



AES

Advanced Encryption Standard



Inhalt

Entstehung

Eigenschaften

Funktionsweise

Erzeugung Rundenschlüssel



ENTSTEHUNG

Advanced Encryption Standard



Entwickelt von zwei belgischen Kryptographen,
Vincent Rijmen und Joan Daemen

Oktober 2000 ausgewählt nach Wettbewerb um
DES (Data Encryption Standard) Ablösung

Beruhrt auf Rijndael Block Cipher, wurde aber
leicht modifiziert mit fixen Schlüsselgrößen



EIGENSCHAFTEN

Advanced Encryption Standard



Übersicht

- Feste Blockgrösse 128 Bit
- Variable Schlüssellänge von 128 Bit, 192 Bit und 256 Bit – Symmetrisch verschlüsselt
- Variable Anzahl Runden gemäss Schlüssellänge
 - *128 Bit - 10 Runden, 192 Bit – 12 Runden, 256 Bit – 14 Runden*
- Operationen pro Runde
 - *SubByte*
 - *ShiftRow*
 - *MixColumn*
 - *AddRoundKey*
- Geschwindigkeit: Gleichmässig gute Performance über mehrere Plattformen wie z.b. 64-Bit, 32-Bit Prozessoren oder 8-Bit Mikrocontroller
- Speicherbedarf: Sehr geringe RAM- und ROM-Speicher Bedarf. Schlüsselerzeugung kann «on-the-fly» stattfinden. Ideal für Chipkarten.

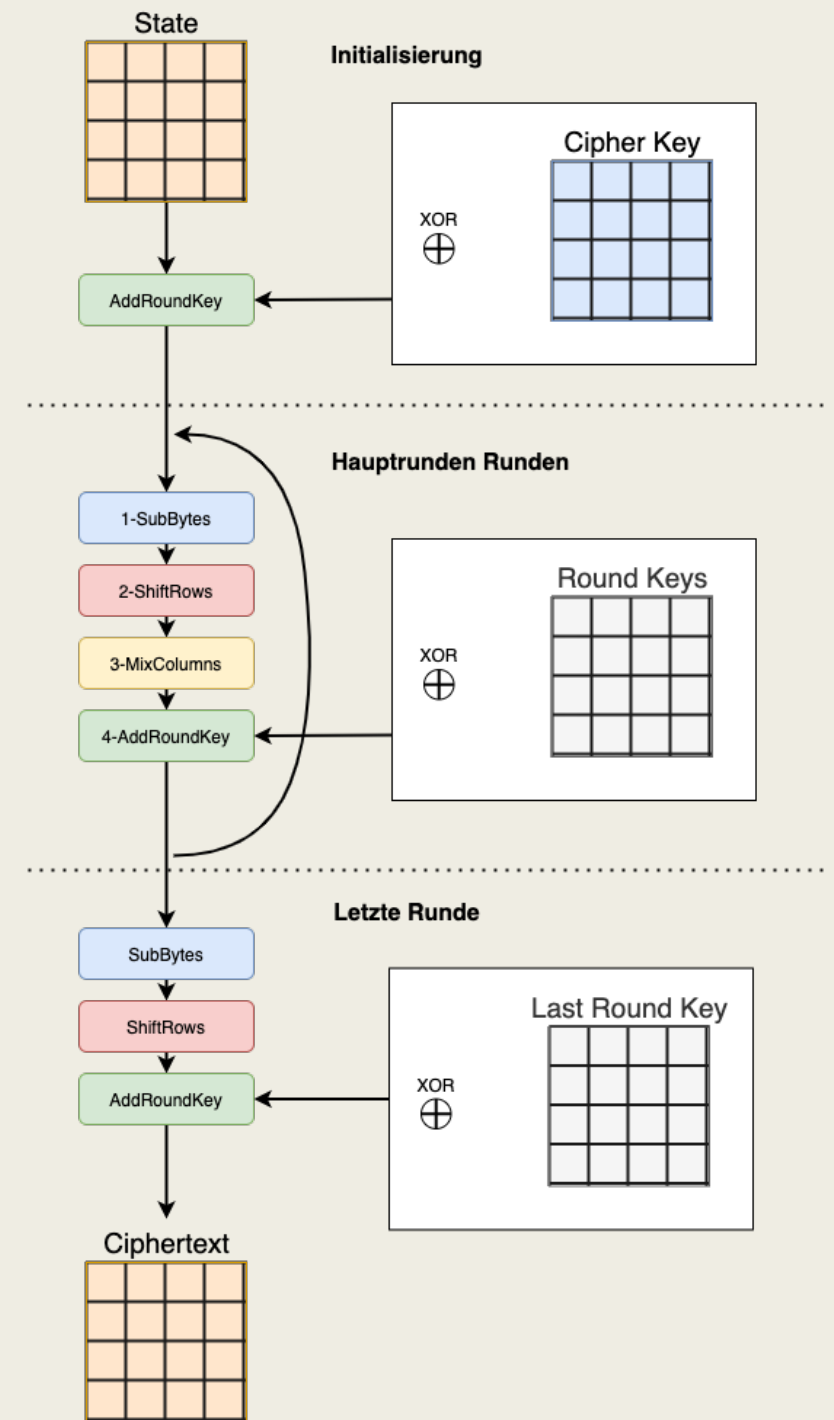
A thick black L-shaped frame is positioned on the left and bottom edges of the slide, framing the central text.

FUNKTIONSWEISE

Advanced Encryption Standard

Übersicht

- Ein 128-Bit Block (State) wird eingelesen
- State wird mit dem Cipher Key XOR-Verknüpft
- Die Operationen SubByte, ShiftRows, MixColumns und AddRoundKey werden gemäss vorgegebener Anzahl Runden durchgeführt
- Der aktuelle State wird erneut XOR-Verknüpft mit dem Round Key
- In der letzten Runde wird die Operation MixColumns ausgelassen
- Die Ausgabe ist ein Ciphertext der mit den selben Cipher Key entschlüsselt werden muss



