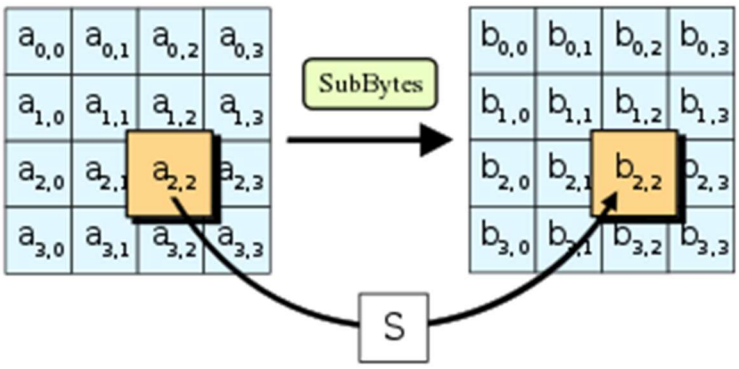
UNIVERSIDAD
DE BURGOS

AES: Formulación matemática y Aplicaciones de sus componentes



Eduardo Mora González

Contenido

1. INTRODUCCIÓN

Según [R1], la criptología (del griego *krypto*: "oculto" y *logos*: "discurso") es la disciplina que se dedica al estudio de los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer para entidades no autorizadas. Esta ciencia está dividida en cuatro ramas:

- **Criptografía:** Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información.
- **Criptoanálisis:** Se ocupa de descifrar sin autorización la información contenida en criptogramas.
- **Esteganografía:** Se ocupa de ocultar información por un canal inseguro, de manera que no sea siquiera percibida.
- **Estegoanálisis:** Se ocupa de detectar información oculta mediante la esteganografía.

Como se puede observar la criptografía y la esteganografía son las ramas que aplican la idea en la que se basa la criptología mientras que las otras dos se encargan de descifrar la información.

Centrándonos un poco más en el concepto de Criptografía (que procede del griego *krypto*: "oculto" y *graphos*: "escribir"), se puede decir que la Criptografía se encarga de ocultar lo escrito. El funcionamiento básico de la criptografía es como se muestra en la siguiente imagen [R2]:

Como vemos, se trata de cifrar un texto mediante técnicas de cifrado (como el AES) con ello, obtenemos un texto cifrado, ininteligible, que el emisor envía al receptor.

Una vez recibido, el receptor, conocedor de la clave, aplica un algoritmo de descifrado (inversa del algoritmo de cifrado), de manera que es capaz de leer el texto plano.

2. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard, también conocido como *Rijndael*, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

El cifrado fue desarrollado por dos criptólogos belgas, *Joan Daemen* y *Vincent Rijmen*, y fue enviado al proceso de selección AES bajo el nombre "Rijndael", como parte de un concurso.

El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

Por lo tanto, el AES es un cifrador en bloque de criptografía simétrica (trabaja cifrando y descifrando bloque a bloque usando la misma clave), la clave generada al menos tiene 128 bits, pero permite aumentar la longitud de clave según necesidades y puede ser implementado tanto en hardware como en software.

2.1. ALGORITMO DE ENCRIPTADO

Según [R3], en el estándar, el algoritmo Rijndael divide los datos de entrada en bloques de 4 palabras de 32 bits, es decir, $4 \times 32 = 128$ bits. Es necesario decir que el algoritmo Rijndael puede trabajar también con bloques mayores de 192 y 256 bits, pero no vienen contemplados en el estándar.

El funcionamiento de AES tiene 4 funciones principales que repite para cifrar los datos. Se necesita un bloque (como se ha mencionado antes de 128 bits) y una contraseña de termino simple; teniendo las dos cosas se proporciona como salida un texto cifrado.

Las funciones que usa son las siguientes:

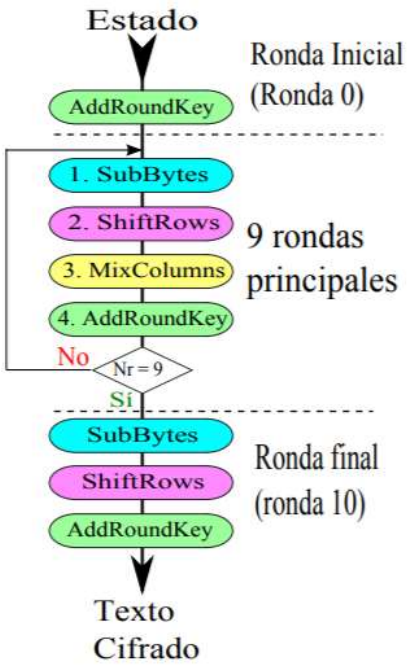
- SubBytes.
- ShiftRows.
- MixColumns.
- AddRoundKey.

