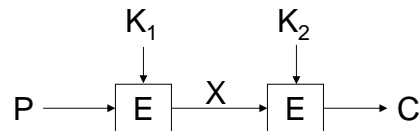


## Improvements of DES (1)

- Double DES

- two encryption stages, two keys

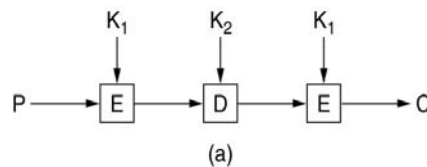


- Meet-in-the-middle Attack
- plaintext attack succeeds with an effort of  $2^{56}$  despite of the key length of 112 bits

## Improvements of DES (2)

- Triple DES encryption

- two encryption stages, one decryption stages



- also used with three keys
- Why not use  $E(K_1, E(K_2, E(K_1, P)))$ ?
  - Hint: Simple DES

## Advanced Encryption Standard (1)

- The algorithm must be a symmetric block cipher.
- The full design must be public.
- Key lengths of 128, 192, and 256 bits supported.
- Both software and hardware implementations required
- The algorithm must be public or licensed on nondiscriminatory terms.

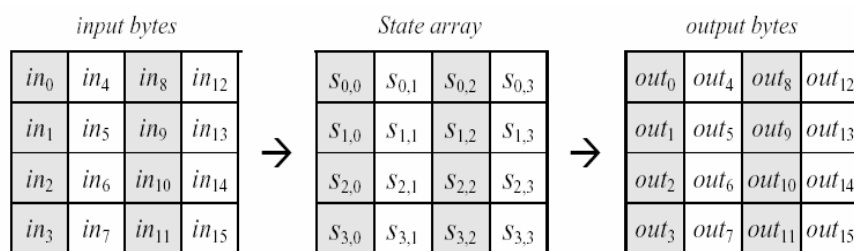
## Advanced Encryption Standard (2)

- Rijndael became the AES in October 2000.
- The standard was introduced in 2001 with some more specifications.
- Block length: 128 bit/16 byte (Rijndael allows other block length as well)
- Key length: 128, 192 oder 256 bit
- A block is encyphered in several rounds.
- Number of rounds depends on the key length.

## Block Treatment

1. Block transfer in State (16 bytes)
  2. AddRoundKey
  3. For  $r=1$  to #rounds-1:
    - SubBytes
    - ShiftRows
    - MixColumns
    - AddRoundKey
  4. SubBytes
  5. ShiftRows
  6. AddRoundKey
  7. State transfer to cipher block (16 bytes)
- } last round

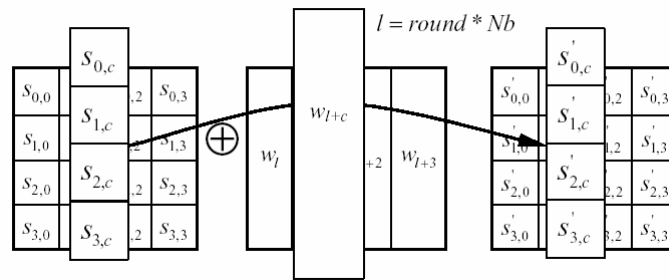
## State



- With AES the state is always a 4x4 matrix.
- Rijndael allows other block sizes, but the number of rows of the state is always 4 (hence with larger blocks the number of columns is increased).

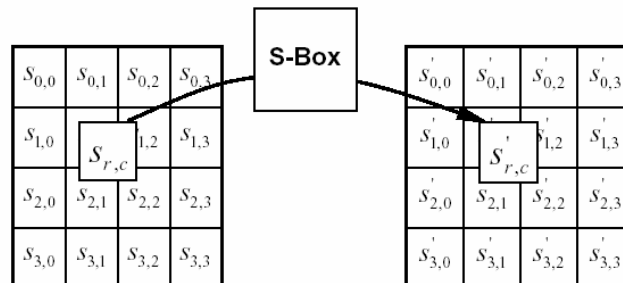
## AddRoundKey

Bitwise XOR of each column of the state with the appropriate round key determined by  $K_E$ .



## SubBytes

SubBytes substitutes each byte of the State by a value determined by a substitution matrix, called S-Box.

