**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

**EXPERIMENT 4**

**Aim** :- write a program in java to perform cryptanalysis or decoding of Vigenere cipher.

**Theory:-** Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenere square or Vigenere table.

* The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.

**Code:-**

import java.util.\*;

class lab4 {

public static String encrypt(String plaintext, String keyword) {

StringBuilder ciphertext = new StringBuilder();

keyword = keyword.toUpperCase();

int keywordIndex = 0;

for (char c : plaintext.toCharArray()) {

if (Character.isLetter(c)) {

char base = Character.isUpperCase(c) ? 'A' : 'a';

int shift = keyword.charAt(keywordIndex) - 'A';

char encryptedChar = (char) ((c - base + shift) % 26 + base);

ciphertext.append(encryptedChar);

keywordIndex = (keywordIndex + 1) % keyword.length();

} else {

ciphertext.append(c)

}

}

return ciphertext.toString();

}

public static String decrypt(String ciphertext, String keyword) {

StringBuilder decryptedText = new StringBuilder();

keyword = keyword.toUpperCase();

int keywordIndex = 0;

for (char c : ciphertext.toCharArray()) {

if (Character.isLetter(c)) {

char base = Character.isUpperCase(c) ? 'A' : 'a';

int shift = keyword.charAt(keywordIndex) - 'A';

char decryptedChar = (char) ((c - base - shift + 26) % 26 + base);

decryptedText.append(decryptedChar);

keywordIndex = (keywordIndex + 1) % keyword.length();

} else {

decryptedText.append(c);

}

}

return decryptedText.toString();

}

public static void main(String[] args) {

Scanner sc = new Scanner(System.in);

System.out.println("Enter plaintext to encrypt:");

String plaintext = sc.nextLine();

System.out.println("Enter Key for encrypting and decrypting:");

String keyword = sc.nextLine();

String encrypted = encrypt(plaintext, keyword);

System.out.println("Encrypted Text is: " + encrypted);

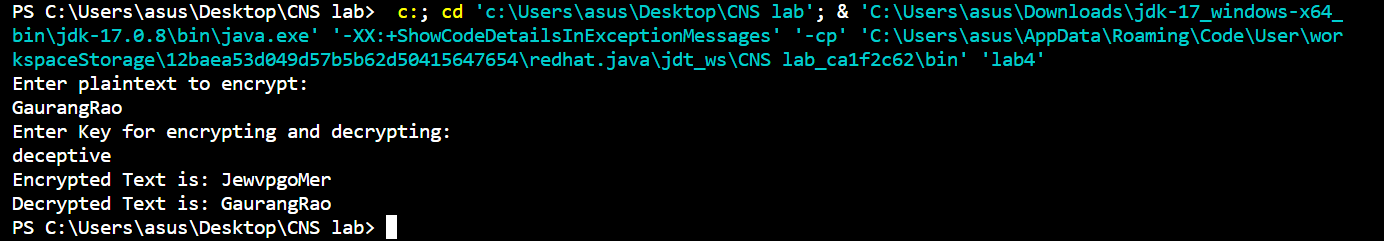
String decrypted = decrypt(encrypted, keyword);

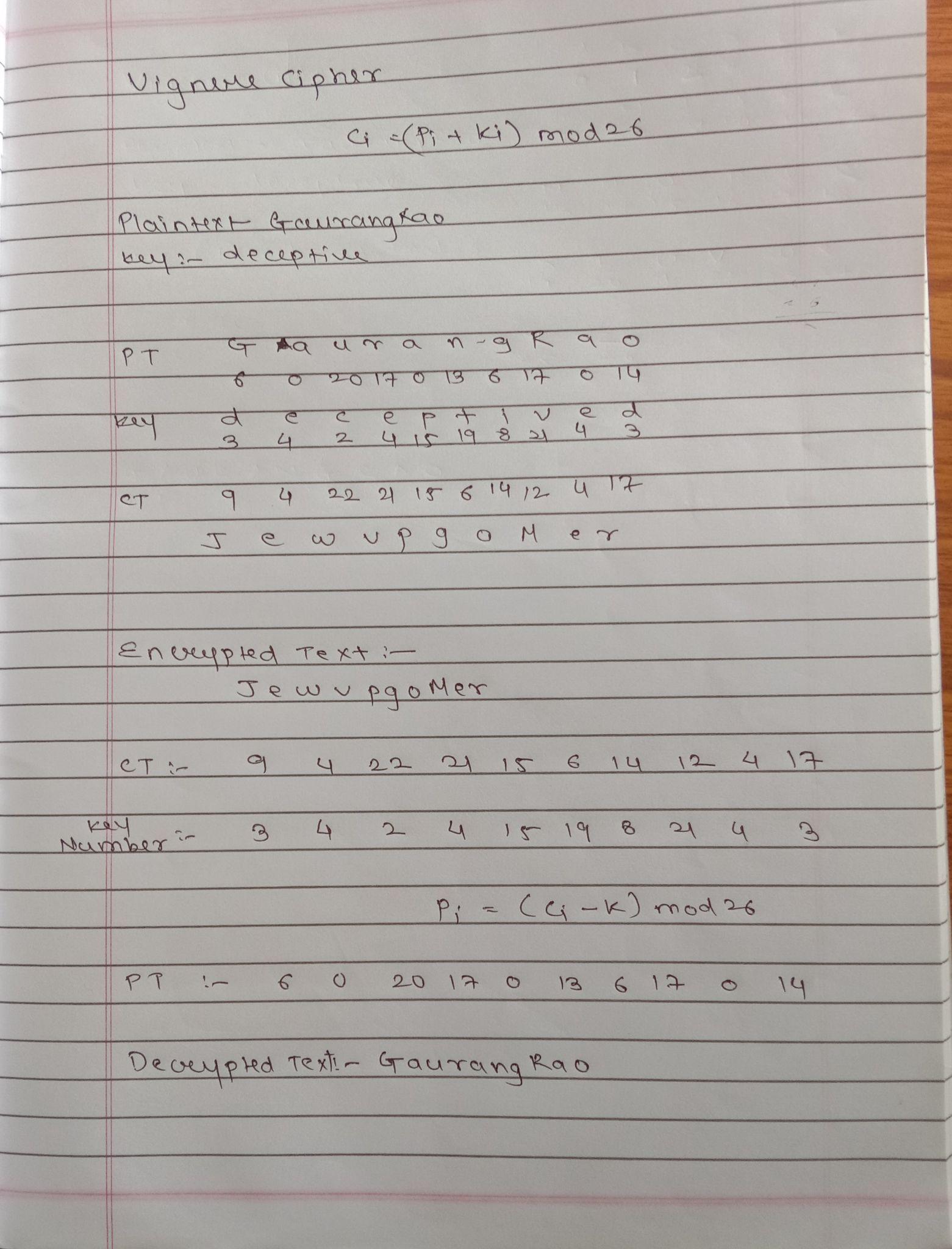
System.out.println("Decrypted Text is: " + decrypted);

}

}

**Output:-**





**Conclusion:-** Vigenere cipher is understood and implemented.