El numero de veces que se repite las funciones del algoritmo depende estrictamente del tamaño de la clave. En la siguiente tabla se muestra distintos ejemplos de dependiendo de las longitudes de clave:

TAMAÑO CLAVE	Nº DE REPETICIONES
128 bits	10
192 bits	12
256 bits	14

Cuando mayor sea el número de clave, más seguro serán los datos, pero el tiempo que tardará el algoritmo en cifrar se vera aumentado significativamente en cada ronda.

El proceso de cifrado es el siguiente para una clave de 128 bits:



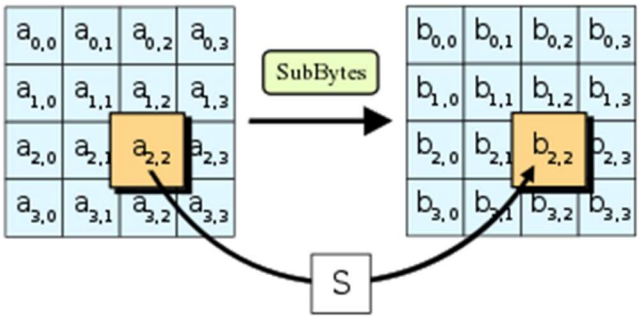
Como vemos, en primer lugar, se realiza una ronda inicial en la que únicamente se aplica una operación AddRoundKey.

Posteriormente, se realizan las nueve rondas principales, en las que se aplican las cuatro operaciones del cifrado en este orden: SubBytes, ShitfRows, MixColumns y AddRoundKey.

Por último, se realiza la ronda final, en la que se aplican las operaciones SubBytes, ShiftRows y AddRoundKey, obteniendo así nuestro texto cifrado.

2.1.1. SUBBYTES

La función *SubBytes* consiste en una sustitución no lineal de cada elemento de la matriz por otro elemento. En la siguiente imagen se muestra el funcionamiento [R4]:



Para calcular el nuevo elemento se utiliza la siguiente formula:

$$S'_{i,j} = M \cdot S_{i,j}^{-1} + C$$

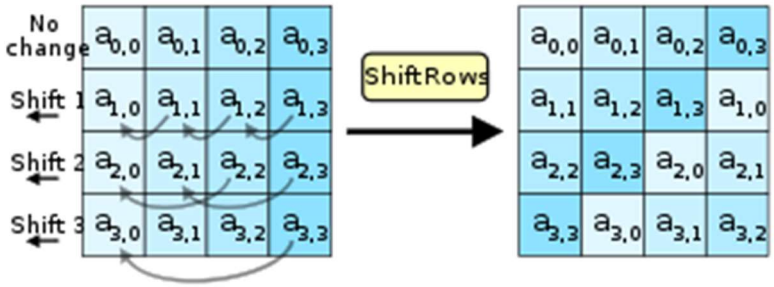
$$\text{Donde } M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Existe una tabla denominada *S-BOX* que aplica la formula anterior para todos los números y permite ver todas las combinaciones posibles, la tabla es la siguiente [R5]:

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

2.1.2. SHIFTROWS

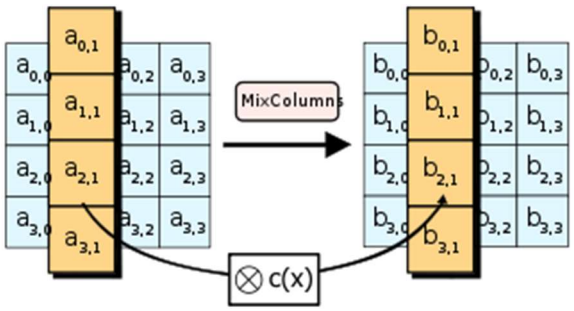
La función ShiftRows consiste en desplazar de manera cíclica las filas de la matriz hacia la izquierda, como se muestra en la siguiente imagen [R6]:



Se puede observar que la primera fila (fila 0) no cambia, la primera fila (fila 2) cambia 1º posición, la 2º (fila 3) dos posiciones y así depende del numero de fila cambian N posiciones (N-1 si no se considera la primera fila como fila 0).

