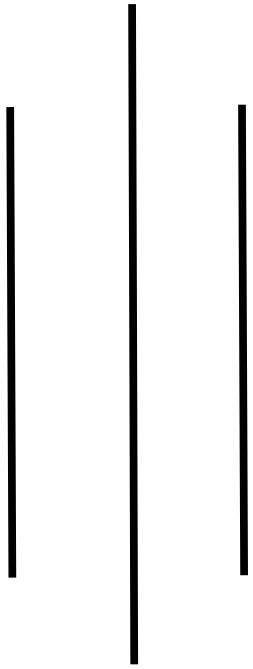
Deerwalk Institute of Technology

Sifal, Kathmandu



Artificial Intelligence Practical

Submitted By:
Name: Sagar Giri
Roll No: 205
Section: A

Submitted To:
Sudan Prajapati

Date:

The Vigenère cipher

The Vigenère cipher is a stronger cipher than the ones we've seen before. There are too many possible keys to brute-force, even with English detection. It cannot be broken with the word pattern attack that worked on the simple substitution cipher. It was possibly first described in 1553 by Italian cryptographer Giovan Battista Bellaso (though it has been reinvented many times, including by Blaise de Vigenère). It is thought to have remained unbroken until Charles Babbage, considered to be the father of computers, broke it in the 19 th century. It was called "le chiffre indéchiffrable", French for "the indecipherable cipher".

Source Code:

Cipher.java

```
package com.vigenere;
import java.util.Scanner;

public class Cipher {
    public void encrypt() {
        Scanner stringReader = new Scanner(System.in);
        System.out.println("Enter a plain text: ");
        String plainText = stringReader.nextLine();

        System.out.println("Enter key: ");
        String key = stringReader.nextLine();

        key = key.toUpperCase();
        plainText = plainText.toUpperCase();

        char cipherText[] = new char[plainText.length()];
        char keyT[] = new char[plainText.length()];

        for(int i = 0, j = 0; i < plainText.length(); i++, j++){
            if (plainText.charAt(i) == ' ') {
                keyT[i] = ' ';
                j = -1;
            }
            else
                keyT[i] = key.charAt(j);
            if(j == key.length() - 1) j = -1;
        }

        for(int i = 0; i < plainText.length(); i++) {
            if (plainText.charAt(i) == ' ') {
                cipherText[i] = ' ';
                continue;
            }
            cipherText[i] = (char)(((plainText.charAt(i) - 65 + keyT[i] - 65) %
26) + 65);
        }
        System.out.println(cipherText);
    }
}
```

Decipher.java

```
package com.vigenere;

import java.util.Scanner;

public class Decipher {

    public void decrypt() {

        Scanner stringReader = new Scanner(System.in);

        System.out.println("Enter a encrypted text: ");
        String cipherText = stringReader.nextLine();

        System.out.println("Enter key: ");
        String key = stringReader.nextLine();

        key = key.toUpperCase();
        cipherText = cipherText.toUpperCase();

        char plainText[] = new char[cipherText.length()];
        char keyT[] = new char[cipherText.length()];

        for(int i = 0, j = 0; i < cipherText.length(); i++, j++){
            if (cipherText.charAt(i) == ' ') {
                keyT[i] = ' ';
                j = -1;
            }
            else
                keyT[i] = key.charAt(j);

            if(j == key.length() - 1) j = -1;
        }

        for(int i = 0; i < cipherText.length(); i++) {
            if (cipherText.charAt(i) == ' ') {
                plainText[i] = ' ';
                continue;
            }
            int value = cipherText.charAt(i) - 65 - (keyT[i] - 65);
            if(value>=0)
                plainText[i] = (char)(value % 26 + 65);
            else
                plainText[i] = (char)( (26 + value)% 26 + 65);
        }
        System.out.println(plainText);
    }
}
```

VigenereMain.java

```
package com.vigenere;

import java.util.Scanner;


public class VigenereMain {

    public static void main(String[] args) {
        int choice;

        System.out.println("Enter 1 to encrypt a text and 2 to decrypt the text:");
        Scanner scanner = new Scanner(System.in);
        choice = scanner.nextInt();
        switch (choice){
            case 1:
                Cipher cipher = new Cipher();
                cipher.encrypt();
                break;
            case 2:
                Decipher decipher = new Decipher();
                decipher.decrypt();
                break;
            default:
                System.out.println("Sorry");
                break;
        }
    }
}
```

Output:

```
Enter 1 to encrypt a text and 2 to decrypt the text:
1
Enter a plain text:
sagar giri is a programmer
Enter key:
sagar
KAMAI YIXI AS S HRUGISMSEI
```

```
Enter 1 to encrypt a text and 2 to decrypt the text:
2
Enter a encrypted text:
KAMAI YIXI AS S HRUGISMSEI
Enter key:
sagar
SAGAR GIRI IS A PROGRAMMER
```