UNIVERSIDAD CENTRAL DEL ECUADOR

COMPUTACIÓN

OCTAVO SEMESTRE

Criptografía y seguridad de la información

TAREA-04-U1-G05

Tema:

Algoritmos simétricos, asimétricos y funciones hash

Integrantes:

Pineda Fernández Marco André

Ramírez Yépez Leonardo David

Vinueza Zambrano Edlith Alejandra

18/11/2024

Resultados del Análisis de Algoritmos de Cifrado

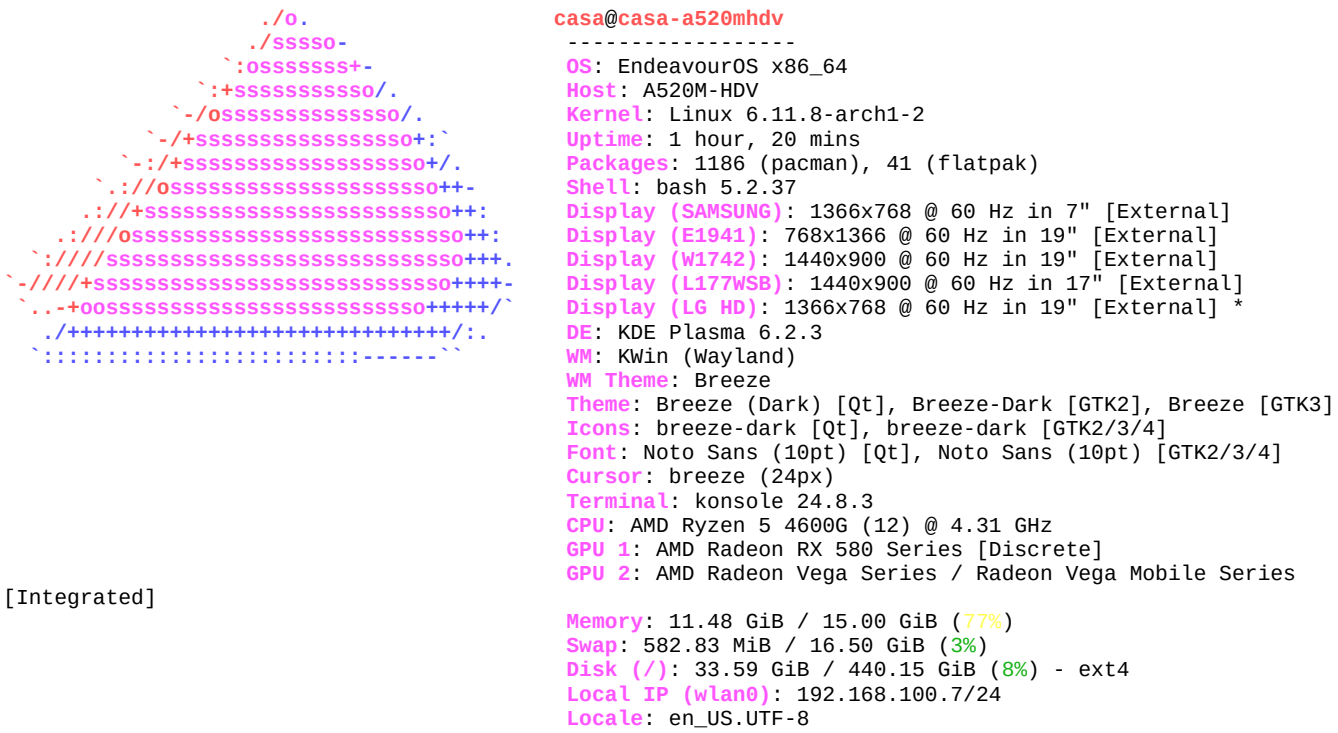
En este documento se presentan los resultados obtenidos al implementar y analizar tres algoritmos de cifrado: un algoritmo simétrico, un algoritmo asimétrico y una función hash. Cada algoritmo fue evaluado utilizando archivos con diferentes cantidades de palabras para medir su rendimiento y comportamiento. Las etapas evaluadas fueron:

1. Leer un archivo con el mensaje a cifrar.
2. Generar e imprimir la clave de cifrado/descifrado.
3. Cifrar e imprimir el texto.
4. Descifrar e imprimir el texto (excepto en funciones hash).

