ANÁLISIS TIEMPO

En el presente documento, se mostraran los tiempos obtenidos para el código realizado en el presente laboratorio, en conjunto con una comparación y análisis correspondiente.

Es importante saber que los tiempos obtenidos, son afectados considerablemente por el hardware con el cual fue compilado el código, debido a que para obtener estos resultados, se necesita considerablemente del uso de un procesador.

En este caso, el procesador y el hardware relevante utilizado utilizado fue el siguiente:

- i5 9400 F
- 16 GB Ram 3000 Hz

Tiempos(s)				
Palabras	MD5	SHA1	SHA256	Carro
1	0.0	0.0	0.0	0.0
10	0.0	0.0	0.0	$101x10^-5$
20	0.0	0.0	0.0	$299x10^-5$
50	0.0	0.0	0.0	$498x10^-5$

Cuadro 1: Tabla de tiempos

Los resultados observados en la tabla, fueron analizados hasta con 20 decimales para ver si era posible ver algún cambio y no mostrar un "cero perfecto". Pero lamentablemente, las funciones que se utilizaron, provenientes de la librería de time en python, deben de estar optimizadas a gran nivel, además, de que deben de funcionar mediante cálculos matemáticos que agilizan el proceso.

Por otro lado, para calcular el hash creado, se utilizaron cálculos matemáticos pero no es posible garantizar un rendimiento óptimo en su totalidad.

ANÁLISIS DE ENTROPÍA

Para poder ver la robustez de una contraseña según el abecedario y el largo que esta contenga es necesario calcular la entropía, la cual se calcula con la siguiente ecuación.

$$H = L * \log_2(W) \tag{1}$$

En donde, W será la cantidad de caracteres que posee la base a utilizar y L el largo de la contraseña. Los valores de la entropía variaron considerablemente según el largo del a base a utilizar, las bases

Entropía		
Encriptado	Base	Entropía
MD5	32	160
SHA1	40	213
SHA256	64	384
Carro	1.114.112	1104

Cuadro 2: Tabla de Entropía

utilizadas están en la tabla publicada anteriormente, y mientras mayor sea el resultado de la entropía, significará que la contraseña es mas robusta.