ComparativaLabCripto

Alejandro Moroso

October 2021

1 Introduction

Comparativa de entropias de los algoritmos, MD5,SHA1,SHA256 y MyHash

Texto	yojamasxdpoder	Largo	Base	Entropia
MyHash	èÙËÎÎÔëÜÔßÓÉ×xsytzu{v—w}x	25	758	239.15135095427732
MD5	046e8fe16a2906b60ffdd4378780cf6e	32	16	128
SHA1	8cc164dee0301da4de320ba8578a7cf620b3181e	40	16	160
SHA256	7aae9aca2f99c16eb2321331f7bcd831655434bb6b2a13fa279786fba345b3e8	64	16	256

En cuanto a entropia nuestro hash tiene mayor que MD5 y SHA1 por lo que estaria ofreciendo mayor seguridad que estos, mientras que el SHA256 tiene mayor entropia debido al largo que tiene la palabra al ser hasheada, por lo que si se querria tener mayor seguridad que SHA256 se tendria que aumentar el largo minimo de nuestro hash

Comparativa segun las entradas de texto del archivo rockyou.txt Cabe decir que

	MD5	MyHash	SHA1	SHA256
1 Entrada	0.0009694099426269531	0.00099945068359375	0.0009984970092773438	0.0010025501251220703
10 Entradas	0.002000093460083008	0.0030028820037841797	0.0020008087158203125	0.0030028820037841797
20 Entradas	0.003003358840942383	0.007001399993896484	0.0034477710723876953	0.003168344497680664
50 Entradas	0.012003898620605469	0.01703929901123047	0.008002281188964844	0.005999326705932617

nuestro algoritmo de hasheo es mas lento que los demqas en todas las pruebas, esto puede ser debido a al gran diccionario que se tiene y el tener que estar verificando constantemente que nuestro caracteres no caigan en los caracteres invalidos que rompen el algoritmo.