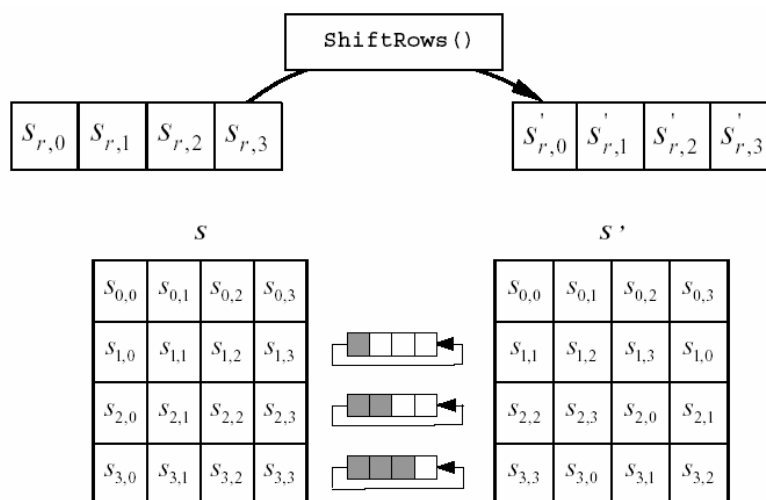


## S-box

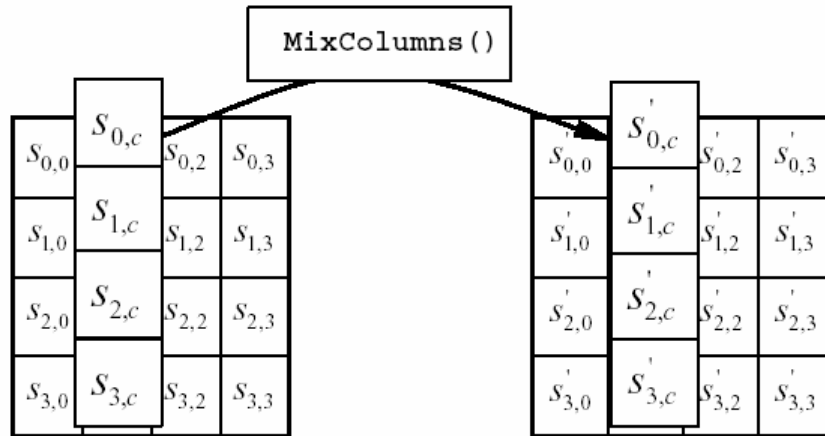
		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	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

Values are given in hexadecimal notation.

## ShiftRows



## MixColumns (1)



## MixColumns (2)

Multiplication of the state with a defined  
polynom column by column:

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Hence:

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

## Key Treatment (AES)

- Key length determines the number of rounds

Key length (bit)	# rounds
128	10
192	12
256	14

- Key expansion
- Round key selection

## Key Expansion (AES) (1)

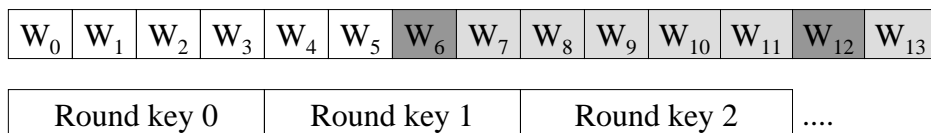
- Cipher key  $K$  is changed into an *expanded* key  $K_E$ .
- Expanded key  $W_0 W_1 W_2 \dots W_{4 \cdot \#rounds + 3}$  consists of  
 $4 \cdot 4 \cdot (\#rounds + 1)$  bytes  
 $= 4 \cdot (\#rounds + 1)$  4-byte-words
- $k$  is the number of columns of the key matrix (always 4 rows)
- $W_0$  to  $W_{k-1}$  correspond with the cipher key.
- $W_{n-k}$  are results of XORs, substitution and rotation.
- All other  $W_i$  are results of the XOR of the (substituted) previous  $W_{i-1}$  and the  $k^{\text{th}}$  predecessor  $W_{i-k}$ .

## Key Expansion (AES) (2)

- $W_0 \dots W_{k-1} = K$
- $i \bmod k \equiv 0$ :  $W_i = W_{i-k} \oplus W$   
with  $W = \text{SubByte}(\text{RotByte}(W_{i-1})) \oplus \text{Rcon}(i/k)$
- RotByte: cyclic left shift of the bytes of the word
- Rcon can be considered as a round constant.
- $i > k-1$  and  $i \bmod k \neq 0$ :  
if  $k > 6$  and  $i \bmod k \equiv 4$ :  $W_i = W_{i-k} \oplus \text{SubByte}(W_{i-1})$   
else:  $W_i = W_{i-k} \oplus W_{i-1}$

## Round Key Selection (AES)

- Round keys are taken from the *expanded* key  $K_E$ .
- Each round key consists of 4 words (4x4 bytes).
- First round key consists of the first 4  $W$ s ( $W_0 \dots W_3$ ), the second round key of the following 4  $W$ s ( $W_4 \dots W_7$ ), ...



(Example for  $k = 6$ )

## Round Key Selection (AES)

- Round keys are taken from the *expanded* key  $K_E$ .
- Each round key consists of 4 words (4x4 bytes).
- First round key consists of the first 4  $W$ s ( $W_0 \dots W_3$ ), the second round key of the following 4  $W$ s ( $W_4 \dots W_7$ ), ...

$W_0$	$W_1$	$W_2$	$W_3$	$W_4$	$W_5$	$W_6$	$W_7$	$W_8$	$W_9$	$W_{10}$	$W_{11}$	$W_{12}$	$W_{13}$
-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	----------	----------	----------	----------

Round key 0	Round key 1	Round key 2	....
-------------	-------------	-------------	------

(Example for  $k = 8$ )



Distributed Systems  
Dipl.-Math. Kerstin Luck

Security in Computer Networks