

Comparativa entre tiempo y entropía: md5, SHA1 y SHA256 vs Hash propio.

Alumno: Maximiliano Angel

Profesor: Victor Manriquez

19/10/2021

Introducción:

En este informe se comparan los tiempos de ejecución y entropía obtenidos al hashear ciertas palabras con los siguientes métodos de hashing:

- SHA1.
- SHA256.
- MD5.
- [Hash-propio](#).

Se mostrarán los resultados de las pruebas con los archivos 1.txt, 10.txt, 20.txt y 50.txt. Cada archivo posee la cantidad de palabras descrita en su nombre, las cuales serán ingresadas al método de hashing.

En la comparación de tiempo se observa una tabla con la cantidad de tiempo, en milisegundos, que se demoran en hashear todas las palabras contenidas en dicho archivo.

En la tabla comparativa sobre la entropía de los distintos métodos de hashing, se utilizaron los datos obtenidos al compilar los scripts con el archivo 50.txt. La entropía se obtiene utilizando el valor ASCII más grande en la palabra ya hasheada como base, y luego aplicando la fórmula de entropía.

$$E = n \log_2 m$$

$n \rightarrow$ longitud de la contraseña

$m \rightarrow$ nº de caracteres de la población usada (pool)

- E = la cantidad de bits.
- N = longitud de la contraseña (varía según el método de hash).
- M = valor ASCII más grande en la palabra.

Análisis:

Comparación de tiempo:

Tiempo (s)	MD5	SHA1	SHA256	Propio
1.txt	0.0128746 03271484 375	0.0045299 53002929 6875	0.0040531 15844726 5625	0.0834465 02685546 875
10.txt	0.0405311 58447265 625	0.0319480 89599609 375	0.0317096 71020507 8125	0.3137588 50097656 25
20.txt	0.0662803 64990234 375	0.0591278 07617187 5	0.0586509 70458984 375	0.6735324 85961914 0625
50.txt	0.1738071 44165039 0625	0.1544952 39257812 5	0.1523494 72045898 4375	2.0766258 23974609 375

Comparación de entropía:

Entropía (bits)	MD5	SHA1	SHA256	Propio
123456	213.06276744 805746	264.58839376 46084	361.20679614 558236	221.40362359 278706
12345	211.67071501 16867	228.01758872 56437	366.58690909 20448	245.74336318 417429
123456789	211.67071501 16867	224.58839376 460833	366.58690909 20448	201.13287100 359196
password	186.65248045 327175	232.29419688 23042	371.67071501 16867	246.41407098 051496
iloveyou	178.71880002 307702	232.29419688 23042	426.12553489 61149	246.41407098 051496

princess	211.19721094 99881	263.99651368 74851	361.20679614 558236	246.41407098 051496
1234567	186.65248045 327175	265.17426480 318437	364.82814196 10299	192.0
rockyou	212.13941184 25475	228.01758872 56437	366.58690909 20448	192.0
12345678	212.60339807 27912	265.75424759 0989	427.03522188 61757	246.41407098 051496
abc123	181.51761094 308787	266.32845931 00718	357.43760004 615405	221.40362359 278706
nicole	212.60339807 27912	226.89701367 885985	424.27882368 5095	221.40362359 278706
daniel	213.06276744 805746	266.89701367 88598	373.30496090 65435	221.40362359 278706
babygirl	185.00351083 278912	231.25438854 098638	363.03522188 617575	246.41407098 051496
monkey	183.29345454 60224	266.32845931 00718	427.03522188 61757	221.40362359 278706
lovely	185.83535750 584335	223.39850002 884629	366.58690909 20448	221.40362359 278706
jessica	181.51761094 308787	224.58839376 460833	371.67071501 16867	192.0
654321	186.65248045 327175	223.39850002 884629	366.58690909 20448	221.40362359 278706
michael	213.51761094 308785	224.58839376 460833	423.34143002 33734	192.0
ashley	213.06276744 805746	264.58839376 46084	373.30496090 65435	221.40362359 278706
qwerty	182.41407098 051496	266.32845931 00718	366.58690909 20448	221.40362359 278706
111111	180.60339807 279118	265.75424759 0989	422.39442189 99762	221.40362359 278706
iloveu	178.71880002 307702	266.89701367 88598	424.27882368 5095	221.40362359 278706

000000	212.60339807 27912	265.75424759 0989	363.03522188 617575	221.40362359 278706
michelle	183.29345454 60224	228.01758872 56437	366.58690909 20448	246.41407098 051496
tigger	213.51761094 308785	263.99651368 74851	370.00702166 557824	221.40362359 278706
sunshine	178.71880002 307702	266.89701367 88598	363.03522188 617575	246.41407098 051496
chocolate	212.60339807 27912	263.99651368 74851	366.58690909 20448	201.13287100 359196
password1	212.13941184 25475	265.75424759 0989	426.12553489 61149	201.13287100 359196
soccer	178.71880002 307702	233.31560056 65897	373.30496090 65435	221.40362359 278706
anthony	213.51761094 308785	223.39850002 884629	357.43760004 615405	192.0
friends	213.06276744 805746	233.31560056 65897	364.82814196 10299	192.0
butterfly	212.13941184 25475	229.11681818 2528	371.67071501 16867	201.13287100 359196
purple	181.51761094 308787	229.11681818 2528	427.03522188 61757	221.40362359 278706
angel	186.65248045 327175	266.89701367 88598	359.34143002 337333	245.74336318 417429
jordan	180.60339807 279118	264.58839376 46084	422.39442189 99762	221.40362359 278706
liverpool	186.65248045 327175	231.25438854 098638	425.20679614 55824	201.13287100 359196
justin	212.60339807 27912	266.32845931 00718	425.20679614 55824	221.40362359 278706
loveme	213.06276744 805746	225.75424759 098897	368.31280013 8462	221.40362359 278706
fuckyou	211.19721094 99881	229.11681818 2528	359.34143002 337333	192.0

123123	181.51761094 308787	232.29419688 23042	426.12553489 61149	221.40362359 278706
football	178.71880002 307702	232.29419688 23042	423.34143002 33734	246.41407098 051496
secret	186.65248045 327175	228.01758872 56437	423.34143002 33734	221.40362359 278706
andrea	212.13941184 25475	231.25438854 098638	373.30496090 65435	221.40362359 278706
carlos	211.67071501 16867	228.01758872 56437	427.03522188 61757	221.40362359 278706
jennifer	211.19721094 99881	265.75424759 0989	423.34143002 33734	246.41407098 051496
joshua	180.60339807 279118	266.89701367 88598	364.82814196 10299	221.40362359 278706
bubbles	212.13941184 25475	230.19550008 653877	424.27882368 5095	192.0
1234567890	213.51761094 308785	263.99651368 74851	368.31280013 8462	246.85585656 531592
superman	184.15640006 9231	263.99651368 74851	366.58690909 20448	246.41407098 051496
hannah	185.00351083 278912	265.75424759 0989	361.20679614 558236	221.40362359 278706

Conclusión:

Al analizar los datos se encuentra que el hash propio es el más lento a la hora de hashear cadenas de caracteres, incluso siendo superado, por poco, por MD5, el cual es un algoritmo deprecado al encriptar claves.

En el caso de la entropía, se observa una competición cerrada entre el hash propio, SHA1 y MD5. Superando, el hash propio, casi en los cincuenta casos a MD5 y manteniéndose en un rango muy cercano con SHA1, pero sin acercarse a SHA256.

Anexos:

[Codigo de Github](#)