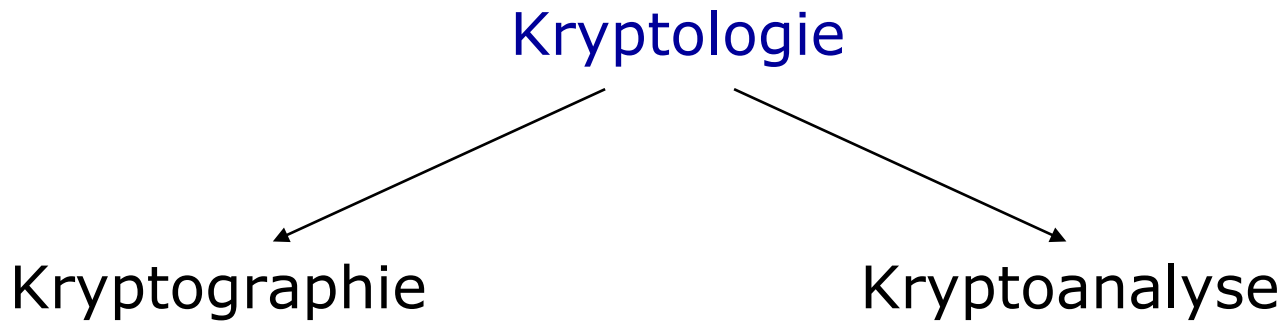
# Operating Systems & Security

Stefan Köpsell
(Slides [mainly] created by Andreas Pfitzmann)
Technische Universität Dresden, Faculty of Computer Science, D-01062 Dresden
Nöthnitzer Str. 46, Room 3067
Phone: +49 351 463-38272, e-mail: sk13@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

# SYMMETRISCHE KRYPTOGRAPHISCHE ALGORITHMEN




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

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

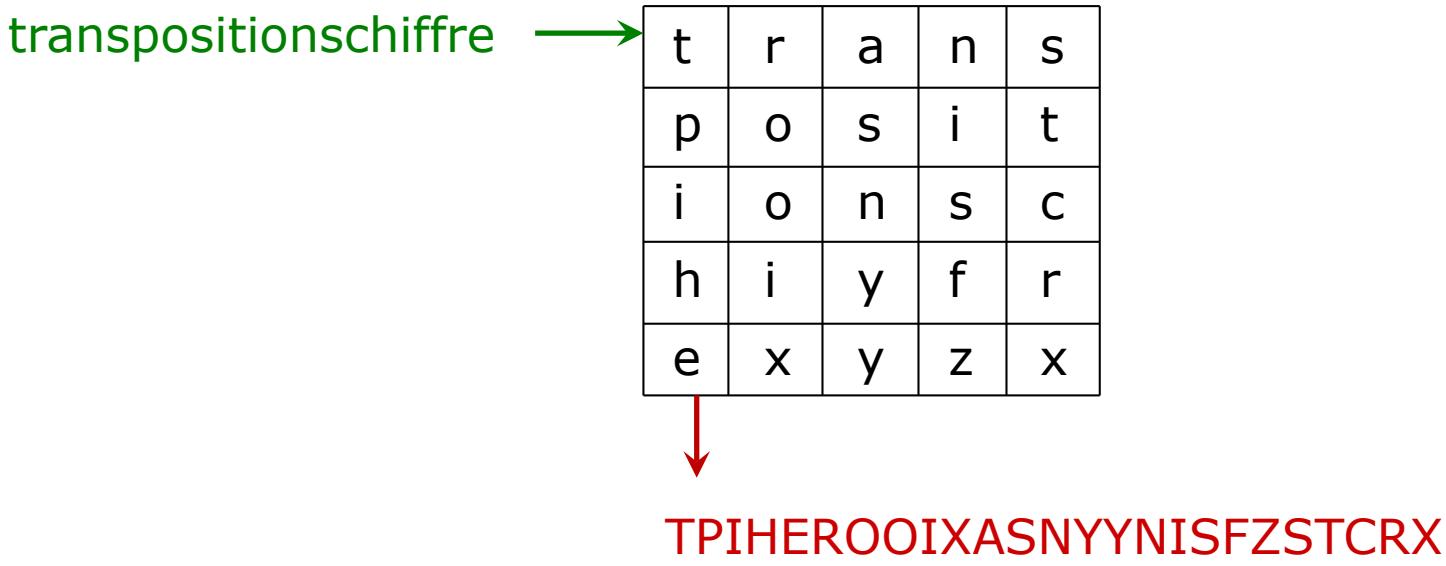
## Krypt[o]analyse (griech. „kryptos“+ „analyein“)

