

UNIVERSIDAD CENTRAL DEL ECUADOR



FACULTAD DE INGENIERÍA Y CIENCIAS
APLICADAS

CARRERA: COMPUTACIÓN

ASIGNATURA: Criptografía

Trabajo en grupo

ESTUDIANTES: Kevin Andrade, Jordy
Chamba, Joel Luna, Rensso Para, Kevin
Pozo, Emil Verkade

Tabla de resultados

	# Palabras	# Caracteres entrada	# Caracteres salida	T-E1 Lectura (ms)	T-E2 Generación de clave (ms)	T-E3 Cifrado (ms)	T-E4 Descifrado (ms)	T-Total
3DES	10	65	80	498.91	0.05 ms	5.11	0.23	504.52
DSA	10	65	96	4.55	977.80	0.99	0.76	984.41
MD4	10	65	32	336.35	0.07	N/A	N/A	336.43
3DES	100	710	720	155.70	0.04	0.24	0.13	156.25
DSA	100	710	96	5.32	708.55	1.39	0.99	716.25
MD4	100	710	32	370.05	0.06	N/A	N/A	370.11
3DES	1000	7069	7080	140.71	0.04	0.84	0.43	142.39
DSA	1000	7069	96	3.14	456.85	1.81	1.00	462.79
MD4	1000	7069	32	206.43	0.31	N/A	N/A	206.75
3DES	10000	70257	70272	164.88	0.03	3.48	3.37	172.66
DSA	10000	70257	96	2.86	1329.79	0.89	0.72	1334.26
MD4	10000	70257	32	249.58	0.36	N/A	N/A	249.94
3DES	100000	702048	702064	185.83	0.04	33.62	36.86	265.18
DSA	100000	702048	96	4.39	493.56	3.21	3.27	504.43
MD4	100000	702048	32	524.46	0.99	N/A	N/A	525.45
3DES	1000000	7017945	7017960	329.99	0.03	399.87	397.30	1444.29
DSA	1000000	7017945	96	17.67	324.17	23.49	30.23	395.56
MD4	1000000	7017945	32	437.13	9.42	N/A	N/A	446.55
3DES	10000000	70195141	70195152	1139.67	0.03	3487.43	3430.41	10345.33
DSA	10000000	70195141	96	197.30	610.07	267.18	272.64	1347.19
MD4	10000000	70195141	32	1196.71	131.31	N/A	N/A	1328.02

Conclusiones

3DES, es el cifrado más lento en archivos grandes, su número de caracteres de salida es similar a la entrada porque usa un cifrado por bloques.

DSA, generación de claves lenta, sus números de caracteres de salida es fija porque se tiene una firma en base 64.

MD4 es el más rápido en todos los casos su número de caracteres de salida es fija debida a que se trata de un modelo de hash hexadecimal.