Betriebssysteme und Sicherheit

Symmetrische Kryptographie

WS 2012/2012

Dr.-Ing. Elke Franz
Elke.Franz@tu-dresden.de

Überblick

1 Einführung

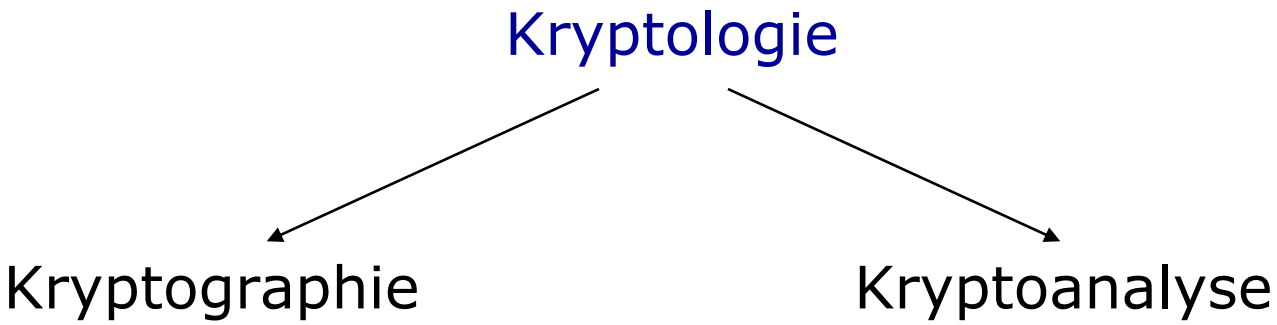
2 Erreichbare Schutzziele

3 Prinzip symmetrischer Systeme

4 Anmerkungen zur Sicherheit

Beispiel: Vernam-Chiffre

5 Beispiel: AES



Kryptographie (griech. „kryptos“+ „graphein“)

Wissenschaft von den Methoden der Ver- und Entschlüsselung von Informationen.

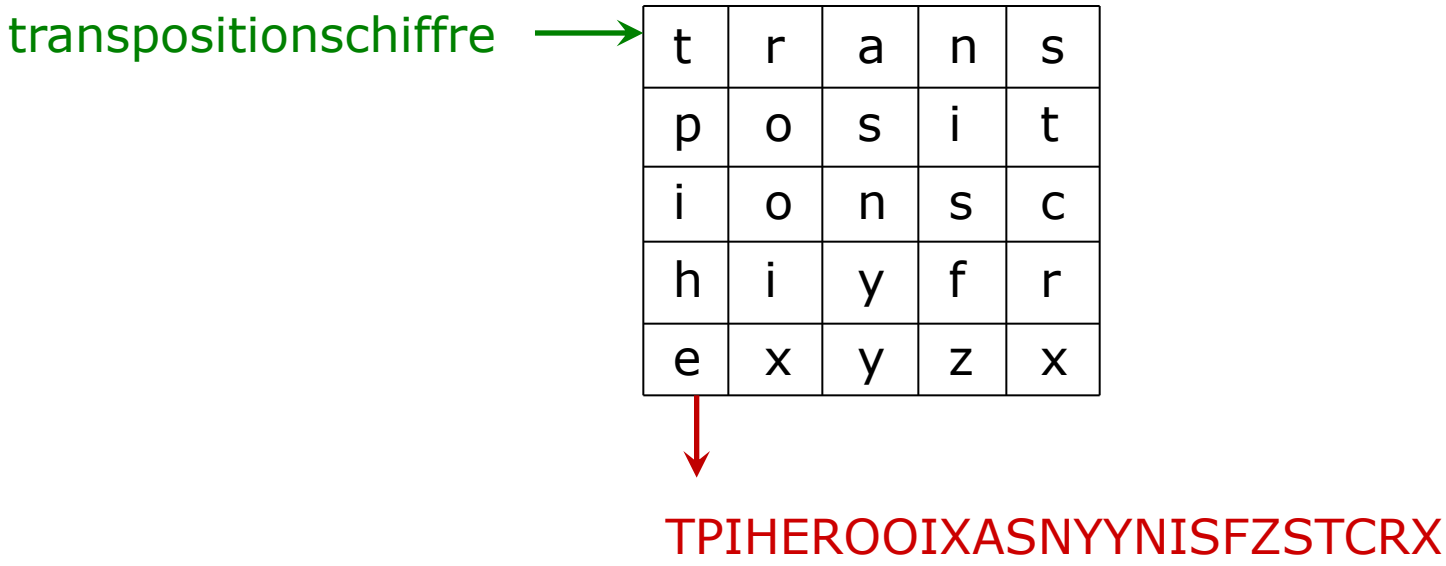
Kryptoanalyse (griech. „kryptos“+ „analyein“)

Wissenschaft vom Entschlüsseln von Nachrichten ohne Kenntnis dazu notwendiger geheimer Informationen.

Historische Verfahren

- Transpositionen
  Verwürfeln der Klartextzeichen, Permutation der Stellen des Klartextes (Permutationschiffren)

Beispiel: Skytala (Matrixtransposition)



Historische Verfahren

- MM-Substitutionen (monoalphabetisch, monographisch)

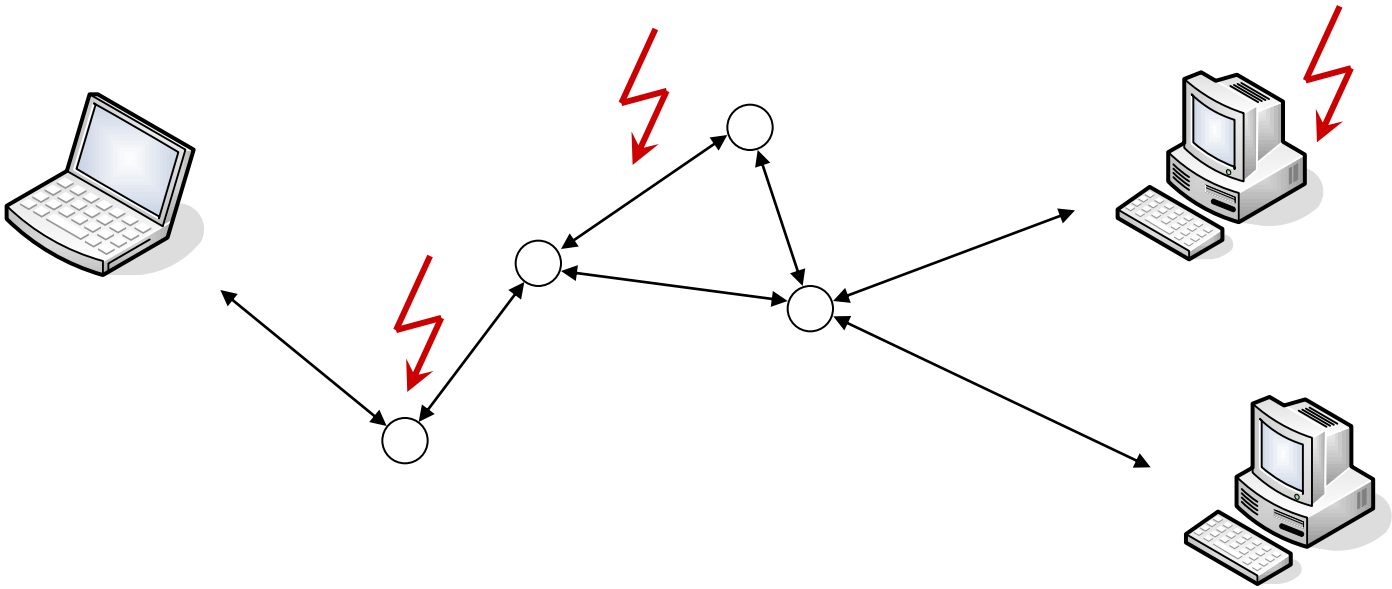
  Beispiel: Cäsarchiffre

Nachricht	a	b	c	d	e	f	g		…		x	y	z
Schlüsseltext	D	E	F	G	H	I	J		…		A	B	C

b e i s p i e l ⟶ E H L V S L H O

- PM-Substitutionen (polyalphabetisch, monographisch)
  Beispiel: Vigenère-Chiffre

Mögliche Bedrohungen durch Angriffe



- Unbefugte Kenntnisnahme der Informationen
- Verfälschen von Informationen (bei Nachrichten auch von deren Absendern)
- Stören der Verfügbarkeit

Unterteilung der Schutzziele

	Inhalte	**Umstände**
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

Mittels Kryptographie erreichbare Schutzziele

- **Vertraulichkeit**
  Informationen werden nur Berechtigten bekannt.

