Mapeo de cadena de caracteres a numero entero

Allan y Jhon

April 25, 2016

1 Codificación

En presente trabajo si se quiere usar el modo multiCAPTCHA se usa el esquema de Secreto Compartido. El algoritmo de secreto compartido se realiza con enteros y no con cadenas de caracteres, por lo que es necesario convertir la cadena de caracteres a un entero. Como se explica a continuacón.

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 realizar la conversión es el siguiente:

1. Tomamos una cadena de caracteres y la separamos caracter por caracter y los intercambiamos por su correspondiente número 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 $\Psi \longleftarrow bin_6(\alpha_0)||bin_6(\alpha_1)||...||bin_6(\alpha_m$
3. La cadena binaria Ψ la convertimos a entero $v \longleftarrow toInt(\Psi)$

El entero v que obtenemos 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 $\alpha = \{0, 1, 2\}$

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 $\Psi = 000000000001000010$

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

3 Decodificación

Tambien es necesario convertir un entero a una cadena de caracteres y para esto se realiza el proceso inverso:

1. El entero v es convertido en un número binario $z = toBin_6(v)$
2. Separamo z en cadenas de 6 bits y cada una de ellas la interpretamos como un entero $toInt(z_0)||toInt(z_1)||...||toInt(z_w)$
3. Cada uno de estos valores son convertidos a su correspondiente caracter en AL y concatenados para generar la cadena de caracteres final.

4 Ejemplo

El entero $v = 66$ se representa como una cadena de 18 bits $z = 000000000001000010$, la cual se divide en sub cadenas 6 bits quedando $z_0 = 000000, z_1 = 000001, z_2 = 000010$, para cada uno de estos números binarios se procede a convertirlo en un entero $toInt(z_0) = 0, toInt(z_1) = 1, toInt(z_2) = 2$, por último estos son intercambiados por sus correspondientes caracteres en AL y concatenados resultando en $s = `ABC`$