Universidad Central del Ecuador
Facultad de Ingeniería y Ciencias Aplicadas

Criptografía y Seguridad de la Información

Algoritmos Simétricos, Asimétricos y Funciones Hash

Resultados

Integrantes

Cristian Arboleda

Andrés Benavides

Erick Chávez

Paúl Merizalde

Christian Moya

2023 -2023

Algoritmos Utilizados

Algoritmos Simétricos

- DES3
- TwoFish

Algoritmos Asimétricos

- RSA

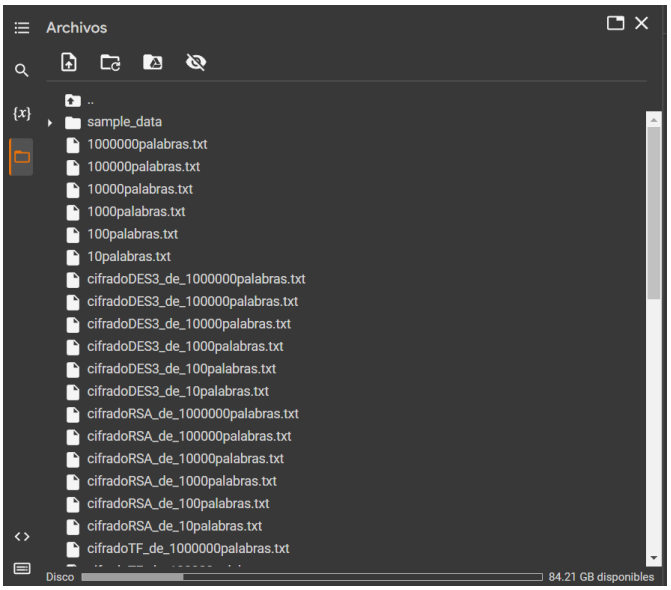
Función Hash

- MD5

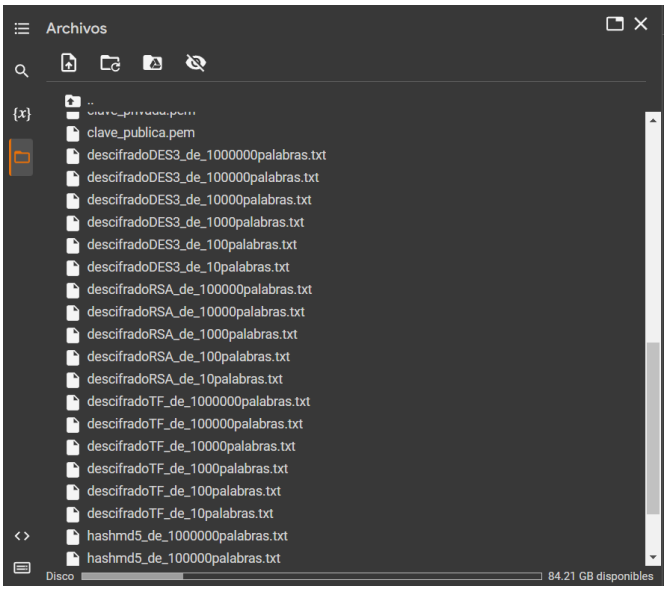
Etapas (E)

1. Leer un archivo con el texto del mensaje a cifrar.
2. Generar e imprimir la(las) claves de cifrado y/o descifrado.
3. Cifrar e imprimir el texto.
4. Descifrar e imprimir el texto.

Los archivos generados de claves de cifrado y/o descifrado, texto de cifrado y/o descifrado se guardaron en tiempo de ejecución y se muestran en las siguientes capturas.



Captura 1. Archivos generados en ejecución



Captura 2. Archivos generados en ejecución

(T-E#) = tiempo de cada etapa.

Cada proceso en función de la cantidad de palabras está separado por color.