Beispiel Eingabe

Hexadecimalblock aus
Eingabe in 128 Bit

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

Binärwerte = 8 4 2 1 | 8 4 2 1

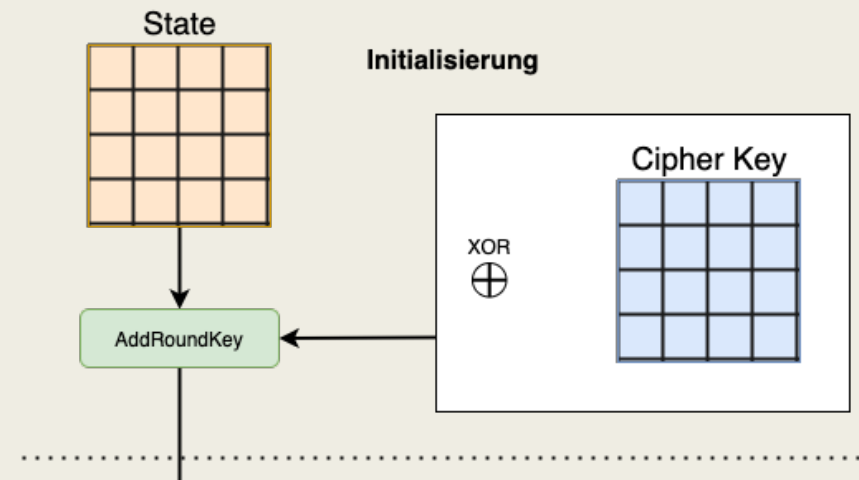
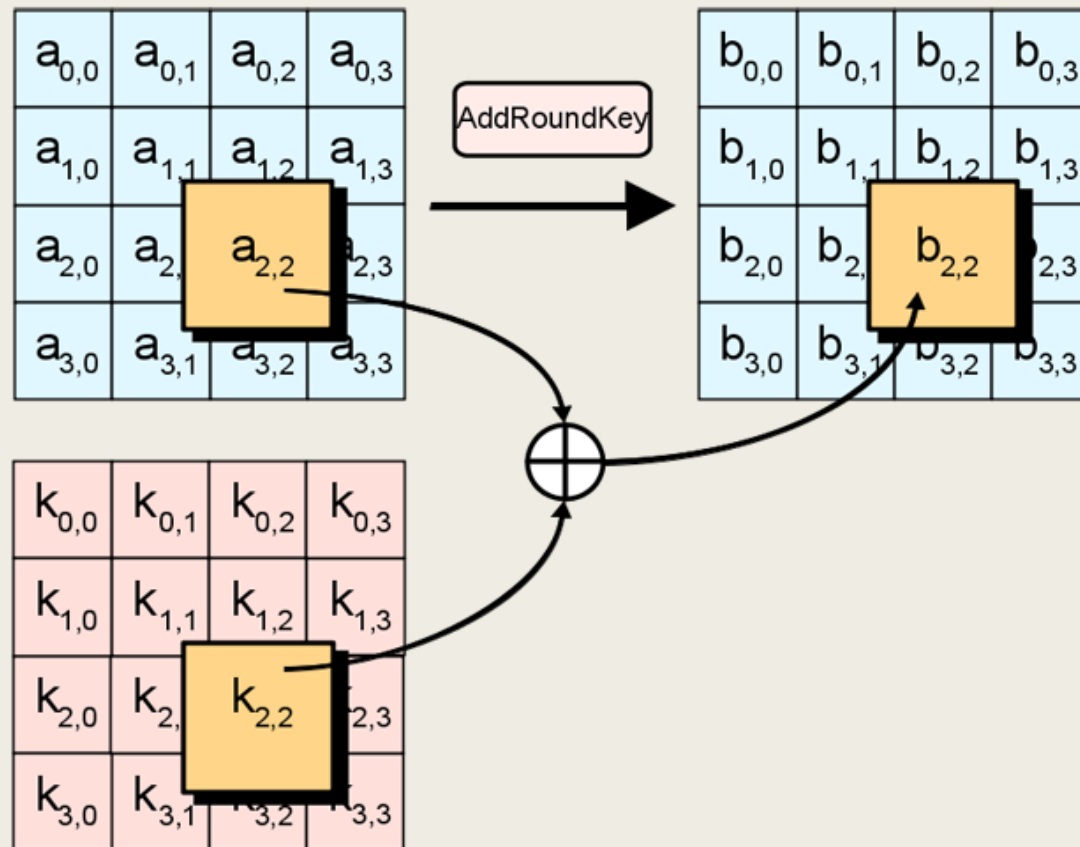
32 = 00110010 ← 1 Byte

