CAESAR CIPHER ALGORITHM

Name:-Samir Singh Chhetri

Student Id:-NP03S190055

AGENDA

- Introduction
- Problem Definition
- History
- Working Mechanism
- Pseudo Code
- Code
- Time Complexity
- Application
- Limitation
- Conclusion

INTRODUCTION

- The Caesar Cipher technique is known as one of the earliest and simplest method of encryption technique.
- It's simply a type of substitution cipher.
- The method is apparently named after Julius Caesar.

PROBLEM DEFINITION

- It was initially developed to hide secret message .
- To prevent form message and document leaks.

HISTORY

- The Julius Caesar was first recorded person to use by Caesar Cipher.
- It was used to communicate with his officials.
- It was likely to have been reasonably secure.

WORKING MECHANISM

To cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

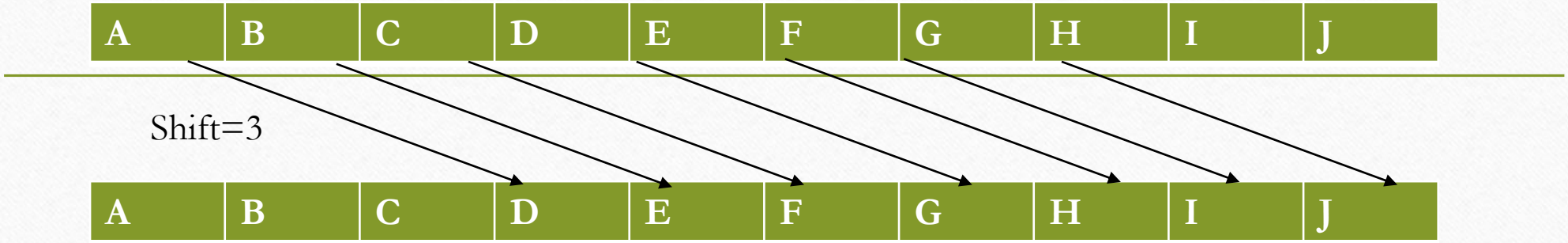
ENCRYPTION

$En(x)=(x+n) \bmod 26$

DECRYPTION

$Dn(x)=(x-n) \bmod 26$

Plain Text

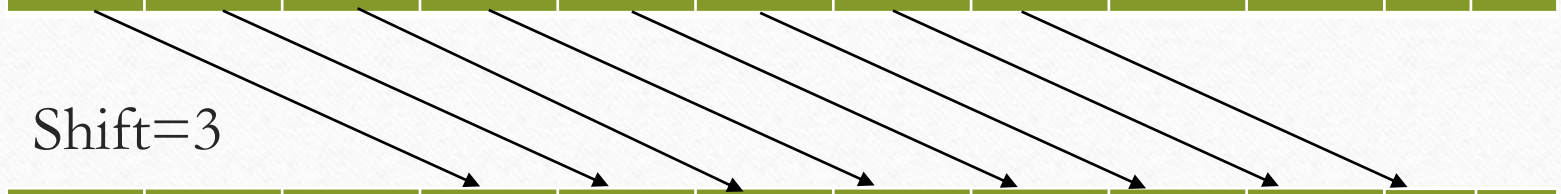


Cipher Text

Example

Plain Text:-Hello

H	I	J	K	L	M	N	O	P	Q	R	S
7	8	9	10	11	12	13	14	15	16	17	18



Shift=3

H	I	J	K	L	M	N	O	P	Q	R	S
7	8	9	10	11	12	13	14	15	16	17	18

Cipher Text:-khoor

Special case of Caesar Cipher

- ROT13 is special case in which 13 shift is used to encrypt and decrypt information.
- In this case decrypting code is same as encrypting code.

Pseudo Code

- Alphabet, called Text.
- An Integer between 0-25 denoting the required shift.
- **Procedure:**
- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Return the new string generated

CODE

Encryption:-

```
import java.util.Scanner;
public class CaesarCipherEncryption
{
  // Encrypts text using a shift od s
  public static StringBuffer encrypt(String text, int s)
  {
     StringBuffer result= new StringBuffer();
```

```
for (int i=0; i<text.length(); i++)
{
    if (Character.isUpperCase(text.charAt(i)))
    {
        char ch = (char)(((int)text.charAt(i) +
                        s - 65) % 26 + 65);
        result.append(ch);
    }
```

```
else
            {
                char ch = (char)(((int)text.charAt(i) +
                                s - 97) % 26 + 97);
                result.append(ch);
            }
        }
        return result;
    }
```

```
public static void main(String[] args)
    {
        System.out.println("Enter your messege:-");
        String text = new Scanner(System.in).nextLine();
        System.out.println("Enter Shift:-");
        int s = new Scanner(System.in).nextInt();
        System.out.println("Text  : " + text);
        System.out.println("Shift : " + s);
        System.out.println("Cipher: " + encrypt(text, s));
    }
}
```

- Decryption:-

```
import java.util.Scanner;
public class CaesarCipherDecryption
{
    // Encrypts text using a shift od s
    public static StringBuffer encrypt(String text, int s)
    {
```

```
StringBuffer result= new StringBuffer();

        for (int i=0; i<text.length(); i++)
        {
char ch = (char)(((int)text.charAt(i) - s + 65) % 26 + 65);
            result.append(ch);




        }
        return result;
    }
```

```
public static void main(String[] args)
    {
        System.out.println("Enter Cipher Code:-");
        String text1 = new Scanner(System.in).nextLine();

        ---------------------------------------------------------------

        String text=text1.toUpperCase();
        System.out.println("Enter Shift:-");
        int s = new Scanner(System.in).nextInt();
        System.out.println("Cipher Text  : " + text);
        System.out.println("Shift : " + s);
        System.out.println("Plain Text: " + encrypt(text, s));
    }
}
```

Time Complexity Analysis

- Caesar Cipher is algorithm having linear time complexity i.e. O(n).

Application.

- Caesar Cipher is used in Network Security.
- ROT13 is special case of Caesar Cipher which is used in online forms.
- It was used to hide email address from spam bots.

Limitation

- It is less secure type of network security .
- It can be cracked easily.

Conclusion

- This algorithm is easy to crack and provides some sort security and has limitations due to which other ciphers technique is found .

REFRENCE

- https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/
- https://en.wikipedia.org/wiki/Caesar_cipher

THANK YOU