Los algoritmos empleados fueron: AES (Simétrico), RSA(Asimétrico) y MDS (Función Hash). Cada algoritmo fue implementado en un entorno independiente para garantizar la correcta medición de tiempos. La tabla incluye:

- **#palabras**: Número de palabras en el archivo de entrada.
- **#caracteres_entrada**: Número de caracteres en el archivo de entrada.
- **#caracteres_salida**: Número de caracteres en el texto cifrado/salida de la función hash.
- **T-E1**: Tiempo de ejecución para la etapa de lectura del archivo.
- **T-E2**: Tiempo de ejecución para la generación de claves.
- **T-E3**: Tiempo de ejecución para cifrar el texto.
- **T-E4**: Tiempo de ejecución para descifrar el texto (o generar el hash).
- **T-Total**: Tiempo total de ejecución.

El codigo fue ejecutado en un sistema con las siguientes especificaciones:



Algoritmo	#Palabras	#Caracteres de entrada	#Caracteres de salida	T-E1	T-E2	T-E3	T-E4	T-TOTAL
AES	10	105	152	0.004446992	0.000003406	0.046559659	0.000304713	0.051314770
AES	100	1117	1496	0.006235738	0.000007995	0.052491287	0.000501022	0.059236042
AES	1000	10735	14316	0.003691306	0.000004709	0.049377459	0.002106348	0.055179822
AES	10000	106060	141420	0.005919956	0.000008106	0.049656797	0.006985467	0.062570326
AES	100000	1060221	1413632	0.008915065	0.000010820	0.068086122	0.014818230	0.091830237
AES	1000000	10590848	14121152	0.020701900	0.000026570	0.133962400	0.052541986	0.207232856
AES	10000000	105900209	141200300	0.131234925	0.000032861	0.378469279	0.318404278	0.828141343

Algoritmo	#Palabras	#Caracteres de entrada	#Caracteres de salida	T-E1	T-E2	T-E3	T-E4	T-TOTAL
RSA	10	105	803	0.000027	0.0089876	0.000082	0.004975	0.0140716
RSA	100	1117	8565	0.000034	0.0089876	0.000188	0.060257	0.0694666
RSA	1000	10735	82430	0.000116	0.0089876	0.001234	0.597264	0.6076016

RSA	10000	106060	831850	0.000295	0.0089876	0.008410	5.995687	6.0133796
RSA	100000	1060221	8135653	0.001044	0.0089876	0.076921	60.406173	60.4931256
RSA	1000000	10590848	81271087	0.013212	0.0089876	0.771371	598.834867	599.6284376
RSA	10000000	105900209	812625555	0.086311	0.0089876	7.792832	6002.426351	6010.3144816

Algoritmo	#Palabras	#Caracteres de entrada	#Caracteres de salida	T-E1	T-E2	T-E3	T-E4	T-TOTAL
MD5	10	105	16	0.000080	N/A	0.000005	N/A	0.0000850
MD5	100	1117	16	0.000081	N/A	0.000009	N/A	0.0000819
MD5	1000	10735	16	0.000199	N/A	0.000053	N/A	0.0002520
MD5	10000	106060	16	0.000355	N/A	0.000630	N/A	0,0009850
MD5	100000	1060221	16	0.001941	N/A	0.004913	N/A	0,0068540
MD5	1000000	10590848	16	0.009492	N/A	0.049350	N/A	0,0588420
MD5	10000000	105900209	16	0.131872	N/A	0.492622	N/A	0,6244940