3 hex 2 hex

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

AddRoundKey - Initial

- Vor Beginn der Hauptrunden wird die Eingabe mit dem Cipher Key XOR-verknüpft



AddRoundKey - Initial

State

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

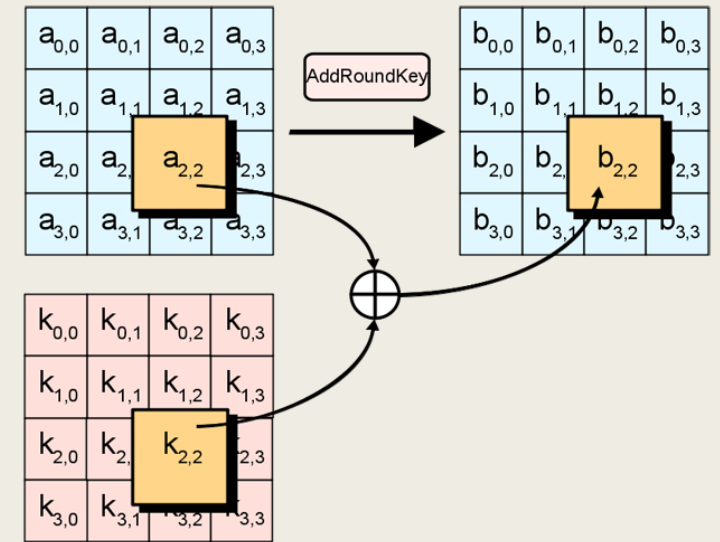
Cipher
Key

2b	28	ab	09
73	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

32 = 00110010

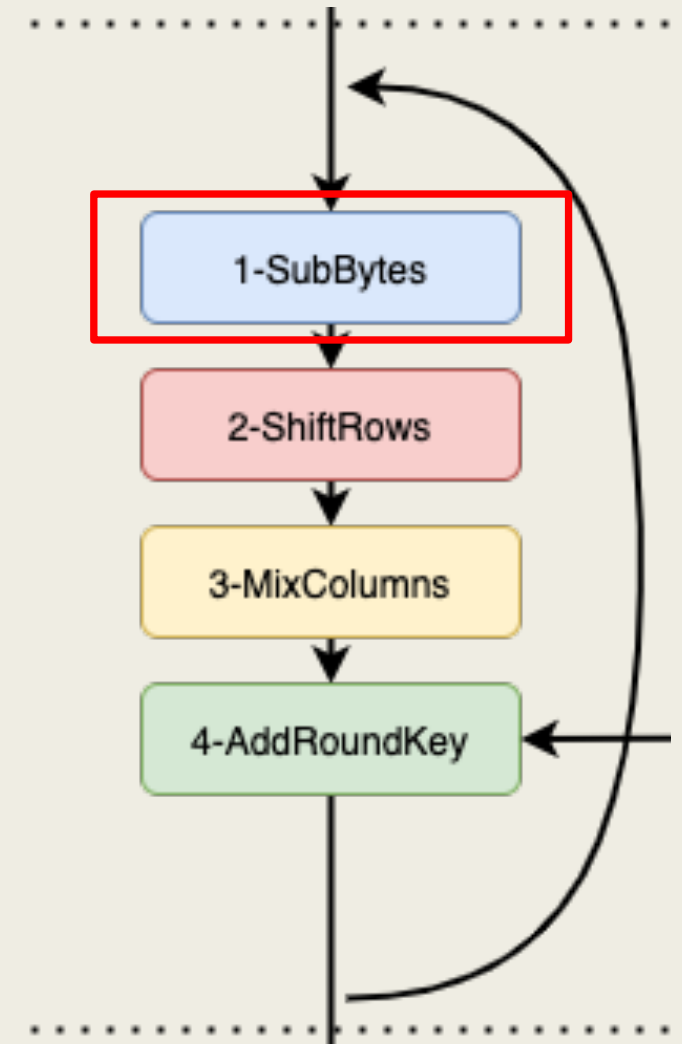
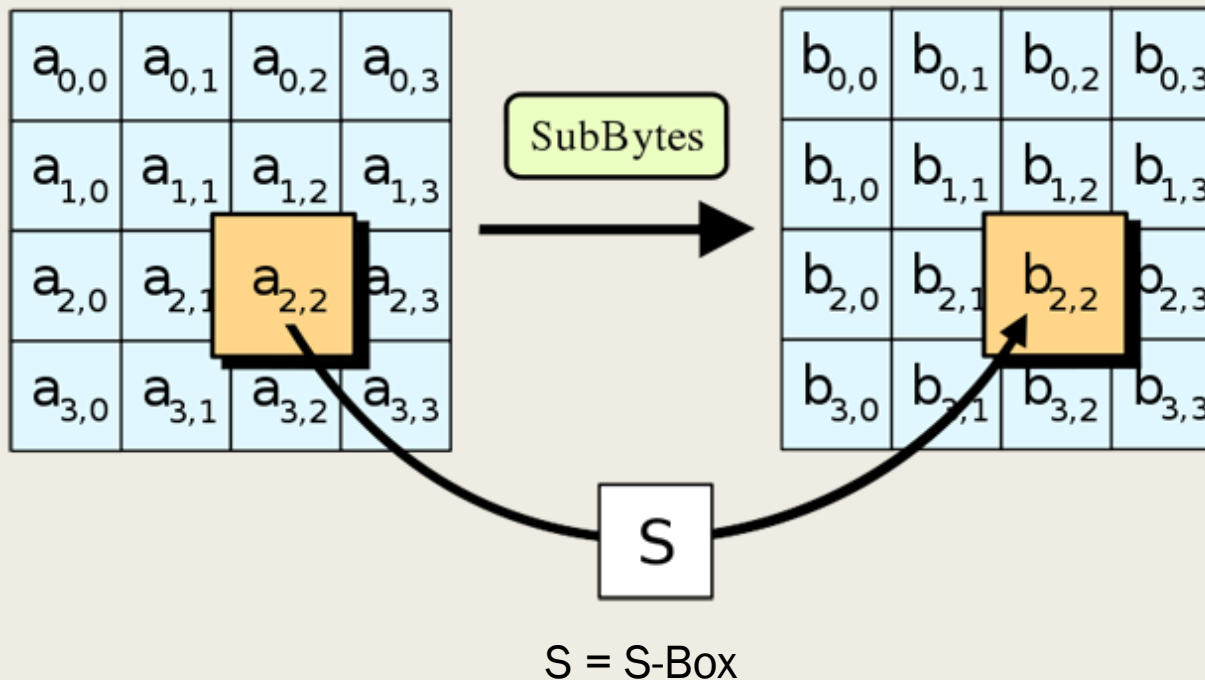
2b = 00101011

\oplus = 00011001 = 19



SubBytes

- State wird durch eine Rijndael S-Box substituiert
- S-Box ist unabhängig von der Eingabe
- Wird in vorberechneter Form verwendet falls genügend Speicher vorhanden ist (256 Bytes)



S-Box

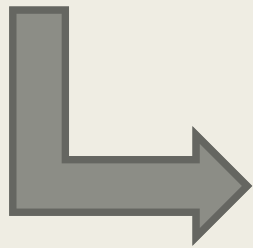
19	→	d4
3d	→	27
e3	→	11
be	→	ae

Hex	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

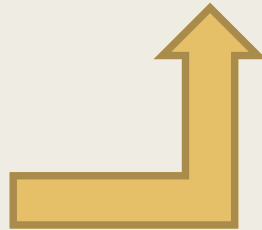
SubBytes

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

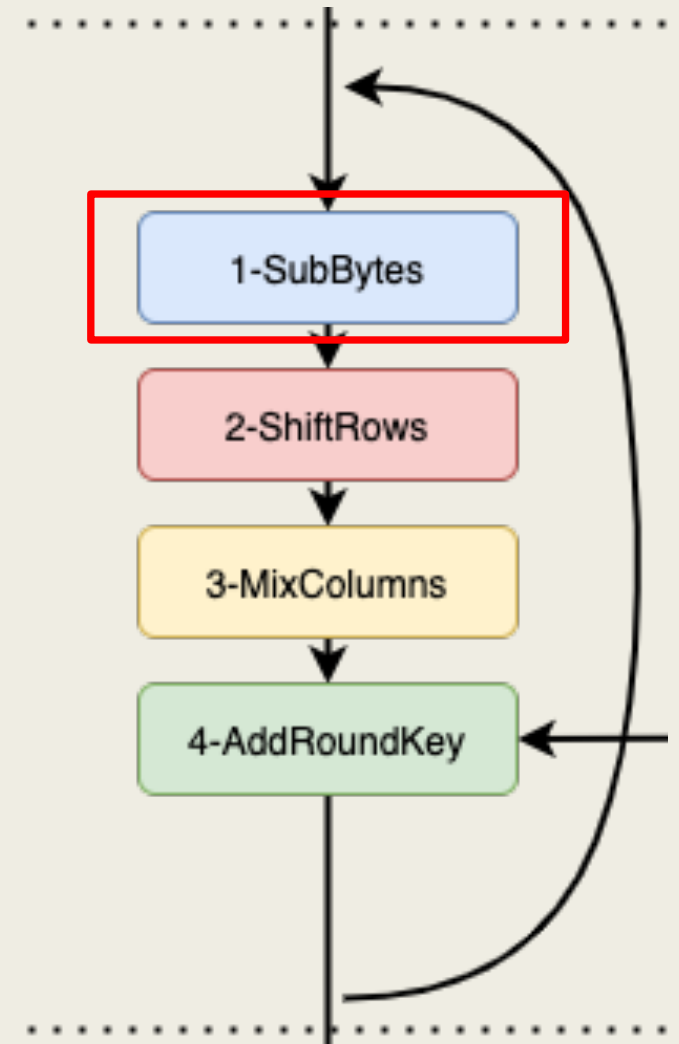
d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30