- **Integrität**
  Informationen können nicht unerkannt modifiziert werden.

- **Zurechenbarkeit**
  Dem Sender einer Nachricht kann das Senden (auch gegenüber Dritten) nachgewiesen werden.
  (Nachweis des Empfangs sowie des Zeitpunktes des Sendens/Empfangens erfordert weitere Maßnahmen.)

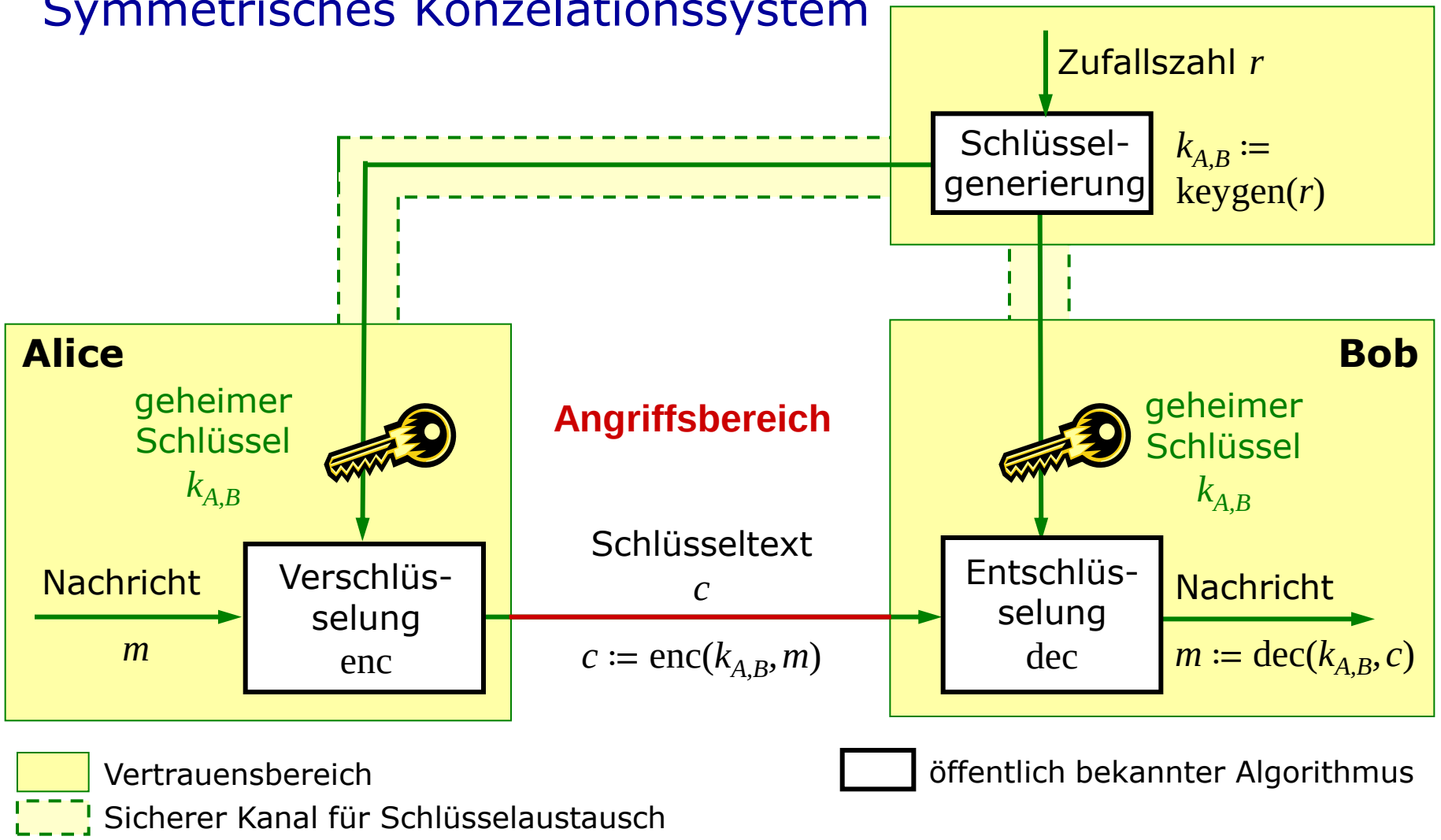
Kriterien für eine Einteilung

- Zweck
  - Konzelationssysteme
    Systeme zum Schutz der Vertraulichkeit der Daten
  - Authentikationssysteme
    Systeme zum Schutz der Integrität der Daten
    - digitale Signatursysteme (spezielle Authentikationssysteme)
      Systeme zur Realisierung von Zurechenbarkeit von Daten
- Schlüsselverteilung
  - Symmetrische Verfahren: $k_e = k_d$
  - Asymmetrische Verfahren: $k_e \neq k_d$

