert the shifted numerical value back to a letter to create the ciphertext.

**Decryption:**

* Divide the ciphertext into individual letters and convert them to numerical values.
* For each letter, determine the shift value using the corresponding keyword letter.
* Reverse the shift (subtract the shift value, mod 26).
* Convert the shifted numerical value back to a letter to retrieve the original plaintext.

**Advantages:**

* Stronger security due to polyalphabetic nature and keyword-driven shifts.
* Reduces susceptibility to frequency analysis.
* Key space increases with keyword length, enhancing security.

**Disadvantages:**

* Vulnerable to key length repetition for shorter keywords.
* Security can weaken if the keyword is short or predictable.

**Encryption**

The plaintext(P) and key(K) are added modulo 26.

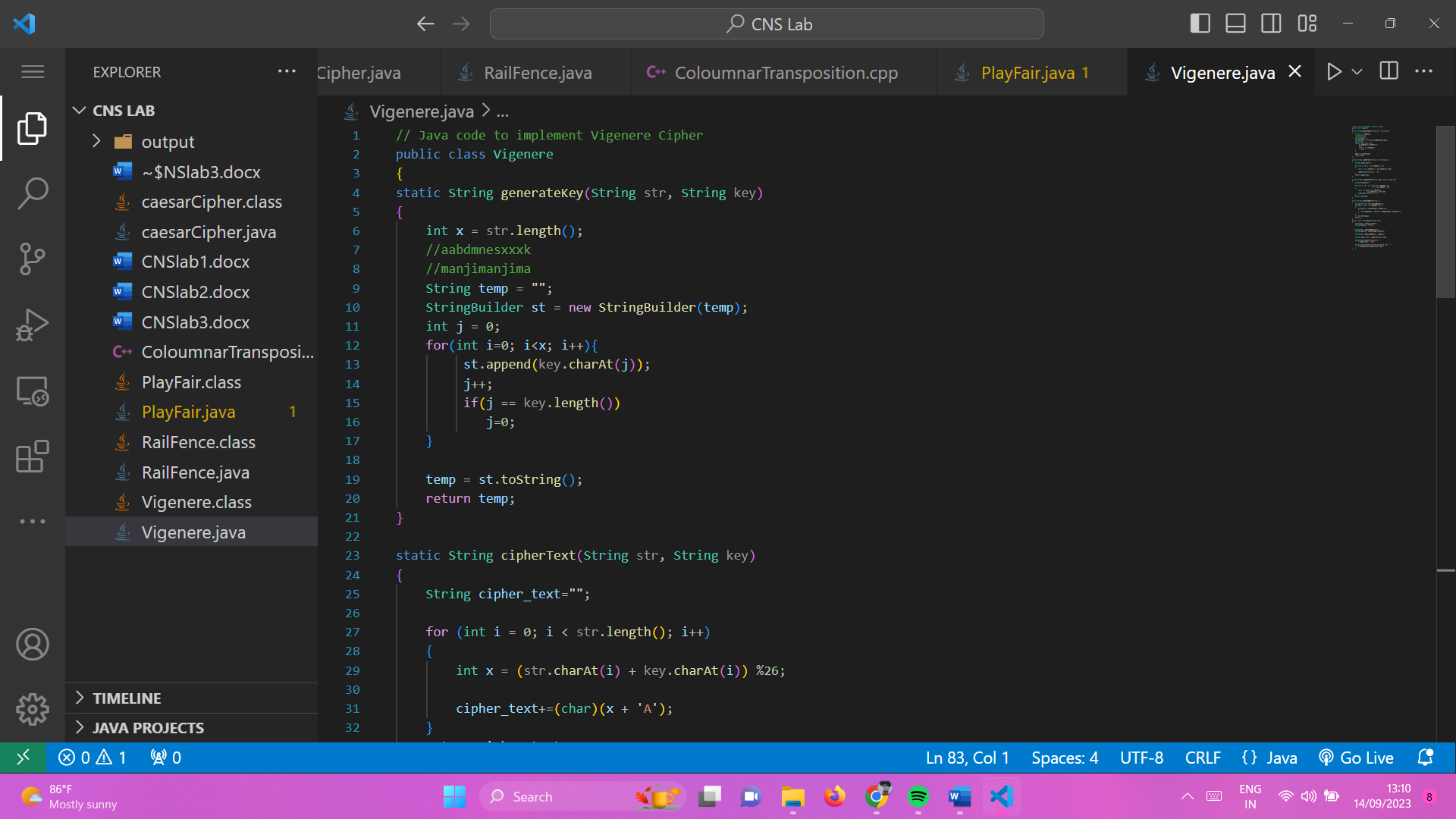
Ei = (Pi + Ki) mod 26

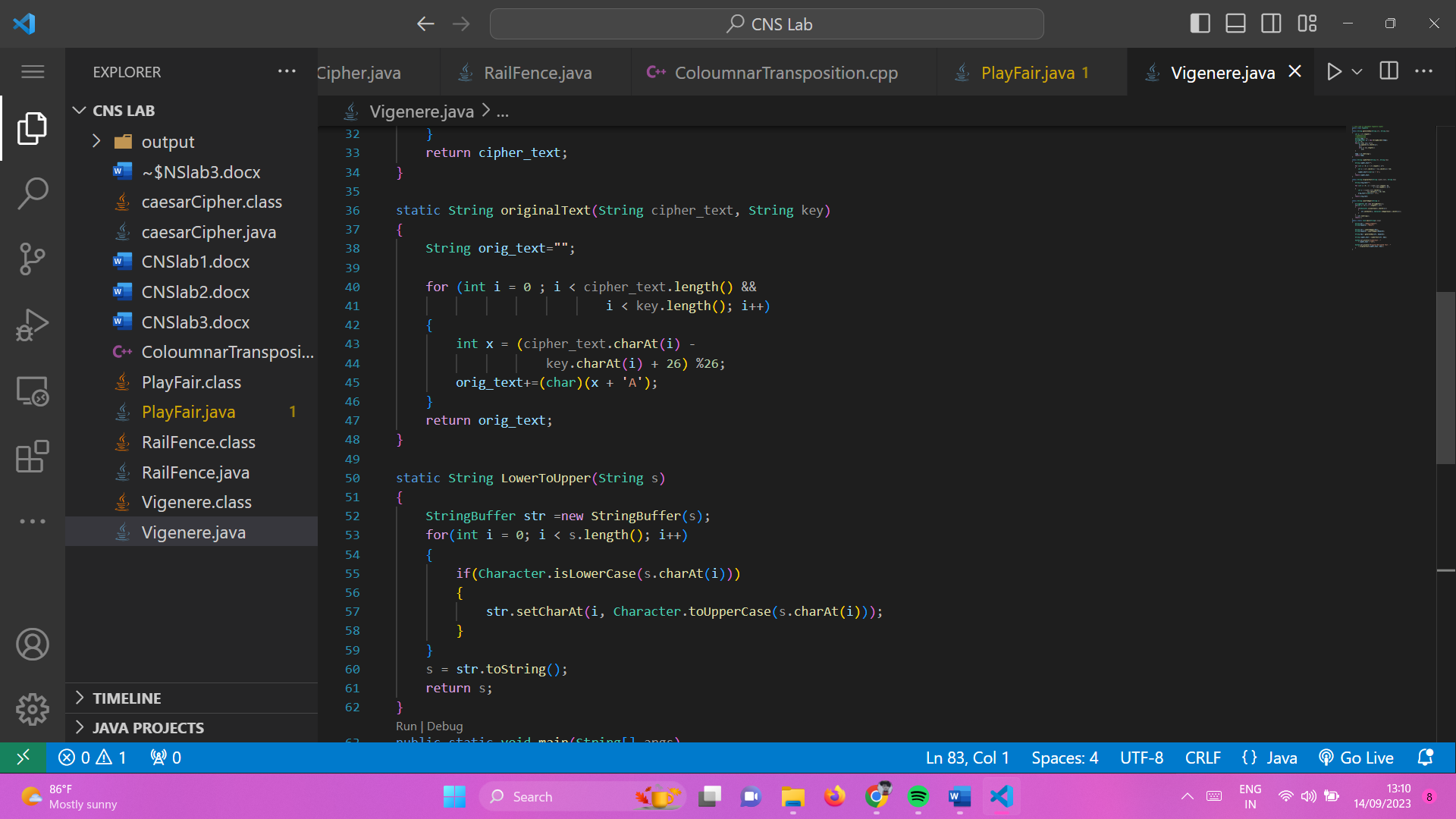
**Decryption**

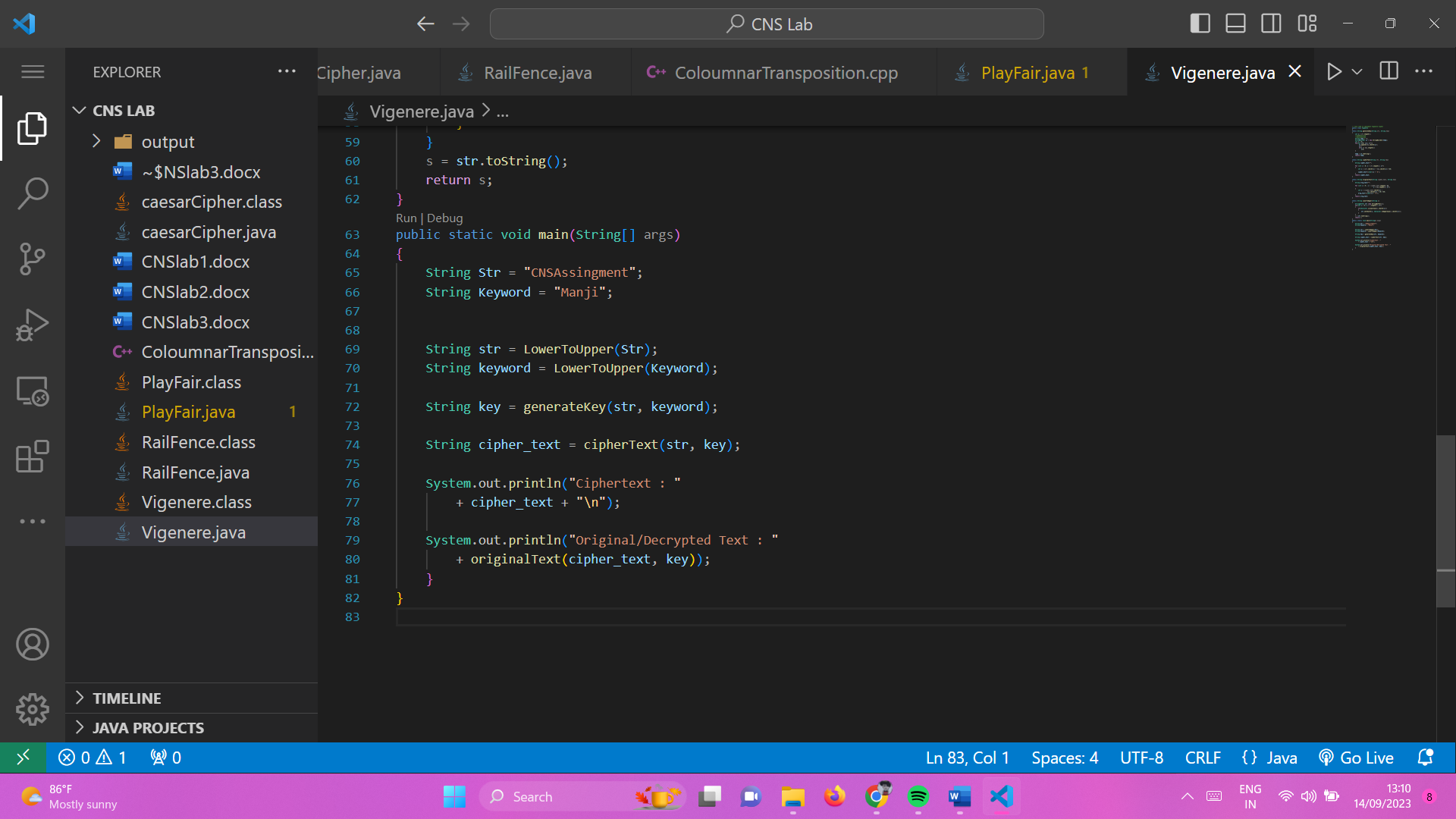
Di = (Ei - Ki +26) mod 26

**Code:**

Implementation in java:







**Output:**

