AES (Advanced Encryption Standard)

The AES process

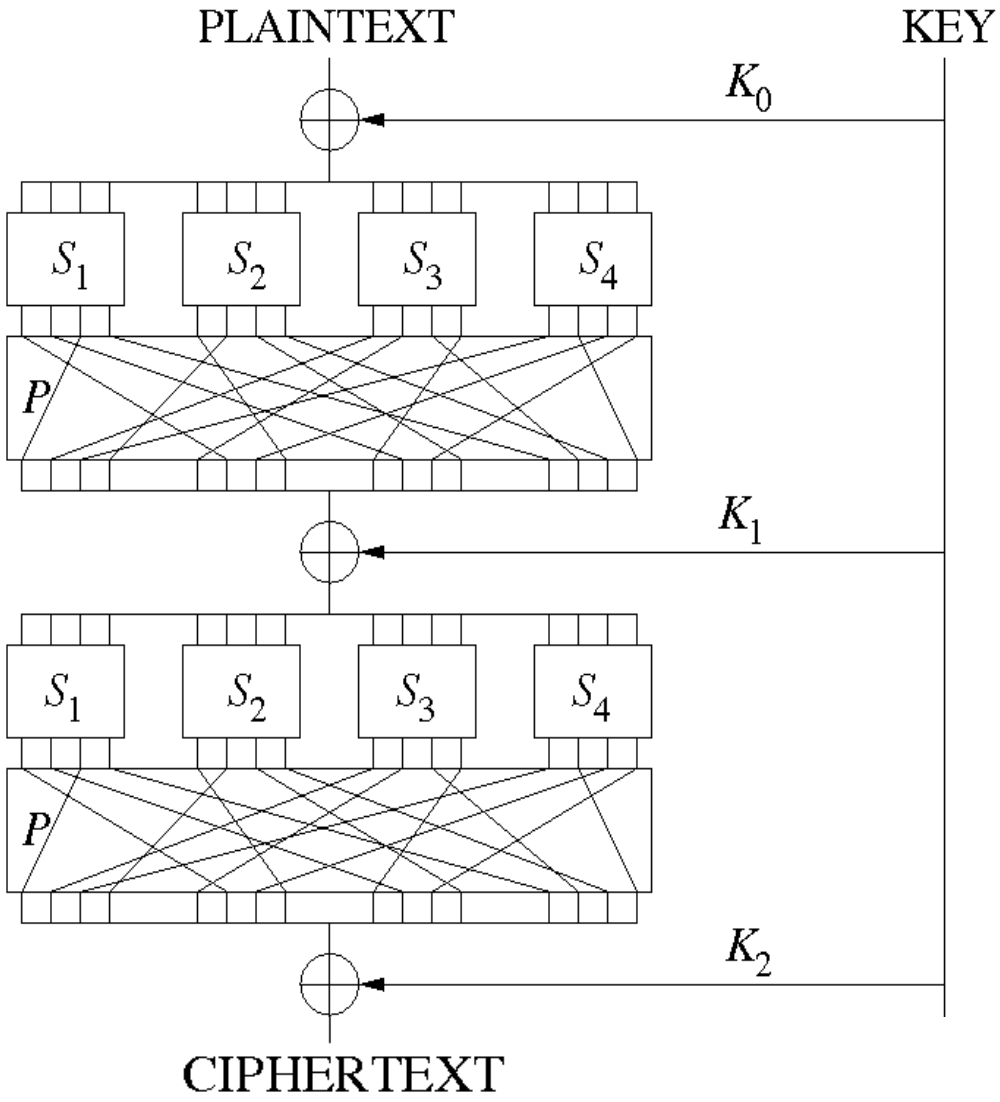
- 1997: NIST publishes request for proposal
- 1998: 15 submissions. Five claimed attacks.
- 1999: NIST chooses 5 finalists
- 2000: NIST chooses Rijndael as AES (designed in Belgium)