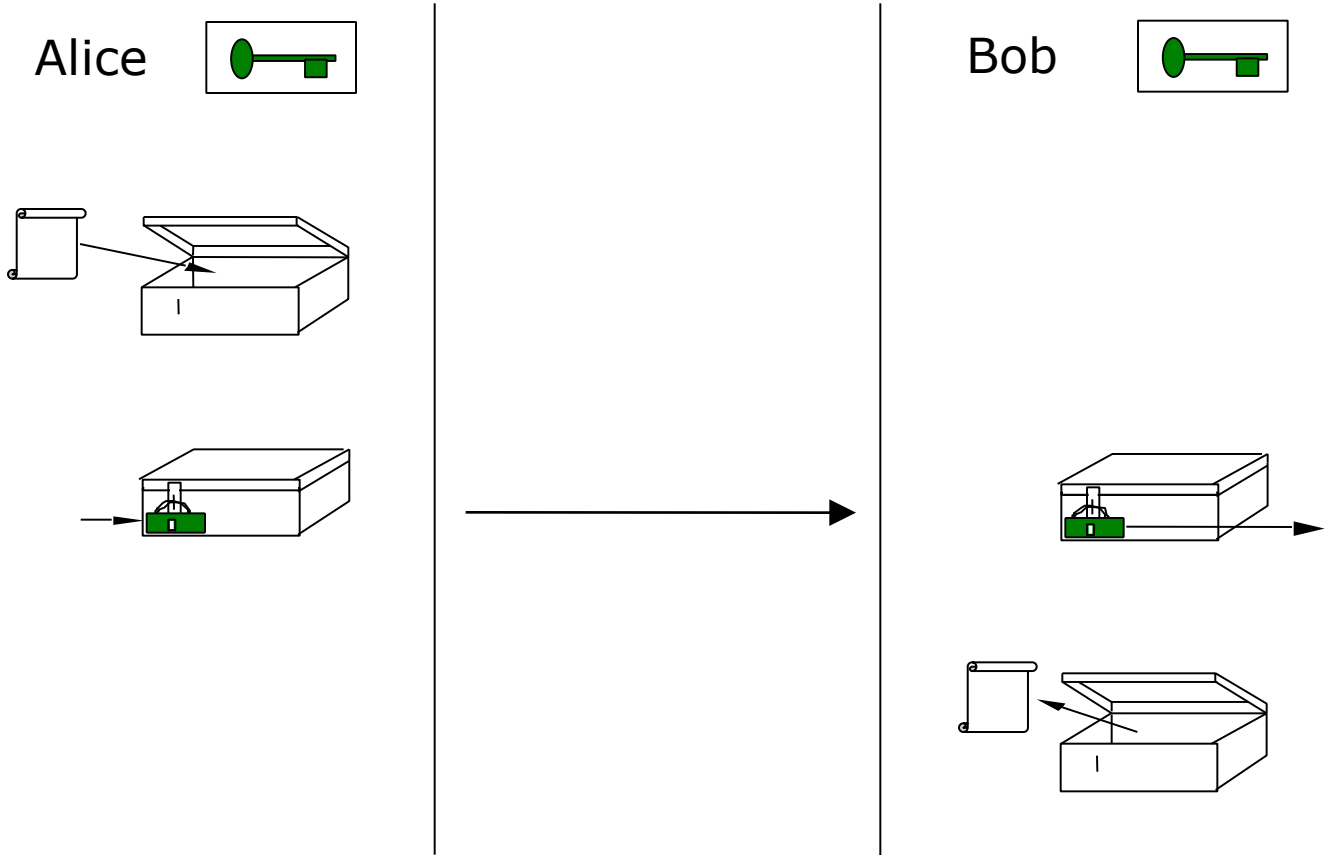
Notation:

$k_{A,B}$:	symmetrischer Schlüssel für Kommunikation zwischen Teilnehmern *A* und *B*
$k_{e,A}/k_{d,A}$:	Schlüssel zur Ver-/Entschlüsselung des Teilnehmers *A* (asymmetrisches System)

Symmetrisches Konzelationssystem



Symmetrisches Konzelationssystem



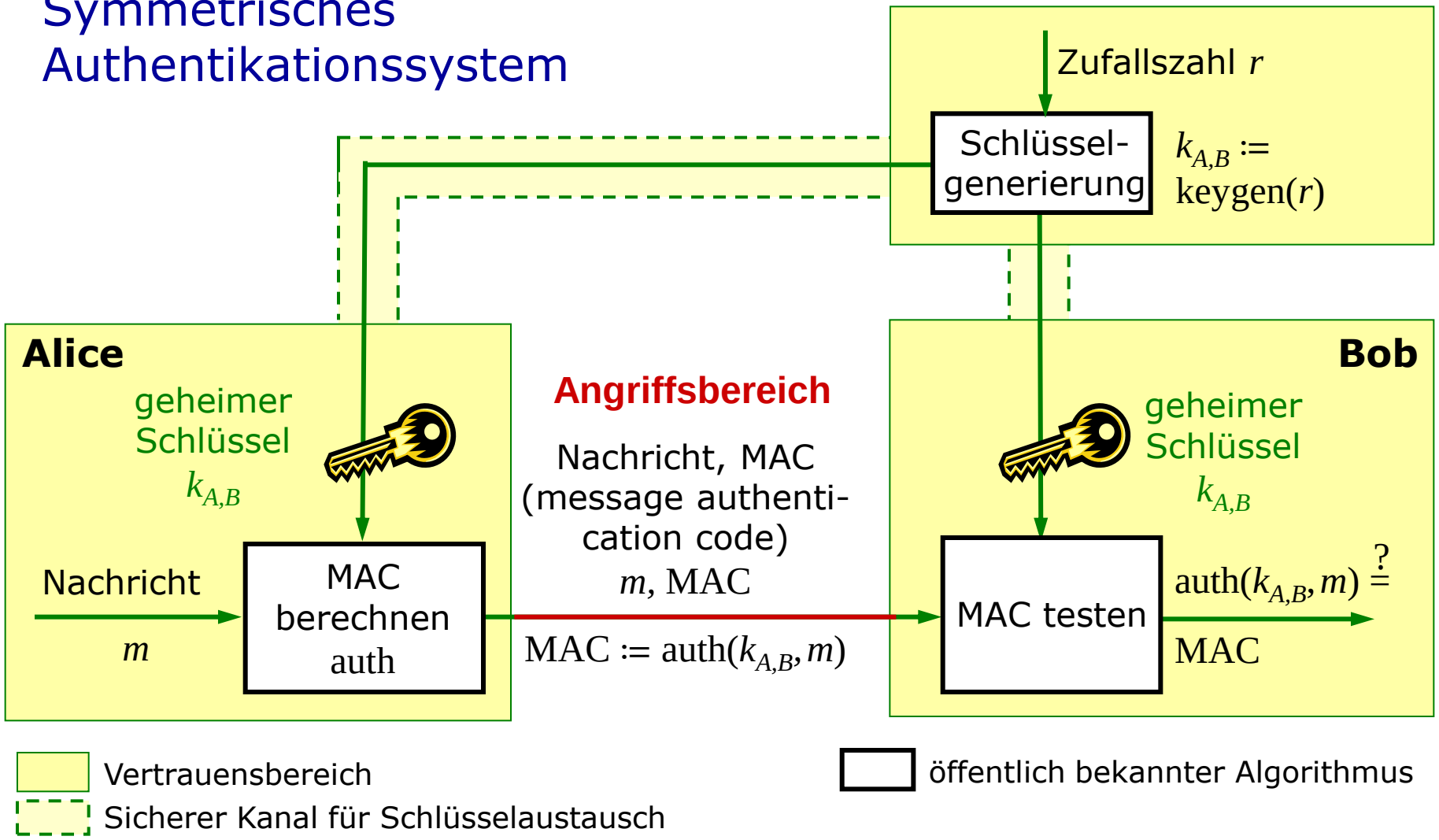
3 Prinzip symmetrischer Systeme

- Schlüsselaustausch
  - Notwendig: sicherer Kanal für Schlüsselaustausch
  - Offenes System: Sender und Empfänger können sich nicht vorab treffen

  → Lösung: Schlüsselverteilzentrale X
    - Jeder Teilnehmer (z.B. A) meldet sich an und tauscht einen geheimen Schlüssel $k_{A,X}$ mit X aus
    - Kommunikation mit Teilnehmer B: Anfrage an X nach geheimem Schlüssel $k_{A,B}$
    - X generiert Schlüssel $k_{A,B}$ und sendet ihn an A und B

  - Problem: X kann alle Nachrichten lesen
  - Verbesserung: verschiedene Schlüsselverteilzentralen verwenden und geheime Schlüssel lokal berechnen

Symmetrisches Authentikationssystem



Kerckhoffs-Prinzip

Die Sicherheit eines Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen, sondern nur von der Geheimhaltung des Schlüssels.

[Auguste Kerkhoffs: *La Cryptographie militaire.* Journal des Sciences Militaires, Januar 1883.]

