

Teoría de la Computación 2024

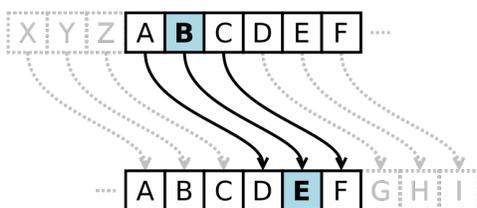
Proyecto 3

22.octubre.2024

Este proyecto consiste en simular una máquina de Turing para encriptar y decriptar un mensaje mediante el cifrado *Caesar*.

1 Cifrado César

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, es una de las técnicas de cifrado más simples y conocidas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de $k = 3$, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etcétera.

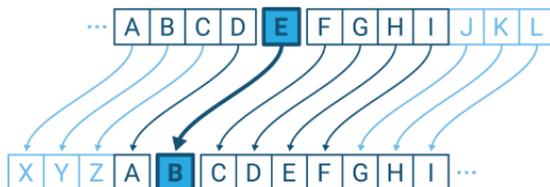


En general, si se usa un alfabeto Σ con n símbolos, se pide que el cifrado use una **llave** $0 \leq k < n$. En este caso, el mecanismo de encriptación César funciona como

$$E(x) = x + k \pmod{n},$$

mientras que el mecanismo de decriptación sería

$$D(x) = x - k \pmod{n}.$$



El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación, como el cifrado Vigenère, e incluso tiene aplicación computacionales como en el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad y en la práctica no ofrece ninguna seguridad en la comunicación.

2 Proyecto

Objetivos

- Investigar la implementación computacional de las máquinas de Turing.
- Simular máquinas de Turing para encriptar y decriptar mensajes mediante un cifrado César.

Deberá implementar en Python, dos máquinas de Turing (pueden ser tradicionales, multicinta, o extensiones de las máquinas de Turing), la primera debe encriptar mensajes mediante el cifrado César, y la segunda debe decriptar dichos mensajes.

Especificaciones

a) Entrada:

– Archivo (.txt, .json, .ml, .yaml, o similares) con la estructura de su máquina de Turing:

- * conjunto de estados Q ,
- * alfabeto input Σ ,
- * alfabeto de cinta Γ ,
- * estado inicial q_0 ,
- * conjunto de estados de aceptación F ,
- * tabla de transiciones (o en su defecto, el listado de 4-tuplas).

- cadena input $w \in \Sigma^*$. Esta cadena debe consistir de la llave $llave \in \Sigma$ (primer símbolo de la cadena), seguido del mensaje a cifrar. La llave servirá para identificar cuál debe ser la rotación a usar en el cifrado.

b) Salida:

- para la máquina de Turing de encriptación, la salida debe ser la cadena del mensaje encriptado.
- para la máquina de Turing de decriptación, la salida debe ser la cadena del mensaje decriptado (el mensaje original).

Por ejemplo, para la máquina de Encriptación, una posible entrada sería:

$w = 3 \# \text{ROMA NO FUE CONSTRUIDA EN UN DIA}$

ó

$w = D \# \text{ROMA NO FUE CONSTRUIDA EN UN DIA}$

y la salida debería ser

$z = \text{URPD QR IXH FRQVWUXLGD HQ XQ GLD}$

Para la máquina de Decriptación, la entrada debe ser, de nuevo:

$w = 3 \# \text{URPD QR IXH FRQVWUXLGD HQ XQ GLD}$

ó

$w = D \# \text{URPD QR IXH FRQVWUXLGD HQ XQ GLD}$

y la salida debería ser

$z = \text{ROMA NO FUE CONSTRUIDA EN UN DIA}$

Mostrar algunos ejemplos de mensaje encriptados y su respectiva decriptación.

Ponderación

El proyecto en total tiene un valor de 15 puntos.

Entregables

- Informe técnico de la implementación, incluyendo ejemplos.
- Código de la simulación.