CriptoSistemas Básicos
Clase 1/2

Criptografía
2019

Instituto de Computación
Facultad de Ingeniería
Universidad de la República

Contenido

Simétrica vs Asimétrica

- simétrica: el emisor y receptor comparten la misma clave secreta
  Ejemplo: AES.
- asimétrica: solamente el receptor necesita una clave secreta para desencriptar el mensaje.
  Se utiliza una clave pública para encriptar el mensaje.
  Ejemplo: RSA.

RSA: Rivest Shamir Adleman

- la seguridad radica en la dificultad en descomponer en factores primos un entero muy grande.

Diffie - Hellman

- Goal: acordar una clave secreta en común entre dos participantes.
- Esta clave luego se utiliza con un sistema simétrico
- La seguridad radica en la dificultad de computar el logaritmo discreto.

Main Goal of Crypto

- el objetivo principal es que alguien quiere enviar un mensaje por un canal inseguro y otro está escuchando con malas intenciones. El intruso no debe ser capaz de entender el mensaje.
- Actores de la literatura:
  - Bob envía un mensaje a Alice y Eve está escuchando malintencionadamente el canal.
  - Eve no puede desencriptar el mensaje sin la clave secreta (o de acuerdo a su objetivo).

Parámetro de Seguridad

- forma de medir cuán difícil es para un adversario quebrar un criptosistema.
- Ejemplos:
  - el espacio de claves
  - RSA: el parametro de seguridad es la longitud en bits del módulo n (n=pq).

Primitivas Criptográficas

- la seguridad de las primitivas criptograficas se basan en la dificultad de problemas dificiles.
- si Eve pudiera encontrar el mensaje, luego sería también capaz de resolver un problema dificil y abierto.
  $\rightarrow$ reducción.

One-way function

- f es una función one-way: dado x debe ser fácil de computar $y = f(x)$
- dado algún y elegido de forma aleatoria y uniforme en el codominio de f debe ser dificil encontrar su pre-imágen x
- Ejemplos:
  - multiplicación es fácil de computar pero dado N hallar los factores primos es dificil.
  - logaritmo discreto y exponenciación

Trapdoor function

- f es una función one-way pero que conociendo un secreto S se vuelve fácil de computar la pre-imagen x a partir de y.
- en RSA se utiliza una función trapdoor.

Otros objetivos de Eve

- recuperar parcialmente el mensaje
- determinar un predicado sobre el mensaje:
  - ocurre la palabra bomba?
- no determinarlo para todos los mensajes sino solamente para algunos

Nociones de Seguridad (Cap. 9)

- Recursos y Objetivos de los Ataques
- Ejemplos de ataques: chosen plaintext attack.
- Noción de indistinguibilidad: Eva pide encriptar dos textos y se le devuelve un cifrado. Luego debe distinguir con probabilidad mayor a un medio cual de los dos textos fue encriptado. Indistingubilidad significa ser resistente a este ataque.

AES: Advanced Encryption Standard

- Seleccionado entre 15 candidatos en 1997 por el NIST como reemplazo de DES.
- Criptografía simétrica

AES: Generalidades

- Longitud de bloque de 128 bits y soporta claves de largo 128, 192 y 256 bits.
- es un cifrado iterativo: secuencia de cuatro operaciones es aplicada una cierta cantidad de veces.
- 10 rondas para 128, 12 rondas para 192 y 14 rondas para 256. Cada ronda aplica las cuatro operaciones (excepto en la última).
- Modos de operación

AES: Operaciones

Las cuatro operaciones son:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

Cada operación toma una palabra de 128-bit y devuelve una palabra de 128-bit.

AES: Overview de las Operaciones

Denotamos el número de rondas como N_r y al estado como S.

1. Dado el texto plano x, se inicializa el estado S con x y se ejecuta *AddRoundKey*, lo cual hace un $x - or$ de la *RoundKey* con S
2. Para cada una de las rondas $N_r - 1$ se hace:
    1. una sustitución SubBytes en S utilizando una $S - box$
    2. se hace una permutación ShiftRow en S
    3. se aplica MixColumns en S
    4. se hace AddRoundKey
3. En la última ronda se hace SubBytes, ShiftRows y AddRoundKey.
4. el texto cifrado se define como el estado S