S-Box

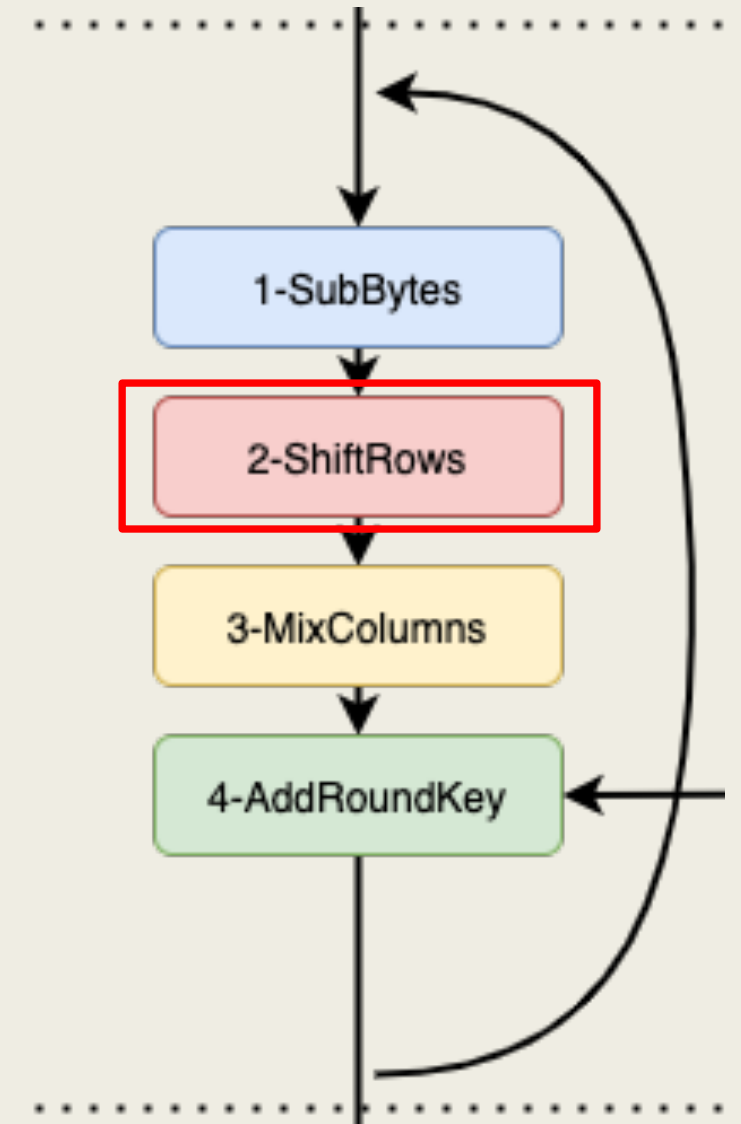
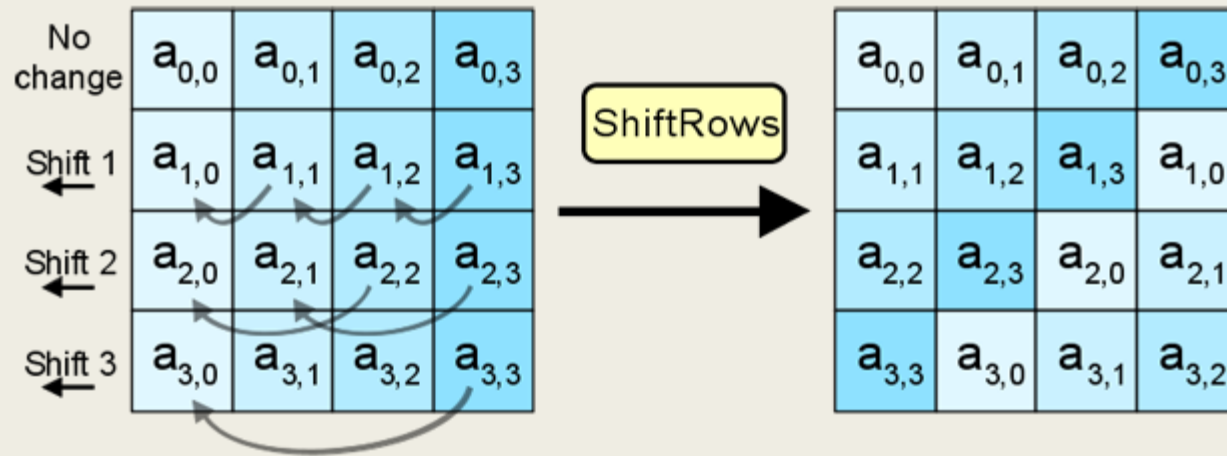


Der neue State wird weitergegeben an ShiftRows.



ShiftRows

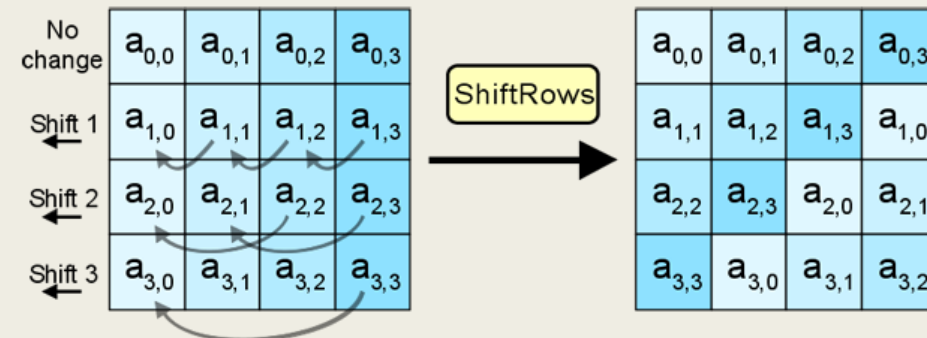
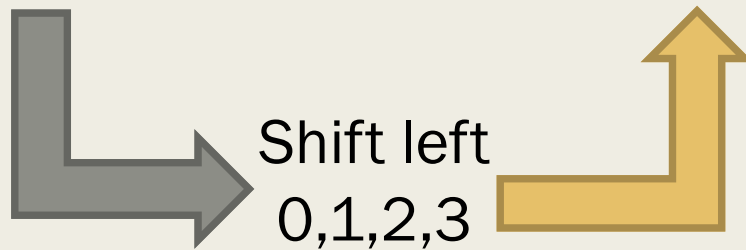
- Jede Zeile des State wird um ihre Zeilennummer nach links verschoben.
- 0, 1, 2, 3 Bytes nach links



