**VU1F14150\_\_**

***Experiment No-2***

***Aim***: Write a program to encrypt and decrypt using vigener/autokey cipher .

***Theory****:*

The Vigenère cipher, was invented by a Frenchman, Blaise de Vigenère in the 16th century.The Vigenère cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword. It is a form of polyalphabetic substitution.Unlike the monoalphabetic ciphers, polyalphabetic ciphers are not susceptible to frequency analysis, as more than one letter in the plaintext can be represented by a single letter in the encryption.

In order to cipher a text, take the first letter of the message and the first letter of the key, add their value (letters have a value depending on theirrank in the alphabet, starting with 0). The result of the addition modulo 26 (26=the number of letter in the alphabet) gives the rank of the ciphered letter.

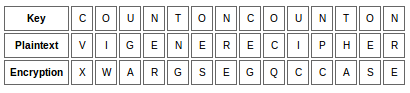
The maths behind the Vigenère cipher can be written as follows:

To encrypt a message: Ca = Ma + Kb (mod 26)

To decrypt a message: Ma = Ca – Kb (mod 26)

(Where C = Code, M = Message, K = Key, and where a = the ath character of the message bounded by the message, and b is the bth character of the Key bounded by the length of the key.)

So, if we were to encode a message using the key COUNTON, we write it as many times as necessary above our message. To find the encryption, we take the letter from the intersection of the Key letter row, and the Plaintext letter column.



To decipher the message, the recipient needs to write out the key above the ciphertext and reverse the process.

***Program:***

import java.util.\*;

public class VigenereCipher

{

public static String encrypt(String text, final String key)

{

String res = "";

text = text.toUpperCase();

for (int i = 0, j = 0; i < text.length(); i++)

{

char c = text.charAt(i);

if (c < 'A' || c > 'Z')

continue;

res += (char) ((c + key.charAt(j) - 2 \* 'A') % 26 + 'A');

j = ++j % key.length();

}

return res;

}

public static String decrypt(String text, final String key)

{

String res = "";

text = text.toUpperCase();

for (int i = 0, j = 0; i < text.length(); i++)

{

char c = text.charAt(i);

if (c < 'A' || c > 'Z')

continue;

res += (char) ((c - key.charAt(j) + 26) % 26 + 'A');

j = ++j % key.length();

}

return res;

}

public static void main(String[] args){

Scanner sc = new Scanner(System.in);

String key = "VIGENERECIPHER";

System.out.print("Enter the message: ");

String message = sc.nextLine();

String encryptedMsg = encrypt(message, key);

System.out.println("String: " + message);

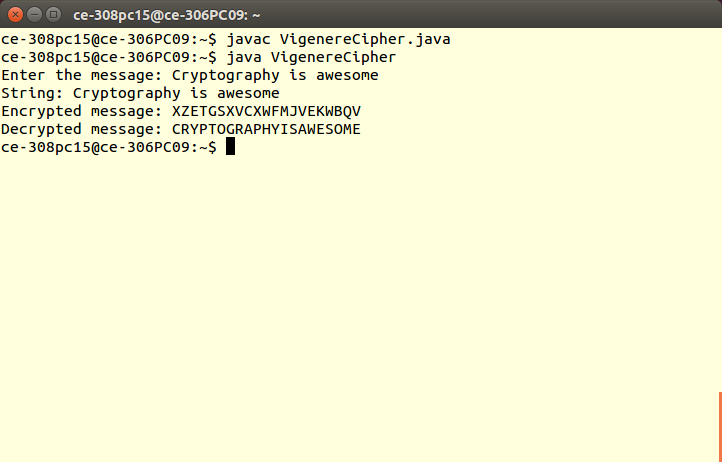
System.out.println("Encrypted message: " + encryptedMsg);

System.out.println("Decrypted message: " + decrypt(encryptedMsg, key));

}

}

***Output:***



***Conclusion:*** Thus, program to encrypt and decrypt using vigener/autokey cipher has been successfully studied and implemented.