Sistema de cifrado embebido sobre MSP432

Máster Universitario en Ingeniería Informática

Alumno: Carlos López Benito

Consultor: Jordi Bécares Ferrés

Fecha: 22 de enero de 2018

ÍNDICE DE CONTENIDOS

- INTRODUCCIÓN
- OBJETIVOS
- ESTADO DEL ARTE
- SOFTWARE
- HARDWARE
- DIAGRAMA DEL SISTEMA
- ALGORITMO DES
- ALGORITMO TDES
- ALGORITMO AES
- ALGORITMO RSA
- ESTUDIO COMPARATIVO
- CONCLUSIONES

INTRODUCCIÓN

- Motivación del proyecto
- Sistema de Cifrado
- Limitaciones de los sistemas empotrados
- FreeRTOS
- MSP432

OBJETIVOS

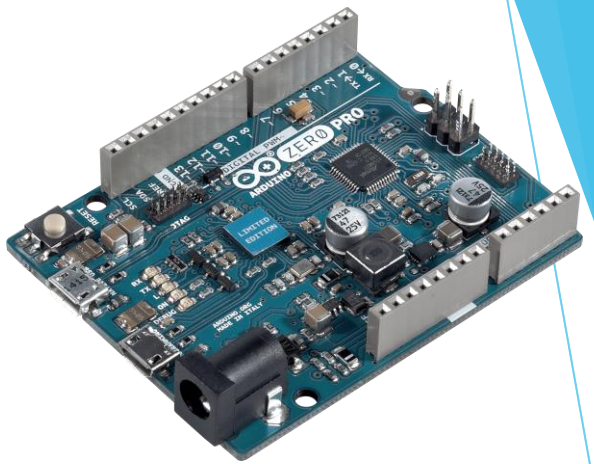
- Algoritmo de cifrado DES.
- Algoritmo de cifrado TDES.
- Algoritmo de cifrado AES (Software y Hardware).
- Algoritmo de cifrado RSA.
- Estudio comparativo.
- Aplicación de Escritorio.
- Sistema de Autentificación.

Estado del Arte

- Algoritmos Actuales.
  - Algoritmos Simétricos: DES, TDES, AES, TWOFISH, RC4, RC5
  - Algoritmos Asimétricos: RSA, DSA, DHKA
- Usos de la Criptología
  - Confidencialidad
  - Autentificación
  - Verificación de la integridad
  - No repudio
- A dónde vamos.
- Puntos débiles.

HARDWARE

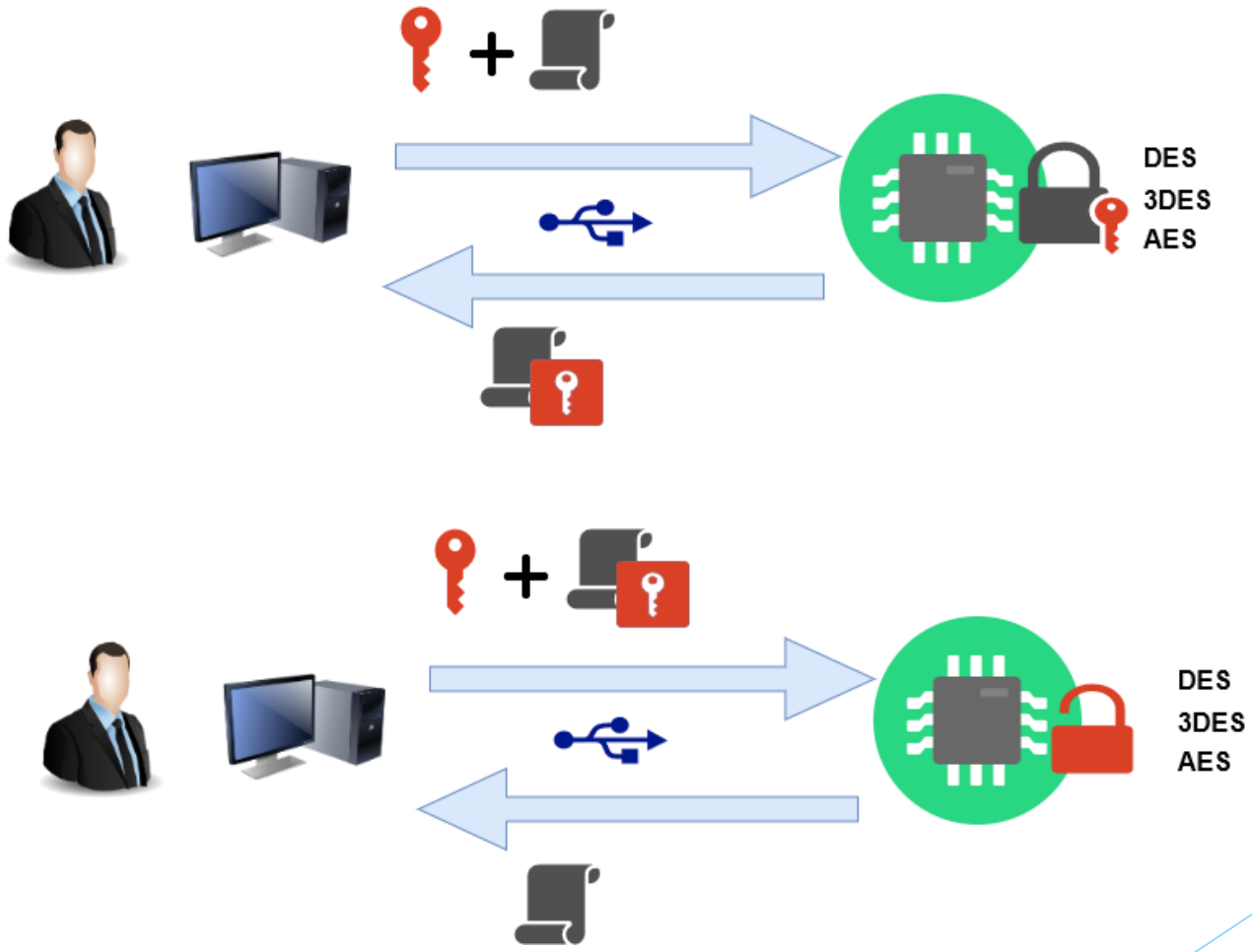
MSP432P401R	
Frecuencia (MHz)	48
Flash (KB)	256
RAM	64
Resolución ADC (Bits)	14
Velocidad muestreo ADC (MSPS)	1
Canales ADC	24
GPIO	48, 64, 84
Serial I/O	8
Seguridad	Aceleración criptográfica Seguridad de depuración Identidad del dispositivo
SPI	8
UART	4
I2C	4
DMA	8
Comparadores (#)	2