- Keine „Security by Obscurity"
- Annahme: Angreifer kennt das Verfahren und die öffentlichen Parameter
- Sicherheit des Verfahrens begrenzt durch
  - Sicherheit der Schlüsselgenerierung und
  - Sicherheit des Schlüsselaustauschs

Klassifizierung von Kryptosystemen nach ihrer Sicherheit

- informationstheoretisch sicher
  Auch einem unbeschränkten Angreifer gelingt es nicht, das System zu brechen.
  („unconditional security“, „perfect secrecy“)
- beste erreichbare Sicherheit

- Verschiedene Begriffe zur Bewertung der Sicherheit der übrigen Systeme
- Annahmen über Möglichkeiten des Angreifers, Betrachtung der Sicherheit unter bestimmten Angriffen

Informationstheoretische (perfekte) Sicherheit

[Claude Shannon: *Communication Theory of Secrecy Systems.* Bell Systems Technical Journal, 28(1949), 656-715.]

- Informelle Beschreibung (bzgl. Konzelationssystem):

> Selbst ein unbeschränkter Angreifer gewinnt aus seinen Beobachtungen keinerlei zusätzliche Informationen über Klartext oder Schlüssel.

- „unbeschränkt“: beliebiger Rechen- und Zeitaufwand
- „zusätzliche Informationen“: nicht besser als bloßes Raten

- Aussagen bzgl. Sicherheit gelten nur für den Algorithmus!

4 Anmerkungen zur Sicherheit

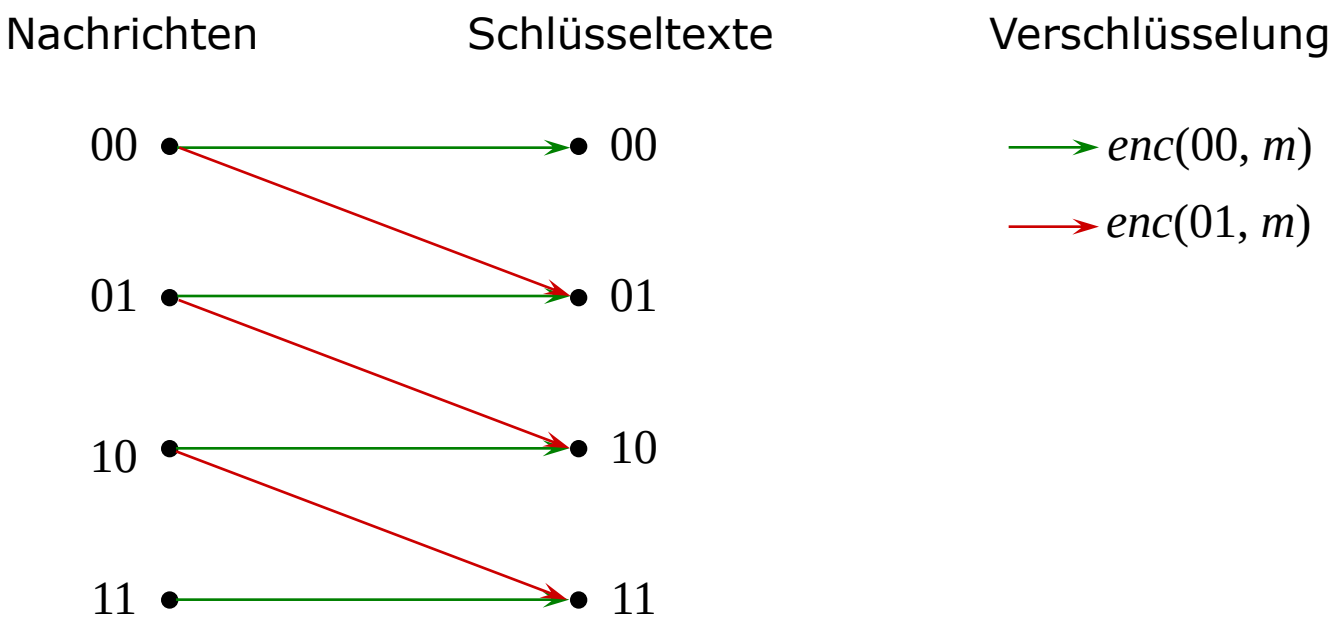
→ Notwendige und hinreichende Bedingung für informationstheoretische Sicherheit:

$$\forall\, m \in M\, \forall\, c \in C\colon\ p(c|m) = p(c).$$

→ Nachrichten und Schlüsseltexte müssen stochastisch unabhängig voneinander sein.

- Daraus abgeleitet: Anforderungen an die Schlüssel
  - Notwendige Anzahl
  - Wahrscheinlichkeiten
  - Auswahl

Beispiel für die Anforderungen an die Schlüssel



→ nicht informationstheoretisch sicher
→ Beispiel: Anzahl der Schlüssel

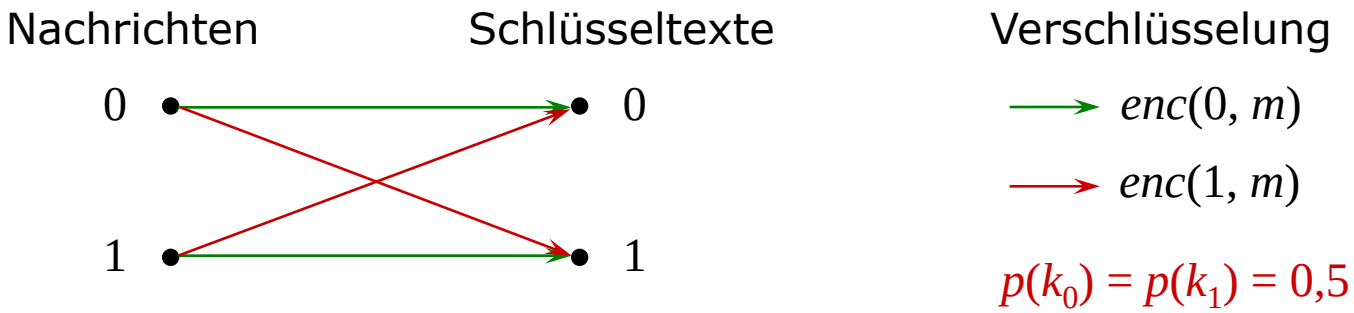
Vernam-Chiffre (one-time pad)

- Jeder Schlüssel wird nur einmal verwendet
- Schlüssellänge und Länge des Klartextes sind gleich
- Schlüssel sind zufällig

→ Einzige informationstheoretisch sicheres Chiffre.

- Binäre Vernam-Chiffre

$$c = \mathrm{enc}(k_i, m_i) = m_i \oplus k_i \qquad m = \mathrm{dec}(k_i, c_i) = c_i \oplus k_i$$



Anmerkungen zur informationstheoretischen Sicherheit

- Informationstheoretische Sicherheit kann nur von symmetrischen Systemen erreicht werden
- Systeme, die ein und denselben Schlüssel mehrfach verwenden, können nicht informationstheoretisch sicher sein

- Probleme:
  - Schlüsselmanagement
  - Schutzziel „Zurechenbarkeit" kann nicht mit symmetrischen System erbracht werden

→ Verwendung von nicht informationstheoretisch sicheren Systemen notwendig

→ Annahmen über den Angreifer notwendig (notwendige Berechnungen des Angreifers sind *nicht effizient* möglich)

AES (Advanced Encryption Standard)

- 1997 Ausschreibung eines öffentlichen Wettbewerbs für die Einreichung eines kryptographischen Algorithmus “AES” als Nachfolger des DES durch das National Institute of Standards and Technology (NIST) der USA

- Sieger des Wettbewerbs:
  Rijndael (Vincent **Rij**men und Joan **Dae**men, Belgien)

