TRABAJO FINAL DE GRADO

REDES NEURONALES APLICADAS AL CRIPTOANALISIS DEL ADVANCED ENCRYPTION STANDARD

Pedro Novas Otero

Grado en Ingeniería Informática

Inteligencia Artificial

Consultor:
David Isern Alarcón

Junio de 2018

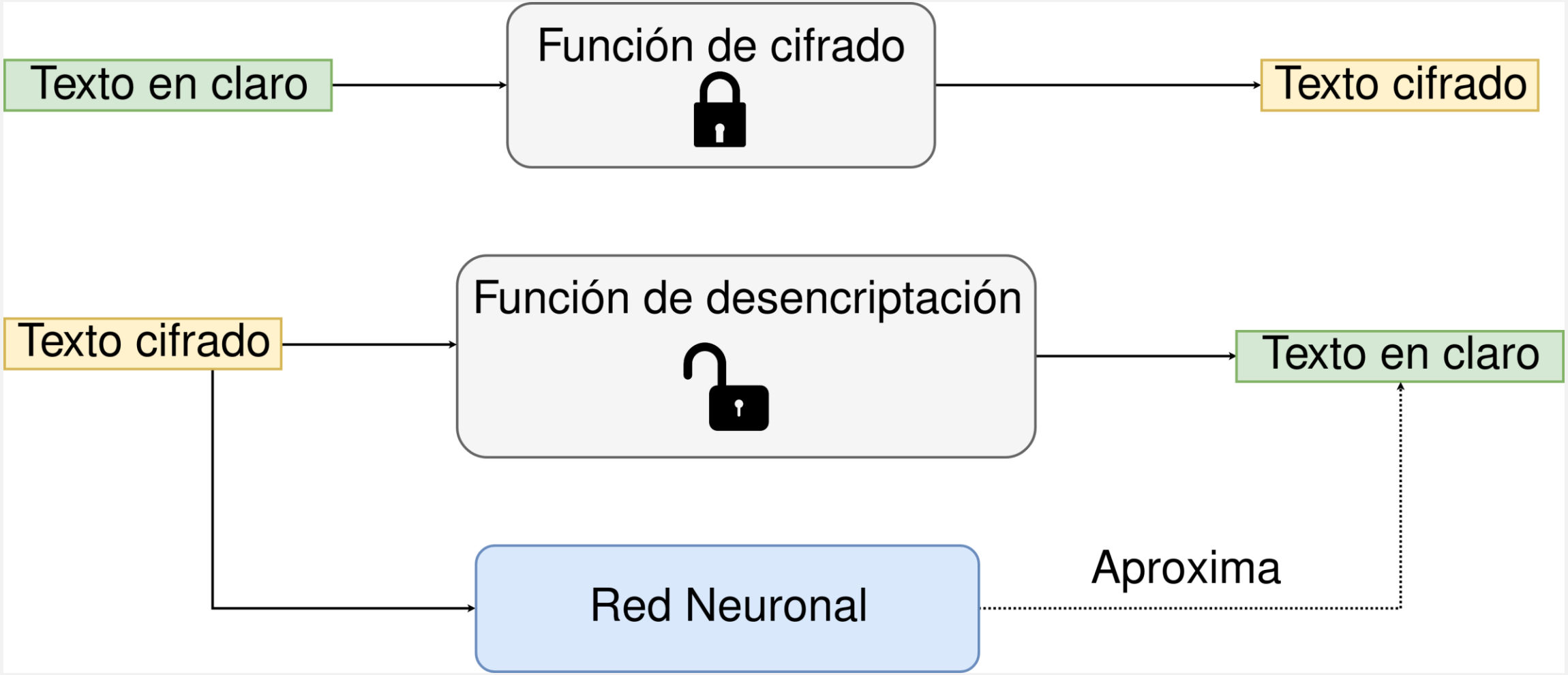
AGENDA

- Motivación del Proyecto
- Descripción del criptoanálisis propuesto
- Redes Neuronales
- AES
- Implementacion
- Resultados
- Conclusiones

