

AES-Verschlüsselung

Advanced Encryption Standard

AES Verfahren

- Symmetrisches Verfahren:
 - Gleicher Schlüssel für Verschlüsselung und Entschlüsselung
- Verbreitet z.B. zur Sicherung von Daten
- Blockverschlüsselung:
 - Verarbeitet Daten in Blöcken fester Größe (128 Bit)

Verschlüsselungsprozess: AddRoundKey

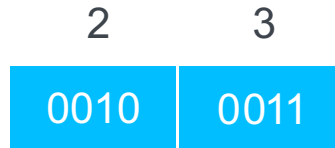
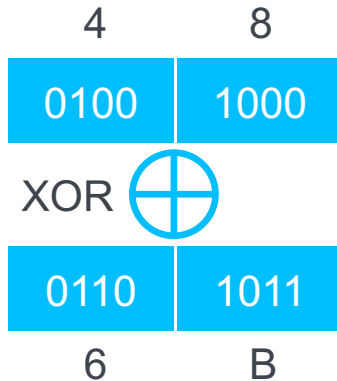
AddRoundKey

Block

48				6C	6C
				7C	20
61	73	20	69		
73	74	20	65		

Schlüssel

6B				6A	64
				7	75
3B	68	38	39		
51	60	6F	2C		



23				06	08
				55	5F
5A	1B	18	50		
22	14	4F	49		

Verschlüsselungsprozess: SubBytes

SubBytes

Text

→

23	00	06	08
1C	4B	55	5F
5A	1B	18	50
22	14	4F	49

→

26	63	6F	30
9C	B3	FC	CF
BE	AF	AD	53
93	FA	84	3B

	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	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
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

Verschlüsselungsprozess: ShiftRows

ShiftRows

26	63	6F	30
9C	B3	FC	CF
BE	AF	AD	53
93	FA	84	3B

← um 1 verschieben

← um 2 verschieben

← um 3 verschieben



Verschlüsselungsprozess: MixColumns

MixColumns

26	63	6F	30
B3	FC	CF	9C
AD	53	BE	AF
3B	93	FA	84

2	3	1	1	26
1	2	3	1	B3
1	1	2	3	AD
3	1	1	2	3B

Umwandlung in
Potenzen von x

2	26	⊕	3	B3	⊕	1	AD	⊕	1	3B
0010	0010	0110								
x	x ⁵ + x ² + x									
	x ⁶ + x ³ + x ²									
	0100 1100									

x ⁷	x ⁶	x ⁵	x ⁴	x ³	x ²	x ¹ (=x)	x ⁰ (=1)	
				0	0	1	0	2
0	0	1	0	0	1	1	0	26

Verschlüsselungsprozess: MixColumns

MixColumns

26	63	6F	30
B3	FC	CF	9C
AD	53	BE	AF
3B	93	FA	84

2	3	1	1	26
1	2	3	1	B3
1	1	2	3	AD
3	1	1	2	3B

x^7	x^6	x^5	x^4	x^3	x^2	$x^1 (=x)$	$x^0 (=1)$	
				0	0	1	0	2
0	0	1	0	0	1	1	0	26
				0	0	1	1	3
1	0	1	1	0	0	1	1	B3

2	26	⊕	3	B3	⊕	1	AD	⊕	1	3B
0010	0010 0110		0011	1011 0011						
x	$x^5 + x^2 + x$		x + 1	$x^7 + x^5 + x^4 + x + 1$						
$x^6 + x^3 + x^2$			$x^8 + x^6 + x^5 + x^2 + x + x^7 + x^5 + x^4 + x + 1$							
0100 1100			1100 1110							

Verschlüsselungsprozess: MixColumns

MixColumns

26	63	6F	30
B3	FC	CF	9C
AD	53	BE	AF
3B	93	FA	84

2	3	1	1	26
1	2	3	1	B3
1	1	2	3	AD
3	1	1	2	3B

x^7	x^6	x^5	x^4	x^3	x^2	$x^1 (=x)$	$x^0 (=1)$	
				0	0	1	0	2
0	0	1	0	0	1	1	0	26
				0	0	1	1	3
1	0	1	1	0	0	1	1	B3

