UNIVERSIDAD DIEGO PORTALES

FACULTAD DE INGENIERÍA Y CIENCIAS
ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES

Criptografía y Seguridad en Redes
Laboratorio Nº 4 (Hito III)

Profesor: Victor Manriquez
Ayudantes: Nicolás Pino, Sebastian Campos
Código : CIT-2108
Estudiantes: Brayan Espina

Santiago, Chile, Octubre del 2021

Índice

1. Introducción

En el presente reporte se realizará una comparativa de entropía entre el algoritmo de hash desarrollado con otros algoritmos de hash conocidos como (SHA1, SHA256 Y MD5).

Asimismo debe efectuar una comparativa de rendimiento entre los diferentes algoritmos a fin de tener claridad de su velocidad al calcular el Hash del texto de entrada. Para la realización de las pruebas de rendimiento, se sugiere una distribución de la siguiente forma:

- Prueba 1 : 1 entrada de texto.
- Prueba 2: 10 entradas de texto.
- Prueba 3 : 20 entradas de texto.
- Prueba 4: 50 entradas de texto.

2. Comparativa hash

Consulte la Tabla 1, donde se aprecian las diferencias primordiales entre los algoritmos de hash.

Algoritmo de hash	Base utilizada	Entropia	Velocidad 1 entrada	Velocidad 10 entradas	Velocidad 20 entradas	Velocidad 50 entradas
Algoritmo Creado	94	163	0.0007562637329101562	0.009054183959960938	0.01862621307373047	0.07768011093139648
SHA1	16	160	0.0	0.0038712024688720703	0.010442495346069336	0.026409626007080078
SHA256	16	256	0.0008227825164794922	0.006069660186767578	0.01511073112487793	0.03210568428039551
MD5	16	128	0.0003654956817626953	0.004673004150390625	0.012891530990600586	0.02914571762084961

Tabla 1: Comparación de los algoritmos de hash

Cabe recordar que la entropía de una password es la cantidad de variación de caracteres dentro de ésta. Se calcula como:

$$H = L \cdot log_2(W)$$

, donde

- W: es la base utilizada.
- L: es el largo del string.

Bajo este contexto, la entropía visualizada en la Tabla 1 es referente al hash final que otorga el algoritmo, no a la password ingresada por el usuario.

Primeramente, referente a la base empleada por cada algorimto, el que posee una mayor base a la hora de obtener el hash a partir de una contraseña empleada es el algoritmo creado en la experiencia, puesto que en comparación a los otros algoritmos, estos utilizan una base hexadecimal para representar el hash. Asimismo, el algoritmo que posee una entropía mayor en comparación al resto en SHA256, este resultado se debe a que el largo del string final juega un factor clave a la hora de obtener la entropía.

Por otro lado, para efectuar un análisis de velocidad se utilizaron diversas entradas de texto, donde se puede observar que la velocidad de entrada de texto de una password, el algoritmo SHA1 arroja un valor de 0.0, esto se puede deber a que la diferencia de tiempo entre que se inicio la captura de tiempo y el fin es tan poca, que *Python* arroja un valor de 0. Cabe mencionar que el algoritmo creado es el segundo algoritmo más lento, ya que SHA256 lleva la ventaja en esta primera instancia.

También, dentro de la lectura de las 10 password se puede apreciar que el algoritmo más lento es el script creado, esto puede deberse a las diversas operaciones que realiza, donde no son tan óptimas en comparación a los demás.

Por último en las lecturas de 20 y 50 password el algoritmo por excelencia en SHA1, quedando en segundo lugar MD5, tercero SHA256 y el script creado en último.

Como un análisis genérico se puede obtener que el algoritmo que posee un comportamiento de velocidad superior a los demás es SHA1, aunque estos resultados pueden variar dependiendo de la maquina donde se hagan las pruebas y la cantidad de lineas que se están leyendo, específicamente los datos del equipo donde se efectuaron las pruebas son:

- Lenovo Ideapad 720s.

- Sistema Operativo: Windows.
- Ram 8gb.
- 1 TB ssd.