MOTIVACIÓN DEL PROYECTO

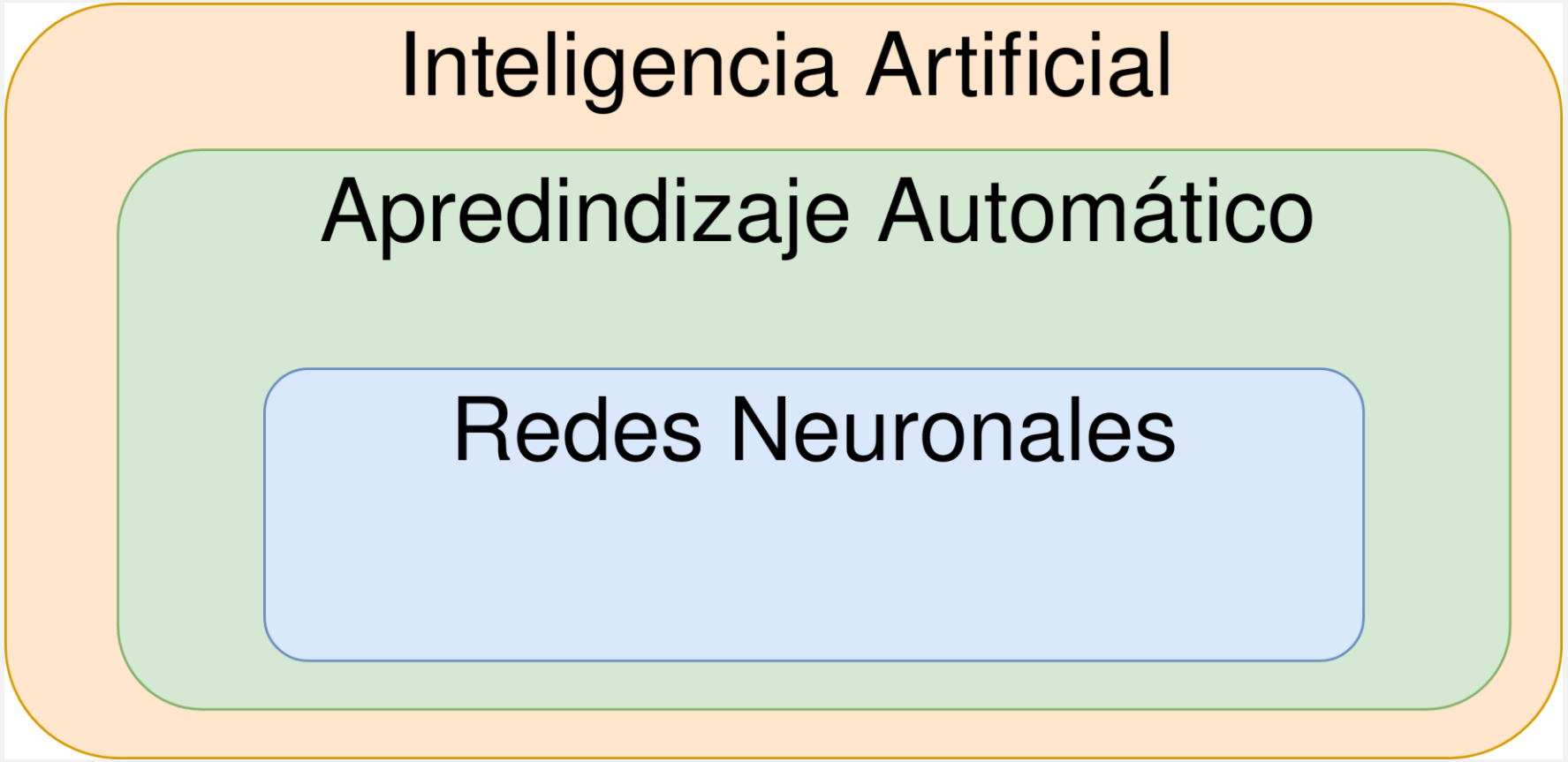
- Efectividad de la aplicacion de las redes neuronales en el criptoanálisis de otros algoritmos de cifrado de bloques: DES, Triple-DES.
- No existen estudios sobre la efectividad de las redes neuronales en el algoritmo de cifrado de bloque más utilizado actualmente: AES.

