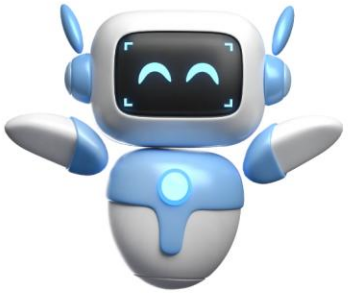
Lab de Arquitectura de Computadores y Ensambladores 1
Grupo 12

Informe de Impacto

Algoritmo de Desencriptación

AES-128



Integrantes:
201610975 - Michael Cristian Itzep Ixcayau
202104727 - López Suy, Luigi Anderson
202202055 - González Espinoza, Fernando Andhré
202300652 - González Pereira, Vasti Abigail

Contents

Resumen:

La criptografía ha sido de gran importancia a lo largo de la historia, incluso decidió el curso de una guerra, específicamente en la segunda guerra mundial en donde se usó para descifrar la máquina Enigma y con ello plantear estrategias que llevaron a la ruina a los alemanes. Por lo que el aprendizaje de las bases de criptografía es significativo para los desarrolladores, por lo que se realiza el algoritmo de desencriptación simétrica AES de 128 que utiliza el lenguaje ensamblador ARM64. Este tiene como objetivo traducir un proceso de descifrado complejo y sus operaciones inversas con el uso de un lenguaje de bajo nivel, manejando bytes para recuperar el texto original a través de cadenas cifradas.

Optimización y Ventajas:

- Acceso más directo al hardware
- Extiende capacidades
- Traducción de instrucciones a código eficiente
- Mejor rendimiento
- Eficiencia energética

Aritmética Exacta: El uso de Campos de Galois es fundamental en criptografía porque permite realizar procesos inversos (cifrar y descifrar) sin errores de redondeo o truncamiento, a diferencia de la aritmética real.

Seguridad y Confiabilidad:

- Aritmética exacta (Campos de Galois), permite realizar procesos inversos sin temer por errores de redondeo o truncamiento, tal como pasaría si se usara una aritmética real.
- El uso de AES-128 consiste en la utilización de 128 bits para descifrar bloques de datos de 128 bits. Realiza 10 rondas de operaciones matemáticas.
- Por su eficacia desde 2002 se ha utilizado AES-128

Desarrollo en Área profesional:

- Permite usar hardware más económico y reduce el gasto eléctrico en dispositivos móviles y servidores.
- Minimiza la latencia en la recuperación de información cifrada mediante un set reducido de instrucciones (RISC)
- Maximiza el uso de registros y memoria RAM, evitando el sobreuso de recursos del sistema

Aplicaciones en la vida real:

- IoT:
    - Con las ventajas que ofrece el lenguaje a bajo nivel, logra alargar la vida de las baterías y reduce el costo de mantenimiento
- Telecomunicaciones:
    - La desencriptación a bajo nivel reduce el tiempo de respuesta en la transmisión de datos cifrados en tiempo real (como llamadas de voz sobre IP o streaming seguro).
- Seguridad sin Errores:
    - Al utilizar la aritmética del Campo de Galois, se garantiza que no existan errores de redondeo o truncamiento, lo que evita fallos en la integridad de los datos que podrían costar millones en recuperaciones de sistemas.
- Centros de Datos
    - Implementar algoritmos de seguridad en ensamblador permite procesar más peticiones por segundo en un mismo servidor. Esto reduce la cantidad de servidores necesarios para manejar la carga de tráfico, impactando directamente en la reducción de costos operativos de energía y enfriamiento.
- Cloud Computing
    - Implementar algoritmos de seguridad en ensamblador permite procesar más peticiones por segundo en un mismo servidor. Esto reduce la cantidad de servidores necesarios para manejar la carga de tráfico, impactando directamente en la reducción de costos operativos de energía y enfriamiento.
- Desarrollo de Firmware y Drivers de Seguridad
    - Las empresas de hardware aplican estas técnicas para crear "módulos de seguridad de hardware" (HSM) donde la velocidad de la desencriptación es clave para no generar cuellos de botella en el sistema operativo.