

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 código fue ejecutado en un sistema con las siguientes especificaciones:

```

./0.
./SSSS0-
:OSSSSSS+-
`:+SSSSSSSSS0/.
`-/OSSSSSSSSSSS0/.
`-/+SSSSSSSSSSSSSSS0+:`
`-:/+SSSSSSSSSSSSSSSSS0+/.
`.://OSSSSSSSSSSSSSSSSSSS0++-
.://+SSSSSSSSSSSSSSSSSSSSS0++:
.:///OSSSSSSSSSSSSSSSSSSSSSSS0++:
`.:///SSSSSSSSSSSSSSSSSSSSSSS0+++.
-:///+SSSSSSSSSSSSSSSSSSSSSSS0++++-
`..-+OSSSSSSSSSSSSSSSSSSSSSSS0+++++/-
./+++++

```

```

casea@casea-a520mhdv
-----
OS: EndeavourOS x86_64
Host: A520M-HDV
Kernel: Linux 6.11.8-arch1-2
Uptime: 1 hour, 20 mins
Packages: 1186 (pacman), 41 (flatpak)
Shell: bash 5.2.37
Display (SAMSUNG): 1366x768 @ 60 Hz in 7" [External]
Display (E1941): 768x1366 @ 60 Hz in 19" [External]
Display (W1742): 1440x900 @ 60 Hz in 19" [External]
Display (L177WSB): 1440x900 @ 60 Hz in 17" [External]
Display (LG HD): 1366x768 @ 60 Hz in 19" [External] *
DE: KDE Plasma 6.2.3
WM: KWin (Wayland)
WM Theme: Breeze
Theme: Breeze (Dark) [Qt], Breeze-Dark [GTK2], Breeze [GTK3]
Icons: breeze-dark [Qt], breeze-dark [GTK2/3/4]
Font: Noto Sans (10pt) [Qt], Noto Sans (10pt) [GTK2/3/4]
Cursor: breeze (24px)
Terminal: konsole 24.8.3
CPU: AMD Ryzen 5 4600G (12) @ 4.31 GHz
GPU 1: AMD Radeon RX 580 Series [Discrete]
GPU 2: AMD Radeon Vega Series / Radeon Vega Mobile Series

Memory: 11.48 GiB / 15.00 GiB (77%)
Swap: 582.83 MiB / 16.50 GiB (3%)
Disk (/): 33.59 GiB / 440.15 GiB (8%) - ext4
Local IP (wlan0): 192.168.100.7/24
Locale: en_US.UTF-8

```

[Integrated]

| Algoritmo | #Palabras | #Caracteres de entrada | #Caracteres de salida | T-E1 | T-E2 | T-E3 | T-E4 | T-TOTAL |
|-----------|-----------|------------------------|-----------------------|-----------------|-----------------|-----------------|-----------------|-------------|
| AES | 10 | 105 | 152 | 0.004446 992 | 0.000003 406 | 0.046559 659 | 0.000304 713 | 0.051314770 |
| AES | 100 | 1117 | 1496 | 0.006235 738 | 0.000007 995 | 0.052491 287 | 0.000501 022 | 0.059236042 |
| AES | 1000 | 10735 | 14316 | 0.003691 306 | 0.000004 709 | 0.049377 459 | 0.002106 348 | 0.055179822 |
| AES | 10000 | 106060 | 141420 | 0.005919 956 | 0.000008 106 | 0.049656 797 | 0.006985 467 | 0.062570326 |
| AES | 100000 | 1060221 | 1413632 | 0.008915 065 | 0.000010 820 | 0.068086 122 | 0.014818 230 | 0.091830237 |
| AES | 1000000 | 10590848 | 14121152 | 0.020701 900 | 0.000026 570 | 0.133962 400 | 0.052541 986 | 0.207232856 |
| AES | 10000000 | 105900209 | 141200300 | 0.131234 925 | 0.000032 861 | 0.378469 279 | 0.318404 278 | 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 | 0.008987 6 | 0.000082 | 0.004975 | 0.0140716 |
| RSA | 100 | 1117 | 8565 | 0.000034 | 0.008987 6 | 0.000188 | 0.060257 | 0.0694666 |
| RSA | 1000 | 10735 | 82430 | 0.000116 | 0.008987 6 | 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 |