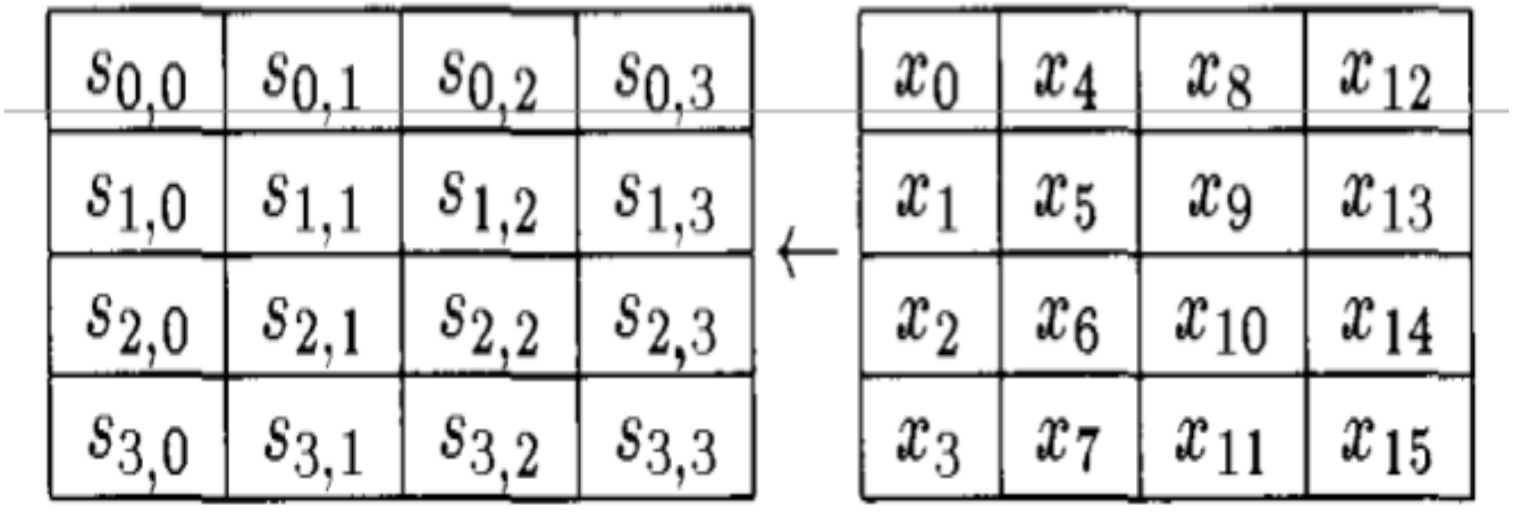
AES: Estado

- Todas las operaciones en AES son en bytes.
- El texto plano x consiste en 16 bytes denotado como $x_0, x_1, \ldots, x_{15}$
- El estado S es representado como una matriz de bytes de tamaño 4x4.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

AES: Init

- Inicialmente el estado se define como los 16 byte del texto plano x
- Utilizamos notación hexadecimal para representar el contenido de un byte. Cada byte se escribe como dos digitos hexadecimales.



AES: SubBytes

- Se procesa 1 byte (8 bits).
- Ejecuta una sustitución en cada byte del estado de forma independiente.
- Se utiliza una $S - box$, llamada, π_S que es una permutación de $\{0,1\}^8$

AES: S-Box

Es más eficiente implementada por una búsqueda en tabla. Ejemplo:

- Entrada: 01010011 $\rightarrow$ 53
- Salida: ED $\rightarrow$ 11101101

	Y															
X	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

AES: S-Box

- En contraste con DES, en AES S-box puede ser definido de forma algebráica.
- El cuerpo finito F_{2^8} definido por el siguiente polinomio irreductible $m = t^8 + t^4 + t^3 + t + 1 \in F_2[t]$

$\mathbb{F}_{256} = \mathbb{F}_{2^8} \ni a = a_7t^7 + a_6t^6 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$,
with all $a_i \in \mathbb{F}_2 = \{0, 1\}$.
Representation: 8 bits for an element = 1 byte.
Addition: XOR, $(a + b)_i = a_i + b_i$.
Multiplication: as for polynomials modulo $t^8 + t^4 + t^3 + t + 1$.
Example $\texttt{57} \cdot \texttt{83} = \texttt{C1}$:

$$
\begin{aligned}
&(t^6 + t^4 + t^2 + t + 1) \cdot (t^7 + t + 1) \\
&\quad = t^{13} + t^{11} + t^9 + t^8 + t^7 \\
&\qquad + t^7 + t^5 + t^3 + t^2 + t \\
&\qquad + t^6 + t^4 + t^2 + t + 1 \\
&\quad = t^{13} + t^{11} + t^9 + t^8 + t^6 + t^5 + t^4 + t^3 + 1 \text{ in } \mathbb{Z}_2[t] \\
&\quad = t^7 + t^6 + 1 \text{ in } \mathbb{Z}_2[t]/(t^8 + t^4 + t^3 + t + 1).
\end{aligned}
$$

