

Criptografía Simétrica

Algoritmo AES

(Estándar de cifrado avanzado).

Lic.Tte. Daymé Almeida Echevarria
Dirección de Criptografía



Junio del 2018

Contenido de la Clase

1 Criptografía Simétrica

- Fundamentos y principios de la criptografía simétrica.
- Algoritmo DES y AES.

2 Algoritmo AES.

- Bases y funcionamiento del mismo.
- Descripción del AES
- Propiedades del AES

3 Ejercicios prácticos sobre el funcionamiento del Algoritmo de cifrado en bloque AES.



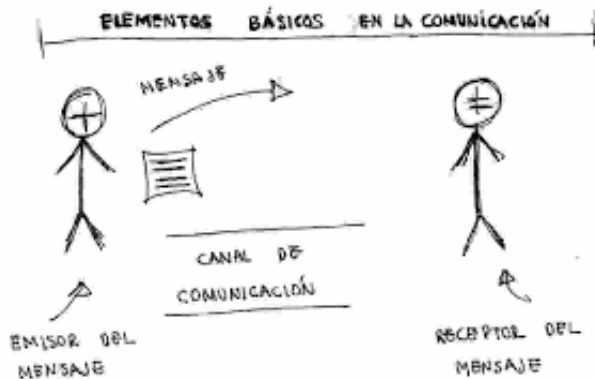
J. Daemen y V. Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, 2002.



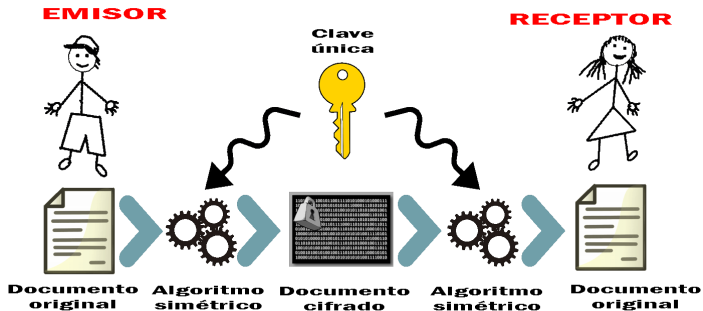
B. Schneier. Applied Cryptography. Segunda Edición. 1996.



A. J. Menezes et al. Handbook of Applied Cryptography. 1997.



Los algoritmos de cifrado simétricos, en particular los cifrados en bloques realizan repetidamente algunas transformaciones de base en los bloques del texto claro que deberán satisfacer toda una serie de exigencias, en primer lugar, deberán ser **simplemente realizables** y en segundo lugar, con una pequeña cantidad de iteraciones **deberán manifestarse como transformaciones analíticamente complejas**.



Usualmente se emplean transformaciones de base de dos tipos, la primera de estas transformaciones fue denominada como **confusión**, y la segunda **difusión**.

Confusión

Transformación sobre el texto claro con el objetivo de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre la llave y el texto cifrado. Para lograrlo se usa la técnica de sustitución donde los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en el cifrado. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.

Difusión

Transformación sobre el texto claro con el objetivo de dispersar las propiedades estadísticas del lenguaje sobre todo el texto cifrado. Para lograrlo se usan técnicas de transposición o permutación donde los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

Usualmente se emplean transformaciones de base de dos tipos, la primera de estas transformaciones fue denominada como **confusión**, y la segunda **difusión**.

Confusión

Transformación sobre el texto claro con el objetivo de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre la llave y el texto cifrado. Para lograrlo se usa la técnica de sustitución donde los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en el cifrado. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.

Difusión

Transformación sobre el texto claro con el objetivo de dispersar las propiedades estadísticas del lenguaje sobre todo el texto cifrado. Para lograrlo se usan técnicas de transposición o permutación donde los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

Usualmente se emplean transformaciones de base de dos tipos, la primera de estas transformaciones fue denominada como **confusión**, y la segunda **difusión**.

