Reflexión

Nombre: Carlos Daniel Díaz Arrazate

Matrícula: A01734902

Los hash tables son una forma de poder guardar la información de manera segura dentro de una estructura, sin embargo, la seguridad radica en la función mediante la cual se genera el hash code en sí.

Es ahí donde se vuelve relevante las ventajas y desventajas de cada uno de los hash functions. Por ejemplo, en el caso de la familia de funciones SHA-2, particularmente la función SHA-256, una función con una complejidad de O(1), debido a que esta genera un hash de una longitud fija (256 bits); esta es una función que permite enviar mensajes de manera relativamente segura, por lo que este algoritmo es utilizado en distintos protocolos de envío de mensajes. Aunado a ello, debido a que se construyó en base al algoritmo SHA-1, es más difícil el poder encontrar mensajes que tengan el mismo hash code. Sin embargo, una de las desventajas es que este algoritmo no es seguro para guardar contraseñas. (Steven, 2021)

En cuanto a la situación manejada, no considero que el uso de un hash table sea lo mejor, aunque no es necesariamente malo, puesto que no hay necesidad de convertir parte de la información a un hash code, puesto que estos son particularmente útiles para “revolver” un mensaje, lo cual no es lo que se busca en sí.

Referencias

Steven, J. (18 de octubre de 2021). What's the difference between Sha2 vs. Sha1?: Synopsys. Software Integrity Blog. Recuperado de https://www.synopsys.com/blogs/software-security/sha2-vs-sha1/.

Wagner, L. (20 de octubre de 2021). How sha-256 works step-by-step. Qvault. Recuperado de https://qvault.io/cryptography/how-sha-2-works-step-by-step-sha-256.