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

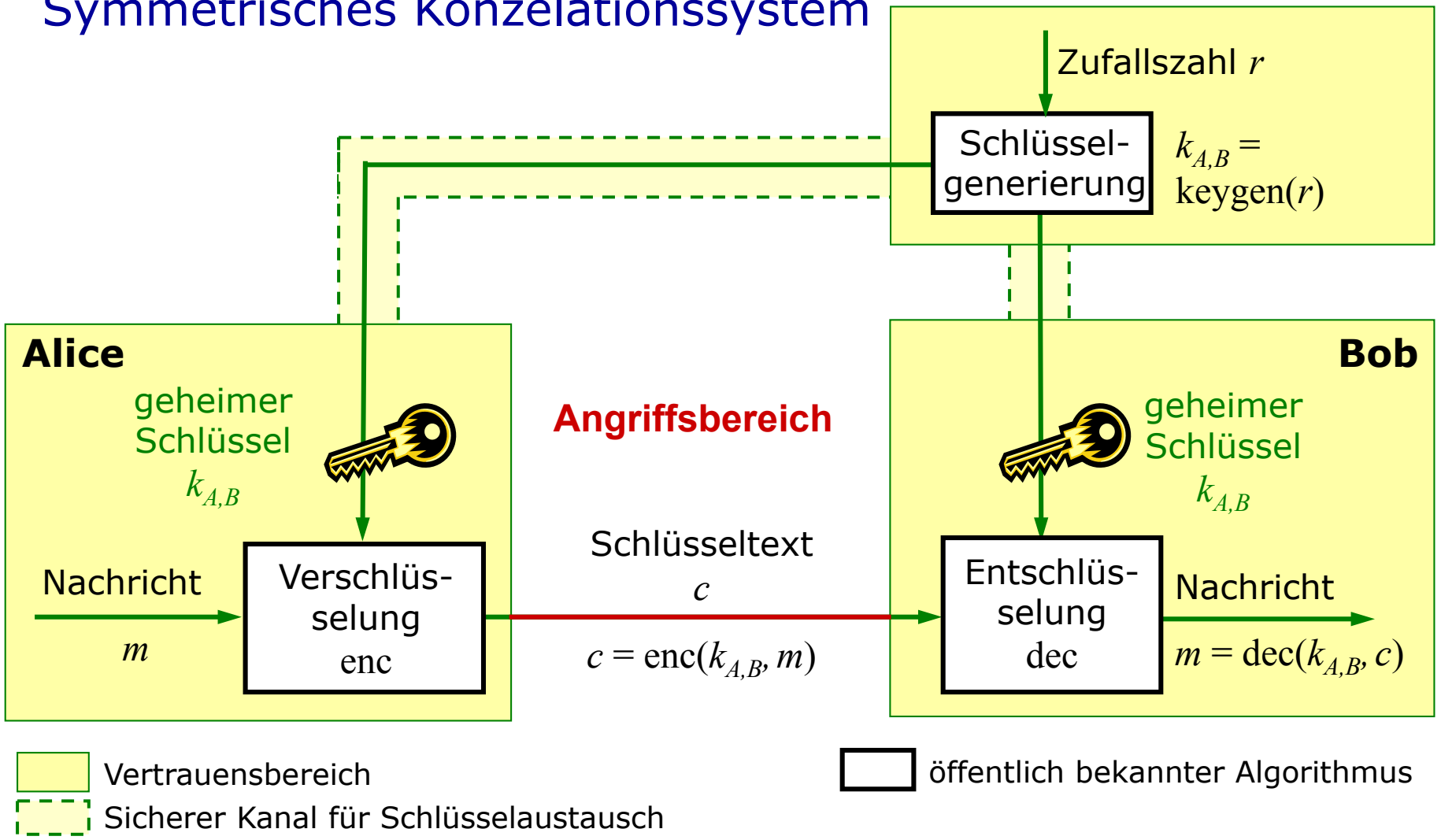
## Kriterien für eine Einteilung