2	26	⊕	3	B3	⊕	1	AD	⊕	1	3B
0010	0010 0110		0011	1011 0011		0001	1010 1101		0001	0011 1011
x	$x^5 + x^2 + x$		$x + 1$	$x^7 + x^5 + x^4 + x + 1$						
	$x^6 + x^3 + x^2$			$x^7 + x^6 + x^3 + x^2 + x$						
	0100 1100	⊕		1100 1110	⊕		1010 1101	⊕		0011 1011

Jedes Byte der Spalte hat
Einfluss auf jedes Byte der
transformierten Spalte

Verschlüsselungsprozess: MixColumns

MixColumns

26	63	6F	30
B3	FC	CF	9C
AD	53	BE	AF
3B	93	FA	84

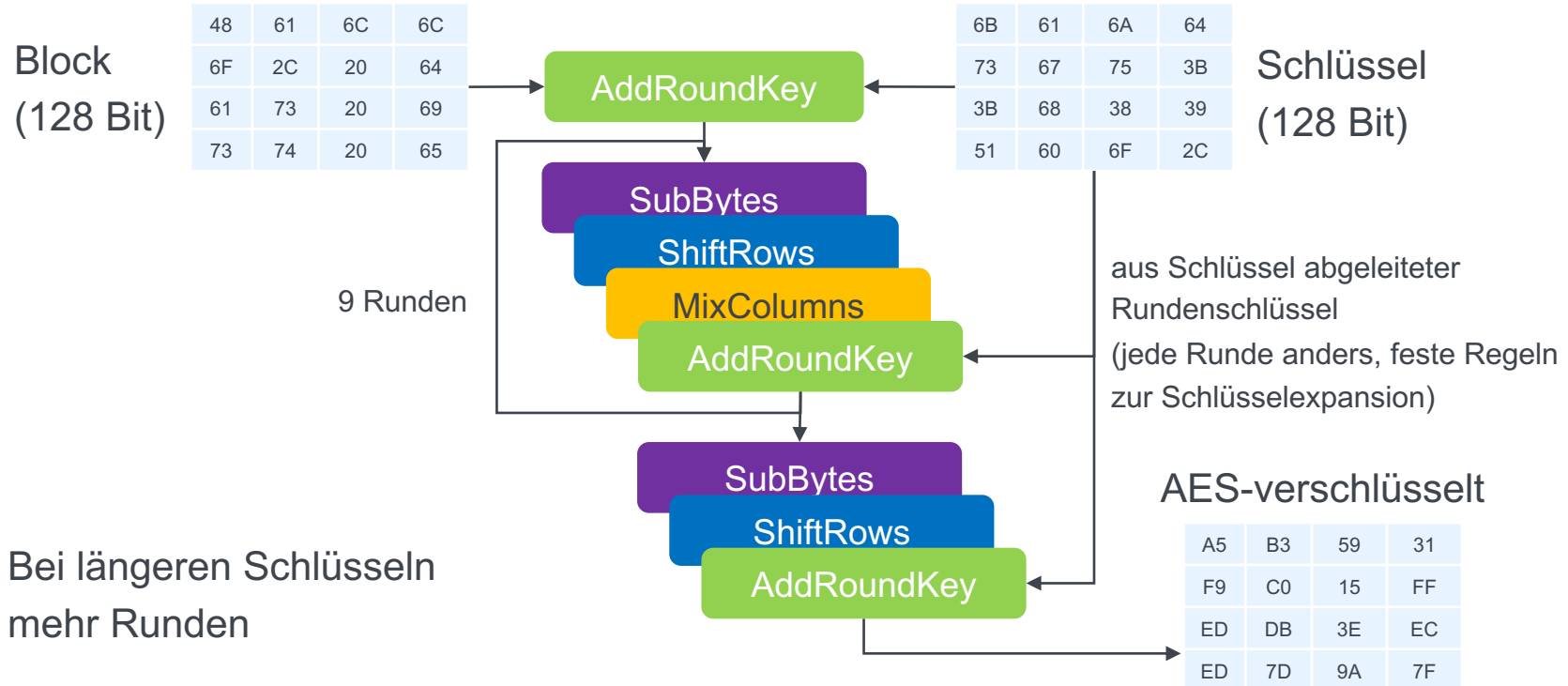
14	19	D0	F4
8C	E6	C9	7D
99	97	D2	7E
02	37	2F	70