Arduino Zero	
Frecuencia (MHz)	48
Flash (KB)	256
RAM	32
Resolución ADC (Bits)	12
Velocidad muestreo ADC (MSPS)	1
Canales ADC	6
GPIO	20
Seguridad	Depurador incrustado Generador de CRC de 32 bits
SPI	SS, MOSI, MISO, SCK
UART	2
I2C	1
DMA	12
Comparadores (#)	2

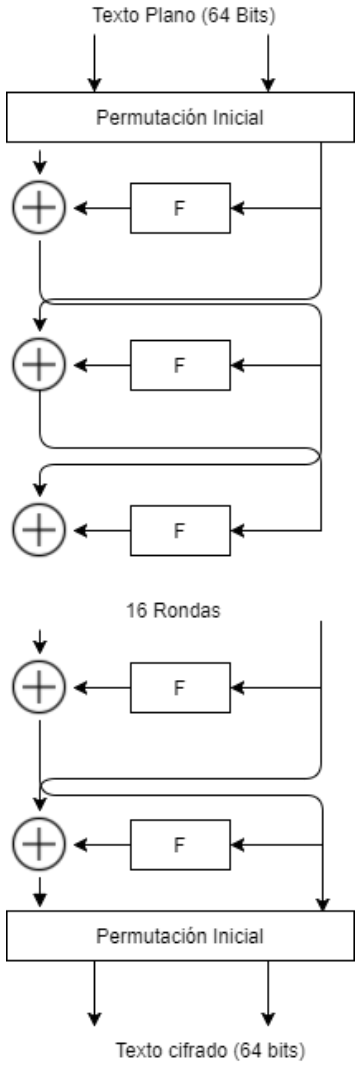
SOFTWARE

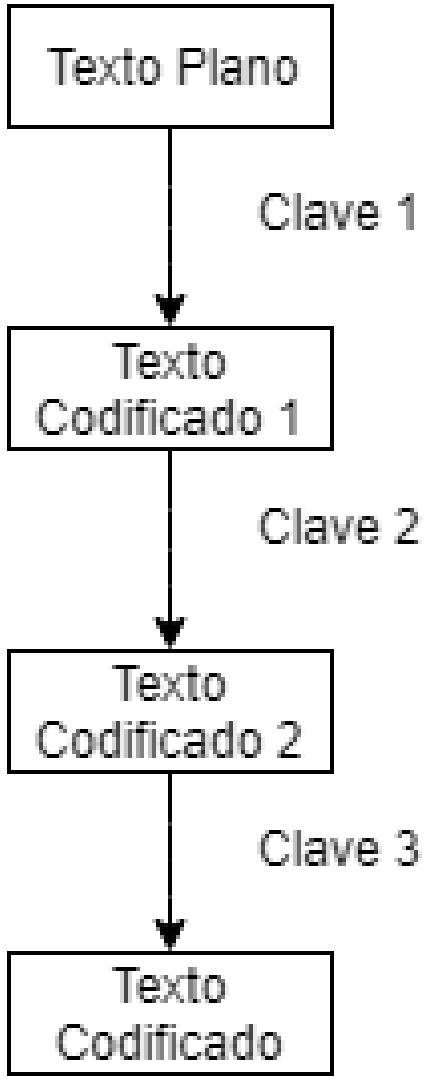
DIAGRAMA DEL SISTEMA



ALGORITMO DES

- Cifrado Simétrico
- Clave 56 bits (64 bits con los bits de paridad)
- Cifrado bloques 64 bits
- Permutación inicial
- Función de Feistel (16 Rondas)
  - Expansión
  - Mezcla
  - Sustitución
  - Permutación
- Permutación Final