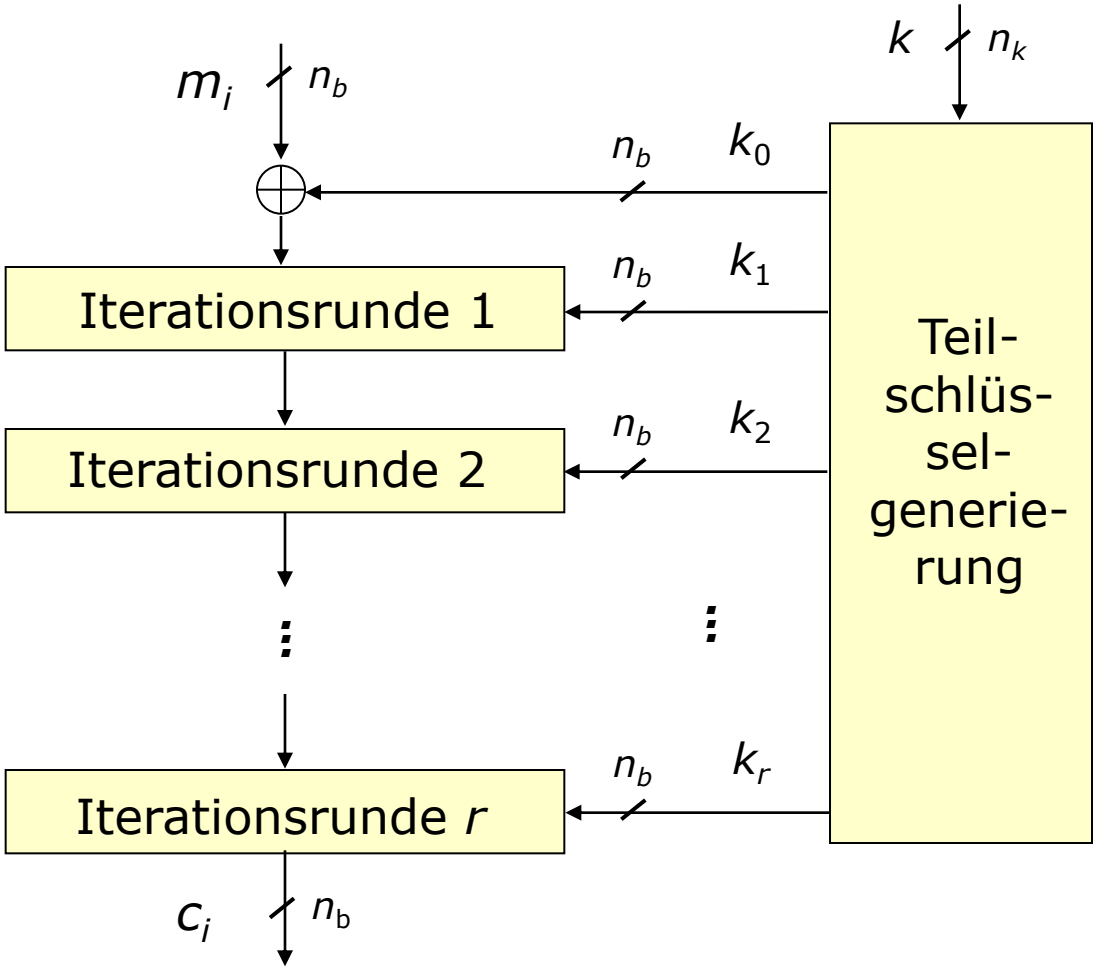
- Publikation als Standard im Herbst 2001 (FIPS Standard „Specification for the Advanced Encryption Standard“, FIPS 197)
- 2002 trat AES in Kraft
- Einsatz z.B.: Verschlüsselungsstandard 802.1 für Wireless LAN bzw. für Wi-Fi WPA2, SSH, IPSec, 7-Zip, PGP

Überblick über den Algorithmus

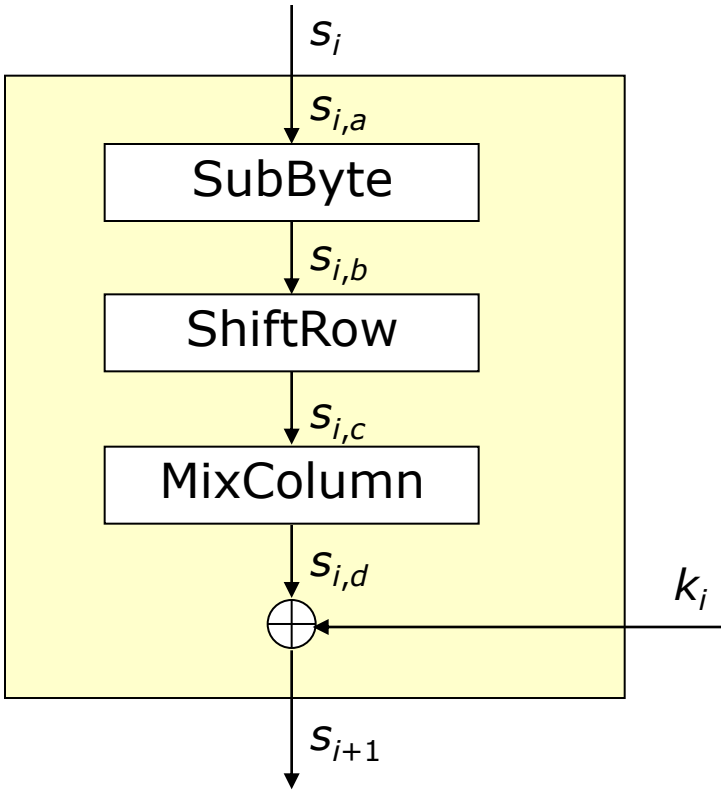
- Verschlüsselung von Klartextblöcken der Länge 128 Bit (vorgeschlagene Längen von 192 und 256 Bits nicht standardisiert)
- Schlüssellänge wahlweise 128, 192 oder 256 Bits
- Mehrere Runden, jeweils Substitutionen, Permutationen und Schlüsseladdition
- Anzahl der Runden *r* hängt von Schlüssel- und Klartextlänge ab:

Schlüssel-	Blocklänge des Klartextes n_b		
länge n_k	128 Bit	192 Bit	256 Bit
128 Bit	10	12	14
192 Bit	12	12	14
256 Bit	14	14	14

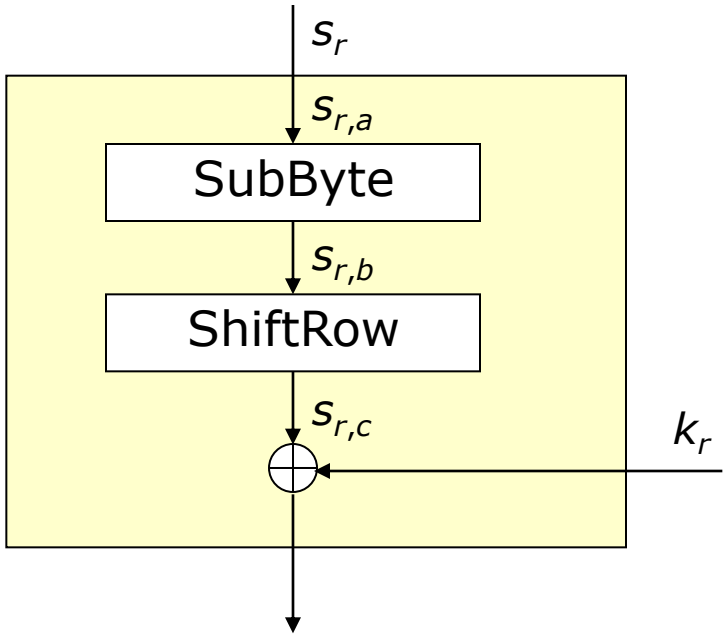
Struktur des AES



Struktur der Iterationsrunden



Runde i, i = 1, 2, …, r-1



Runde r

Notation

- Darstellung eines Bytes als Folge von Bits:
  $a = \{a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0\}_2, \quad a_i \in \{0,1\}$