Confusión

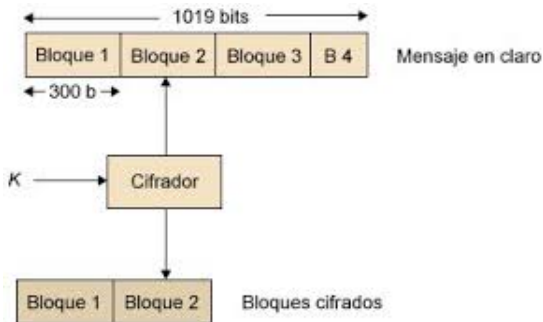
Transformación sobre el texto claro con el objetivo de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre la llave y el texto cifrado. Para lograrlo se usa la técnica de sustitución donde los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en el cifrado. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.

Difusión

Transformación sobre el texto claro con el objetivo de dispersar las propiedades estadísticas del lenguaje sobre todo el texto cifrado. Para lograrlo se usan técnicas de transposición o permutación donde los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

Siendo así que una gran parte de los algoritmos de cifrado simétrico en bloque operen dividiendo el mensaje que se pretende codificar en bloques de tamaño fijo, y apliquen sobre cada uno de ellos una combinación más o menos compleja de operaciones de confusión (sustituciones) y difusión (permutaciones).

Como regla general el alfabeto sobre el cual actúa un cifrado en bloque es el conjunto de bloques de vectores binarios del texto claro de igual longitud (64, 128, etc) esto se debe a que realizar una transformación en un alfabeto más grande es una tarea muy compleja.



Sean que X, K, Y los conjuntos finitos de los posibles textos claros, llaves y textos cifrados, respectivamente, se define $E_k : X \rightarrow Y$ como la regla de cifrado con la llave $k \in K$. El conjunto $\{E_k : k \in K\}$ se puede representar como E , y el conjunto $\{E_k(x) : x \in X\}$ por medio de $E_k(x)$. Sea $D_k : E_k(X) \rightarrow X$ la regla de descifrado con la llave $k \in K$, y que D representa el conjunto $\{D_k : k \in K\}$, entonces podemos definir formalmente un esquema de cifrado de la siguiente manera:

Definición (Modelo algebraico del cifrado)

Llamaremos esquema de cifrado al conjunto

$$\Sigma_A = (X, K, Y, E, D)$$

de los 5 conjuntos introducidos anteriormente, para los cuales se cumplen las siguiente propiedades:

- 1** *para cualquier $x \in X$ y $k \in K$ se cumple la igualdad*
$$D_k(E_k(x)) = x;$$
- 2** $Y = \bigcup_{k \in K} E_k(X)$

Algoritmo DES y AES

Surgimiento

- En 1973 el Buró Nacional de Estándares NBS (National Bureau of Standards) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para cifrar información no clasificada.
- En 1974 la Agencia Nacional de Seguridad NSA (National Security Agency) declara desierto el primer concurso.
- En 1974 publica unas segundas especificaciones.

Surgimiento

- En 1973 el Buró Nacional de Estándares NBS (National Bureau of Standards) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para cifrar información no clasificada.
- En 1974 la Agencia Nacional de Seguridad NSA (National Security Agency) declara desierto el primer concurso.
- En 1974 publica unas segundas especificaciones.

Especificaciones

- El sistema debe poseer un nivel de seguridad computacional alto.
- El algoritmo debe ser fácil de entender.
- El algoritmo debe estar especificado en todos sus detalles.
- El sistema no debe comprometerse con la publicación del algoritmo.
- Debe estar disponible para cualquier usuario.
- Deberá poder usarse en diferentes aplicaciones.
- Fabricación con dispositivos electrónicos de bajo costo.
- Se debe poder usar como validación.
- Debe ser exportable.