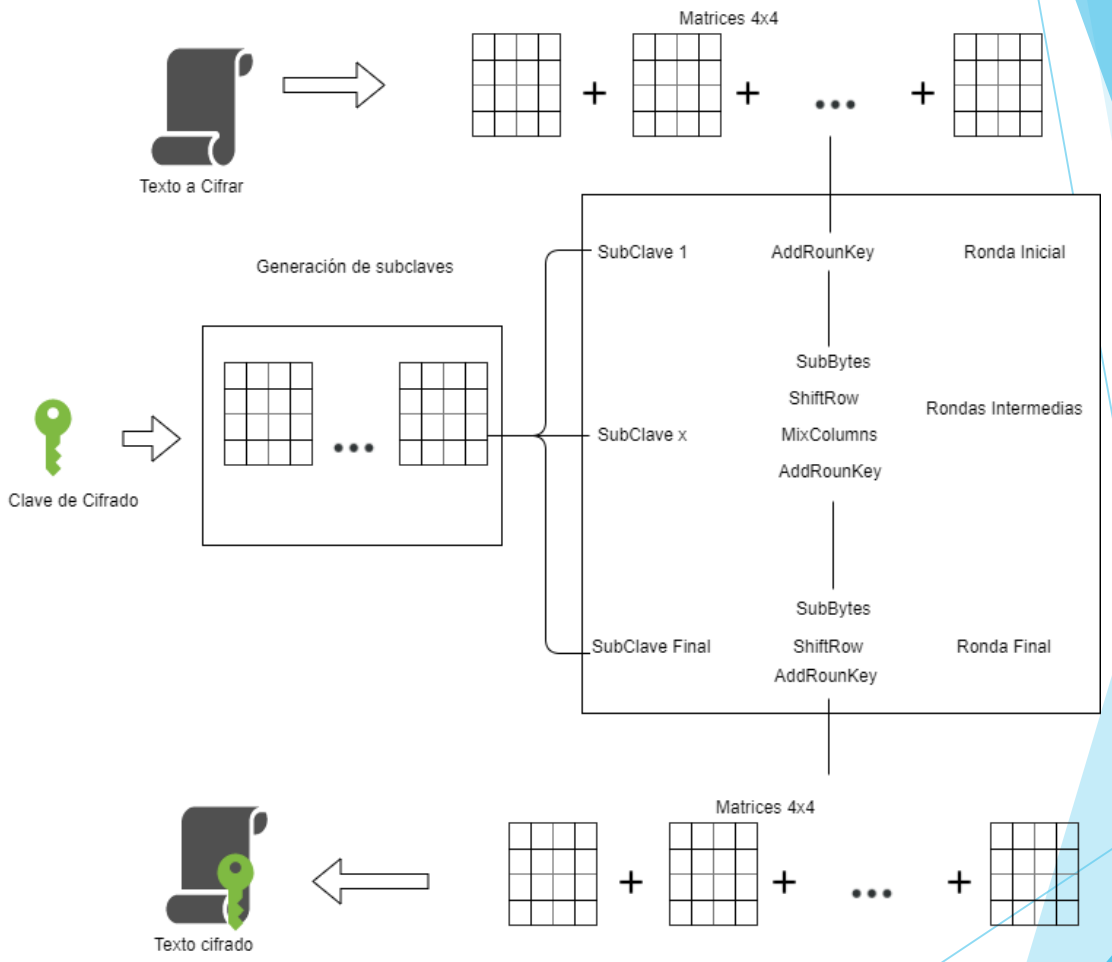


Algoritmo TDES

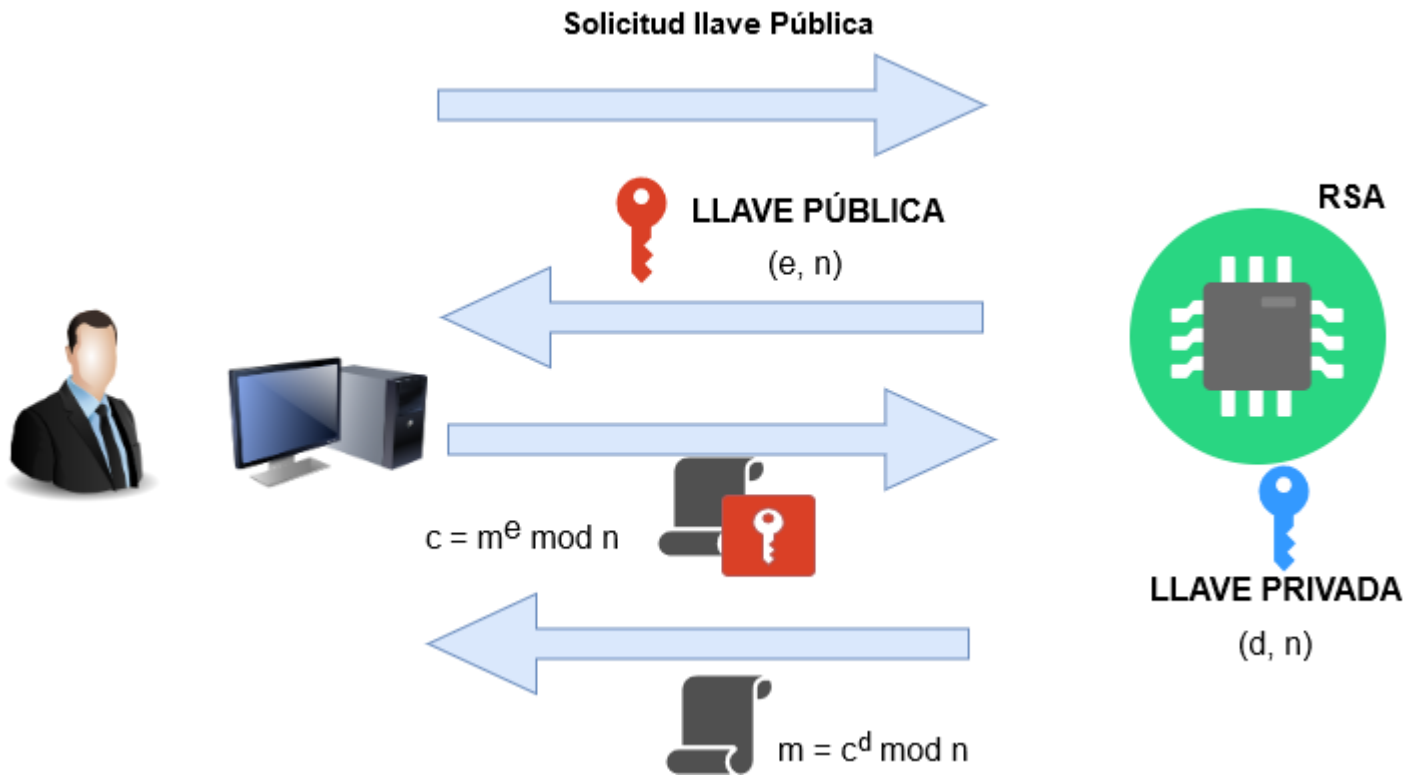
- Aplicación de 3 veces el algoritmo DES
- Cifrado en bloques de 64 bits
- Clave de 168 bits (192 bit con los bits de paridad)
- Tipos: DES-EEE3, DES-EDE3, DES-EEE2 y DES-EDE2

Algoritmo AES

- Cifrado bloques 128 bits.
- Claves de 128, 192 y 256 bits.



