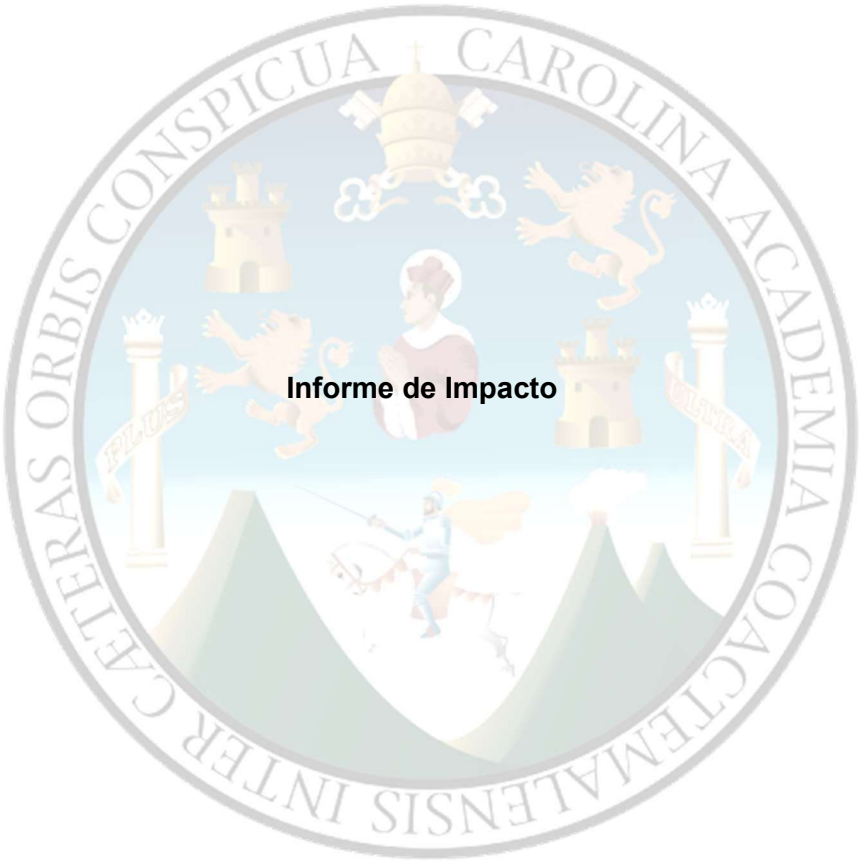
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
SEGUNDO SEMESTRE
2025
ESTRUCTURAS DE DATOS



Informe de Impacto

Nombre	Carné
Yury Urbano Santos Chagil	202113318

Introducción

El presente informe de impacto tiene como objetivo analizar las implicaciones técnicas, académicas y prácticas derivadas del desarrollo del proyecto “Implementación del algoritmo AES-128 en ensamblador ARM64”.

Este proyecto busca demostrar la aplicación directa de los principios de arquitectura de computadores y criptografía, implementando un algoritmo de cifrado simétrico de estándar internacional (AES) desde el nivel más bajo del hardware.

Además de su valor académico, este desarrollo tiene un impacto potencial en eficiencia computacional, reducción de costos de software criptográfico y formación de competencias técnicas avanzadas en el área de ingeniería en sistemas.

Contexto de aplicación

El cifrado AES-128 es un estándar aprobado por el National Institute of Standards and Technology (NIST) y ampliamente usado en comunicaciones seguras, almacenamiento de datos, dispositivos IoT y aplicaciones de autenticación.

En la actualidad, la mayoría de las implementaciones se realiza en lenguajes de alto nivel (C, Java, Python), lo que facilita la portabilidad, pero reduce el control sobre el rendimiento en hardware específico.

La implementación directa en ensamblador ARM64 tiene relevancia en contextos como:

- Dispositivos embebidos y de bajo consumo, donde cada ciclo de CPU y cada byte de memoria son valiosos.
- Procesadores ARM en teléfonos móviles y sistemas IoT, que requieren cifrado local eficiente.
- Entornos académicos y de investigación, para comprender la interacción entre algoritmos criptográficos y arquitectura de procesadores.

Por lo tanto, este proyecto se ubica en el punto de convergencia entre el aprendizaje académico y la optimización práctica del hardware.

Impacto técnico

Eficiencia y rendimiento

La versión en ensamblador permite controlar directamente los registros y operaciones lógicas, eliminando las capas de abstracción presentes en los lenguajes de alto nivel.
Esto conlleva las siguientes mejoras observables:

- Optimización de tiempo de ejecución:
  El cifrado completo de 128 bits se ejecuta en ciclos mínimos, aprovechando las instrucciones EOR, ADR, LDRB, STRB, BL, y operaciones vectorizadas cuando es posible.