Especificaciones

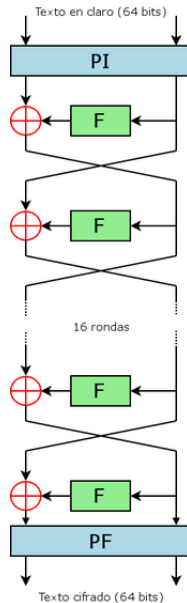
- El sistema debe poseer un nivel de seguridad computacional alto.
- El algoritmo debe ser fácil de entender.
- El algoritmo debe estar especificado en todos sus detalles.
- El sistema no debe comprometerse con la publicación del algoritmo.
- Debe estar disponible para cualquier usuario.
- Deberá poder usarse en diferentes aplicaciones.
- Fabricación con dispositivos electrónicos de bajo costo.
- Se debe poder usar como validación.
- Debe ser exportable.

- En 1974 se elige Lucifer, algoritmo original de IBM en los años 70, con algunas variaciones.
- En 1976 el Estándar para Cifrado de Datos DES (Data Encryption Standard) se adopta como estándar y se autoriza para ser utilizado en las comunicaciones **no clasificadas del gobierno**.

- En 1974 se elige Lucifer, algoritmo original de IBM en los años 70, con algunas variaciones.
- En 1976 el Estándar para Cifrado de Datos DES (Data Encryption Standard) se adopta como estándar y se autoriza para ser utilizado en las comunicaciones **no clasificadas del gobierno**.

Funcionamiento general del DES

- Procesa un bloque de entrada / salida de 64 bits.
- Se aplica una permutación inicial PI (a nivel de bits).
- Se aplican 16 rondas de Feistel.
- Se aplica una permutación final PF (inversa de PI).



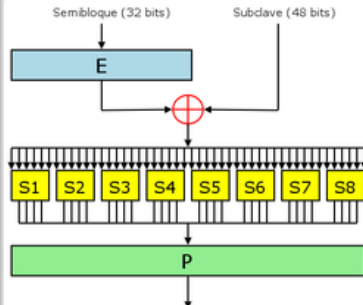
Función de Feistel del DES

La función de Feistel en el DES realiza cuatro operaciones

- Expansión
- Mezcla
- Sustitución
- Permutación

y se define de la siguiente forma

$$F(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$



Surgimiento

- En 1997 el Instituto Nacional de Estándares y Tecnologías NIST (National Institute of Standards and Technology) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para procesar **información sensible no clasificada**.
- En 2001, después de un proceso de estandarización de 5 años, se anuncia el **algoritmo criptográfico Rijndael** como el Estándar de Cifrado Avanzado AES (Advanced Encryption Standard).
- En 2003 la NSA anuncia que el AES podía ser usado para procesar información clasificada, sin embargo **se declaró nuevamente no apropiado para el procesamiento de información clasificada**.
- En 2014 la Agencia de la Unión Europea para las Redes y la Seguridad de la Información ENISA (European Union Agency for Network and Information Security) recomienda al algoritmo AES como uno de los algoritmos de cifrado en bloque con los que se puede contar en el futuro.

Surgimiento

- En 1997 el Instituto Nacional de Estándares y Tecnologías NIST (National Institute of Standards and Technology) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para procesar **información sensible no clasificada**.
- En 2001, después de un proceso de estandarización de 5 años, se anuncia el **algoritmo criptográfico Rijndael** como el Estándar de Cifrado Avanzado AES (Advanced Encryption Standard).
- En 2003 la NSA anuncia que el AES podía ser usado para procesar información clasificada, sin embargo **se declaró nuevamente no apropiado para el procesamiento de información clasificada**.
- En 2014 la Agencia de la Unión Europea para las Redes y la Seguridad de la Información ENISA (European Union Agency for Network and Information Security) recomienda al algoritmo AES como uno de los algoritmos de cifrado en bloque con los que se puede contar en el futuro.