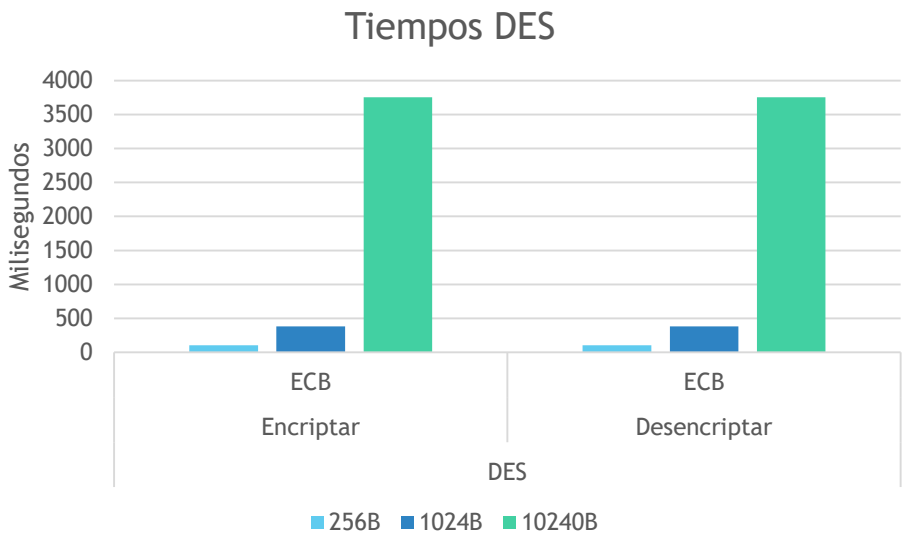
Algoritmo RSA

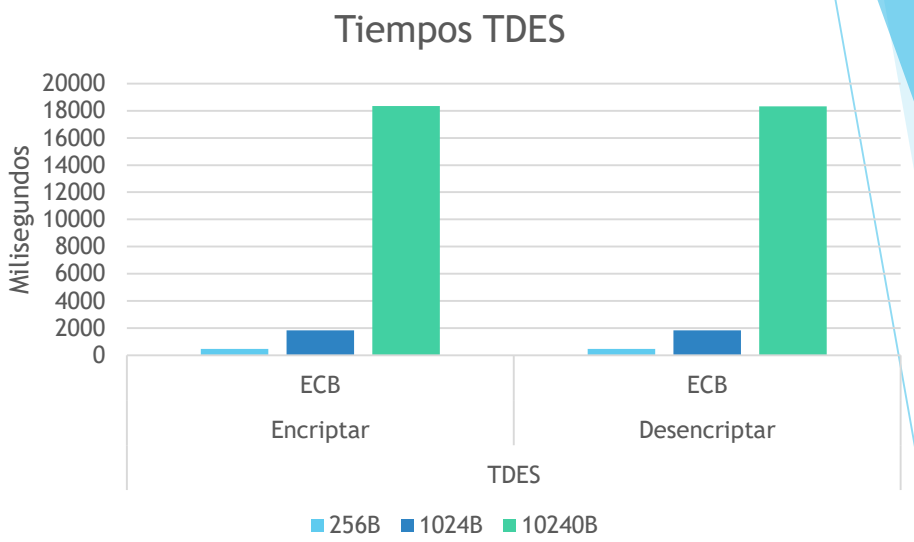


Cómo se ha hecho el estudio

- Tiempos
  - Textos de 256B, 1024B y 10240B
  - En los modos ECB, CBC, CFB, OFB y PCBC
  - Claves de distintos tamaños
- Memoria RAM
  - Calculado para textos de 256B, 1024B y 10240B
  - Claves de 128, 192 y 256 bits en caso de AES
- Memoria Flash

Tiempos DES y TDES

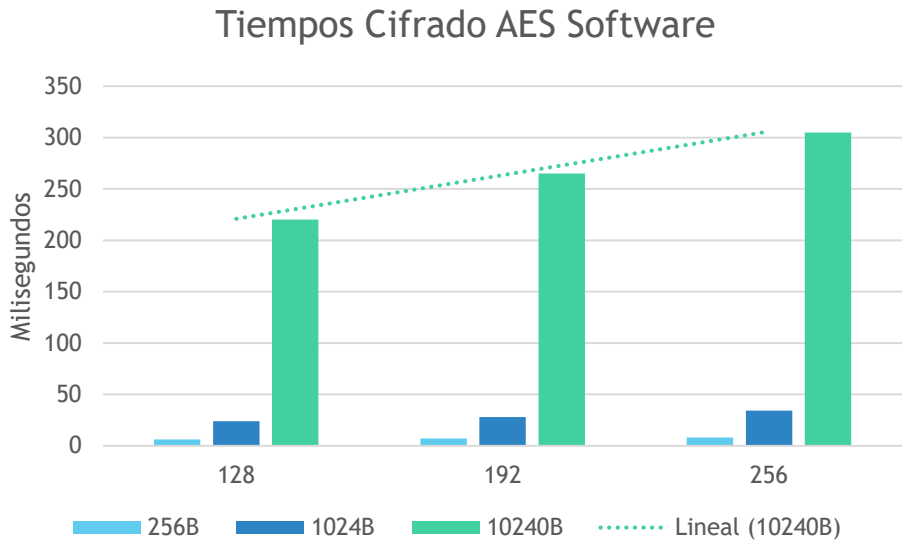


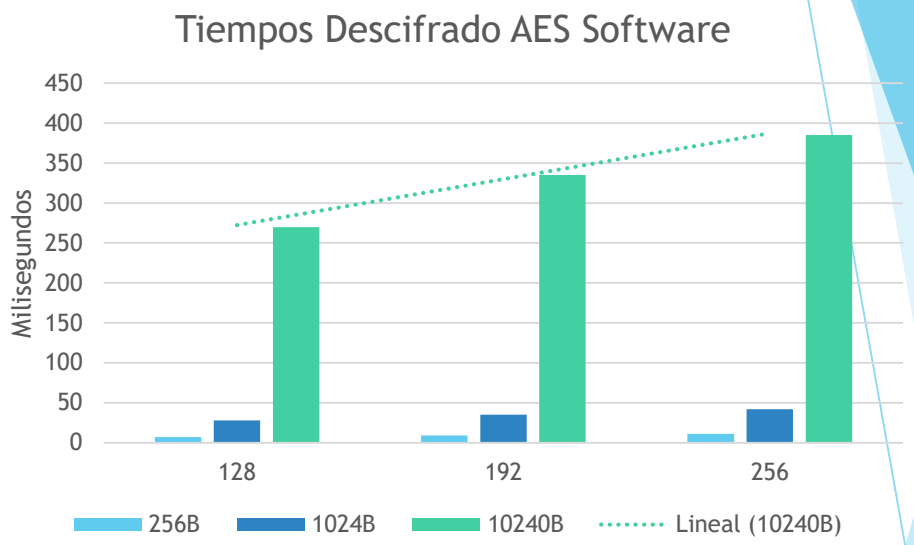


	DES*		TDES*	
	Cifrar	Descifrar	Cifrar	Descifrar
256B	102	102	462	465
1024B	382	383	1840	1836
10240B	3752	3753	18352	18332