Key sizes: 128, 192, 256 bits. Block size: 128 bits

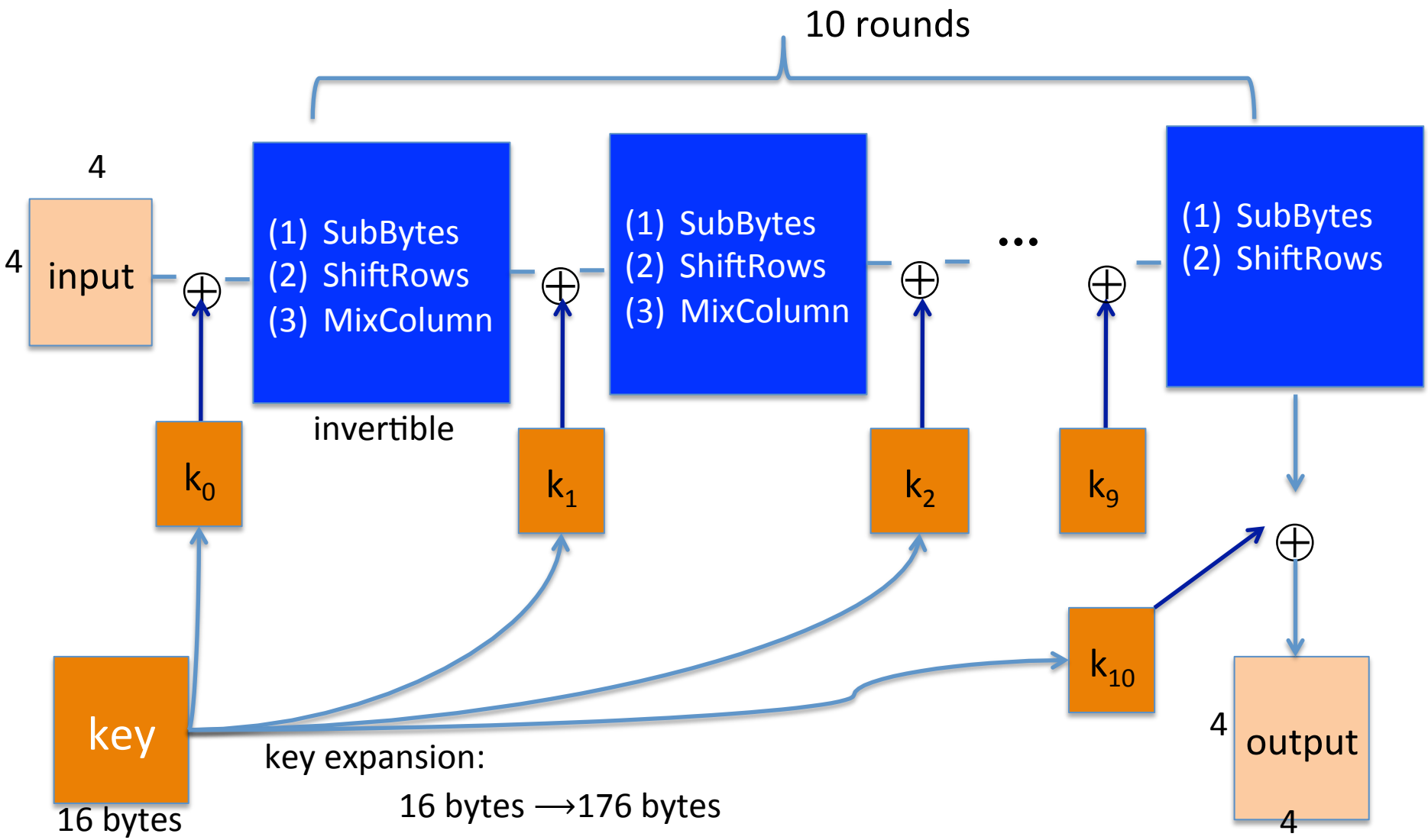
AES Overview

- Substitution-Permutation Network (not Feistel)
- Rounds
  - 10 rounds for 128-bit keys
  - 12 rounds for 192-bit keys
  - 14 rounds for 256-bit keys
- operates on a 4×4 column-major order matrix of bytes (*state*)