Surgimiento

- En 1997 el Instituto Nacional de Estándares y Tecnologías NIST (National Institute of Standards and Technology) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para procesar **información sensible no clasificada**.
- En 2001, después de un proceso de estandarización de 5 años, se anuncia el **algoritmo criptográfico Rijndael** como el Estándar de Cifrado Avanzado AES (Advanced Encryption Standard).
- En **2003 la NSA** anuncia que el AES podía ser usado para procesar información clasificada, sin embargo **se declaró nuevamente no apropiado para el procesamiento de información clasificada**.
- En 2014 la Agencia de la Unión Europea para las Redes y la Seguridad de la Información ENISA (European Union Agency for Network and Information Security) recomienda al algoritmo AES como uno de los algoritmos de cifrado en bloque con los que se puede contar en el futuro.

Surgimiento

- En 1997 el Instituto Nacional de Estándares y Tecnologías NIST (National Institute of Standards and Technology) convoca a un concurso público para establecer un algoritmo criptográfico de cifrado en bloques como estándar para procesar **información sensible no clasificada**.
- En 2001, después de un proceso de estandarización de 5 años, se anuncia el **algoritmo criptográfico Rijndael** como el Estándar de Cifrado Avanzado AES (Advanced Encryption Standard).
- En **2003 la NSA** anuncia que el AES podía ser usado para procesar información clasificada, sin embargo **se declaró nuevamente no apropiado para el procesamiento de información clasificada**.
- En 2014 la Agencia de la Unión Europea para las Redes y la Seguridad de la Información ENISA (European Union Agency for Network and Information Security) recomienda al algoritmo AES como uno de los algoritmos de cifrado en bloque con los que se puede contar en el futuro.



Vincent Rijmen



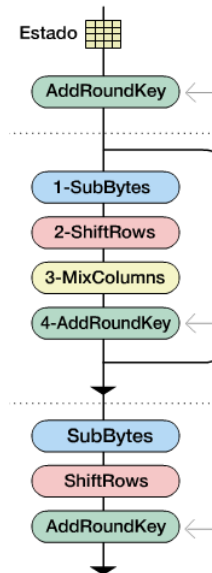
Joan Daemen

Especificaciones

- Ser de dominio público, disponible para todo el mundo.
- Soportar bloques como mínimo de 128 bits.
- Utilizar llaves variables de 128, 192 y 256 bits.
- Ser implementable tanto en hardware como en software.
- Resistir los ataques lineal y diferencial.

Funcionamiento general del AES

- Procesa un bloque de entrada/salida de 128 bits.
- Se aplica una suma x-or con la llave.
- El número de rondas está determinado por el tamaño de la llave.
- En la última ronda se elimina la función MixColumns.



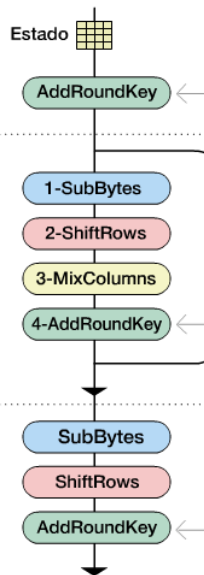
Funciones de cifrado del AES

En el AES se realizan cuatro transformaciones

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

y se define de la siguiente forma

$$F(St, K) = MC(SR(SB(St))) \oplus K$$



Algoritmo AES

Estructura algebraica

El AES trabaja a nivel de bytes, por lo cual las operaciones del mismo se realizan sobre el campo $\text{GF}(2^8)$ construido a propuesta de los diseñadores mediante el polinomio irreducible $\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1$ sobre $\text{GF}(2)$.

Estados

AES opera bloques de 128 bits de longitud en forma de matriz de 4 filas y 4 columnas, llamada estado.