- Darstellung als Polynom:

$$a = \sum_{i=0}^{7} a_i x^i$$

- Darstellung als Hexadezimalzahl

Darstellung der Operanden

Byte-Matrizen mit 4 Zeilen und N_b (N_k) Spalten
mit N_b (N_k): Blocklänge n_b (Schlüssellänge n_k) / 32

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

Matrix (*state*) für Blocklänge

128, 192, 256

Bit

Schlüssel für Schlüssellänge

128, 192, 256

Bit

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$	$k_{0,6}$	$k_{0,7}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$	$k_{1,6}$	$k_{1,7}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$	$k_{2,6}$	$k_{2,7}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$	$k_{3,6}$	$k_{3,7}$

Mathematische Grundlagen

- Alle Verschlüsselungsschritte basieren auf Operationen in endlichen Körpern
- Alle Bytes als Elemente des Körpers GF(2^8) interpretierbar:

$$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \bmod m(x)$$

mit $m(x) = x^8 + x^4 + x^3 + x + 1$ (irreduzibles Polynom)

- Addition $\oplus$:

$a = \{a_7a_6a_5a_4a_3a_2a_1a_0\}$, $b = \{b_7b_6b_5b_4b_3b_2b_1b_0\}$

$c = a \oplus b$ mit $c_i = a_i \oplus b_i$

- Multiplikation $\odot$:

$c = a \odot b = a \cdot b \bmod m(x)$

5 Beispiel: AES

- Polynome dritten Grades mit Koeffizienten aus GF(2^8):
  Polynomring GF(2^8)[x]/(x^4+1)

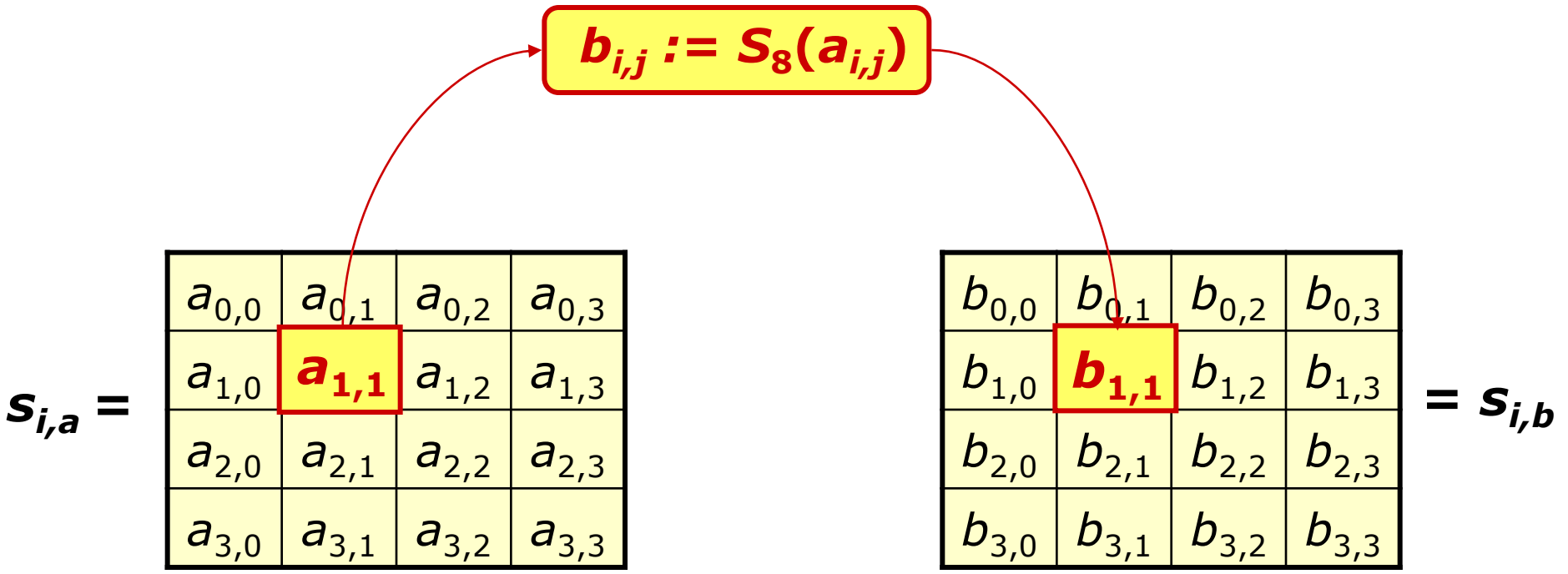
  $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ mit $a_i \in$ GF(2^8)

- Addition $\oplus$:
  $c(x) = a(x) \oplus b(x) =$
  $(a_3 \oplus b_3)x^3 + (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x + (a_0 \oplus b_0)$

- Multiplikation $\otimes$:
  $c(x) = a(x) \otimes b(x) = a(x) \odot b(x) \bmod (x^4+1)$

Schritt 1: SubByte

- Alle Bytes einer Matrix werden unabhängig voneinander substituiert

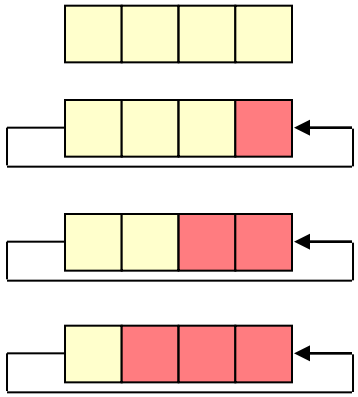


Substitutionsbox $S_8(a_7a_6a_5a_4a_3a_2a_1a_0)$

$a_7a_6a_5a_4$	$a_3a_2a_1a_0$															
	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
⋮	⋮															
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