- 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: $k_e \neq k_d$

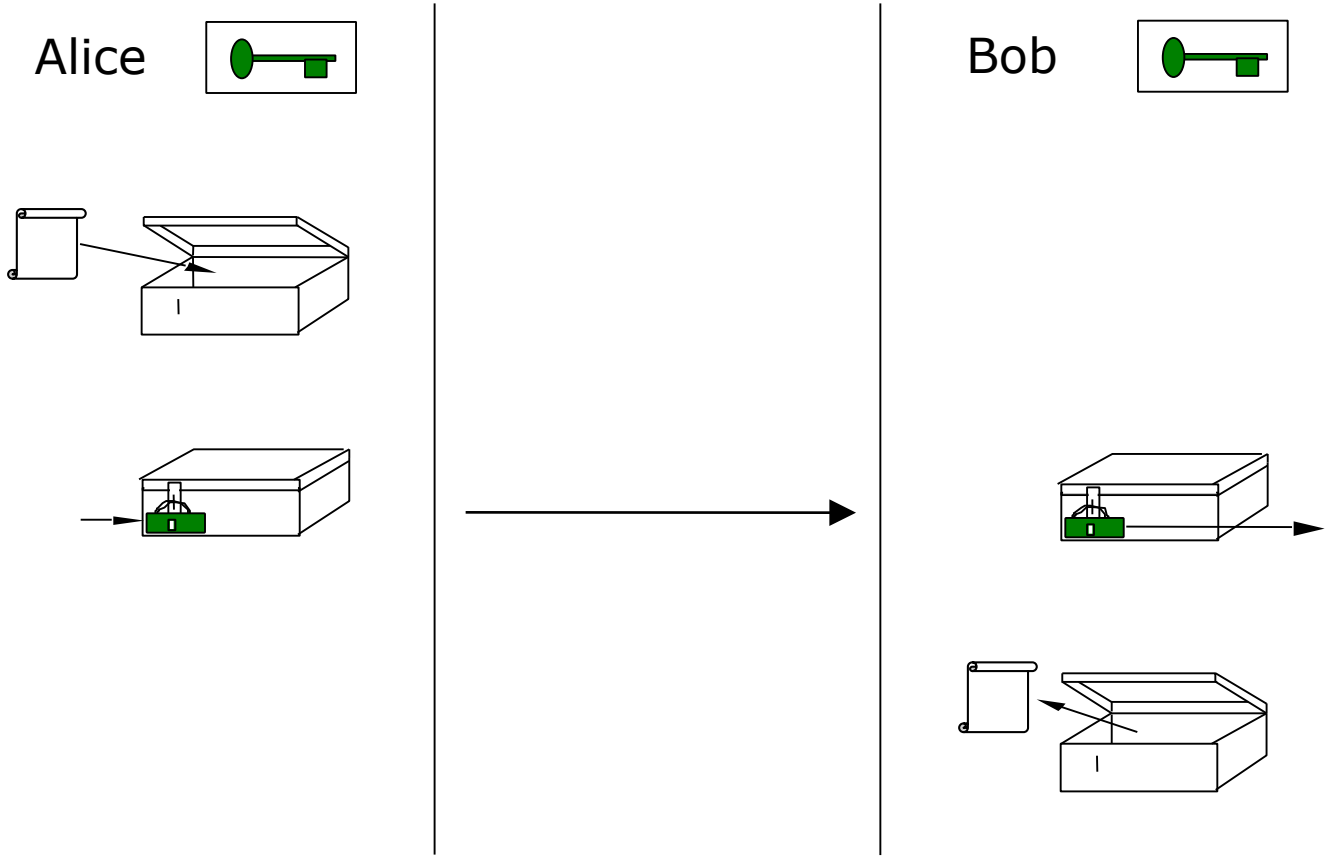
Notation:

| | |
|---|---|
| $k_{A,B}$: | 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



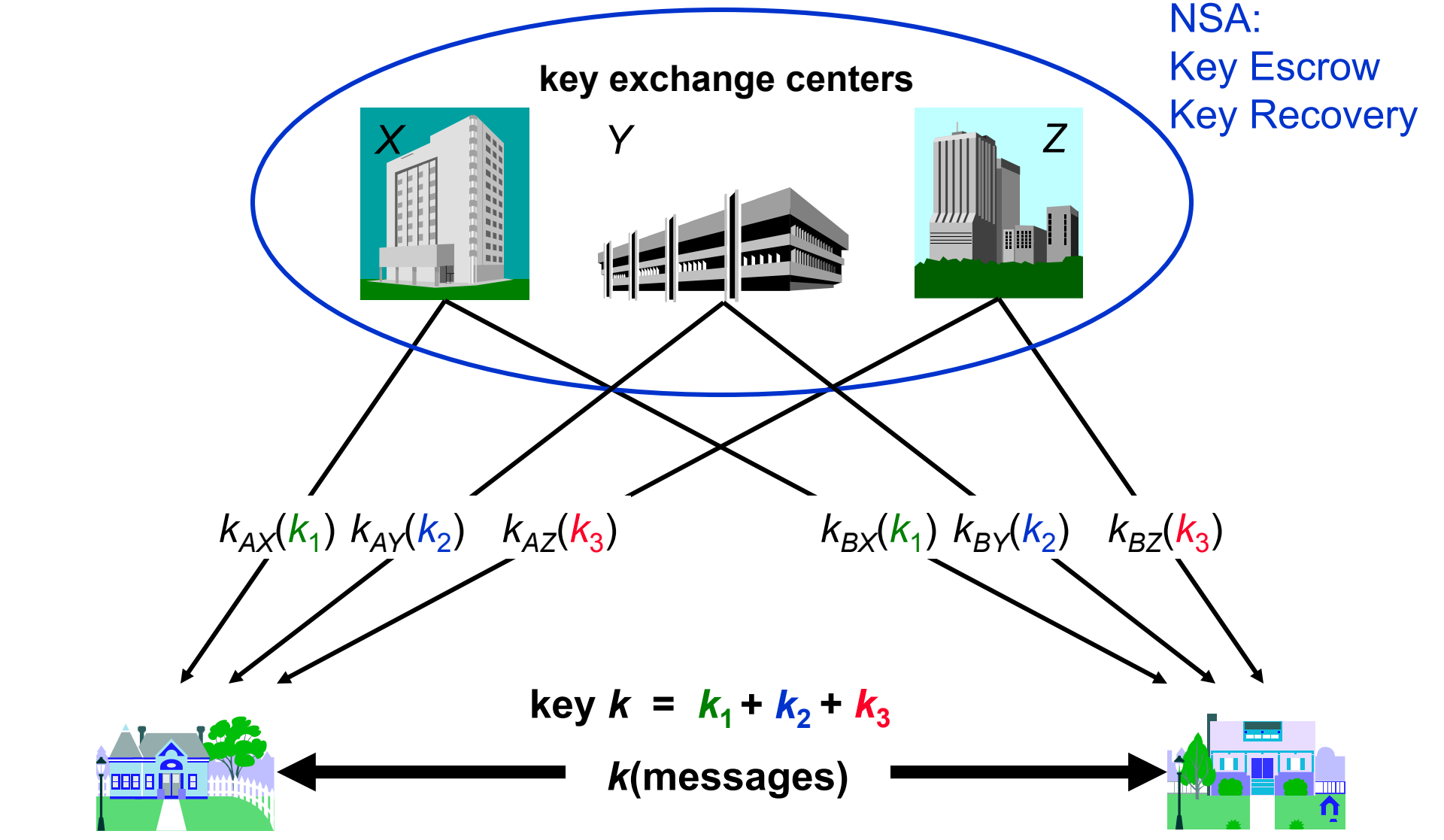
# 3 Prinzip symmetrischer Systeme

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

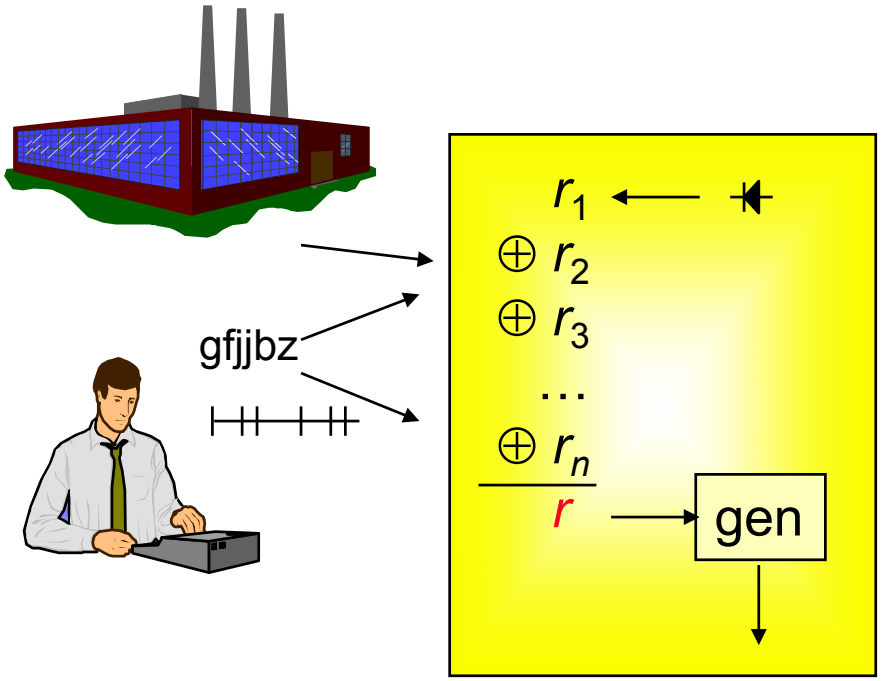
  → Lösung: Schlüsselverteilzentrale $X$
    - Jeder Teilnehmer (z.B. $A$) meldet sich an und tauscht einen geheimen Schlüssel $k_{A,X}$ mit $X$ aus
    - Kommunikation mit Teilnehmer $B$: Anfrage an $X$ nach geheimem Schlüssel $k_{A,B}$
    - $X$ generiert Schlüssel $k_{A,B}$ und sendet ihn an $A$ und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

