Daniel Francisco Acosta Vazquez
A01736279

Reflexión Actividad 5.2

El hashing es una herramienta extremadamente útil cuando manejamos cualquier tipo de información. Con una buena función de hash uno puede guardar cantidades enormes de información, y acceder a cada una de ellas de una manera eficiente y muy segura. Con esto se pueden realizar muchos otros procesos de maneras eficientes y seguras, como verificación de contraseñas (sin guardar las mismas), verificar la integridad de archivos, al igual que almacenar mucha información en la tabla de hash.

Claro que el tamaño de este hash debe ser proporcional a la seguridad requerida al igual que a la cantidad de datos con los que se desea tratar y al poder de procesamiento disponible. Por ejemplo está el SHA-256, o conocido como **Secure Hash Algorithm - 256** , el 256 ya que este algoritmo de hash produce un valor final siempre de 256 bits. Esto hace que este algoritmo sea extremadamente fuerte en contra de ataques brutos de descifrado, y por ende ser muy utilizado para verificación de integridad, contraseñas, verificación de firma digital, entre muchas otras funciones. Claro que en estos datos, se trata de datos muy delicados al igual que en cantidades absurdamente grandes. Así que dependiendo de la importancia y cantidad de datos que se traten en esta situación problema, puede que sea una buena implementación. Sin embargo, si la cantidad de datos no es masiva y su naturaleza no es de alta importancia, con solo un buen algoritmo de hashing puede ser suficiente.

Referencias:
-Jena, B. K. (2022, November 11). *What is SHA-256 algorithm: How it works and applications [2022 edition]: Simplilearn*. Simplilearn.com. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm