udp Escuela de Informática y Telecomunicaciones

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.

$$E = n \log_2 m$$
$$n \rightarrow longitud\ de\ la\ contraseña$$
$$m \rightarrow nº\ de\ caracteres\ dela\ población\ usada\ (pool)$$

- 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	0.0012874603271484375	0.0004529953002929687 5	0.0004053115844726562 5	0.0008344650268554687 5
10.txt	0.0090014934539792 492	0.0060014724731445 31	0.0049972534179687 5	0.0060021877288818 36
20.txt	0.0169990062713623 05	0.0163669586181640 62	0.0099983215332031 25	0.0079984664916992 19
50.txt	0.0299961566925048 83	0.0280008316040039 06	0.0300042629241943 36	0.0230038166046142 58

Comparación de entropía:

Entropía (bits)	MD5	SHA1	SHA256	Propio
123456	213.0627674480 5746	264.5883937646084	361.2067961455 8236	221.4036235927 8706
12345	211.6707150116867	228.0175887256437	366.5869090920448	245.7433631841 7429
123456789	211.6707150116867	224.5883937646 0833	366.5869090920448	201.1328710035 9196
password	186.6524804532 7175	232.2941968823042	371.6707150116867	246.4140709805 1496
iloveyou	178.7188000230 7702	232.2941968823042	426.1255348961149	246.4140709805 1496

princess	211.1972109499881	263.9965136874851	361.20679614558236	246.41407098051496
1234567	186.65248045327175	265.17426480318437	364.8281419610299	192.0
rockyou	212.1394118425475	228.0175887256437	366.5869090920448	192.0
12345678	212.6033980727912	265.754247590989	427.0352218861757	246.41407098051496
abc123	181.5176109430878 7	266.3284593100718	357.4376000461540 5	221.40362359278706
nicole	212.6033980727912	226.8970136788598 5	424.2788236850 95	221.40362359278706
daniel	213.0627674480574 6	266.8970136788598	373.3049609065435	221.40362359278706
babygirl	185.0035108327891 2	231.2543885409863 8	363.0352218861757 5	246.41407098051496
monkey	183.2934545460224	266.3284593100718	427.0352218861757	221.40362359278706
lovely	185.8353575058433 5	223.3985000288462 9	366.5869090920448	221.40362359278706
jessica	181.5176109430878 7	224.5883937646083 3	371.6707150116867	192.0
654321	186.65248045327175	223.3985000288462 9	366.5869090920448	221.40362359278706
michael	213.5176109430878 5	224.5883937646083 3	423.3414300233734	192.0
ashley	213.0627674480574 6	264.5883937646084	373.3049609065435	221.40362359278706
qwerty	182.4140709805149 6	266.3284593100718	366.5869090920448	221.40362359278706
111111	180.6033980727911 8	265.754247590989	422.3944218999762	221.40362359278706
iloveu	178.7188000230770 2	266.8970136788598	424.2788236850 95	221.40362359278706

000000	212.6033980727912	265.754247590989	363.03522188617575	221.40362359278706
michelle	183.2934545460224	228.0175887256437	366.5869090920448	246.41407098051496
tigger	213.51761094308785	263.9965136874851	370.00702166557824	221.40362359278706
sunshine	178.71880002307702	266.8970136788598	363.03522188617575	246.41407098051496
chocolate	212.6033980727912	263.9965136874851	366.5869090920448	201.13287100359196
password1	212.1394118425475	265.754247590989	426.1255348961149	201.13287100359196
soccer	178.71880002307702	233.3156005665897	373.3049609065435	221.40362359278706
anthony	213.51761094308785	223.39850002884629	357.43760004615405	192.0
friends	213.06276744805746	233.3156005665897	364.8281419610299	192.0
butterfly	212.1394118425475	229.116818182528	371.6707150116867	201.13287100359196
purple	181.51761094308787	229.116818182528	427.0352218861757	221.40362359278706
angel	186.65248045327175	266.8970136788598	359.34143002337333	245.74336318417429
jordan	180.60339807279118	264.5883937646084	422.3944218999762	221.40362359278706
liverpool	186.65248045327175	231.25438854098638	425.2067961455824	201.13287100359196
justin	212.6033980727912	266.3284593100718	425.2067961455824	221.40362359278706
loveme	213.06276744805746	225.75424759098897	368.3128001384462	221.40362359278706
fuckyou	211.1972109499881	229.116818182528	359.34143002337333	192.0

123123	181.51761094308787	232.2941968823042	426.1255348961149	221.40362359278706
football	178.71880002307702	232.2941968823042	423.3414300233734	246.41407098051496
secret	186.65248045327175	228.0175887256437	423.3414300233734	221.40362359278706
andrea	212.1394118425475	231.25438854098638	373.3049609065435	221.40362359278706
carlos	211.6707150116867	228.0175887256437	427.0352218861757	221.40362359278706
jennifer	211.1972109499881	265.754247590989	423.3414300233734	246.41407098051496
joshua	180.60339807279118	266.8970136788598	364.8281419610299	221.40362359278706
bubbles	212.1394118425475	230.195500086653877	424.2788236825095	192.0
1234567890	213.51761094308785	263.9965136874851	368.312800138462	246.85585656531592
superman	184.156400069231	263.9965136874851	366.5869090920448	246.41407098051496
hannah	185.00351083278912	265.754247590989	361.20679614558236	221.40362359278706

Conclusión:

Luego de analizar los datos, se puede observar que el hash propio posee una entropía que oscila entre 192 y 246, lo cual le permite competir en entropía de bits contra md5 y SHA1.
No limitado en esto, se observa que la velocidad obtenida en este hash se corona como el más rápido entre los hash medidos, específicamente en los archivos 20.txt y 50.txt.
El hash propio es utilizable para hashear más de 20 credenciales de forma rápida sin preocuparse por colisiones, por lo que es útil para revisar integridad de datos.

Anexos:

Codigo de Github