DESCRIPCIÓN DEL ATAQUE

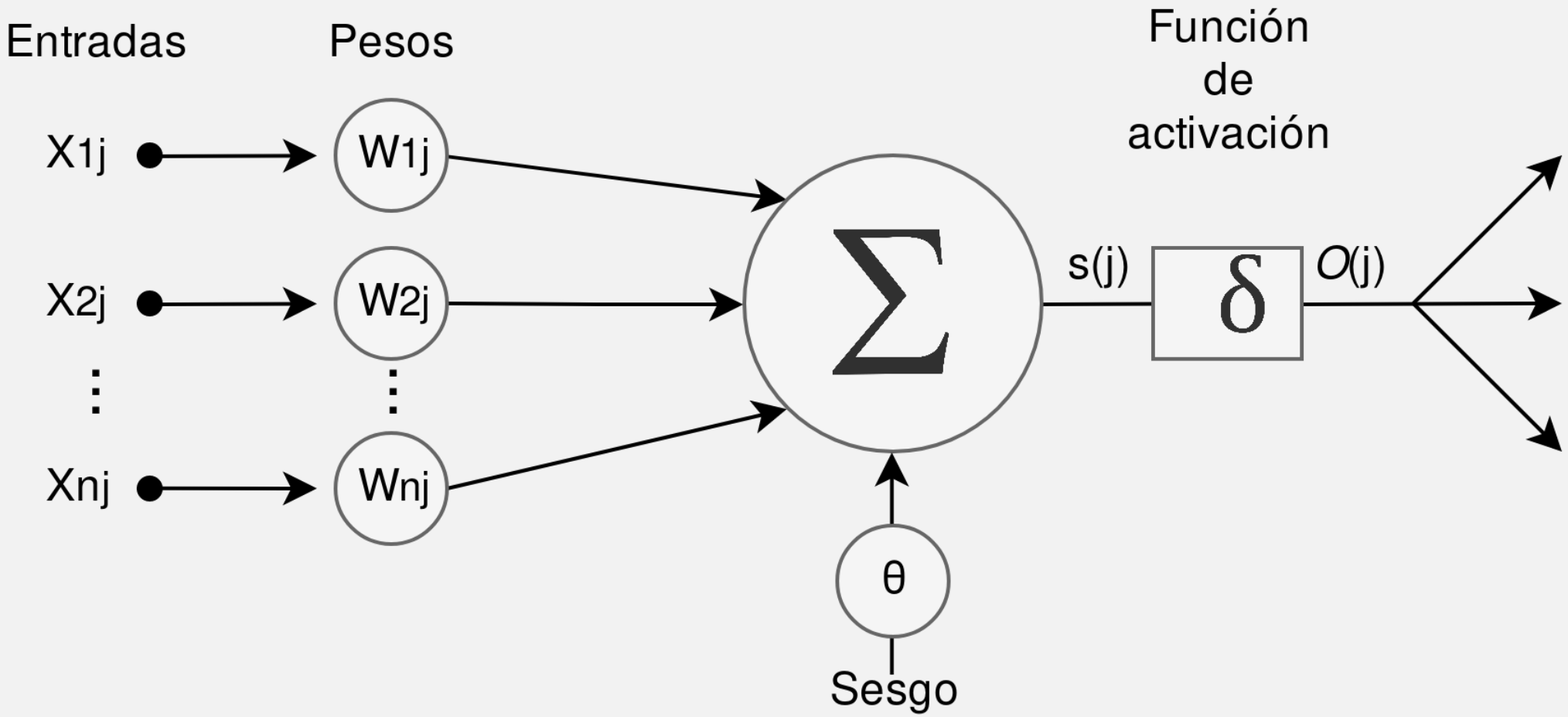


REDES NEURONALES

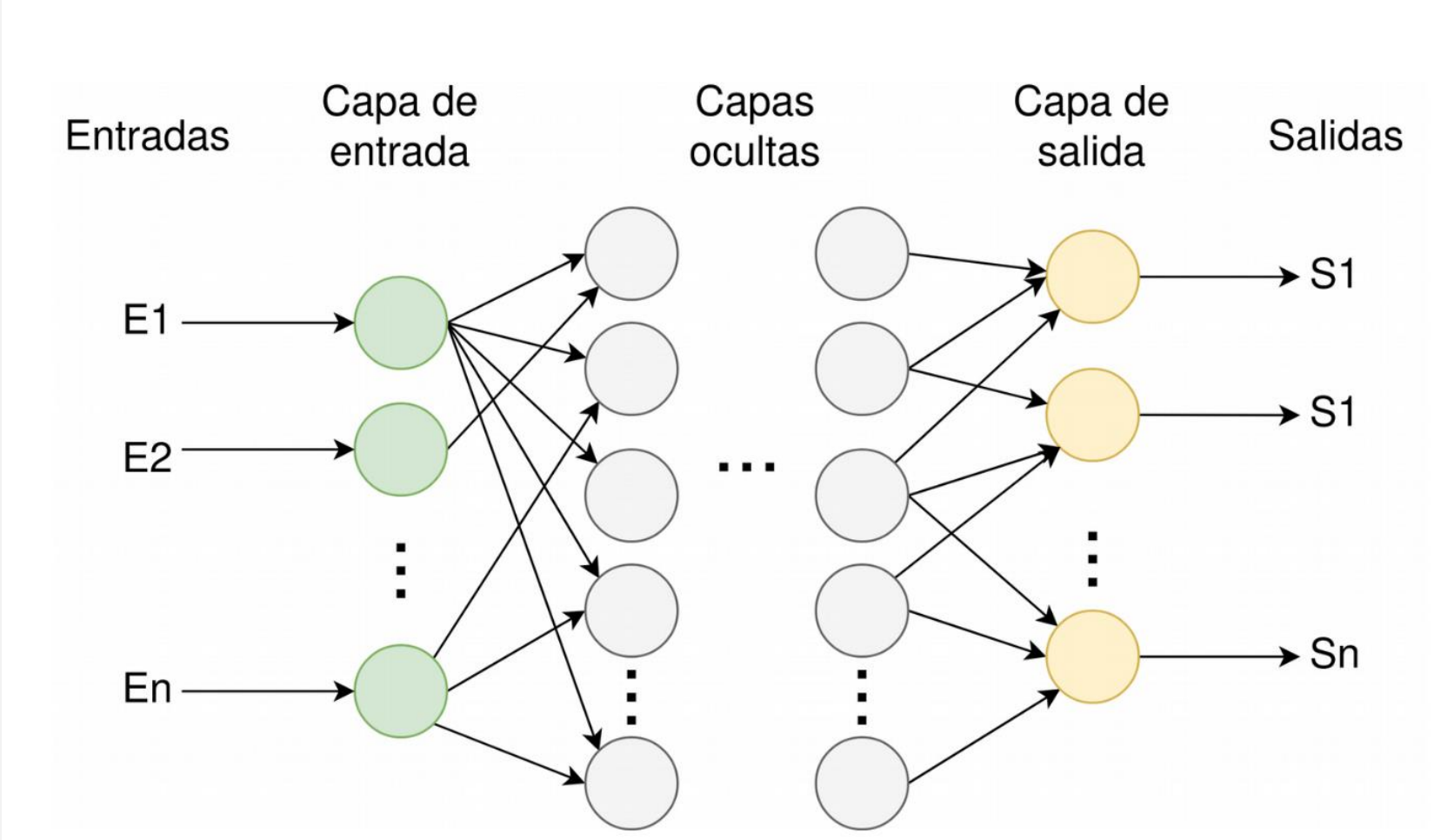
REDES NEURONALES: INTRODUCCIÓN



REDES NEURONALES: REPRESENTACIÓN DE LA INFORMACIÓN



REDES NEURONALES: ARQUITECTURAS



REDES NEURONALES: APRENDIZAJE

- Cada ejemplo de entrenamiento de la red neuronal realiza una predicción. La diferencia entre esta predicción y el valor esperado determina el coste de ese ejemplo. La función que a un ejemplo le hace corresponder su **coste** se conoce como **función de coste**.