* No se representan todos los modos porque sus valores son muy cercanos

Tiempos AES (Software)

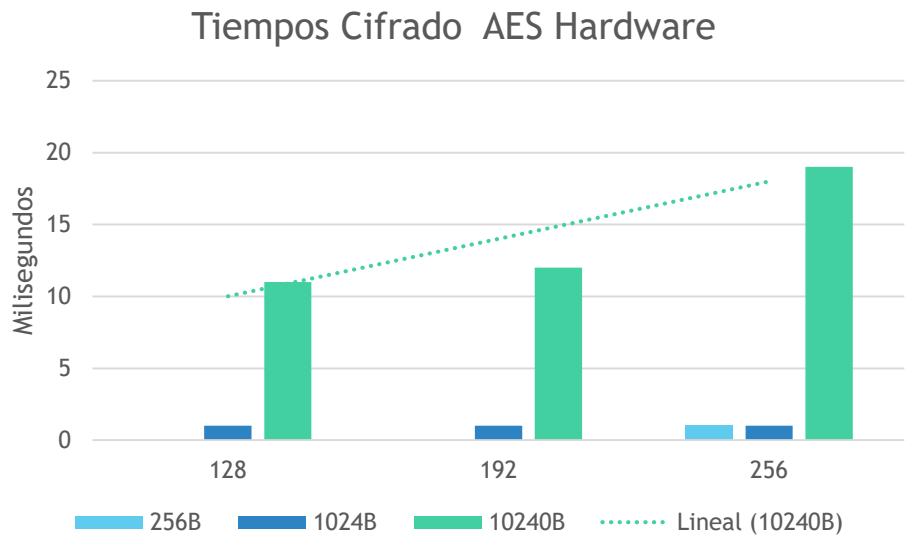


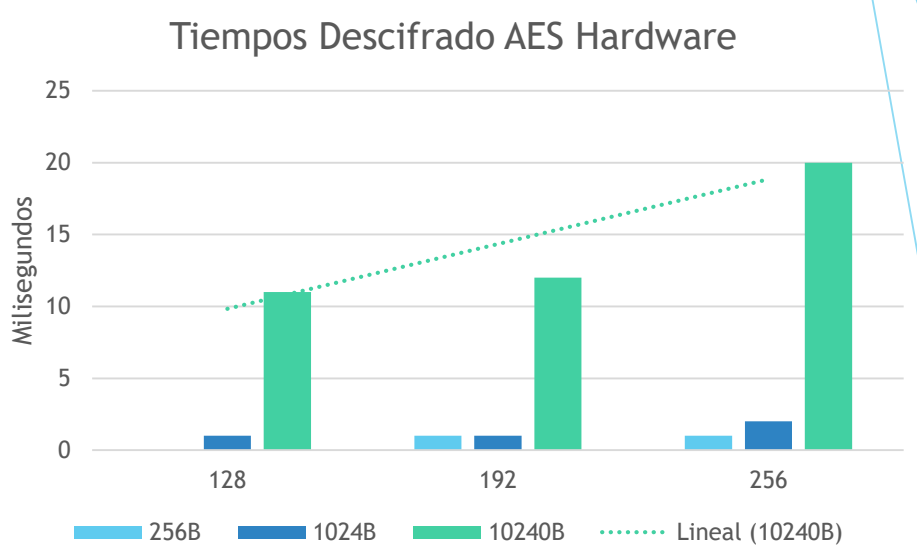


	Cifrar*			Descifrar*		
	128	192	256	128	192	256
256B	6	7	8	7	9	11
1024B	24	28	34	28	35	42
10240B	220	265	305	270	335	385

* No se representan todos los modos porque sus valores son muy cercanos

Tiempos AES (Hardware)