- Si $P = p_1 p_2 \cdots p_{16}$ es el bloque de entrada entonces el estado inicial se conforma a partir del mismo como sigue

$$\text{St}_{i,j} = p_{4(j-1)+i} \quad 1 \leq i, j \leq 4$$

- Si $C = c_1 c_2 \cdots c_{16}$ es el bloque de salida entonces el mismo se conforma a partir del estado final como sigue

$$c_{4(j-1)+i} = \text{St}_{i,j} \quad 1 \leq i, j \leq 4$$

Ejercicio

Formar el estado a partir del "bloque de entrada"

YONOSECOMOESESTO

Ejercicio

Formar el estado a partir del "bloque de entrada"

0A2410EFCDB63C0F5F975F2BE8AAB699

Entonces el estado inicial $St_{i,j} = \begin{pmatrix} 0A & CD & 5F & E8 \\ 24 & B6 & 97 & AA \\ 10 & 3C & 5F & B6 \\ EF & 0F & 2B & 99 \end{pmatrix}$

Ejercicio

Formar el estado a partir del "bloque de entrada"

0A2410EFCDB63C0F5F975F2BE8AAB699

Entonces el estado inicial $St_{i,j} = \begin{pmatrix} 0A & CD & 5F & E8 \\ 24 & B6 & 97 & AA \\ 10 & 3C & 5F & B6 \\ EF & 0F & 2B & 99 \end{pmatrix}$

Llaves

El AES soporta llaves de 128, 192 o 256 bits de longitud, organizada en forma de matriz de 4 filas y N_k columnas, donde N_k es el tamaño de la llave dividido por 32, es decir, $N_k = 4, 6, 8$ respectivamente. **A diferencia del DES que solo soporta llaves de tamaño fijo 64 bits.**

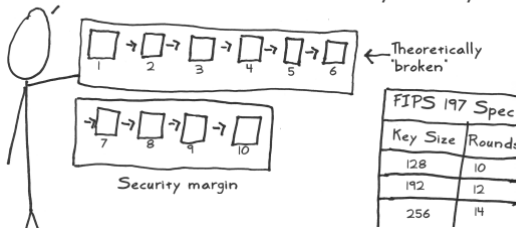
En la literatura se conoce como AES-128, AES-192 y AES-256, a la variante de AES que utiliza 128, 192 o 256 bits de llave respectivamente.

Estructura

AES es un cifrador de bloques iterado cuya estructura es una red Sustitución - Permutación. El estado inicial es modificado durante un cierto número de rondas hasta obtener el estado final. El número de rondas en AES está determinado por la ecuación $N_r = N_k + 6$.

AES posee 6 rondas de seguridad probada ante los ataques existentes, y es añadida 1 ronda como margen de seguridad cada 32 bits de la llave.

When I was being developed, a clever guy was able to find a shortcut path through 6 rounds. That's not good!
I added 4 extra rounds. This is my 'security margin.'



Expansión de la llave

De forma independiente al proceso de cifrado, Rijndael cuenta con un algoritmo de expansión de llave, permitiendo obtener $N_r + 1$ llaves de ronda $\text{ExK}[0], \text{ExK}[1], \dots, \text{ExK}[N_r]$ cada una en forma de matriz y de igual tamaño que el texto claro.

Ejercicio

Formar la matriz de la llave inicial

2B7E151628AED296ABFE158809CF4F3C

Entonces el estado inicial $K_{i,j} = \begin{pmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & 96 & 88 & 3C \end{pmatrix}$

Expansión de la llave

De forma independiente al proceso de cifrado, Rijndael cuenta con un algoritmo de expansión de llave, permitiendo obtener $N_r + 1$ llaves de ronda $\text{ExK}[0], \text{ExK}[1], \dots, \text{ExK}[N_r]$ cada una en forma de matriz y de igual tamaño que el texto claro.

Ejercicio

Formar la matriz de la llave inicial

2B7E151628AED296ABFE158809CF4F3C

Entonces el estado inicial $K_{i,j} = \begin{pmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & 96 & 88 & 3C \end{pmatrix}$