ShiftRows

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

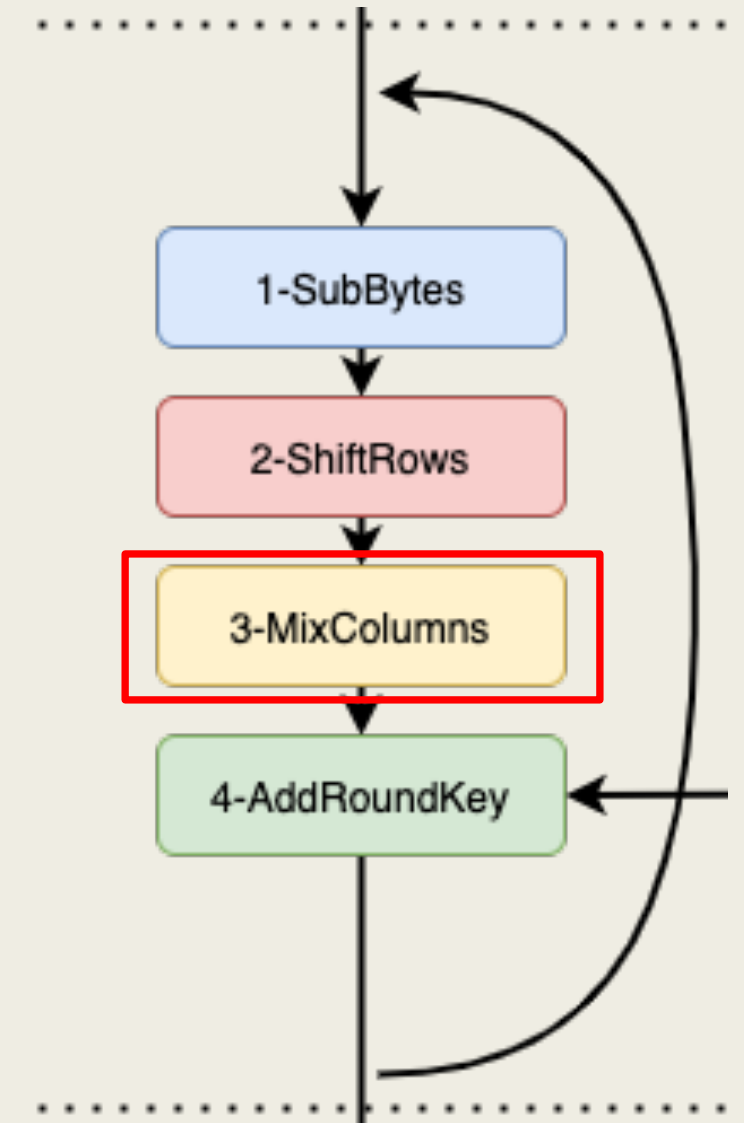
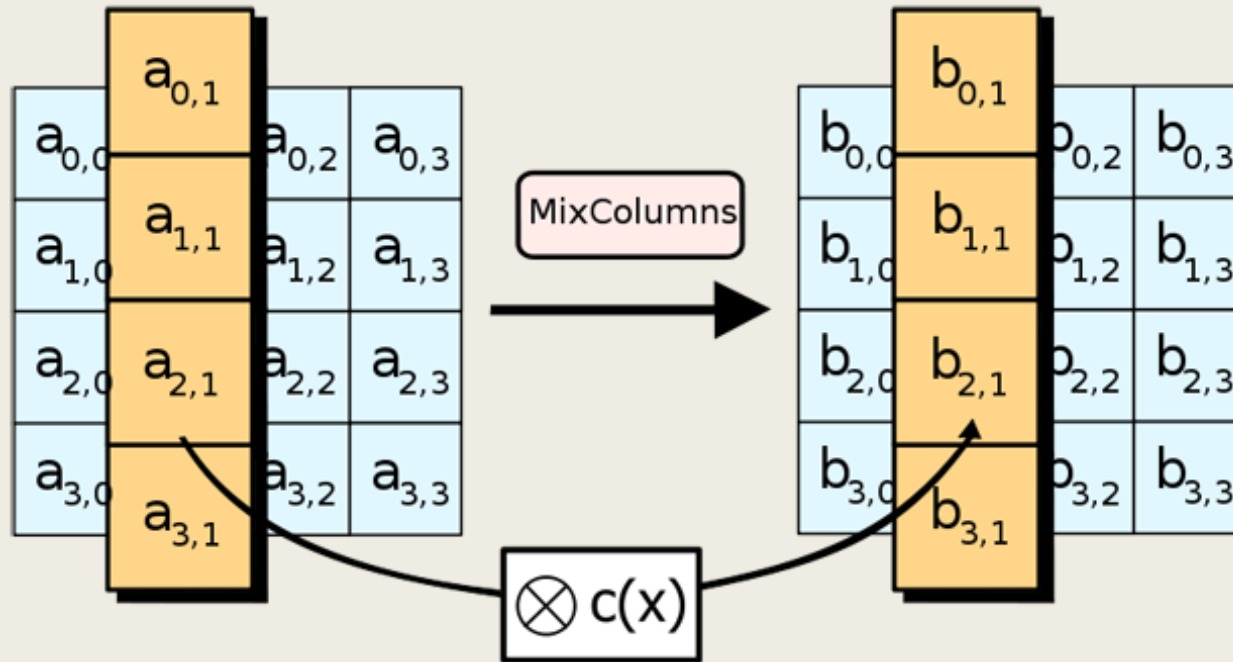
d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5



Der neue State wird weitergegeben an MixColumns.

MixColumns

- Durch die Multiplikation im Galois-Feld $GF(2^8)$
- Dies ist mit Abstand die komplizierteste Operation



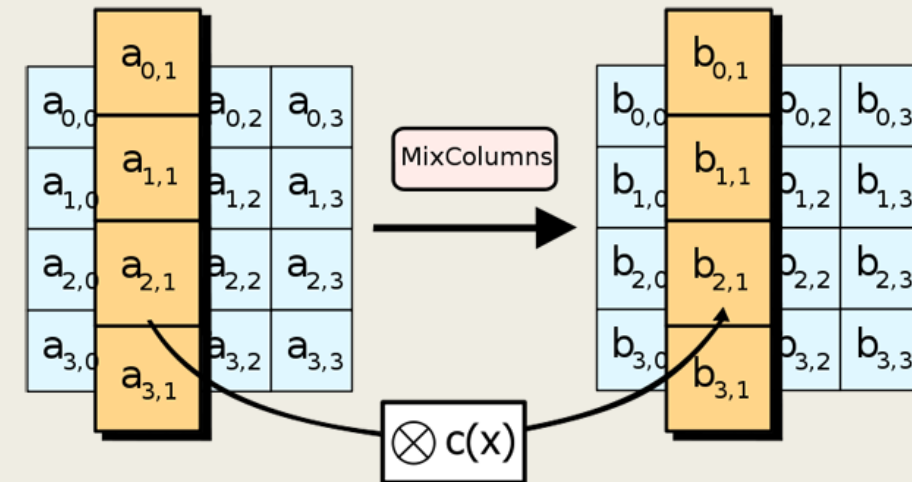
MixColumns

$$b_{0,0} = a_{0,0} * c_{0,0} + a_{0,1} * c_{0,1} + a_{0,2} * c_{0,2} + a_{0,3} * c_{0,3} \\ d4 * 02 + bf * 03 + 5d * 01 + 30 * 01 = 04$$

$$\begin{array}{cccccccc} \text{----- } d4 \text{ -----} & & & & & & & \text{----- } 02 \text{ -----} \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ x^7 & x^6 & & x^4 & & x^2 & & \\ & & & & & & & * \\ & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & & & & & & & & & & & & x & & \\ = & & & & & & & & & & & & & & & \\ & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ & x^8 & x^7 & & x^5 & & x^3 & & & & & & & & \end{array}$$