- El proceso de aprendizaje consiste en optimizar esa función de coste y el método utilizado para optimizar la función estará determinado por el **optimizador** del modelo.

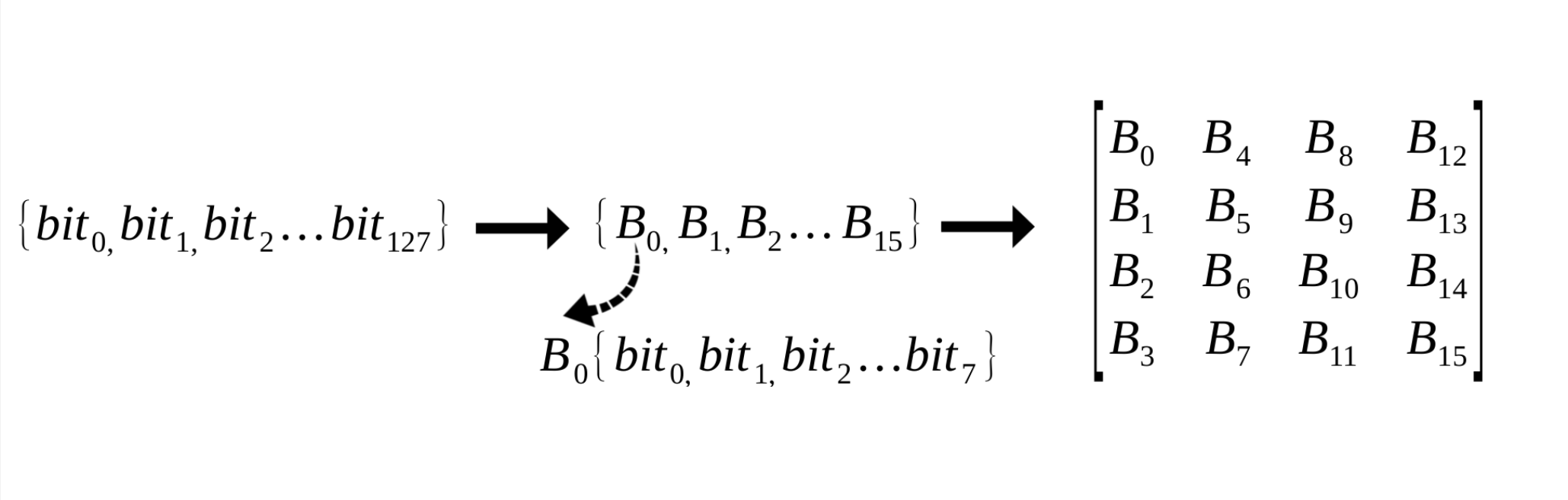
ADVANCED ENCRYPTION STANDARD

AES: INTRODUCCIÓN

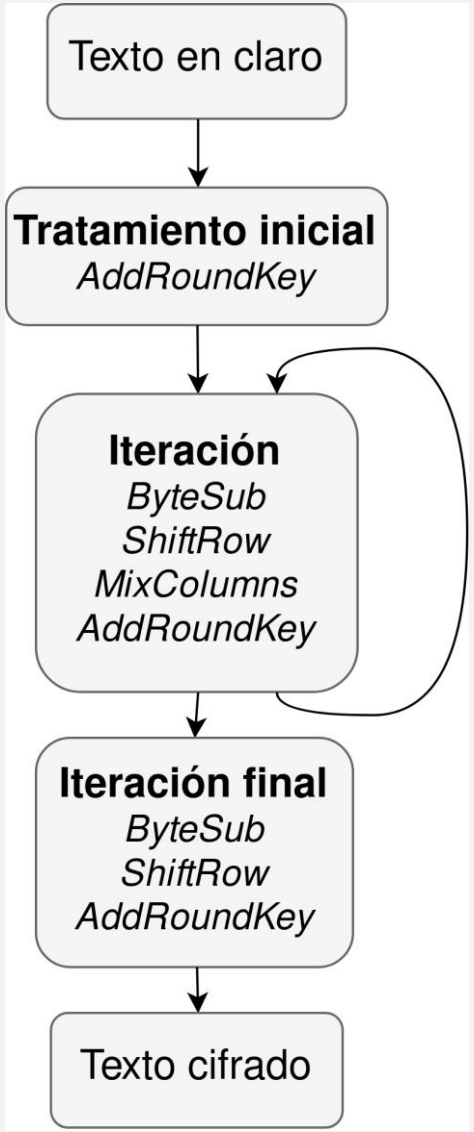
- Cifrado de bloque simétrico.
- En la decada de los 90, tras varios ataques al algortimo de cifrado de bloque DES, el gobierno de EEUU hace un llamamiento para que se presente propuestas para un nuevo estandard. **Rijdael** es el ganador de este concurso y se adapta para pasar a ser el Adavanced Encryption Standard.