Substitution-Permutation Network

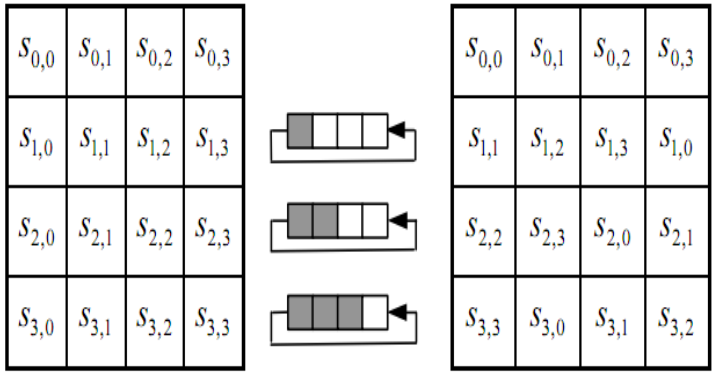


AES-128

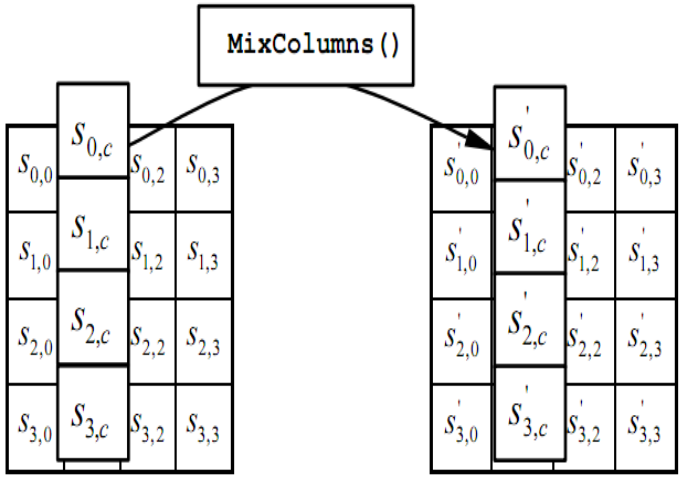

10 rounds
4
4
input
(1) SubBytes
(2) ShiftRows
(3) MixColumn
invertible
(1) SubBytes
(2) ShiftRows
(3) MixColumn
...
(1) SubBytes
(2) ShiftRows
k0
k1
k2
k9
k10
key
16 bytes
key expansion:
16 bytes ⟶176 bytes
4
output
4

The round function

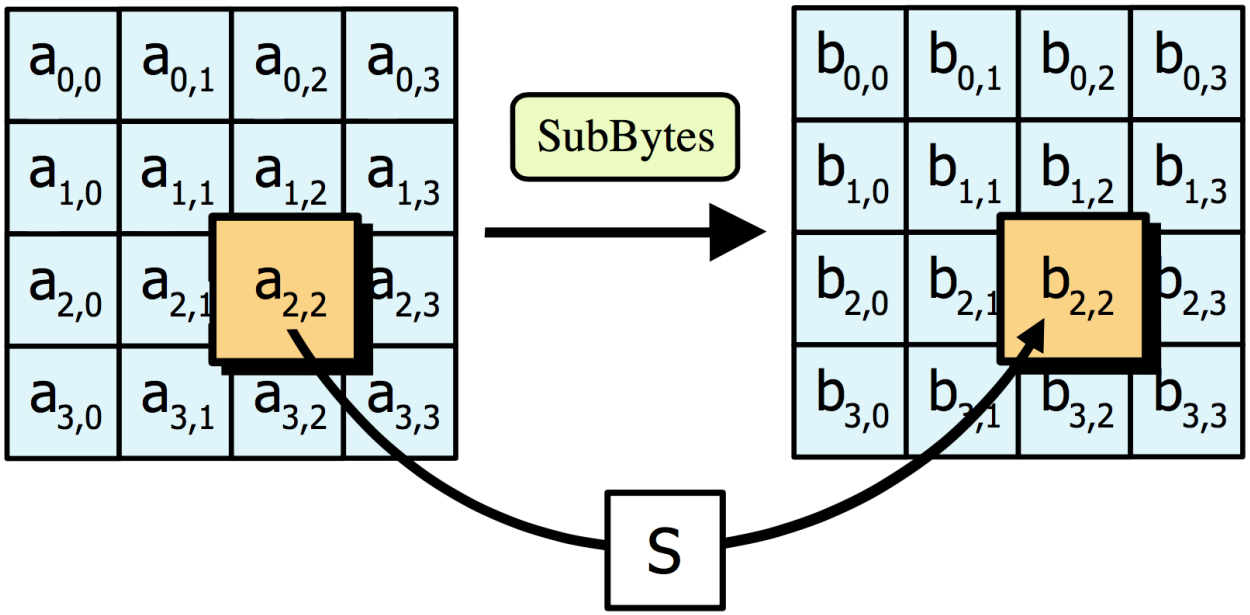
- **ByteSub**: a 1 byte S-box. 256 byte table
  (easily computable)
- **ShiftRows**:



- **MixColumr**



AES SubBytes



- Treat 128 bit block as 4x4 byte array
- b_{ij} = S-box(a_{ij})

AES “S-box”