2.1.3. MIXCOLUMNS

La función MixColumns, los cuatro bytes de cada columna de la notación matricial del estado se combinan utilizando una transformación lineal invertible como se muestra en la imagen [R7]:



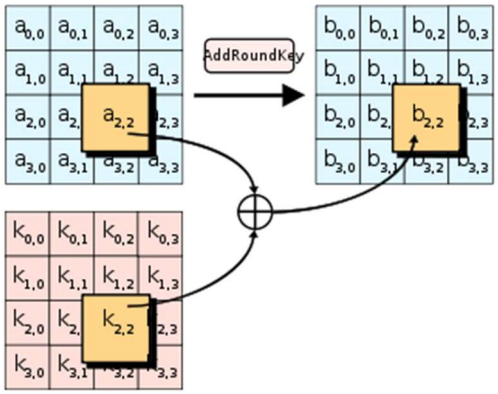
Cada columna se trata como un polinomio y luego se multiplica el módulo $x^4 + 1$ con un polinomio fijo $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$

Visto de una forma matricial, la operación es la siguiente:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_{15} & B_{11} & B_7 & B_3 \\ B_{14} & B_{10} & B_6 & B_2 \\ B_{13} & B_9 & B_5 & B_1 \\ B_{12} & B_8 & B_4 & B_0 \end{pmatrix}$$

2.1.4. ADDROUNDKEY

La función AddRoundKey consiste en la combinación de la subclave de ronda correspondiente con el Estado. Esta combinación se realiza a través de la operación XOR, como se puede observar en la siguiente imagen [R8]:



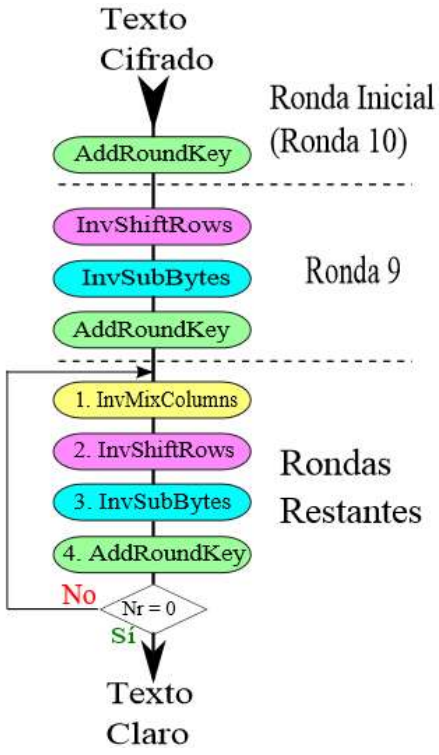
2.2. ALGORITMO DESENCRIPTADOR

En el punto anterior se muestra el proceso que sigue AES para encriptar y las funciones que usa. Para desencriptar se debe hacer el proceso contrario con el mismo número de rondas, pero con funciones inversas.

Las funciones que usa son las siguientes:

- InvSubBytes.
- InvShiftRows.
- InvMixColumns.
- AddRoundKey

La operación AddRoundKey es la misma que en el proceso de encriptación.



2.2.1. INVSUBBYTES

La función InvSubBytes es, al igual que la operación SubBytes, una sustitución no lineal de bytes. Dicha sustitución se realiza aplicando la fórmula:

$$S'_{i,j} = (M^{-1} \cdot (S_{i,j} + C))^{-1}$$

De nuevo, existe una tabla de sustitución fija a la que hemos denominado InvS-box [R9], la cual permite realizar la operación InvSubBytes de manera análoga a la operación SubBytes.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	83	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	a	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	b	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	c	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	d	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	e	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	f	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

2.2.2. INVSHIFTROWS

La función InvShiftRows consiste, en una rotación cíclica hacia la derecha de las filas de la notación matricial del estado, de manera que la primera fila permanece igual, la segunda fila se rota hacia la derecha una posición, la tercera fila se rota hacia la derecha dos posiciones y, por último, la cuarta fila se rota hacia la derecha tres posiciones.

2.2.3. INVMIXCOLUMNS

Es la operación inversa a MixColumns. En ella, cada columna se trata como un polinomio y luego se multiplica el módulo $x^4 + 1$ con un polinomio fijo $a^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$.

Visto de forma matricial la operación es la siguiente:

