Títulos posibles:

- Seguridad en comunicaciones industriales mediante cifrado de la información: implementación de algoritmos de cifrado en un sistema basado en microcontrolador.
- Diseño y evaluación de sistemas de comunicación industrial seguros basados en algoritmos de cifrado modernos.
- Optimización de algoritmos de cifrado para dispositivos embebidos en entornos industriales.
- Estudio comparativo de algoritmos de cifrado en comunicaciones industriales.

Objetivos:

- Estudiar los fundamentos matemáticos de distintos algoritmos tanto de cifrado simétrico como de cifrado asimétrico.
- Implementar estos algoritmos en un microcontrolador que simule el funcionamiento de una planta industrial.
- Implementar un sistema de comunicaciones PC – Microcontrolador para establecer un canal de comunicaciones.
- Comparar los distintos algoritmos para comparar eficiencia y seguridad del cifrado:
    - Comparar los algoritmos de cifrado simétrico entre sí.
    - Comparar los algoritmos de cifrado asimétrico entre sí.
- Estudiar la posibilidad de implementar los algoritmos en sistemas basados en FPGAs si el rendimiento del microcontrolador no fuese suficiente.

Resumen:

En el ámbito de las comunicaciones industriales, garantizar la seguridad de la información es crucial debido a la creciente interconexión de dispositivos y sistemas. Este trabajo se centra en el análisis, implementación y evaluación de distintos algoritmos de cifrado, tanto simétricos como asimétricos, en sistemas basados en microcontroladores. Se presenta un estudio detallado de los fundamentos matemáticos de cada algoritmo y su impacto en la seguridad y eficiencia del cifrado en un entorno industrial simulado.

La implementación incluye un sistema de comunicación entre un PC y un microcontrolador que actúa como nodo de una planta industrial, permitiendo el análisis práctico de la transmisión de datos cifrados. Además, se realiza una comparación entre algoritmos simétricos y asimétricos para determinar su rendimiento en términos de velocidad, consumo de recursos y robustez frente a posibles ataques.

Por último, se explora la viabilidad de migrar estos algoritmos a dispositivos basados en FPGAs como una solución para mejorar el rendimiento en aplicaciones donde los microcontroladores puedan resultar insuficientes. Los resultados obtenidos buscan servir de guía para la implementación de sistemas de comunicación seguros en entornos industriales modernos.