TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1-UNIDAD 2

TIC

Universidad Tecnológica de Pereira

faceIT

Hashing

La seguridad informática va más allá de compartir mensajes de forma secreta entre pares. También incluye la capacidad de validar si un documento o un programa que se va a descargar de internet ha sido alterado. En criptografía se emplean algoritmos conocidos como funciones hash para convertir un documento en un valor de longitud fija único. Esto se conoce como valor hash. Cada que un algoritmo aplica hash al mismo texto usando el mismo algoritmo, se genera el mismo valor hash. Por ese motivo el hash se puede emplear como un identificador único de los datos.

En internet es común que cuando se publica un software para ser descargado, el editor pone el programa instalador junto con el hash. De esta forma, cuando un usuario lo descarga, puede ejecutar la función hash sobre el archivo y compararla con el valor que el editor ha publicado y validar que el programa es auténtico y que no ha sido alterado, ni le han agregado malware u otros componentes indeseados.

El hashing es diferente del cifrado ya que no emplea claves ni codifica información. De hecho, el hash es una función unidireccional. Es decir, no se puede recuperar la información teniendo un hash y la función de hashing y de ninguna manera se puede recuperar la información original a partir del hash.

Existen muchos métodos de hashing, por ejemplo, la familia de algoritmos SHA (secure hash) que generan valores de hash cuya longitud depende del algoritmo en específico. Como es el caso de SHA-256 que genera un valor de hash de 256 bits de longitud.

Firmas digitales

Una firma digital es una aplicación de los algoritmos de hashing. De forma similar a firmar en una hoja de papel, un documento se puede firmar empleando un hash. Una vez que el documento se firma digitalmente, cualquier cambio por mínimo que sea en la información, generaría un valor de hash totalmente distinto al que se generó cuando se realizó el proceso de firma digital. Garantizando que la información no ha sido alterada.

Las firmas digitales son únicas para cada persona que firma un documento. Todas las firmas emplean claves asimétricas, es decir, el usuario que firma tiene una clave privada y el documento queda con la clave pública.