Mapeo de cadena de caracteres a numero entero

Allan y Jhon April 15, 2016

1 Econde Quizá sea mejor usar: Codificación

En el ease particular del presente trabajo si se quiere usar el modo multi-CAPTCHA se tiene que hacer uso del algoritmo de Secreto Compartido. El algoritmo de secreto compartido se realiza con números y no con cadenas de caracteres, para poder hacer que este algoritmo funcione necesario mapear la cadena de caracteres a un numero entero. Cosa que explicaremos a continuación.

Se tiene un conjunto de caracteres AL compuesto por .Se tiene un conjunto de caracteres AL compuesto por $Al = \{A, B, ..., Z\} \cup \{a, b, ..., z\} \cup \{0, 1, ..., 9\} \cup \{+, /\}$ con una cardinalidad |AL| = 64.

Para obtener una representación binaria de 64 elementos son necesarios 6 bits por lo que para todos los elementos $\sigma \epsilon AL$ existe una representación binaria. Una vez establecido esto el procedimiento para el mapeo es el siguiente: realizar la conversión

- 1. Tomamos una cadena de caracteres y la separamos caracter por caracter y los intercambiamos por su correspondiente numero entero en AL $\alpha_0||\alpha_1||...||\alpha_m$
- 2. Posteriormente cada uno de los enteros lo convertimos en un binario de 6 bits y se concatenan uno detrás del otro $\Psi \leftarrow bin_6(\alpha_0)||bin_6(\alpha_1)||...||bin_6(\alpha_m)|$
- 3. la cadena binaria Ψ la convertimos a entero $v \leftarrow toInt(\Psi)$

El entero que obtenemos v es el valor que usaremos en el algoritmo de secreto compartido.

2 Ejemplo

Tenemos la cadena STR=`ABC` de la cual cambiaremos cada caracter por su correspondiente valor entero en AL quedando de la siguiente manera $\alpha=\underbrace{(0,1,2)}_{\text{Aquí, usar llaves en lugar de los paréntesis}}$

Ahora cada uno de los elementos de α lo convertiremos a su correspondiente representacion binaria, $bin_6(0)=000000, bin_6(1)=000001, bin_6(2)=000010$ y concatenamos cada una quedando $\Psi=00000000001000010$

la cadena binaria Ψ se convertirá en un entero $v=toInt(\Psi)$ que da como resultado v=66

3 Decode Quizá sea mejor "Decodificación"

Tambien es necesario tener un mapeo de mumero a letras y para esto se realiza el proceso inverso:

- 1. el entero v es convertido en un numero binario $z = toBin_6(v)$
- 2. separamo z en $\frac{\text{cadenas}}{\text{binarios}}$ de 6 bits y cada una de ellas la interpretamos como to $Int(z_0)||toInt(z_1)||...||toInt(z_w)$
- 3. Cada uno de estos valores enteros con convertidos a su correspondiente caracter en AL y concatenados para generar la cadena de caracteres final.

Por favor reescriban el párrafo siguiente. Hace falta introducir signos de puntuación.

4 Ejemplo

se representa como una cadena de

El entero v=66 es convertido en un numero binario de 18 bits $z=toBin_0(v)$ da como resultado z=00000000001000010, este numero es dividido en numeros 6 bits quedando $z_0=000000$, $z_1=000001$, $z_2=000010$, para cada uno de estos numeros binarios se precede a convertirlo en un entero $toInt(z_0)=0$, $toInt(z_1)=1$, $toInt(z_2)=2$ por ultimo estos son intercambiados por sus correspondientes caracteres en AL y concatenados dandonos s=`ABC`

la cual se divide en subcadenas de