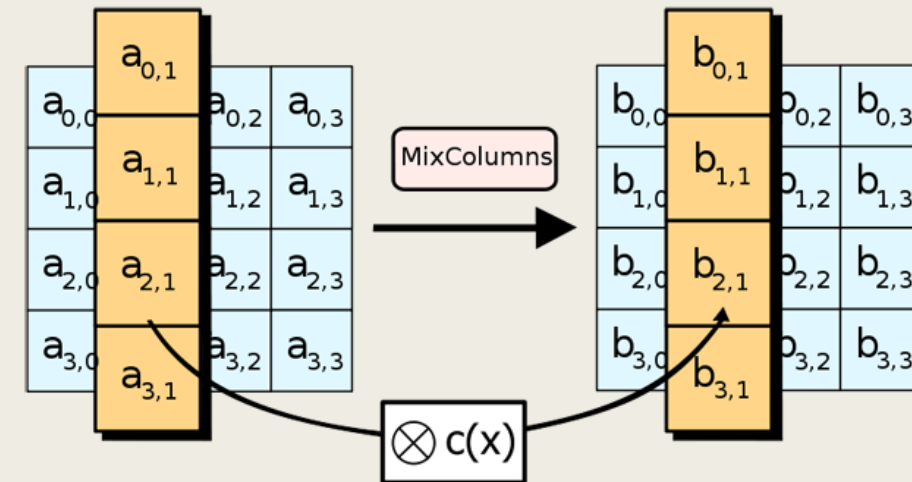
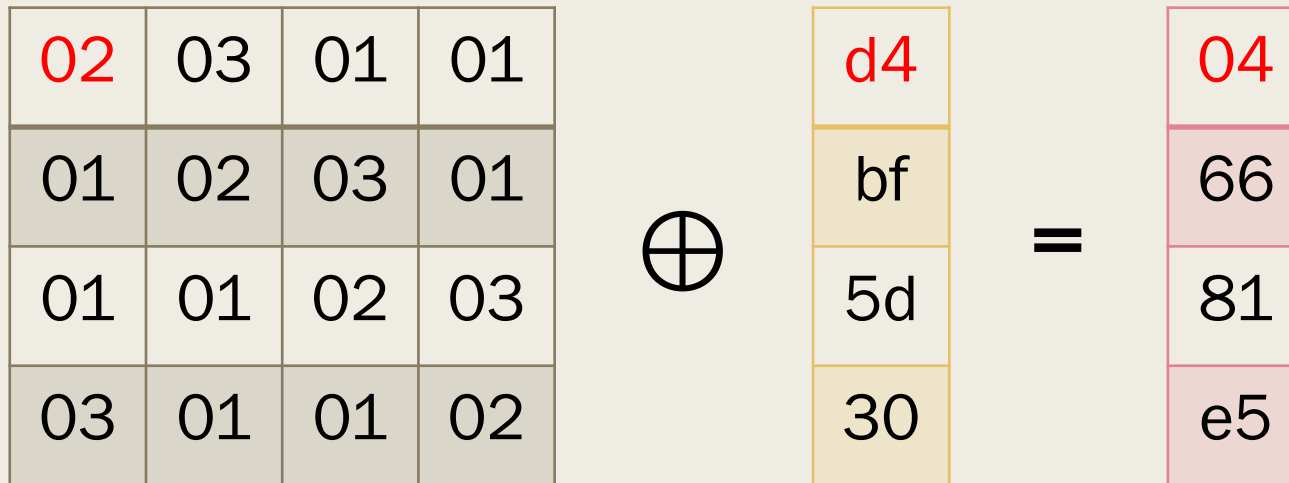
Das Resultat muss reduziert werden da es nun 9 Bit sind.
Division durch ein unreduzierbares Polynom (Primzahl) 8. Grades:
In AES wird dieses Polynom verwendet:
 $x^8 + x^4 + x^3 + x + 1 = \{(01)(1b)\}$

$$\begin{array}{r} 110101000 \\ \oplus \quad 100011011 \\ \hline 010110011 = B3 = d4 * 02 \end{array}$$



MixColumns

- Diese Rechnung wird für jede Position im Block durchgeführt und ergibt anschliessend den neuen State



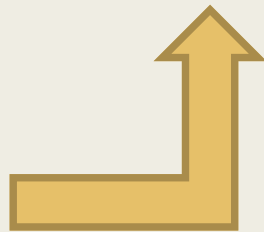
MixColumns

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

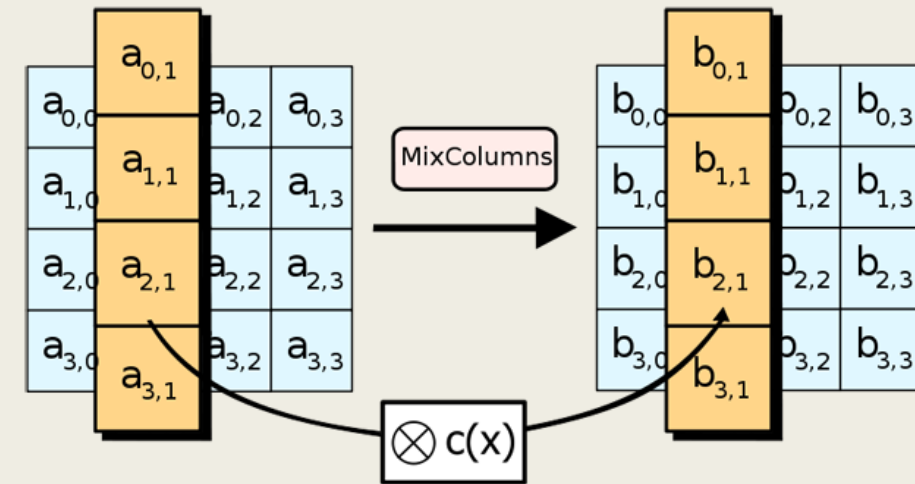
04	e0	48	28
66	cb	f8	06
81	19	d3	24
e5	9a	7a	4c



Mix
 $\text{GF}(2^8)$



Der neue State wird weitergegeben an AddRoundKey.



