Tarea: Presentación Semanal

- Definición del tema de investigación (título, objetivos, definición del problema).

Título: “Securing Data in Low-Resource Systems: Lightweight Block Cryptography Strategies”
Objetivos:

1. Analizar y comparar diferentes algoritmos de encriptación de bloques para determinar su eficacia en sistemas con recursos limitados.
2. Desarrollar y probar implementaciones eficientes de algoritmos de encriptación de bloques adaptados a dispositivos con capacidades de procesamiento limitadas.
3. Evaluar la seguridad y el rendimiento de los algoritmos de encriptación de bloques en entornos con restricciones de recursos, como dispositivos IoT y sistemas embebidos.

Definición del problema:
A pesar de la existencia de algoritmos eficientes de encriptación de bloques diseñados para sistemas con recursos limitados, su implementación efectiva en dispositivos como sistemas embebidos y dispositivos IoT se ve dificultada por factores como decisiones de fabricantes y restricciones de integración. Esta brecha entre la disponibilidad de soluciones de seguridad y su adopción práctica en entornos que manejan información sensible subraya la necesidad de identificar y desarrollar estrategias para implementar estos algoritmos de encriptación de manera efectiva. El objetivo es garantizar la seguridad de la información en entornos con limitaciones significativas de capacidad de procesamiento y memoria, facilitando así su protección en canales inseguros como el aire.

- Listado de por lo menos 5 papers que solucionen el mismo problema.

QTL: A new ultra-lightweight block cipher (Li et al., 2016) drive | source
GIFT: A Small Present (Banik et al., 2017) drive | source
SLIM: A Lightweight Block Cipher for Internet of Health Things (Aboushosha et al., 2020) drive | source
Shadow: A Lightweight Block Cipher for IoT Nodes (Guo et al., 2021) drive | source
DULBC: A dynamic ultra-lightweight block cipher with high-throughput (Yang et al., 2022) drive | source

- Redacción inicial del estado del arte.

El documento .pdf se encuentra adjunto en la entrega semanal y en un repositorio online junto a los archivos fuente.