AES: SubBytes

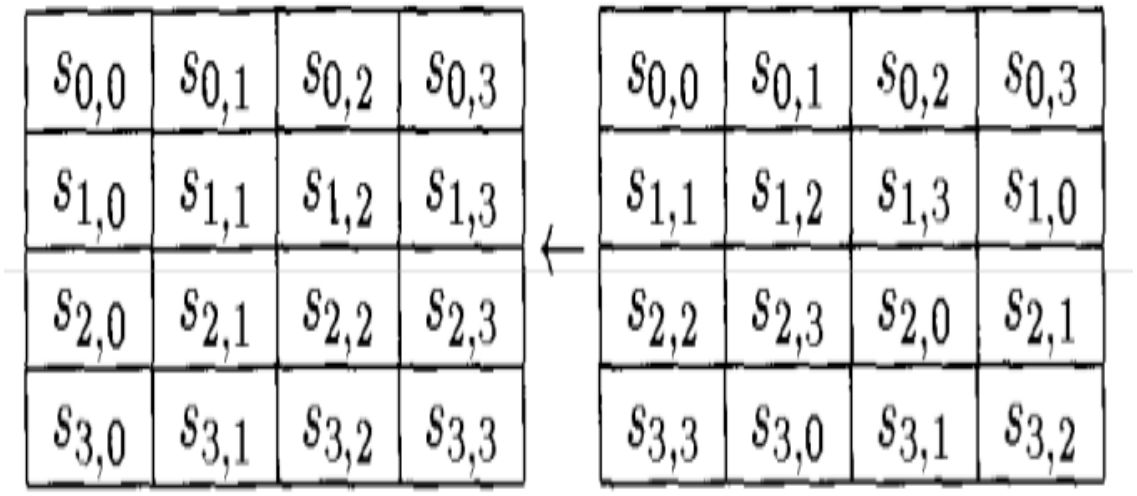
Algorithm 3.4: SUBBYTES$(a_7a_6a_5a_4a_3a_2a_1a_0)$

external FIELDINV, BINARYTOFIELD, FIELDTOBINARY
$z \leftarrow$ BINARYTOFIELD$(a_7a_6a_5a_4a_3a_2a_1a_0)$
if $z \neq 0$
  then $z \leftarrow$ FIELDINV(z)
$(a_7a_6a_5a_4a_3a_2a_1a_0) \leftarrow$ FIELDTOBINARY(z)
$(c_7c_6c_5c_4c_3c_2c_1c_0) \leftarrow (01100011)$
comment: In the following loop, all subscripts are to be reduced modulo 8
for $i \leftarrow 0$ **to** 7
  do $b_i \leftarrow (a_i + a_{i+4} + a_{i+5} + a_{i+6} + a_{i+7} + c_i) \bmod 2$
return $(b_7b_6b_5b_4b_3b_2b_1b_0)$

- BINARYTOFIELD: covierte un byte en un elemento del cuerpo.
- FIELDTOBYNARY: conversión de un elemento del cuerpo a byte
- FIELDINV: el inverso multiplicativo de un elemento del cuerpo. Algoritmo extendido de Euclides.

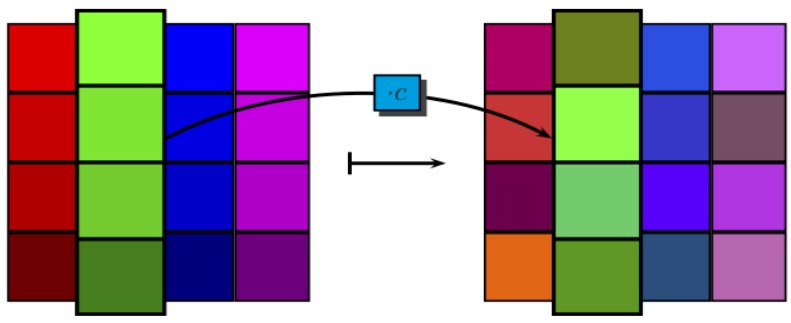
AES: ShiftRows

Cada fila es corrida ciclicamente a la izquierda 0, 1, 2 y 3 bytes respectivamente.



AES: MixColumns

- Se considera una columna (4 bytes) como polinomio en F_{256} de grado menor o igual a 3.
- La suma de polinomios es el $x - or$
- La multiplicación da un polinomio de grado menor o igual a 6, el cual se reduce a grado menor o igual a 3 con módulo $s^4 + 1$



Each column is considered as an element of $\mathbb{F}_{256}[y]/(y^4+1)$
and multiplied by $c = 03y^3 + 01y^2 + 01y + 02$.
Inverse: multiply with $0By^3 + 0Dy^2 + 09y + 0E$.