AddRoundKey – Runde 1

State

04	e0	48	28
66	cb	f8	06
81	19	d3	24
e5	9a	7a	4c

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

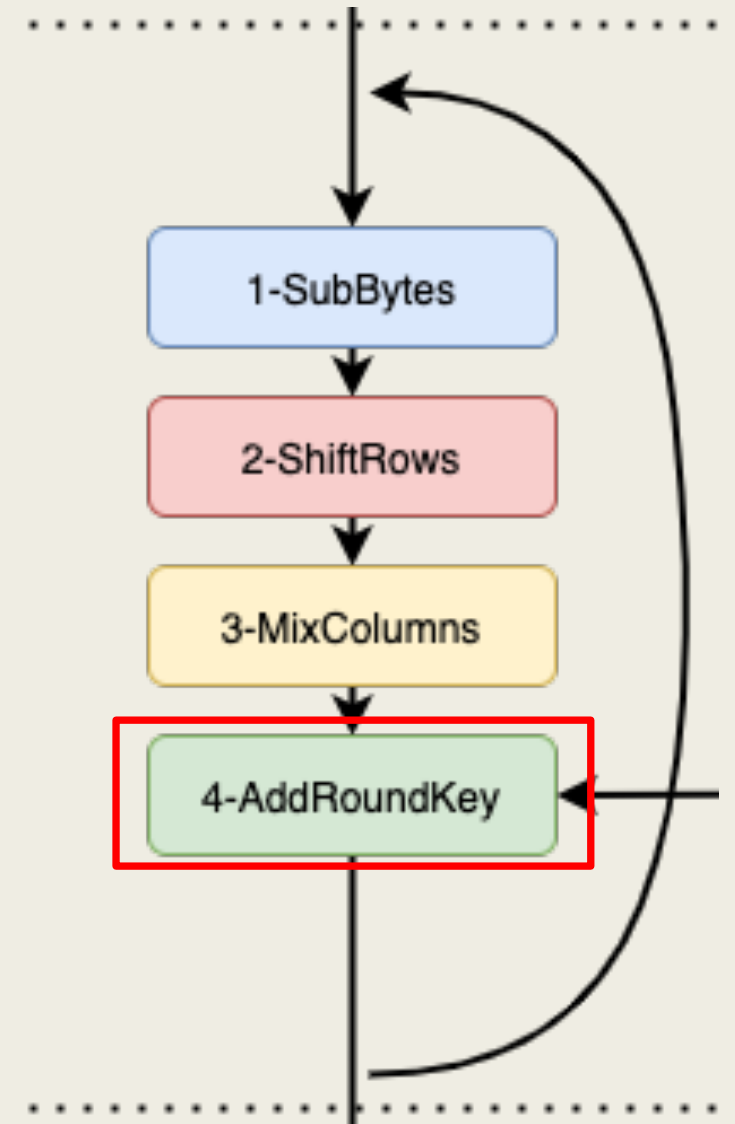
Round
Key 1

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

$$04 = 00000100$$

$$a0 = \underline{10100000}$$

$$\oplus = 10100100 = a4$$

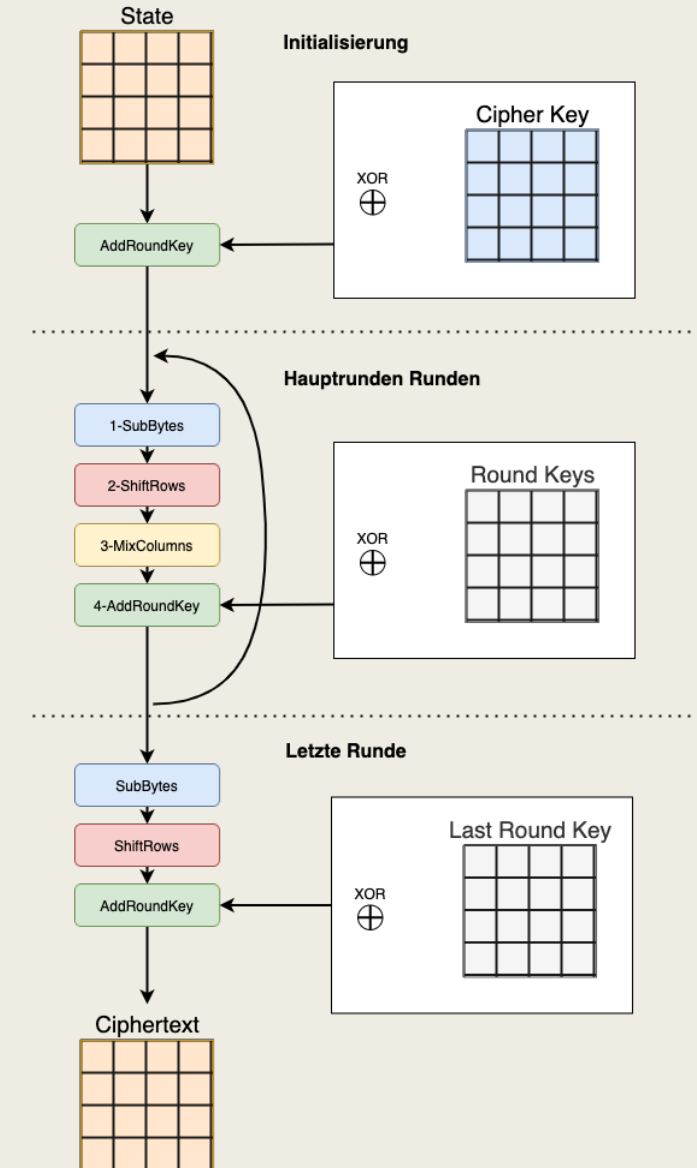


Runde 2 - 10

- Die Operationen SubBytes, ShiftRows, MixColumns und AddRoundKey werden bis zur 9. Runde wiederholt
- In der 10. Runde wird MixColumns ausgelassen