- Uso eficiente de memoria:
  Se reducen las cargas y escrituras innecesarias al reutilizar registros (x0–x7) y direccionamiento inmediato.
  La matriz de estado (16 bytes) y la clave se mantienen en registros o bloques de memoria contigua.

- Paralelismo controlado:
  Al implementarse de manera modular, las rutinas como mixColumns o byteSub pueden adaptarse para aprovechar instrucciones SIMD (Single Instruction, Multiple Data) en futuros procesadores ARM.

Estas características incrementan la eficiencia energética y computacional, haciendo posible integrar esta versión en sistemas donde el consumo de energía o el espacio en memoria son factores críticos.

Robustez y seguridad

El proyecto fortalece la comprensión del flujo interno de AES, permitiendo verificar manualmente cada transformación:

ByteSub → ShiftRows → MixColumns → AddRoundKey.

Esto contribuye a mejorar la transparencia y seguridad del proceso, al no depender de bibliotecas externas o código cerrado.

Además, al ejecutarse directamente en nivel de hardware:

- Se reducen los riesgos de vulnerabilidades por interpretadores o bibliotecas con exploits.
- Se habilita el uso de cifrado local sin conexión, útil para dispositivos que operan en entornos restringidos (por ejemplo, nodos IoT o controladores industriales).

Impacto académico y formativo

Fortalecimiento de competencias

Este proyecto aporta un impacto significativo en la formación del estudiante, al integrar múltiples áreas del conocimiento:

- Arquitectura de procesadores (ARMv8, registros, direccionamiento).
- Programación en bajo nivel y control de flujo
- Criptografía simétrica y manipulación de bytes.
- Estructuración modular de proyectos de ensamblador.
- Validación experimental mediante ejecución controlada en QEMU.

El estudiante adquiere una comprensión real del ciclo de ejecución del cifrado, de cómo los datos se transforman en registros, y del impacto de las decisiones de diseño en el rendimiento.

Transferencia de conocimiento

La documentación y modularización del código facilitan su uso como material de referencia en cursos futuros de Arquitectura de Computadores, Seguridad Informática y Criptografía Aplicada.

Esto contribuye al fortalecimiento del conocimiento técnico dentro del entorno académico, permitiendo que otros estudiantes comprendan los fundamentos del cifrado a bajo nivel.

Impacto económico y de eficiencia de recursos

La implementación de AES en ensamblador puede tener un impacto directo en la reducción de costos y mejora de la eficiencia energética en sistemas reales:

- Eliminación de dependencias de software propietario:
  Al ser un desarrollo propio y abierto, se evita el pago de licencias o dependencias de librerías comerciales de cifrado.

- Menor consumo de CPU y energía:
  Las rutinas optimizadas en ensamblador reducen el número de ciclos de reloj necesarios, prolongando la autonomía de dispositivos móviles y sistemas embebidos.

- Mayor vida útil del hardware existente:
  Dado que el cifrado puede realizarse eficientemente en hardware de bajo costo, se amplía la utilidad de dispositivos con procesadores ARM antiguos o de gama baja.

Estos factores son particularmente relevantes en proyectos de investigación aplicada, dispositivos IoT o sistemas de seguridad con presupuestos limitados.

Impacto social y tecnológico

Desde una perspectiva social y tecnológica, el proyecto promueve:

- Autonomía tecnológica local, al desarrollar soluciones propias sin depender de librerías extranjeras.
- Democratización del conocimiento criptográfico, al compartir código abierto, bien documentado y educativo.
- Fomento de buenas prácticas de seguridad informática en estudiantes e instituciones.
- Conciencia sobre la importancia del cifrado en la protección de datos personales y empresariales.

Asimismo, se abre la posibilidad de extender esta implementación a:

- Sistemas de comunicación cifrada en redes internas.
- Dispositivos IoT con protección de datos sensible.
- Plataformas educativas para enseñanza de arquitectura y seguridad.

Conclusiones

El impacto del proyecto AES-128 en ARM64 Assembly se refleja tanto en el ámbito técnico y académico como en el económico y social.

Su implementación demuestra que es posible construir soluciones criptográficas de alto nivel desde la base del hardware, optimizando recursos, aumentando la transparencia del proceso y fortaleciendo la seguridad digital.

A nivel académico, el proyecto representa un ejercicio integral de aplicación práctica, fortaleciendo las competencias del estudiante en programación ensamblador, arquitectura, criptografía y desarrollo modular.

A nivel tecnológico, abre oportunidades para sistemas más eficientes, económicos y seguros, reafirmando la importancia de la ingeniería de bajo nivel en la era de la ciberseguridad y la computación distribuida.

Referencias

- Larry D. Pyeatt. *ARM 64-Bit Assembly Language (2020).*
- NIST FIPS PUB 197: *Advanced Encryption Standard (AES)*.
- ARM Developer Documentation – Instruction Set Reference.
- Material de cátedra – Universidad de San Carlos de Guatemala.