AES: REPRESENTACIÓN DE LA INFORMACIÓN

- AES es un criptosistema que cifra bloques de texto en claro de 128 bits con claves de cifrado de 128, 192 o 256 bits de longitud.
- Las cadenas de bits (tanto texto en claro como claves) se representan en matrices de bytes.



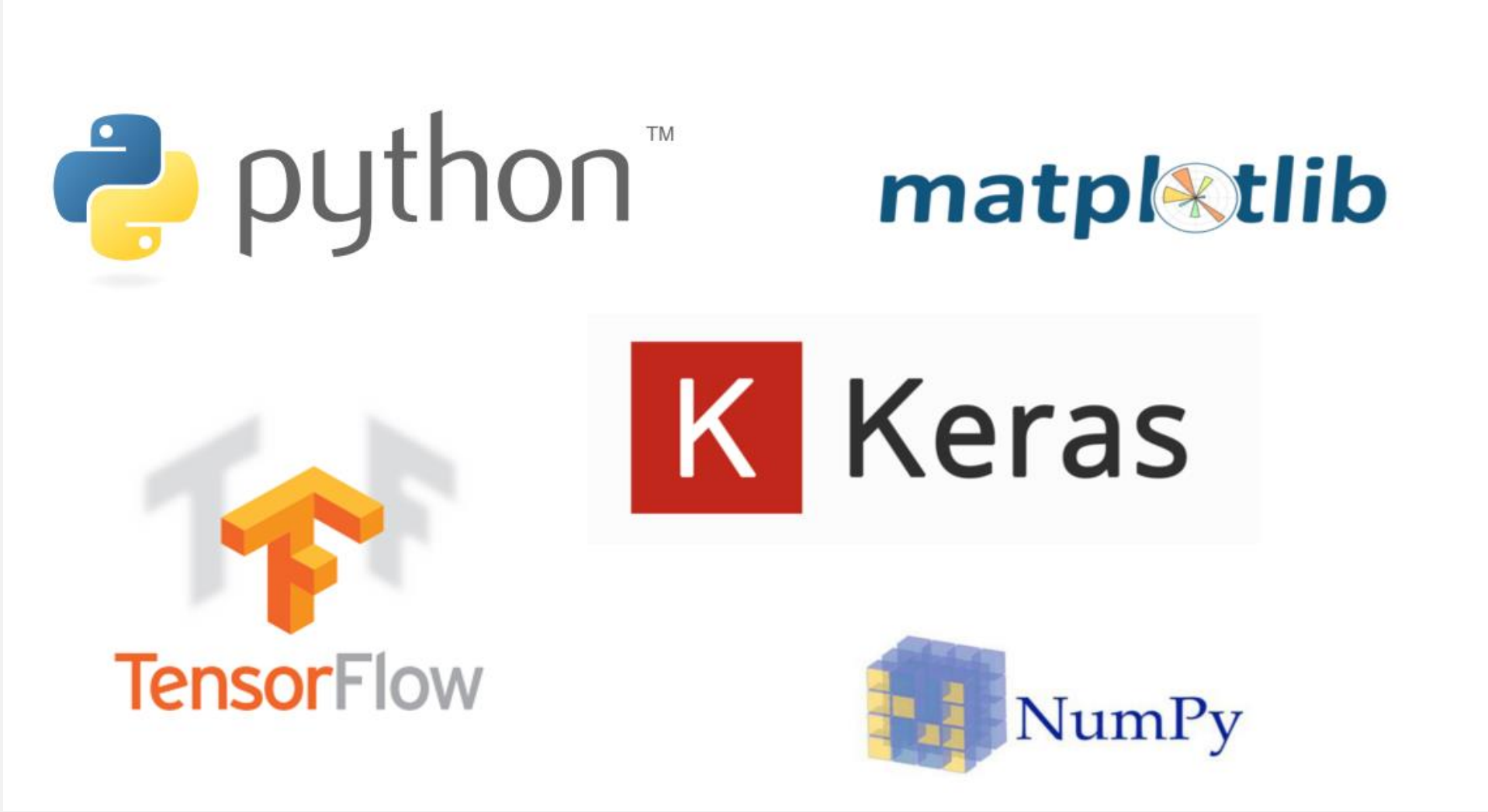
AES: FUNCIONAMIENTO



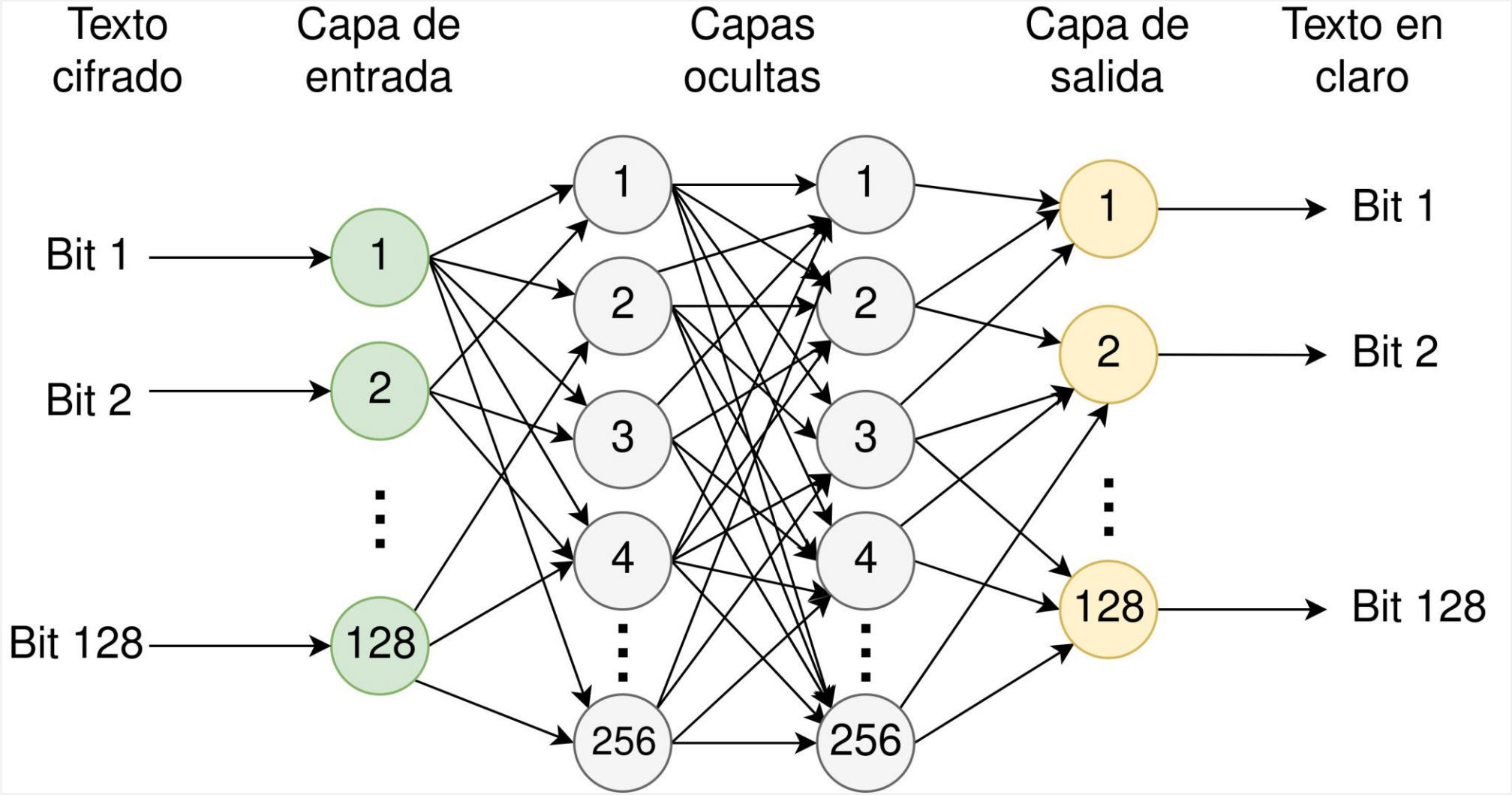
- A la matriz inicial se le aplcia una serie de transormaciones que dan lugar a las matrices estado y por último a la matriz final que se corresponde con el texto cifrado.
- Una parte del proceso es iterativo. El número de iteraciones depende la longitud e la clave. Para la longitud de 128 bits son 10 iteraciones, para longitud 198 son 12 iteraciones y para longitud 256 son 14 iteraciones.
- En este trabajo se estudiaran versiones del algortimo con un número de rondas reducido.
- Todas estas funciones tienen sus funciones inversas correspondientes y aplicandolas en orden inverso se obtiene el texto en claro original.