39	02	dc	19
25	dc	11	6a
84	09	85	0b
1d	fb	97	32

Ciphertext nach der 10. Runde

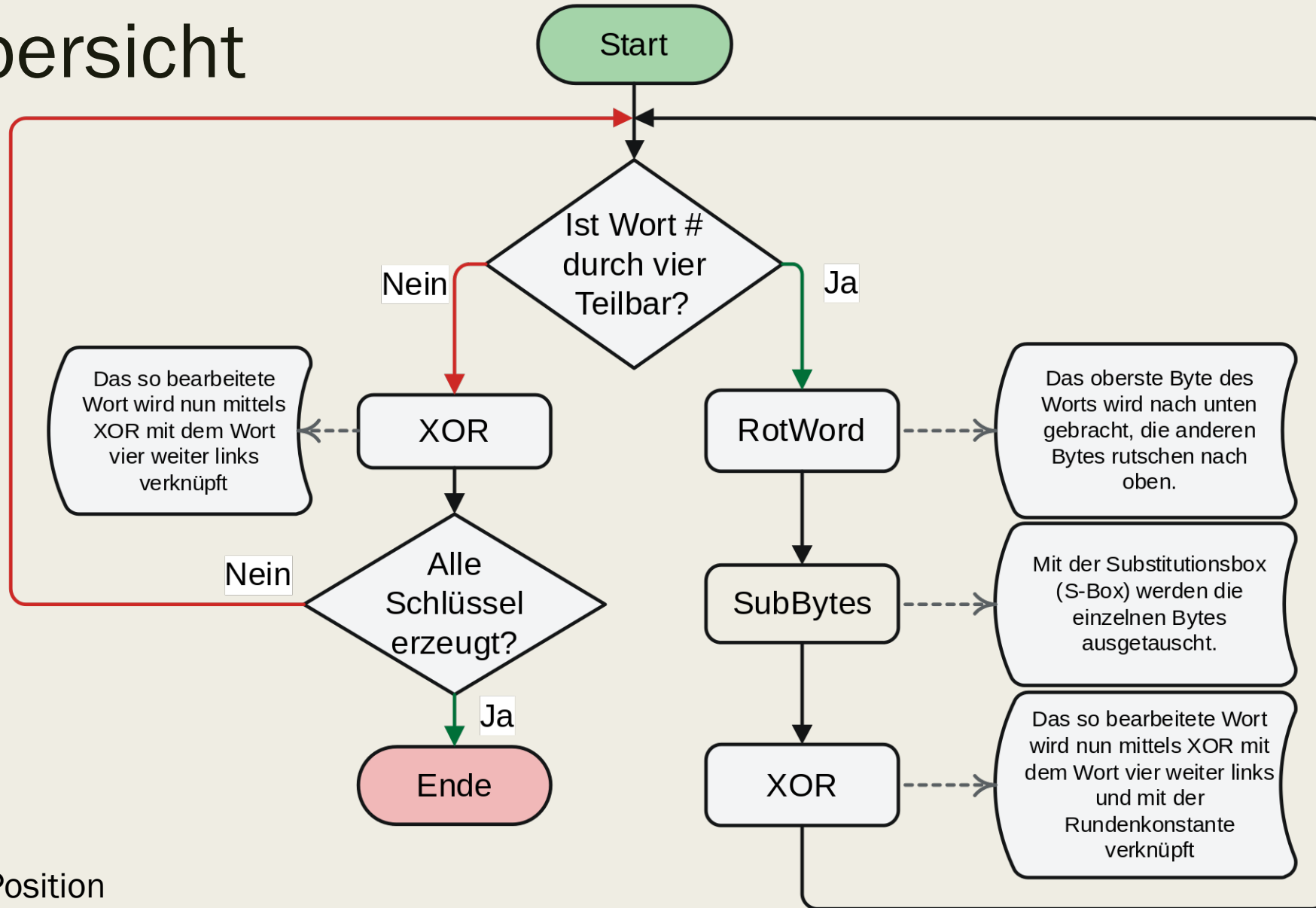


A thick black L-shaped frame surrounds the text. It starts at the top left, goes right, then down, then right again at the bottom.

ERZEUGUNG RUNDENSCHLÜSSEL

Advanced Encryption Standard

Übersicht

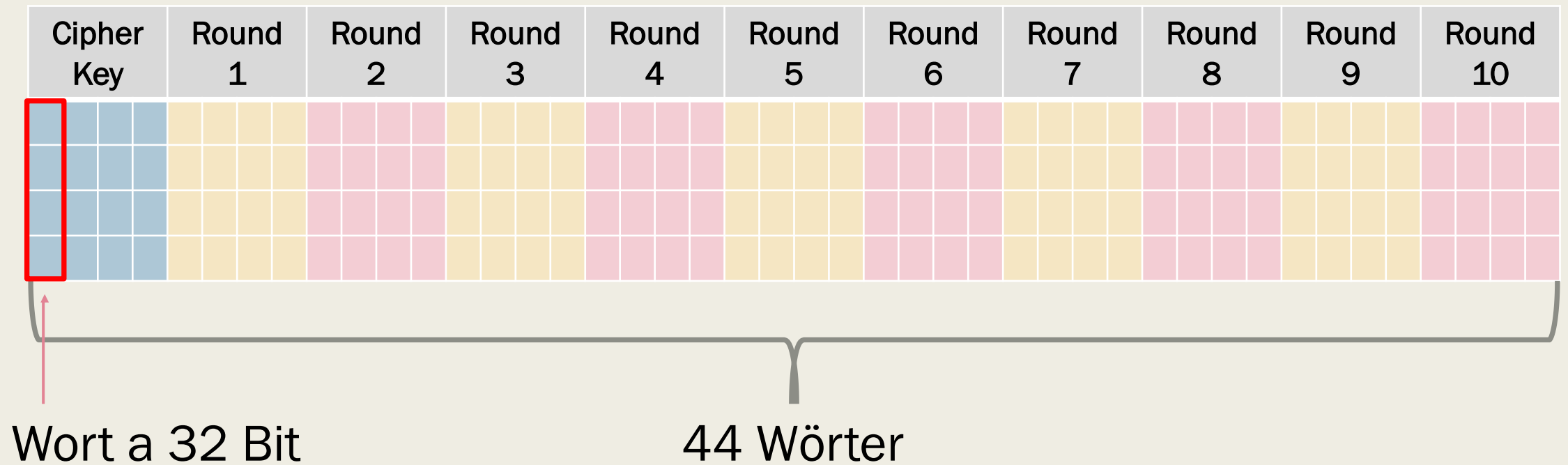


= Position

Erweiterung des Cipher Key

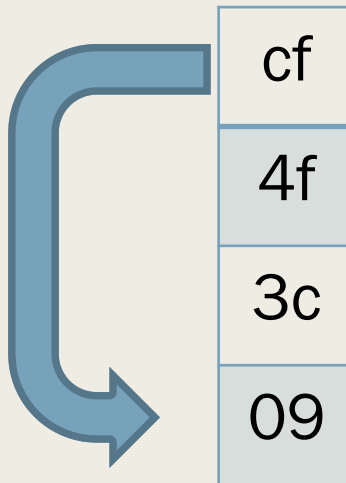
- Im Fall 128 Bit werden 11 Key verwendet
 - *Initial mit dem Cipher Key*
 - *10 weiter in Runden*
- Der erweiterte Key kann als Array von 44 Wörter (0-43) a 32 Bit angesehen werden. Wobei die ersten 4 der Cipher Key sind.
- Wörter die sich im Array an einer Position (#) befinden die durch 4 Teilbar ist, werden neu berechnet. Das vorangehende Wort wird mit folgenden Operationen umgeformt:
 - *RotWord, der Wert an erster Stelle wird an den Schluss gesetzt*
 - *SubBytes, das neue Wort wird durch die S-Box substituiert*
 - *Rcon, Wort vor 4 Positionen und eine Rundenkonstante wird via XOR hinzugefügt*

Erweiterung des Cipher Key



RotWord

2b	28	ab	09
73	ae	f7	cf
15	d2	15	4f
16	a6	88	3c



RotWord

S-Box

cf	→	8a
4f	→	84
3c	→	eb
09	→	01

Hex	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Rcon

2b	28	ab	09
73	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

a0			
fa			
fe			
17			

Rcon - Roundconstants

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

2b
73
15
16



8a
84
eb
01



01
00
00
00

=

a0
fa
fe
17

Wort vor
4 Positionen

S-Box

Rcon

$$\begin{aligned}
 2b &= 00101011 \\
 8a &= \underline{10001010} \\
 \oplus & \quad 10100001 \\
 01 &= \underline{00000001} \\
 \oplus & \quad 10100000 = a0
 \end{aligned}$$

Restliche 32 Bit Wörter des 1. Round Key

2b	28	ab	09
73	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

9 weitere Runden
angefangen bei
RotWord

d0	c9	e1	b6
14	ee	3f	63
f9	25	0c	0c
a8	89	c8	a6

28
ae
d2
a6



a0
fa
fe
17

=

88
54
2c
b1

ab
f7
15
88



88
54
2c
b1

=

23
a3
39
39

09
cf
4f
3c



23
a3
39
39

=

2a
6c
76
05

Wort vor
4 Positionen

Wort vor
4 Positionen

Wort vor
4 Positionen