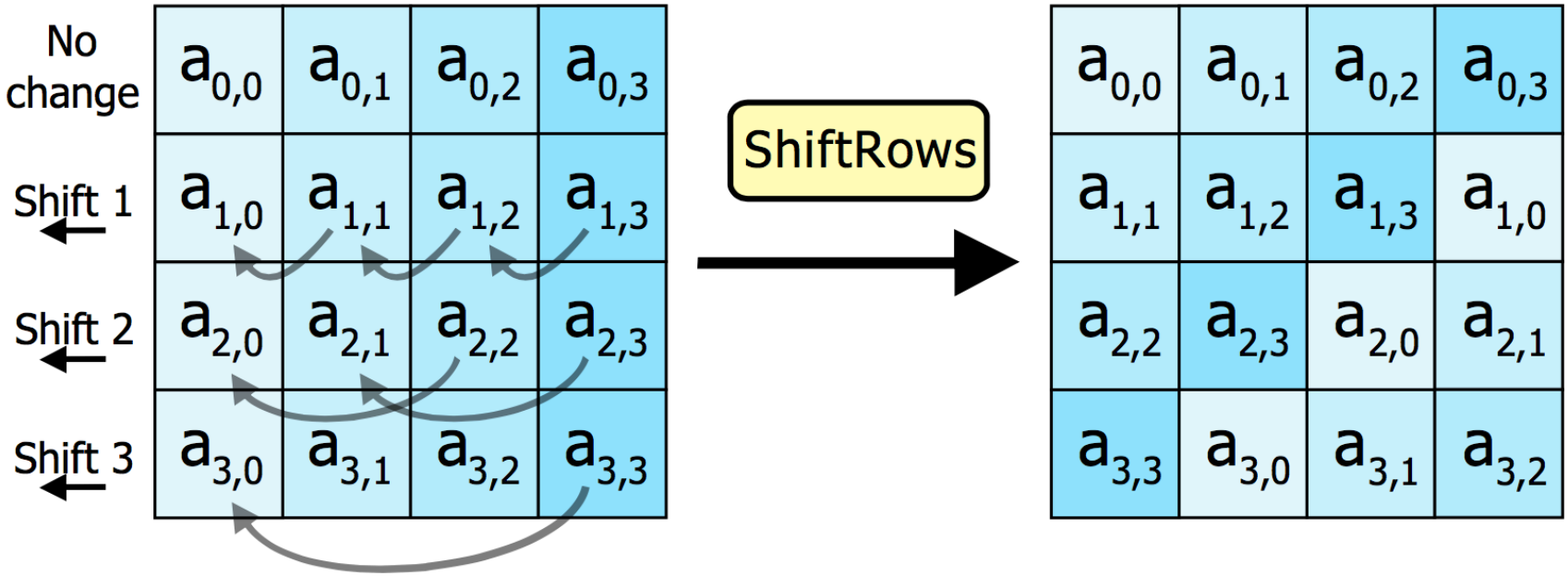
Last 4 bits of input

First 4 bits of input

	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

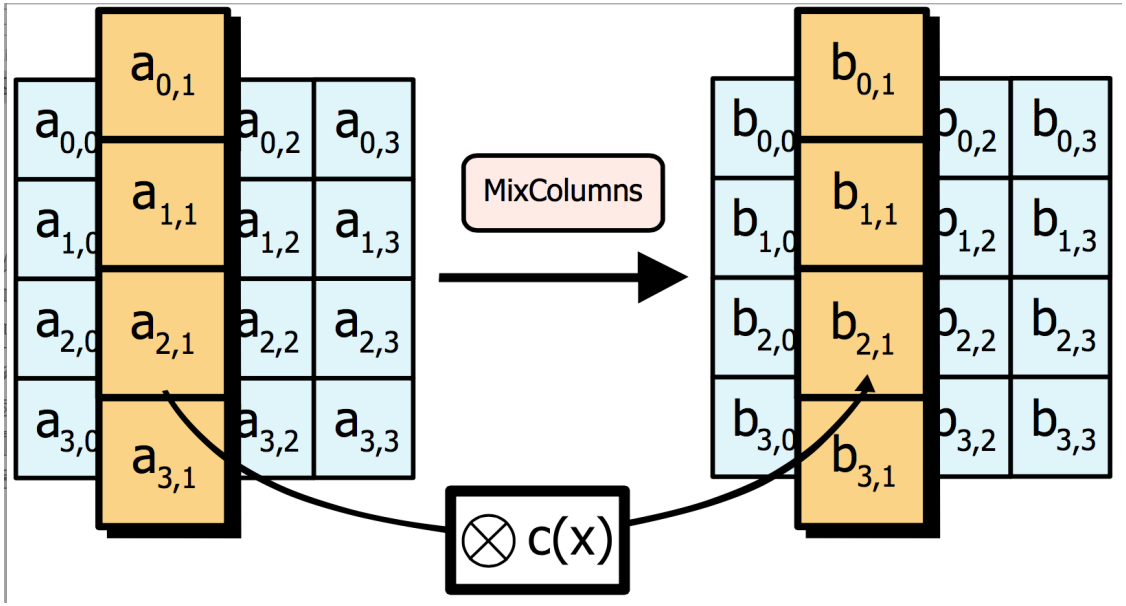
AES ShiftRow

- Cyclic shift rows



AES MixColumn

- Invertible, linear operation to each column



- Implemented as a (big) lookup table

AES Security

- No known practical attacks that can read correctly implemented AES encrypted data.
- Key-recovery attack (2011)
  - for AES-128
    - takes billions of years ($2^{126.1}$)
    - needs 2^{88} bits of data (38 trillion terabytes, more than all the data stored on all the computers on the planet)
  - $2^{189.7}$ for AES-192, $2^{254.4}$ for AES-256
- Key-distinguishing attack on 8-round AES=128
  - takes 2^{48} operations, 2^{32} memory complexity