AES: AddRoundKey

- un bloque de 128-bit y una round key del mismo tamaño se suman bit a bit.
- en AES-128 se necesitan 11 round keys.

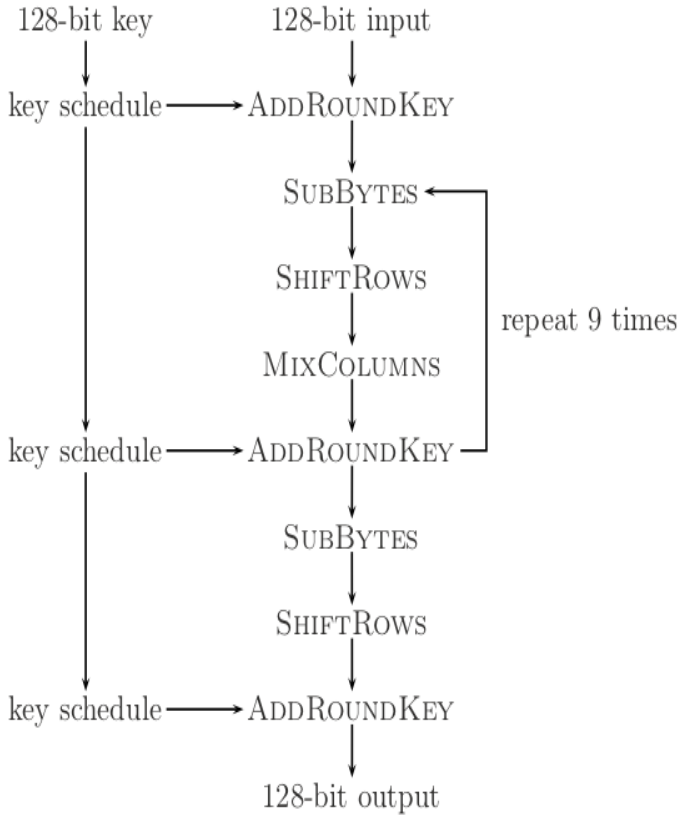


Figure 2.1: AES with a 128-bit key.

AES: Key schedule

- un bloque de 128-bit y una round key del mismo tamaño se suman bit a bit.
- en AES-128 se necesitan 11 round keys.
- $\rightarrow$ key expansion

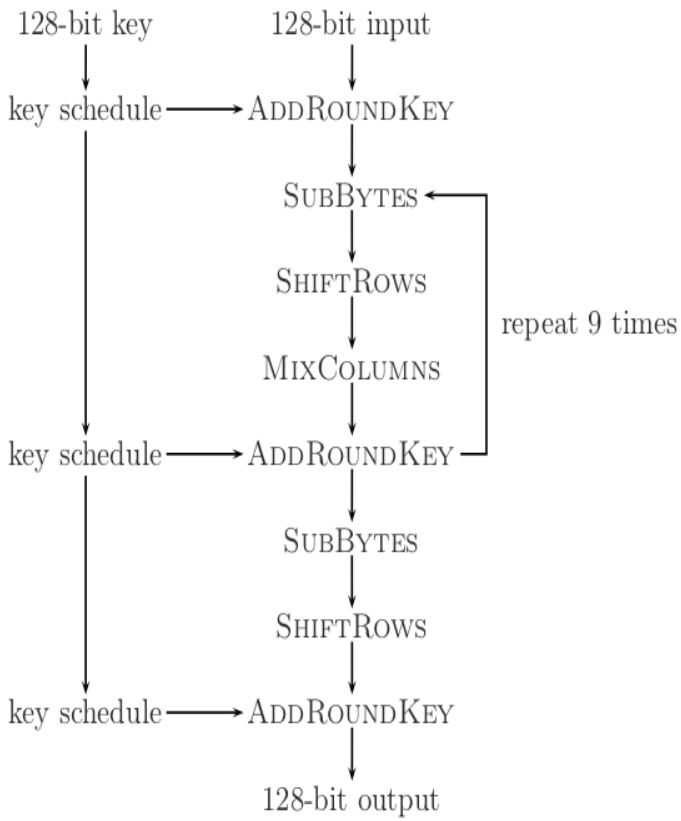


Figure 2.1: AES with a 128-bit key.

AES

- La omisión de MixColumns en la última ronda (paso final de permutación) no decrementa la seguridad dado que los bits del texto cifrado son permutados de una forma pública.

The end.