Schritt 2: ShiftRow

- Zyklische Verschiebung der Zeilen nach links

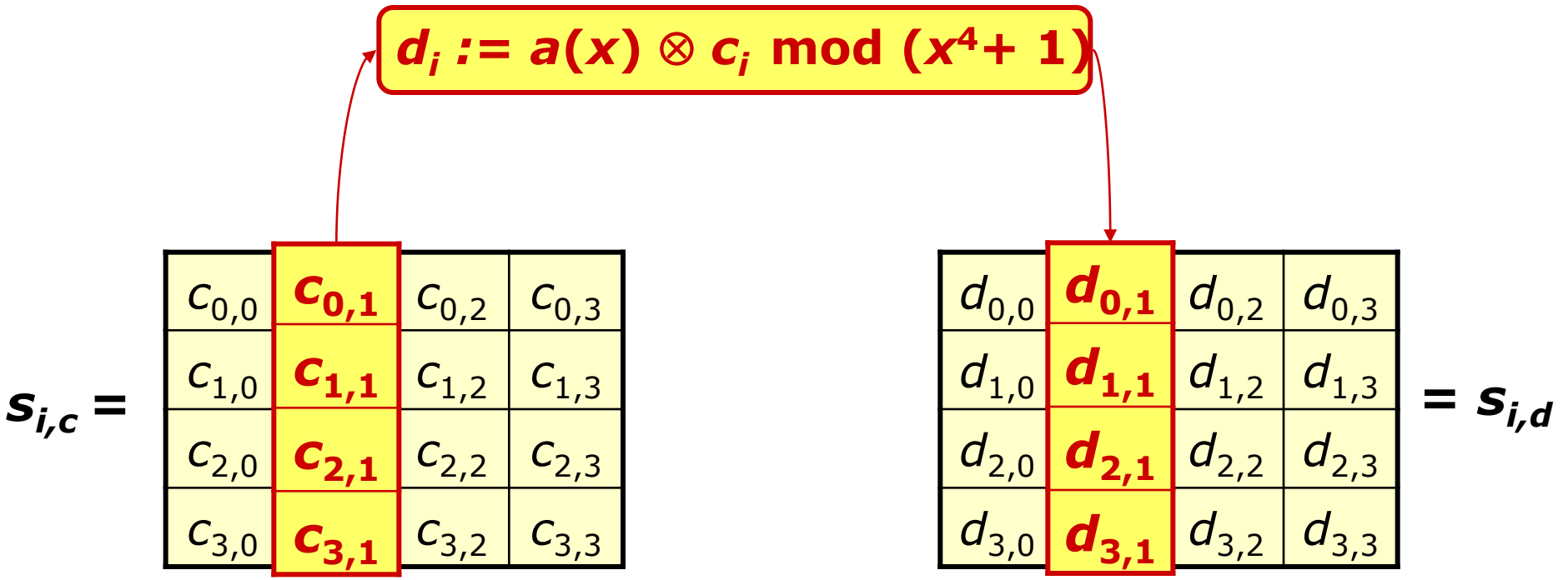


Zeile	0	1	2	3
$N_b = 4$	0	1	2	3
$N_b = 6$	0	1	2	3
$N_b = 8$	0	1	3	4

$$s_{i,b} = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix} \quad \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix} = s_{i,c}$$

Schritt 3: MixColumn

- Operiert jeweils auf Spalten der Matrix (32-Bit Substitution)
- Diffusion



$d_i := a(x) \otimes c_i \bmod (x^4+1)$

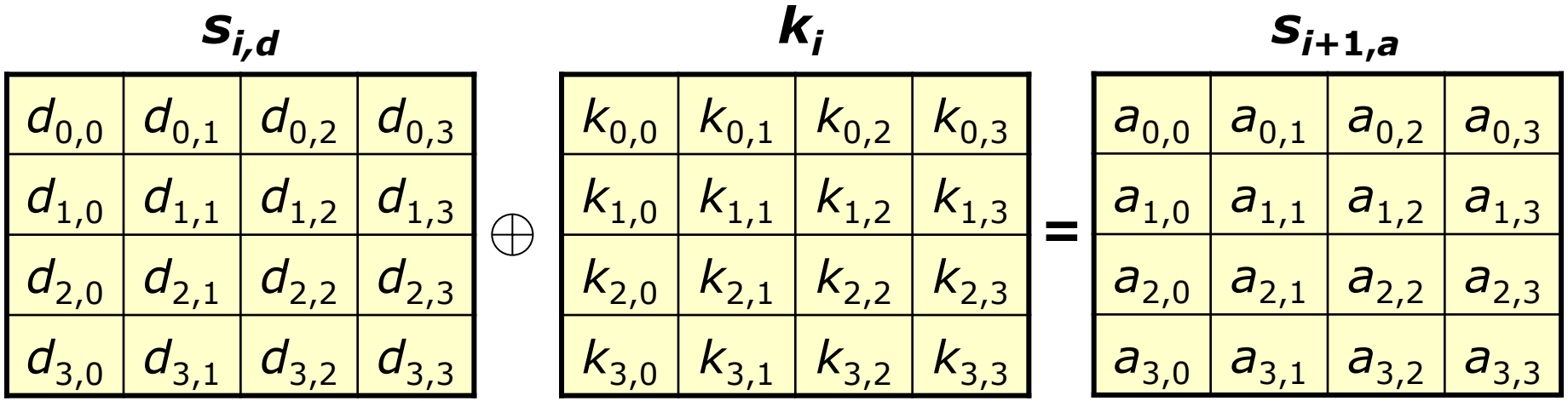
$a(x) = \{03\}\, x^3 + \{01\}\, x^2 + \{01\}\, x + \{02\}$

$$\begin{pmatrix} d_{0,i} \\ d_{1,i} \\ d_{2,i} \\ d_{3,i} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} c_{0,i} \\ c_{1,i} \\ c_{2,i} \\ c_{3,i} \end{pmatrix}$$

$$\begin{aligned} d_{0,i} &= (\{02\}\cdot c_{0,i}) \oplus (\{03\}\cdot c_{1,i}) \oplus c_{2,i} \oplus c_{3,i} \\ d_{1,i} &= c_{0,i} \oplus (\{02\}\cdot c_{1,i}) \oplus (\{03\}\cdot c_{2,i}) \oplus c_{3,i} \\ d_{2,i} &= c_{0,i} \oplus c_{1,i} \oplus (\{02\}\cdot c_{2,i}) \oplus (\{03\}\cdot c_{3,i}) \\ d_{3,i} &= (\{03\}\cdot c_{0,i}) \oplus c_{1,i} \oplus c_{2,i} \oplus (\{02\}\cdot c_{3,i}) \end{aligned}$$

Schritt 4: AddRoundKey

- Macht Iterationsrunden schlüsselabhängig
- Länge des Rundenschlüssels k_i: n_b



Teilschlüsselgenerierung

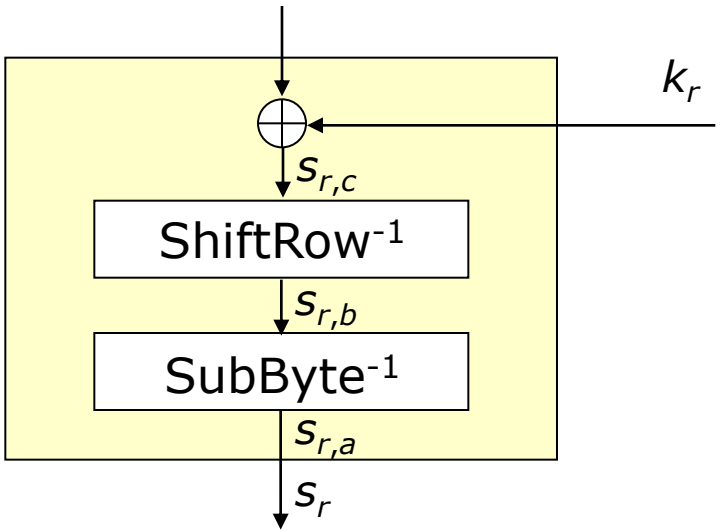
- Expansion des AES-Schlüssels, abhängig von n_b und n_k
- n_b bestimmt Länge der Rundenschlüssel
- n_b und n_k bestimmen Anzahl der Runden → Anzahl der Rundenschlüssel

- Länge des expandierten Schlüssels in Byte = $4N_b(r+1)$:

