



UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y  
DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

**TRABAJO FIN DE GRADO**

**ESTUDIO COMPARATIVO DE  
DIFERENTES ALGORITMOS DE  
ENCRIPTACIÓN PARA  
COMUNICACIONES INDUSTRIALES**

Bogurad Barański Barańska

*Tutor:* Roberto Gonzalez Herranz

*Departamento:* ingeniería eléctrica, electrónica, automática y física  
aplicada.

Madrid, Mes, 2025





UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y  
DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

**TRABAJO FIN DE GRADO**

**TÍTULO DEL TRABAJO**

Firma Autor

*Firma Tutor*



Copyright ©2025. Bogurad Barański Barańska

Esta obra está licenciada bajo la licencia Creative Commons

Atribución-NoComercial-SinDerivadas 3.0 Unported (CC BY-NC-ND 3.0). Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-nd/3.0/deed.es> o envíe una carta a Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, EE.UU.

Todas las opiniones aquí expresadas son del autor, y no reflejan necesariamente las opiniones de la Universidad Politécnica de Madrid.



**Título:** Estudio comparativo de diferentes algoritmos de encriptación para comunicaciones industriales

**Autor:** Bogurad Barański Barańska

**Tutor:** Roberto Gonzalez Herranz

## EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día ..... de ..... de ... en ....., en la Escuela Técnica Superior de Ingeniería y Diseño Industrial de la Universidad Politécnica de Madrid, acuerda otorgarle la CALIFICACIÓN de:

VOCAL

SECRETARIO

PRESIDENTE





# Agradecimientos

Agradezco a .....



# Resumen

Este proyecto se resume en.....

**Palabras clave:** palabraclave1, palabraclave2, palabraclave3.



# Abstract

In this project...

**Keywords:** keyword1, keyword2, keyword3.



# Índice general

<b>Agradecimientos</b>	<b>IX</b>
<b>Resumen</b>	<b>XI</b>
Palabras clave: . . . . .	XI
<b>Abstract</b>	<b>XIII</b>
Keywords: . . . . .	XIII
<b>Índice</b>	<b>xv</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Motivación del proyecto . . . . .	1
1.2. Objetivos . . . . .	1
1.3. Herramientas utilizadas . . . . .	2
1.3.1. LaTeX [1] . . . . .	2
1.3.2. TikzMaker [2] . . . . .	2
1.4. Estructura del documento . . . . .	2
<b>2. Estado del arte</b>	<b>3</b>
<b>3. Fundamentos generales</b>	<b>5</b>
<b>4. Desarrollo</b>	<b>7</b>
<b>5. Resultados y discusión</b>	<b>9</b>
5.1. Resultados . . . . .	9
5.2. Discusión . . . . .	9
<b>6. Conclusiones</b>	<b>11</b>
6.1. Conclusión . . . . .	11
6.2. Desarrollos futuros . . . . .	11
<b>A. Definiciones básicas</b>	<b>13</b>
<b>Bibliografía</b>	<b>15</b>





# Índice de figuras



# Índice de tablas



# Capítulo 1

## Introducción

### 1.1. Motivación del proyecto

Cuando en una instalación industrial se actúa o se mide un proceso, el autómatas que envía las señales puede estar situado a gran distancia de dicho proceso. Por esta razón, las comunicaciones industriales precisan el uso de buses de longitudes considerables o realizar comunicaciones a distancia.

Aunque las comunicaciones a distancia pudieran parecer una solución más económica de implementar, tienen el problema de ser vulnerables a ataques de intermediario (alguien ajeno al proceso intercepta los mensajes enviados), lo cual pone en peligro la confidencialidad de la información. Por esta misma razón, en este trabajo se estudiarán distintos algoritmos propuestos para la encriptación de los mensajes.

### 1.2. Objetivos

Para realizar el proyecto, se proponen los siguientes objetivos:

- Implementar los siguientes algoritmos en C/C++
  - RSA
  - Curvas elípticas
  - AES 256
  - Celosías
  - Algoritmo de Shore
  - Algoritmos post-cuánticos
- Estudiar la eficacia de cifrado
  - Estudiar velocidad de ejecución del algoritmo
  - Estudiar recursos requeridos por el microprocesador
  - Estudiar la robustez del cifrado
  - Estudiar la posibilidad de ataques de canal lateral
- Posibilidad de ejecución en sistemas basados en FPGAs

### 1.3. Herramientas utilizadas

#### 1.3.1. LaTeX [1]

Se ha preferido el uso de  $\text{\LaTeX}$  debido a la facilidad que ofrece para el maquetado de textos, superando a otras herramientas de elaboración de documentos. Además,  $\text{\LaTeX}$  permite crear figuras vectorizadas, representar correctamente ecuaciones y ubicar adecuadamente figuras, tablas y bibliografía.

#### 1.3.2. TikzMaker [2]

Esta herramienta permite crear figuras vectorizadas de  $\text{\LaTeX}$  mediante el paquete de circuitikz. Su principal ventaja radica en la interfaz gráfica que proporciona y en la facilidad para elaborar figuras.

### 1.4. Estructura del documento

A continuación y para facilitar la lectura del documento, se detalla el contenido de cada capítulo:

- En el capítulo 1 se realiza una introducción.
- En el capítulo 2 se hace un repaso de desarrollos anteriores .
- En el capítulo 3 se desarrollan los fundamentos matemáticos del proyecto.
- En el capítulo 4 se describe la implementación de los algoritmos.
- En el capítulo 5 se exponen los resultados obtenidos en el capítulo anterior.
- En el capítulo 6 se comparan los resultados de los distintos algoritmos.

## Capítulo 2

# Estado del arte





## Capítulo 3

# Fundamentos generales



## Capítulo 4

# Desarrollo



## Capítulo 5

# Resultados y discusión

En este capítulo se muestran los resultados obtenidos de aplicar las rutinas desarrolladas con anterioridad.

### 5.1. Resultados

### 5.2. Discusión



## Capítulo 6

# Conclusiones

Se presentan a continuación las conclusiones del proyecto y desarrollos futuros para mejorar la implementación.

### 6.1. Conclusión

Una vez finalizado el proyecto...

### 6.2. Desarrollos futuros

Un posible desarrollo...





## Apéndice A

### Definiciones básicas



# Bibliografía

- [1] Leslie Lamport et al. The latex project, 2024.
- [2] Tikzmaker. <https://tikzmaker.com/editor>, 2024.