IMPLEMENTACIÓN

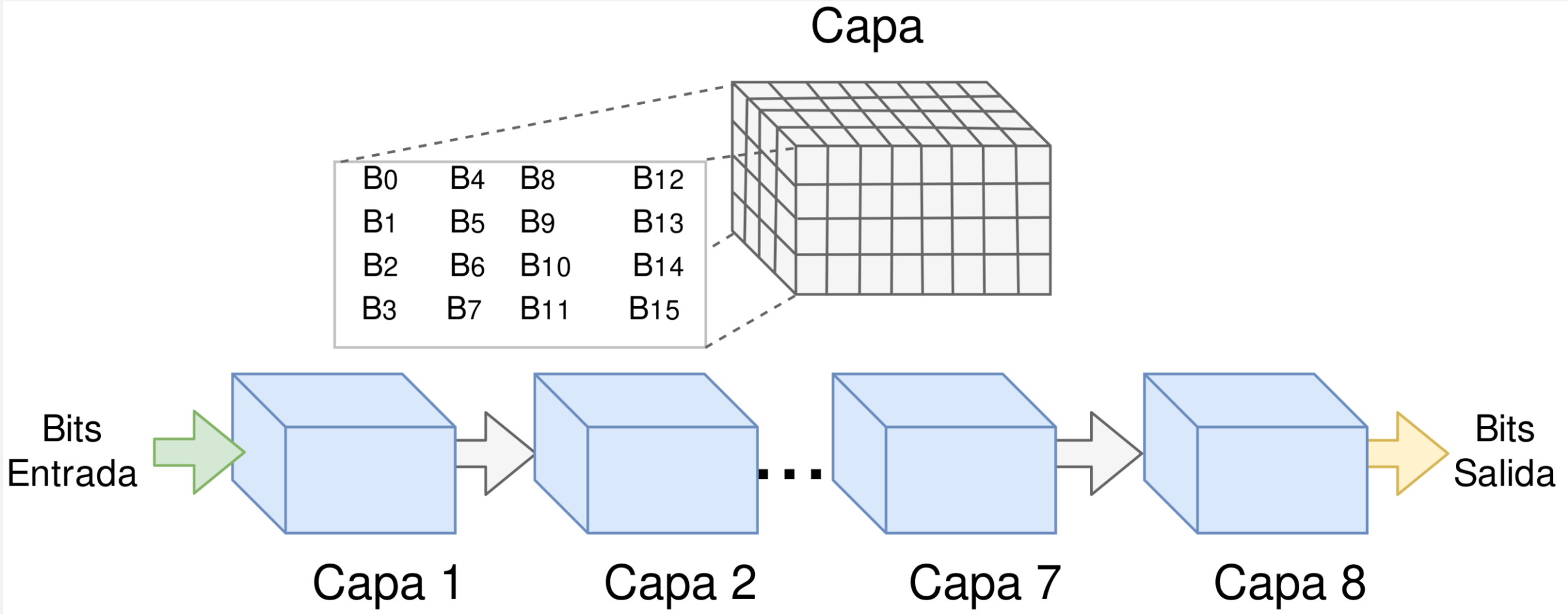
IMPLEMENTACIÓN: TECNOLOGÍAS IMPLICADAS



IMPLEMENTACIÓN: ARQUITECTURA I

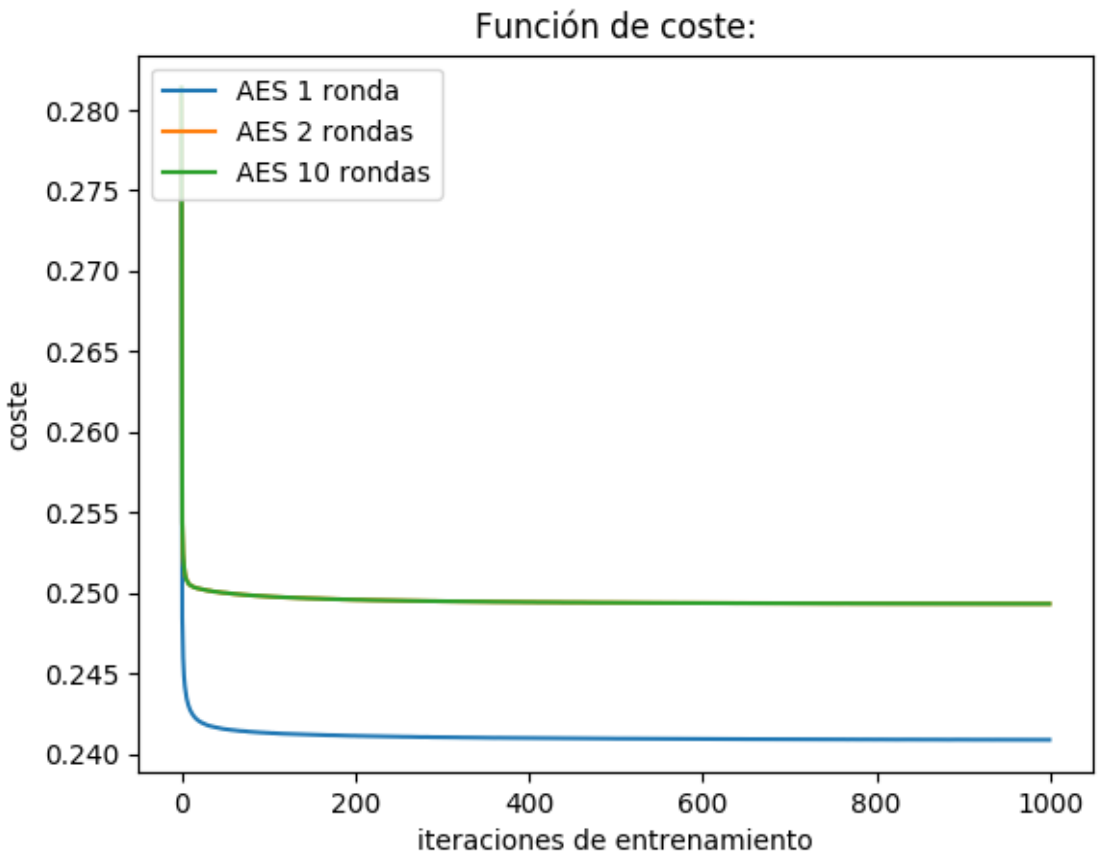


IMPLEMENTACIÓN: ARQUITECTURA II

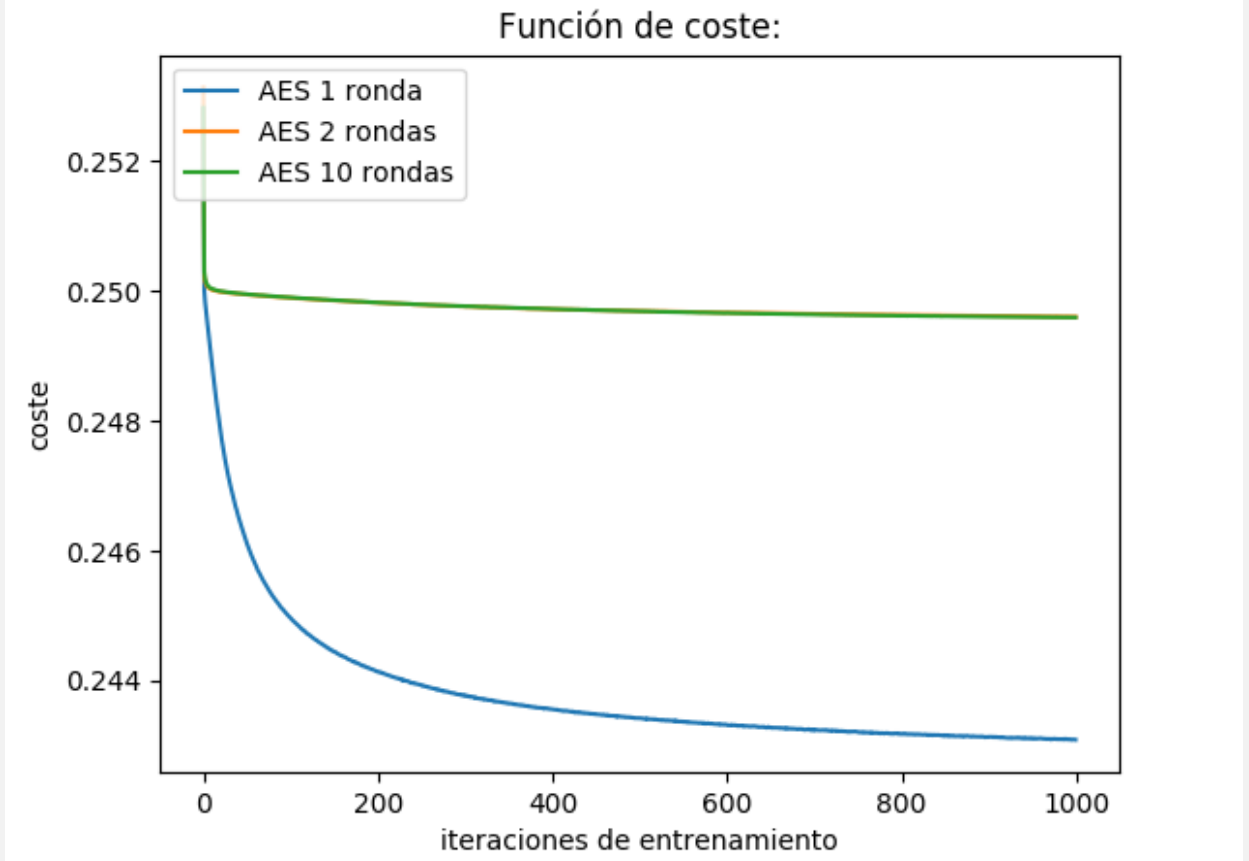


IMPLEMENTACIÓN: ENTRENAMIENTO DE LA RED NEURONAL

Evolución de la función de coste Arquitectura I



Evolución de la función de coste Arquitectura II



IMPLEMENTACIÓN: RESULTADOS

ARQUITECTURA I

	Nº Ejemplos	Nº iteraciones entr.	Tiempo entr. (s)	Precisión
AES 1	2^16	300	1024.45	57.03 %
AES 2	2^16	300	785.40	49.80 %
AES 10	2^16	300	804.24	49.84 %
AES 1 (32% bits) *	2^16	300	1064.12	65.16 %

ARQUITECTURA II

	Nº Ejemplos	Nº iteraciones entr.	Tiempo entr. (s)	Precisión
AES 1	2^16	1000	7705.12	55.66 %
AES 2	2^16	1000	7619.34	49.79 %
AES 10	2^16	1000	7923.27	50.32 %

CONLUSIONES SOBRE EL TRABAJO

- Los mejores resultados obtenidos para la versión reducida de AES 1 ronda oscilan alrededor de un 57% de precisión teniendo en cuenta todos los bits y un 65% teniendo en cuenta los bits sobre los que se espera obtener mejores predicciones.
- En las versiones del algoritmo más de una ronda no se muestra ninguna capacidad de predicción.
- Aunque los resultados del estudio no se pueden considerar un ataque exitoso a AES el proceso ha sido enriquecedor y satisfactorio.

GRACIAS POR SU ATENCIÓN

Pedro Novas Otero

Grado en Ingeniería Informática

Inteligencia Artificial

Consultor:
David Isern Alarcón

Junio de 2018