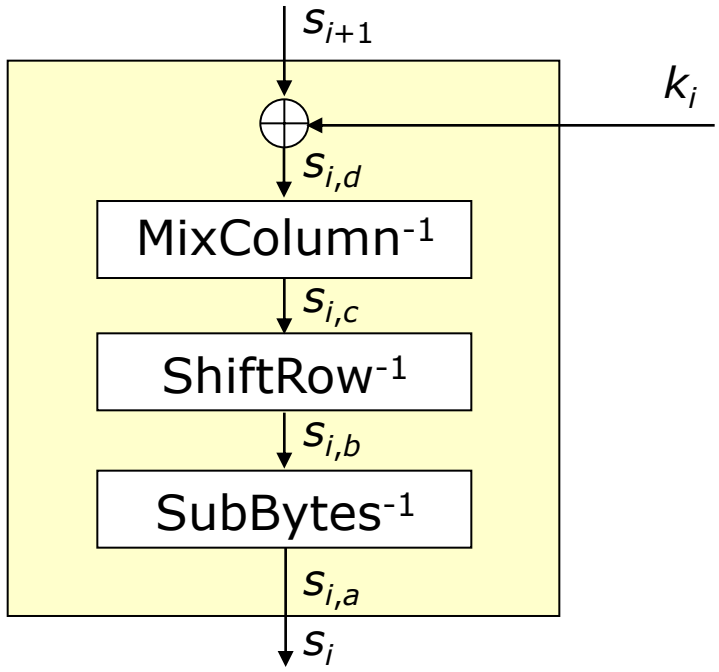
Schlüssel-länge n_k	Blocklänge des Klartextes n_b		
	128 Bit	192 Bit	256 Bit
128 Bit	16·11	24·13	32·15
192 Bit	16·13	24·13	32·15
256 Bit	16·15	24·15	32·15

Entschlüsselung

- Umgekehrte Reihenfolge, inverse Funktionen



Runde r

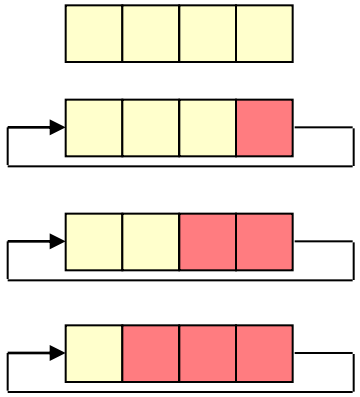


Runde i, $i = r\text{-}1, r\text{-}2, \ldots, 1$

- Zum Schluss Addition des Rundenschlüssels k_0

Inverse Funktionen

- ShiftRow^{-1}:
  zyklische Verschiebung nach rechts



- SubByte^{-1}:
  Anwendung der inversen Substitution $a_{i,j} := S_8^{-1}(b_{i,j})$

- MixColumn^{-1}:
  Multiplikation mit dem multiplikativen Inversen mod $(x^4 + 1)$

$$a^{-1}(x) = (\{03\}\, x^3 + \{01\}\, x^2 + \{01\}\, x + \{02\})^{-1} \bmod (x^4 + 1)$$
$$= \{0b\}\, x^3 + \{0d\}\, x^2 + \{09\}\, x + \{0e\}$$

Entschlüsselung in äquivalenter Reihenfolge

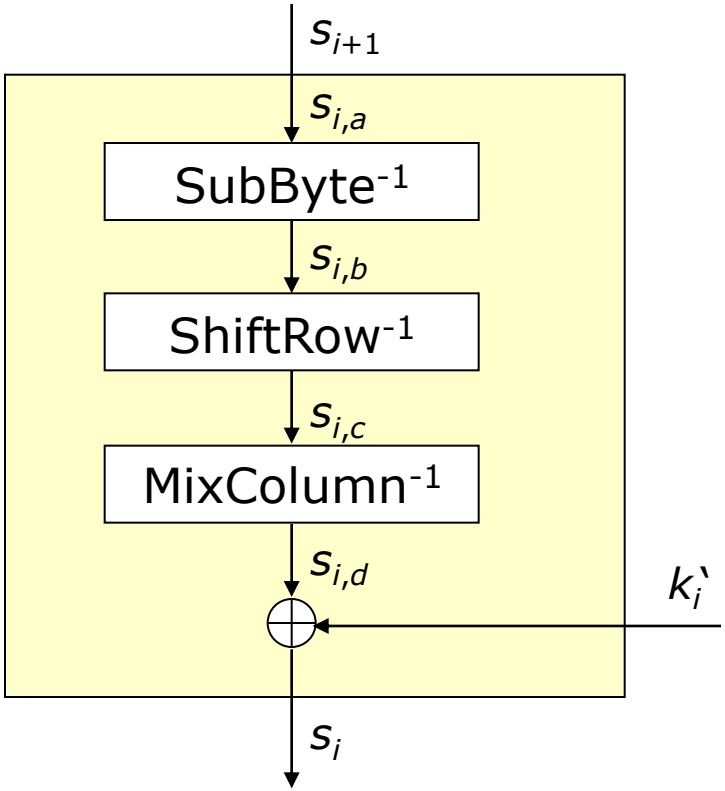
- $\text{SubByte}(\text{ShiftRow}(s_i)) = \text{ShiftRow}(\text{SubByte}(s_i))$
  und
  $\text{SubByte}^{-1}(\text{ShiftRow}^{-1}(s_i)) = \text{ShiftRow}^{-1}(\text{SubByte}^{-1}(s_i))$
- $\text{MixColumn}(s_i \oplus k_i) = \text{MixColumn}(s_i) \oplus \text{MixColumn}(k_i)$
  und
  $\text{MixColumn}^{-1}(s_i \oplus k_i) = \text{MixColumn}^{-1}(s_i) \oplus \text{MixColumn}^{-1}(k_i)$

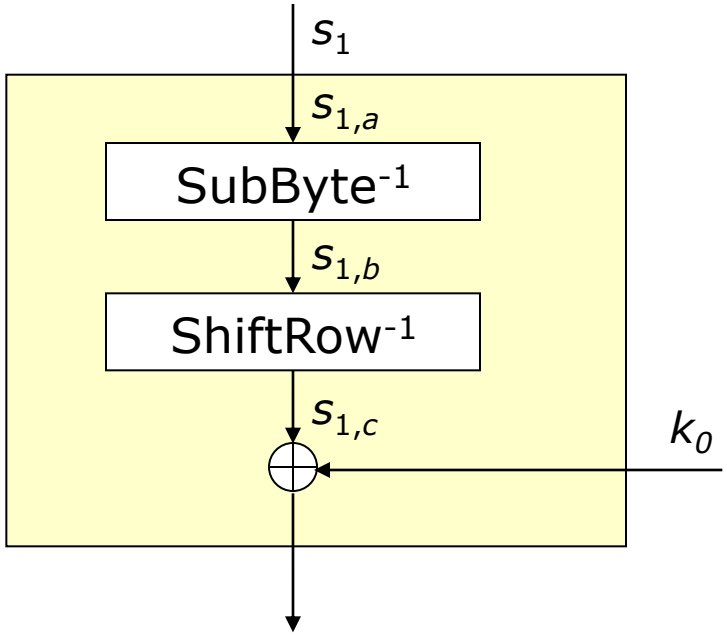
$\rightarrow$ Reihenfolge der Abarbeitung wie bei Verschlüsselung

$\rightarrow k_i' = \text{MixColumn}^{-1}(k_i)$, $i = 1, 2, \ldots, r\text{-}1$

Entschlüsselung in äquivalenter Reihenfolge

- Addition des Rundenschlüssels k_r





Runde i, $i = r\text{-}1, r\text{-}2, \ldots, 1$

Analyse des AES

- Darstellung als algebraische Formel 2001 [FeSW_01]

  (für n_k = 128 ca. 2^{50} Terme, für n_k = 256 ca. 2^{70} Terme)
- XSL-Angriff (Extended Sparse Linearisation) [CoPi_02]

  (Darstellung mit Hilfe eines quadratischen Gleichungssystems; für n_k = 128: 8000 Gleichungen mit 1600 Variablen)
- Weitere Angriffe wie z.B. *Collision attacks*, *Related-key attacks* und Seitenkanalangriffe

- Übersicht über Angriffe z.B. unter:

  http://www.cryptosystem.net/aes/

  http://www.iaik.tugraz.at/content/research/krypto/aes/