Descripción de las transformaciones del Algoritmo AES



SubBytes

La función SubBytes

$$\text{SB} : M_{4 \times 4}(\text{GF}(2^8)) \longrightarrow M_{4 \times 4}(\text{GF}(2^8))$$

es una sustitución no lineal que opera de forma independiente sobre cada byte del estado como una S -caja de 8×8 biyectiva. Esta S -caja es composición de las aplicaciones $\phi_1, \phi_2 : \text{GF}(2^8) \longrightarrow \text{GF}(2^8)$ definidas para todo $x \in \text{GF}(2^8)$ como

$$\phi_1(x) = x^{-1}$$

$$\phi_2(x) = [(x^4 + x^3 + x^2 + x + 1)x \bmod (x^8 + 1)] + (x^6 + x^5 + x + 1)$$

de forma tal que para cada $\text{St} \in M_{4 \times 4}(\text{GF}(2^8))$ y todos $1 \leq i, j \leq 4$

$$\text{SB}(\text{St})_{i,j} = \phi_2(\phi_1(\text{St}_{i,j}))$$

Cada byte es dividido en dos valores hexadecimales, de los cuales el primero se corresponde con las filas y el segundo con las columnas.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

Ejercicio

Halle la matriz de estado luego de la transformación SubByte
la matriz a transformar es $St_{i,j} \oplus K_{i,j}$.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

De forma consecutiva obtenemos la nueva matriz de estado

$$\begin{pmatrix} \text{FD} & \text{D9} & \text{BF} & \text{F8} \\ \text{FC} & \text{AD} & \text{D0} & \text{4D} \\ \text{6B} & \text{28} & \text{D6} & \text{99} \\ \text{3B} & \text{EE} & \text{0A} & \text{06} \end{pmatrix}$$

ShiftRows

La función ShiftRows

$$\text{SR} : M_{4 \times 4}(\text{GF}(2^8)) \longrightarrow M_{4 \times 4}(\text{GF}(2^8))$$

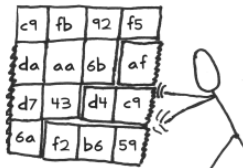
consiste en aplicar a la i -ésima fila del estado un corrimiento de los bytes $i - 1$ posiciones de forma cíclica hacia la izquierda. Luego para cada $\text{St} \in M_{4 \times 4}(\text{GF}(2^8))$ y todos $1 \leq i, j \leq 4$ se tiene que

$$\text{SR}(\text{St})_{i,j} = \text{St}_{i,j-i+1 \bmod N_b}$$

I shift the rows to the left



...and then wrap them around the other side



Ejercicio

Halle la matriz de estado luego de la transformación ShiftRows.

$$\begin{pmatrix} \text{FD} & \text{D9} & \text{BF} & \text{F8} \\ \text{AD} & \text{D0} & \text{4D} & \text{FC} \\ \text{D6} & \text{99} & \text{6B} & \text{28} \\ \text{06} & \text{3B} & \text{EE} & \text{0A} \end{pmatrix}$$

Ejercicio

Halle la matriz de estado luego de la transformación ShiftRows.

$$\begin{pmatrix} \text{FD} & \text{D9} & \text{BF} & \text{F8} \\ \text{AD} & \text{D0} & \text{4D} & \text{FC} \\ \text{D6} & \text{99} & \text{6B} & \text{28} \\ \text{06} & \text{3B} & \text{EE} & \text{0A} \end{pmatrix}$$

Esta transformación aporta dispersión en el estado respecto a sus columnas, en el sentido de que **en cada columna de SR(St) todos los bytes corresponden a distintas columnas de St**, garantizando la resistencia del cifrado contra ataques diferenciales truncados y ataques de saturación para bloques de tamaño superior a 128 bits.

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

→

1	5	9	13
6	10	14	2
11	15	3	7
16	4	8	12

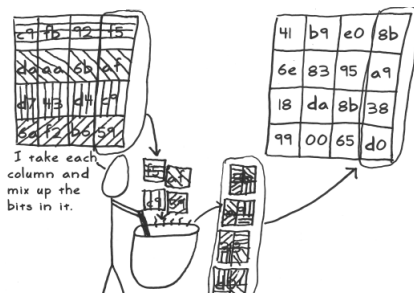
MixColumns

La función MixColumns

$$\text{MC} : M_{4 \times 4}(\text{GF}(2^8)) \longrightarrow M_{4 \times 4}(\text{GF}(2^8))$$