	# palabras	T-E1	T-E2	T-E3	T-E4	T-Total(s)
DES3	10	0.00092	0.00089	0.00108	0.00042	**0.00331**
TF	10	0.00185	7.00E-05	0.00413	0.00028	**0.00085**
RSA	10	3.00E-05	12.27702	0.00029	0.01186	**0.01259**
MD5	10	0.00162		1.00E-05		**0.00163**
DES3	100	9.00E-05	4.00E-05	0.00036	0.00036	**0.00085**
TF	100	9.00E-05	4.00E-05	0.00044	0.00643	**0.00700**
RSA	100	5.00E-05	4.92086	0.02068	0.74859	**5.69018**
MD5	100	9.00E-05		1.00E-05		**0.00010**
DES3	1000	9.00E-05	3.00E-05	0.01172	0.00075	**0.01259**
TF	1000	0.0001	3.00E-05	0.00454	0.01458	**0.01925**
RSA	1000	3.00E-05	4.94788	0.16251	7.50535	**12.61577**
MD5	1000	1.10E-04		2.00E-05		**0.00013**
DES3	10000	0.00028	3.00E-05	0.01631	0.00396	**0.02058**
TF	10000	0.00028	3.00E-05	0.07362	0.02708	**0.10101**
RSA	10000	5.00E-05	1.37067	1.64678	75.96142	**78.97892**
MD5	10000	0.00024		0.00013		**0.00037**
DES3	100000	0.00738	5.00E-05	0.04648	0.03801	**0.09192**
TF	100000	0.00334	0.00097	1.31153	2.17166	**3.48750**
RSA	100000	0.00031	4.19089	17.70787	735.32225	**757.22132**
MD5	100000	0.00289		0.0014		**0.00429**
DES3	1000000	0.02855	0.00107	0.45022	0.35199	**0.83183**
TF	1000000	0.04256	0.00104	141.63276	144.5493	**286.22566**
RSA	1000000	0.004	3.39105	175.29584	7206.1605	**7384.85139**
MD5	1000000	0.01882		0.01294		**0.03176**

Graficas de tendencia según la cantidad de las palabras procesadas.

Ilustración 1. Tendencia al procesar 10 palabras

Ilustración 2. Tendencia al procesar 100 palabras

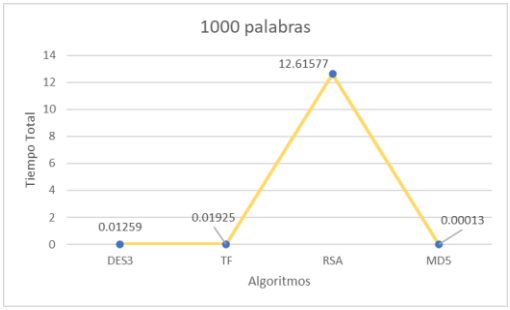


Ilustración 3. Tendencia al procesar 1000 palabras

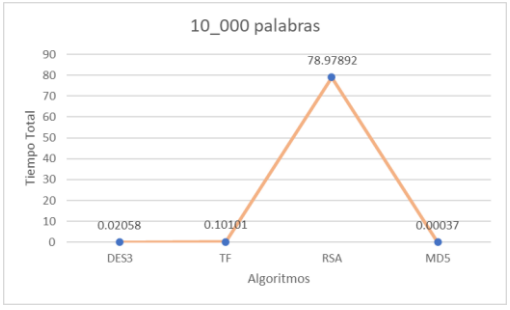


Ilustración 4. Tendencia al procesar 10_000 palabras

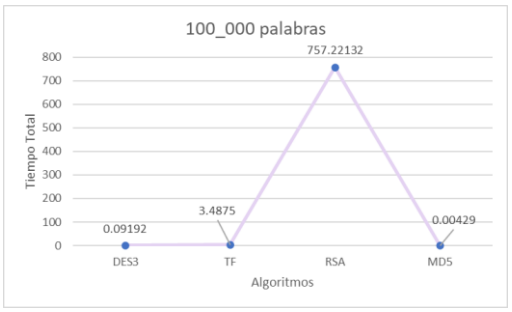


Ilustración 5. Tendencia al procesar 100_000 palabras

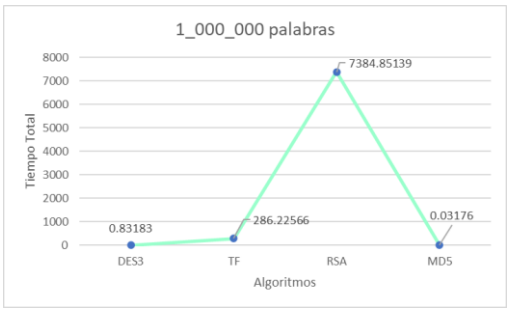


Ilustración 6. Tendencia al procesar 1000_000 de palabras

Conclusión:

En términos de velocidad de ejecución, los algoritmos DES3 y MD5 tienden a ser más rápidos en general en comparación con RSA y TF. Esto los hace preferibles en situaciones en las que la eficiencia de tiempo es crucial.

En las etapas de cifrado (E3) y descifrado (E4), el algoritmo DES3 tiende a ser más rápido en general. Sin embargo, la elección del algoritmo de cifrado no debe basarse únicamente en la velocidad, sino también en la seguridad y otros requisitos específicos.

En cuanto a la escalabilidad, el algoritmo RSA muestra un aumento significativo en el tiempo de ejecución a medida que aumenta la cantidad de palabras, lo que puede dificultar su eficiencia con volúmenes de datos más grandes. Los algoritmos DES3 y MD5 parecen mantener tiempos más estables a medida que aumenta la cantidad de palabras.