José Ángel González Carrera

A01552274

Reflexión Actividad 5.2

El poder trabajar con un hash table me permitió comprender otro tipo de ADT, el cual funciona como un arreglo al cual se accede con un hash code. Se puede decir que el poder y seguridad del hash table radica en la función del hash, la cual define que tan segura puede estar la información en la estructura.

En la actualidad, la ciberseguridad es un aspecto angular de la computación moderna, y el hashing lo es igualmente. El hashing se basa en convertir los datos de un tamaño arbitrario a un dato de tamaño fijo. Una de las funciones de hash más usadas en el mercado es la de SHA-256, la cual genera un output de 256 bits (N-ABLE, 2019)

Básicamente, las ventajas que tiene esta función hash SHA-256 es que, es empleada en el mercado de las criptomonedas para garantizar la seguridad de la información. Adicionalmente, entre sus ventajas se encuentra que no se pueden manipular, y tienen una gran funcionalidad para el manejo de las contraseñas de los usuarios.

Finalmente, para tener un panorama de la complejidad temporal del algoritmo, para realizar 41 pasos de SHA-256 se necesitan $2^{253.5}$ operaciones de la función (Sasaki, 2009, p.1.).

Referencias:

SHA-256 Algorithm Overview. (2019). N-ABLE. Retrieved from: https://www.n-able.com/blog/sha-256-encryption

Sasaki, Y., Wang, L., & Aoki, K. (2009). Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512. IACR Cryptol. ePrint Arch., 2009, 479.