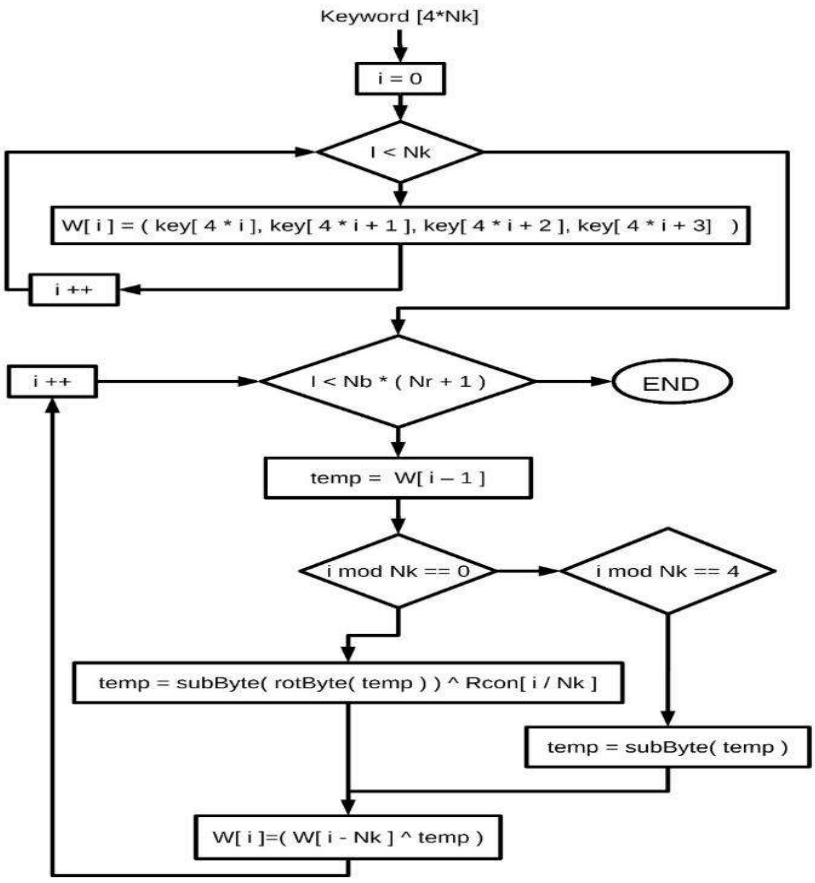
$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \cdot \begin{pmatrix} B_{15} & B_{11} & B_7 & B_3 \\ B_{14} & B_{10} & B_6 & B_2 \\ B_{13} & B_9 & B_5 & B_1 \\ B_{12} & B_8 & B_4 & B_0 \end{pmatrix}$$

2.3. EXPANSIÓN DE CLAVE

En el AES, concretamente en la operación AddRoundKey, se utilizan diferentes subclaves, todas derivadas de la clave original.

La clave expandida es una sucesión de todas las subclaves, puede verse como una matriz de 4 filas por [4 × (Nr + 1)] columnas. Es decir, que la longitud de la clave expandida varía dependiendo de Nr, que a su vez varía dependiendo de la longitud de clave.

El algoritmo usado para la expansión de claves es el siguiente [R10]:



3. APLICACIONES DEL AES

Este método de encriptado se sigue considerando de los más seguros y eficientes y sirve para cifrar los datos de todo tipo y por eso, se suele usar en varios protocolos y técnicas de transmisión.

La protección WPA2 de las redes WiFi utiliza el Advanced Encryption Standard para el estándar SSH o IPsec.

Frecuentemente se usan los métodos AES también en la telefonía a través del internet (Voice over IP, VoIP) con el fin de asegurar los datos de señalización o también los datos útiles.

También se han implementado muchas aplicaciones de encriptado que usan AES, por ejemplo, "*AES Crypt"* [R11] es una aplicación gratuita y de código abierto creada para permitirnos cifrar fácilmente los archivos, esta aplicación aplica un cifrado de 256-bit.

4. CONCLUSIÓN

Realizar este trabajo me ha ayudado a conocer el funcionamiento de esta técnica de encriptado y ampliar mis conocimientos sobre seguridad.

Esta técnica me ha parecido muy interesante y posiblemente intente implementarla para poder comprenderla de una mejor manera.

REFERENCIAS

R1: Manuel José Lucena López. Criptografía y Seguridad en Computadores. Tercera Edición, pages 29–34, 2002.

R2: https://seguridad.cenditel.gob.ve/rootve/wiki/conceptos_basicos_certificacion_electronica

R3: NIST. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, pages 7–24, 2001.

R4: https://commons.wikimedia.org/wiki/File:AES-SubBytes.svg

R5: https://www.redalyc.org/jatsRepo/5122/512253718012/512253718012_gf3.jpg

R6: https://commons.wikimedia.org/wiki/File:AES-ShiftRows.svg

R7: https://commons.wikimedia.org/wiki/File:AES-MixColumns.svg

R8: https://commons.wikimedia.org/wiki/File:AES-AddRoundKey.svg

R9: https://www.redalyc.org/jatsRepo/5122/512253718012/512253718012_gf4.jpg

R10: https://www.redalyc.org/jatsRepo/5122/512253718012/512253718012_gf5.jpg

R11: https://www.aescrypt.com/

BIBLIOGRAFIA Y WEBGRAFIA

- Daemen J. y Rijmen V. (2002) El diseño de Rijndael: AES - el Estándar de cifrado avanzado. Springer-Verlag.
- sinopsis (2003) HSPICE Simulation and Analysis User Guide.
- https://www.slideshare.net/atheistprince/aesadvanced-encryption-standard
- https://www.redalyc.org/jatsRepo/5122/512253718012/html/index.html
- https://www.nfon.com/es/servicio/base-de-conocimiento/base-de-conocimiento-destacar/aes
- https://www.aescrypt.com/