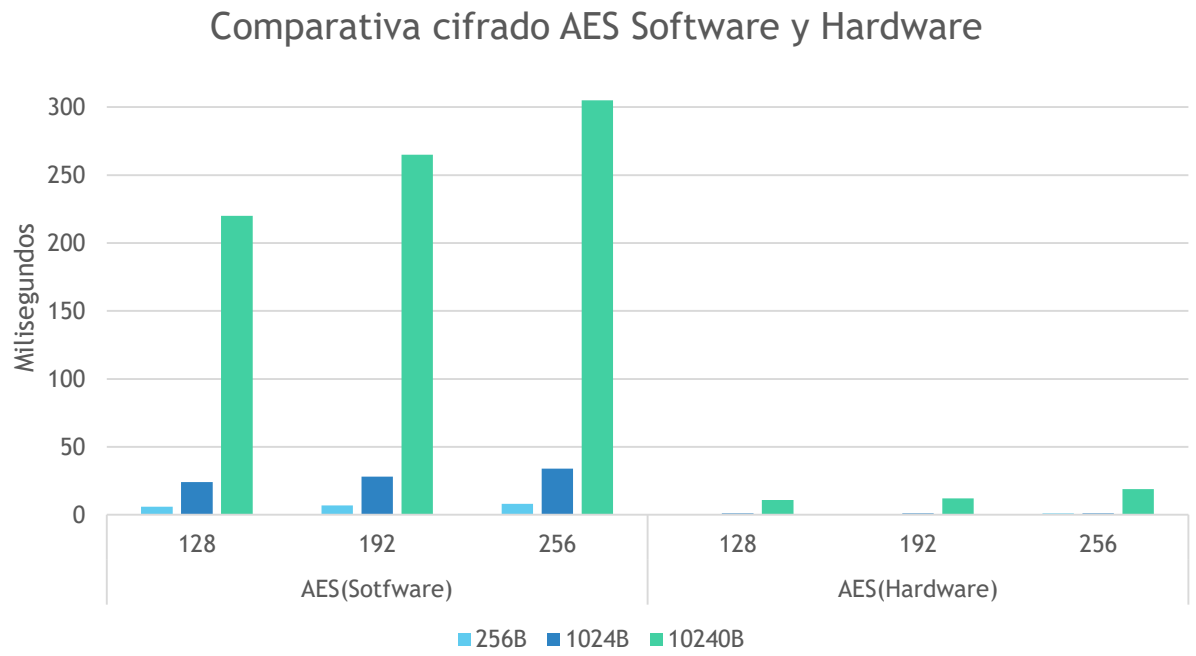




	Cifrado														
	128					192					256				
	ECB	CBC	CFB	OFB	PCBC	ECB	CBC	CFB	OFB	PCBC	ECB	CBC	CFB	OFB	PCBC
256B	0	1	0	0	1	0	1	0	0	1	1	1	1	0	1
1024B	1	2	2	1	2	1	2	2	2	3	1	2	2	2	2
10240B	11	18	17	17	24	12	18	18	18	25	19	21	20	19	26

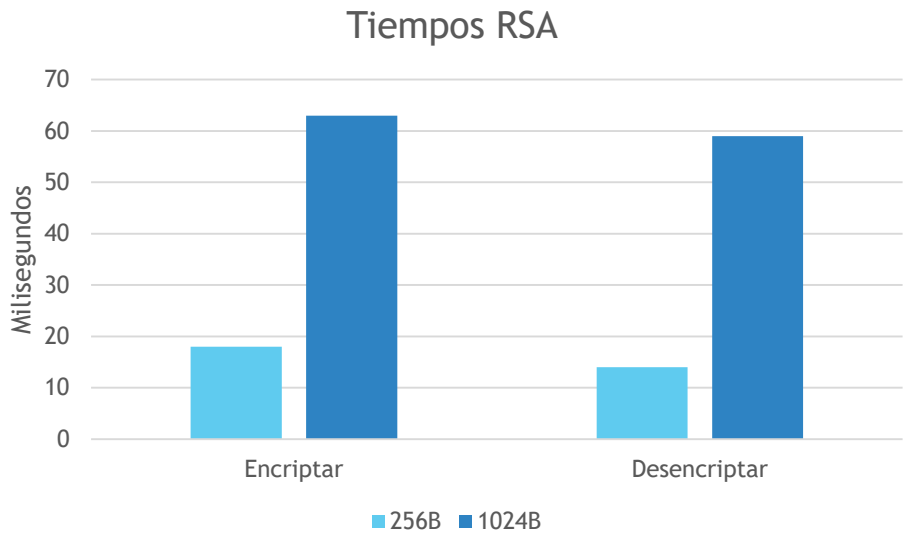
	Descifrado														
	128					192					256				
	ECB	CBC	CFB	OFB	PCBC	ECB	CBC	CFB	OFB	PCBC	ECB	CBC	CFB	OFB	PCBC
256B	0	0	1	0	1	1	0	0	1	1	1	1	1	0	1
1024B	1	2	2	2	3	2	2	2	2	3	1	2	2	2	2
10240B	11	18	18	17	24	12	20	18	19	25	20	20	19	19	26

