

Pruebas de entropía para algoritmos de Hash

A continuación se presentarán los resultados de las pruebas hechas al algoritmo de Hash desarrollado y su comparativa con otros algoritmos de Hash conocidos como Secure Hash Algorithm (SHA1, SHA256) y MD5.

Se midió la entropía para el string “stringparacompararentropiaentrehashes”.

Para el algoritmo hash desarrollado:

```
Input a string you wanna hash and caculate entropy: stringparacompararentropiaentrehashes
stringparacompararentropiaentrehashes | 0xd02ffb3d0xe683553b0xc1ea34700x9a60356e0xa8752db0 | 204.373142062517
```

Para los demás algoritmos:

```
string a hashear: stringparacompararentropiaentrehashes
MD5| stringparacompararentropiaentrehashes | 689b9021f39479d0c581963d39ee3a8c | 128.0 | 0.012494199999999999seg
SHA256| stringparacompararentropiaentrehashes | 9ab39f41685944994b3291403fb2d81bb0b772d248f592d2c74467c209251c4e | 256.0 | 0.0002434000000004488seg
SHA1| stringparacompararentropiaentrehashes | 735263bf862afa162d5125e7d3b66400c6772eb8 | 156.27562382434076 | 0.0127239999999999513seg
```

	Hash desarrollado	MD5	SHA1	SHA256
Entropía	204.37	128.0	156.27	256.0

Pruebas de rendimiento para algoritmos de Hash

En el siguiente cuadro se presenta, cuánto tiempo se demoraron los algoritmos en calcular entradas de texto de distintos tamaños. Para esto se utilizó las primeras 50 entradas del archivo de texto rockyou.txt

Algoritmo de Hash	1 entrada de texto	10 entradas de texto	20 entradas de texto	50 entradas de texto
Hash Desarrollado	0.0020205000000004247seg	0.03449990000000014seg	0.06273540000000022seg	0.1408811999999993seg
MD5	5.9699999999999587e-05seg	0.0023518999999998513seg	0.004658000000000051seg	0.016096499999999736seg
SHA1	4.26000000000003746e-05seg	0.003356600000000043seg	0.004744399999999871seg	0.009884400000000682seg
SHA256	3.55999999999991348e-05seg	0.003131599999999679seg	0.007213300000000089seg	0.018895199999999335seg