$$\begin{array}{r}
 \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \\
 0100 \ 1100 \\
 \oplus 1100 \ 1110 \\
 \oplus 1010 \ 1101 \\
 \oplus 0011 \ 1011 \\
 = 0001 \ 0100 \\
 = 14
 \end{array}$$

26	63	6F	30
B3	FC	CF	9C
AD	53	BE	AF
3B	93	FA	84

2	3	1	1	26
1	2	3	1	B3
1	1	2	3	AD
3	1	1	2	3B

Der komplette Ablauf bei AES



Entschlüsselung bei AES

Symmetrisches
Verfahren

- Funktioniert mit demselben Schlüssel
- Alles rückwärts in umgekehrter Reihenfolge
- Mit inversen Matrizen bzw. umgekehrter Tabelle für SubBytes
- Beginnend mit dem letzten Rundenschlüssel statt dem ersten

Bei der Verschlüsselung nach dem AES-Verfahren werden die Daten blockweise in mehreren Runden mit jeweils mehreren Strategien so verschlüsselt, dass der Zusammenhang zwischen Klartext und Geheimtext besonders geschickt verschleiert wird.

**AES steht für
Advanced Encryption Standard.**

Das AES-Verfahren ist umkehrbar: zur Entschlüsselung reicht es, den Schlüssel zu kennen, der für die Verschlüsselung verwendet wurde.

Die Verschlüsselung und die Entschlüsselung erfolgen also mit ein und demselben Schlüssel. Man bezeichnet solche Verfahren als symmetrische Verfahren.

Bewertung

- Aktuell noch sicheres Verfahren
- Durch (effizientes) Ausprobieren knackbar, aber aktuell noch nicht in realistischer Zeit

Dr. Antje Schweitzer

Universität Stuttgart
Institut für Maschinelle Sprachverarbeitung



Universität Stuttgart

Institut für Maschinelle Sprachverarbeitung
Institut für Software Engineering



Industrie- und Handelskammer
Reutlingen

Reutlingen | Tübingen | Zollernalb



Region Stuttgart



Industrie- und Handelskammer
Karlsruhe



Lizenzbestimmungen

“AES-Verschlüsselung” von Antje Schweitzer, KI B³ / Uni Stuttgart

Das Werk - mit Ausnahme der folgenden Elemente:

- Logos der Verbundpartner und des Förderprogramms
- im Quellenverzeichnis aufgeführte Medien

ist lizenziert unter:

  [CC BY 4.0 \(https://creativecommons.org/licenses/by/4.0/deed.de\)](https://creativecommons.org/licenses/by/4.0/deed.de)

(Namensnennung 4.0 International)

Quellenverzeichnis

Titelfoto: [Markus Spiske \(https://unsplash.com/de/@markusspiske\)](https://unsplash.com/de/@markusspiske), ohne Titel, auf [Unsplash \(https://unsplash.com/de/fotos/matrix-film-standbild-iar-afB0QQw\)](https://unsplash.com/de/fotos/matrix-film-standbild-iar-afB0QQw), lizenziert unter [Unsplash-Lizenz \(https://unsplash.com/license\)](https://unsplash.com/license). Bildausschnitt verändert.