Comparativa AES Software y Hardware



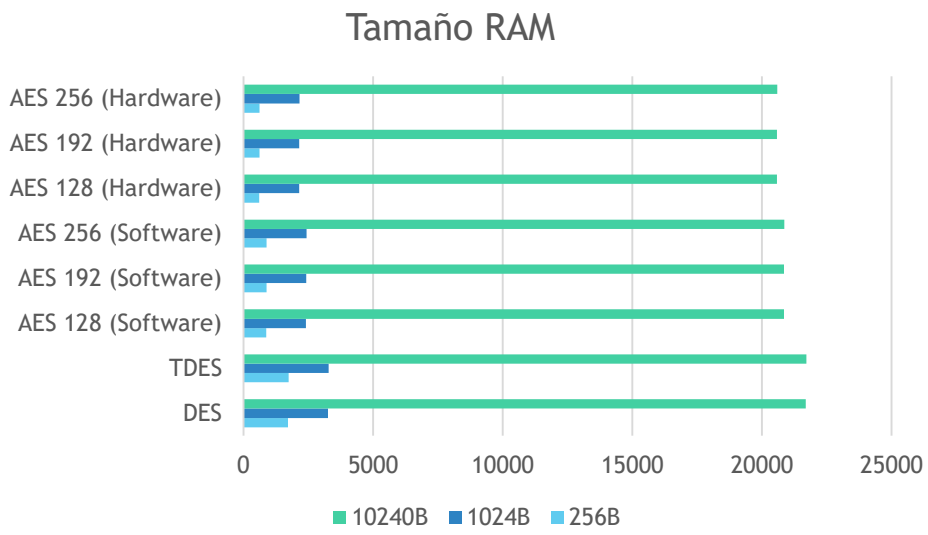
	AES (Software)			AES (Hardware)		
	128	192	256	128	192	256
256B	6	7	8	0	0	1
1024B	24	28	34	1	1	1
10240B	220	265	305	11	12	19

Tiempos RSA



	RSA	
	Encriptar	Desencriptar
256B	18	14
1024B	63	59
10240B	-	-

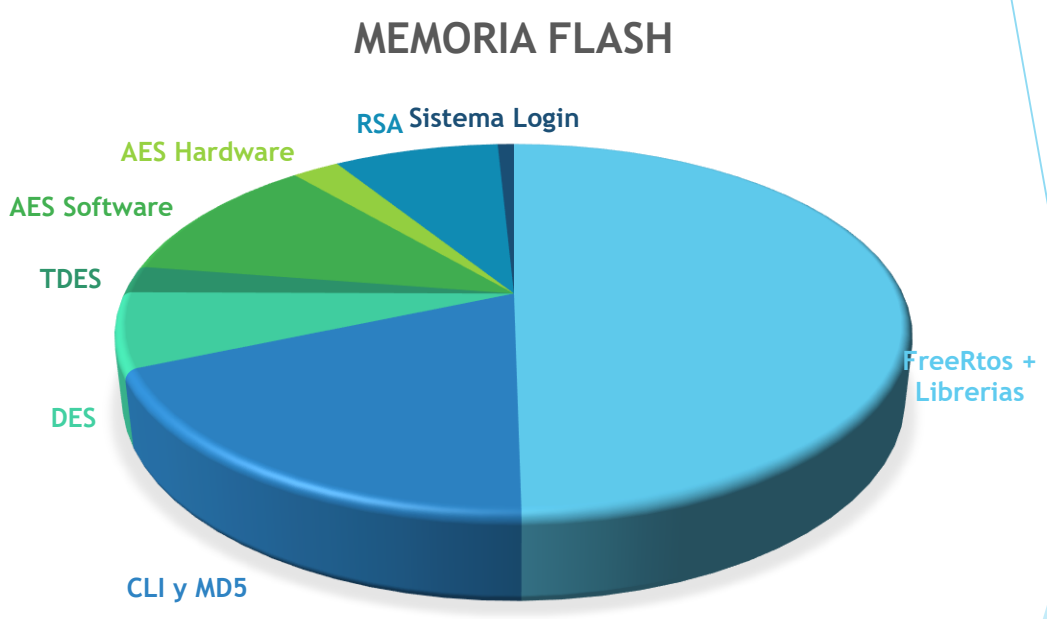
Memoria RAM



	256B	1024B	10240B
DES	1720	3256	21688
TDES	1745	3281	21713
AES 128 (Software)	876	2412	20844
AES 192 (Software)	884	2420	20852
AES 256 (Software)	892	2428	20860
AES 128 (Hardware)	605	2141	20573
AES 192 (Hardware)	613	2149	20581
AES 256 (Hardware)	621	2157	20589
RSA Encriptar	2354	9266	92210
RSA Desencriptar	1576	6184	61480

Memoria Flash

Módulos	Tamaño
FreeRtos + Librerías	35.066
CLI y MD5	13.220
DES	4.664
3DES	1.660
AES Software	7.992
AES Hardware	1.628
RSA	5.696
Sistema Login	560
Tamaño Total	70.486



Conclusiones

- Mejor rendimiento AES Hardware
- Algoritmos Software: Mejor AES, Peor TDES
- Incremento de tiempo proporcional al tamaño del mensaje
- En AES, aumenta el tiempo de cifrado respecto al tamaño de la clave
- Mejor modo: ECB
- Peor modo: PCBC
- A mayor tamaño del mensaje, es necesaria más RAM

Cumplimiento de los Objetivos

- Aplicación de Escritorio. ✓
- Algoritmo de cifrado DES. ✓
- Algoritmo de cifrado TDES. ✓
- Algoritmo de cifrado AES (Software y Hardware). ✓
- Estudio comparativo. ✓
- Algoritmo de cifrado RSA. ✗

¡GRACIAS!