Proyecto Final AES

Shara Teresa González Mena

Moisés Montaño Copca

**Descripción breve del proyecto**:

El proyecto consiste en implementar una solución en código para cifrar y descifrar cualquier archivo usando el algoritmo de encriptación AES (Advanced Encryption Standard) y AES-NI (Advanced Enryption Standard New Instructions) para comparar los tiempos de cifrado y descifrado de diferentes archivos entre ambas arquitecturas. La implementación de AES se deberá hacer de manera nativa, es decir, sin una librería que ya incorpore el algoritmo. En cambio, el algoritmo de AES-NI debe usar alguna librería para que cumpla con las instrucciones requeridas en la arquitectura del procesador.

Para la solución desarrollamos dos programas, uno para AES y otro para AES-NI. A continuación presentamos los resultados de ambos.

**Resultados (captura de pantallas de tu programa vs Cryptool para cada uno de 4 casos seleccionados)**

Archivo: PoliticasEM2018.pdf

Original:

Cifrado-AES:

Descifrado-AES:

Cifrado-AES-NI:

Descifrado-AES-NI:

Cryptool:

Archivo: REC\_1271656.docx

Original:

Cifrado-AES:

Descifrado-AES:

Cifrado-AES-NI:

Descifrado-AES-NI:

Cryptool:

Archivo: OPD.html

Original:

Cifrado-AES:

Descifrado-AES:

Cifrado-AES-NI:

Descifrado-AES-NI:

Cryptool:

**Tabla que muestre el tiempo de cifrado y descifrado sin y con librería AES-NI para al menos 3 archivos de diferentes tamaños**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **AES** | | **AES-NI** | |
| **Nombre del Archivo** | **Tamaño** | **Tiempo de Cifrado** | **Tiempo de Descifrado** | **Tiempo de Cifrado** | **Tiempo de Descifrado** |
| PoliticasEM2018.pdf | 31 KB | 0.3363 s | 2.73301 s |  |  |
| REC\_1271656.docx | 7.9 KB | 0.0988 s | 0.6929 s |  |  |
| OPD.html | 53 KB | 0.5723 s | 4.8061 s |  |  |

**Conclusiones individuales**

Shara:

Moisés:

Implementar AES presentó un gran reto, pero trajo consigo un buen resultado. Es uno de los mejores algoritmos de encriptación a nivel global y pude observar que los tiempos para cifrar y descifrar no son tan grandes, menos cuando se implementan con las instrucciones del AES-NI.

La tecnología sigue desarrollándose sin parar en el mundo, y esto trae consigo muchos retos para la seguridad de la información. Creo que es muy útil conocer la implementación de ciertos algoritmos que sirven para proteger mejor la información, como AES, y veo buenas oportunidades para mi desarrollo personal y profesional con este conocimiento.