opera de forma independiente sobre cada columna de la matriz de estado, interpretando a las mismas como polinomios con coeficientes en $\text{GF}(2^8)$, y aplicando la función $\theta : \text{GF}(2^8)[x] \longrightarrow \text{GF}(2^8)[x]$

$$\theta(P) = (03x^3 + 01x^2 + 01x + 02)P(x) \bmod(01x^4 + 01).$$



MixColumns se aplica sobre estado pre-multiplicando a la matriz

$$M_{\theta} = \begin{array}{|c|c|c|c|} \hline 02 & 03 & 01 & 01 \\ \hline 01 & 02 & 03 & 01 \\ \hline 01 & 01 & 02 & 03 \\ \hline 03 & 01 & 01 & 02 \\ \hline \end{array}$$

por el mismo de forma tal que para cada $St \in M_{4 \times 4}(\text{GF}(2^8))$ y todos $1 \leq i, j \leq 4$

$$\text{MC}(St)_{i,j} = (M_{\theta} St)_{i,j}$$

El impacto de esta transformación en el cifrado, es que por su condición de MDS (Máxima Distancia de Separación) **aporta la mayor difusión local** con respecto a cada columna del estado.

Ejercicio

Halle la matriz de estado luego de la transformación MixColumns.

$$\begin{pmatrix} 0B \\ DF \\ ED \\ 6B \end{pmatrix}$$

Esto se corresponde con la primera columna de la matriz de estado.

Ejercicio

Halle la matriz de estado luego de la transformación MixColumns.

$$\begin{pmatrix} 0B \\ DF \\ ED \\ 6B \end{pmatrix}$$

Esto se corresponde con la primera columna de la matriz de estado.

AddRoundKey

La función AddRoundKey

$$\text{ARK} : M_{4 \times 4}(\text{GF}(2^8)) \times M_{4 \times 4}(\text{GF}(2^8)) \longrightarrow M_{4 \times 4}(\text{GF}(2^8))$$

consiste en aplicar a cada byte del estado una suma X-or con el correspondiente byte de la llave de ronda. De esta forma para cada $\text{ExK}, \text{St} \in M_{4 \times 4}(\text{GF}(2^8))$ y todos $1 \leq i, j \leq 4$

$$\text{ARK}(\text{St}, \text{ExK})_{i,j} = \text{St}_{i,j} \oplus \text{ExK}_{i,j}.$$

Esta es otra capa de confusión añadida al algoritmo para **ocultar la relación existente entre el texto cifrado y el texto claro.**

Difusión

AES alcanza la difusión completa en dos rondas con la aplicación consecutiva de las transformaciones ShiftRows y MixColumns.

Llaves débiles y semidébiles

En el AES no existen llaves débiles o semidébiles debido a que el algoritmo de expansión de llave elimina la simetría de las llaves de ronda.

Ataques clásicos

Ninguno de los ataques conocidos ha sido mas exitoso en el AES que la búsqueda exhaustiva. El ataque mas efectivo, teóricamente, es el Criptoanálisis Diferencial con Llaves Relacionadas que aprovecha la poca difusión de su algoritmo de expansión de llaves.

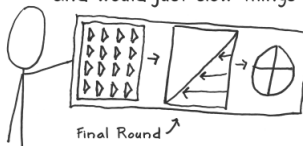
Ataques de canal colateral

El AES ha sido probado susceptible ante ataques de canal colateral. Variantes como el Ataque de Tiempos de Cache, el Ataque de Fallos o el Ataque Diferencial de Potencia has sido exitosos en el AES,

Descifrado

En el AES el proceso de descifrado se realiza de forma similar al proceso de cifrado. En este caso cada una de las transformaciones que operan en la función de ronda posee una inversa, a diferencia del DES donde la inversa esta garantizada por la estructura de Feistel.

In the final round, I skip the 'Mix Columns' step since it wouldn't increase security* and would just slow things down:



*The diffusion it would provide wouldn't go to the next round.

Muchas Gracias

Preguntas