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

# Key exchange using symmetric encryption systems



# Key generation

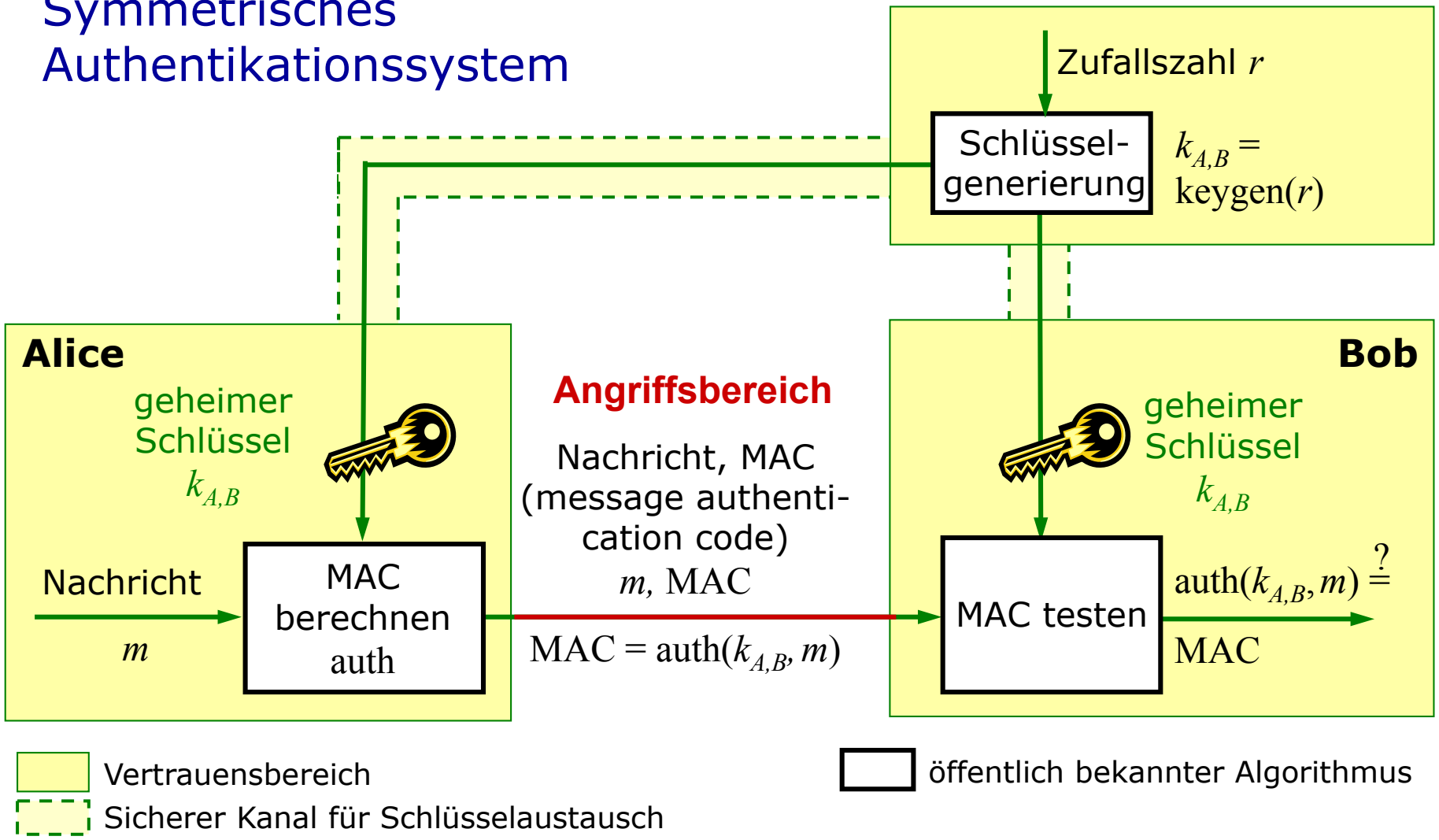



**generation of a random number *r* for the key generation:**

XOR of

- $r_1$, created in device,
- $r_2$, delivered by producer,
- $r_3$, delivered by user,
- $r_n$, calculated from keystroke intervals.

## Symmetrisches Authentikationssystem



# 4 Anmerkungen zur Sicherheit

**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

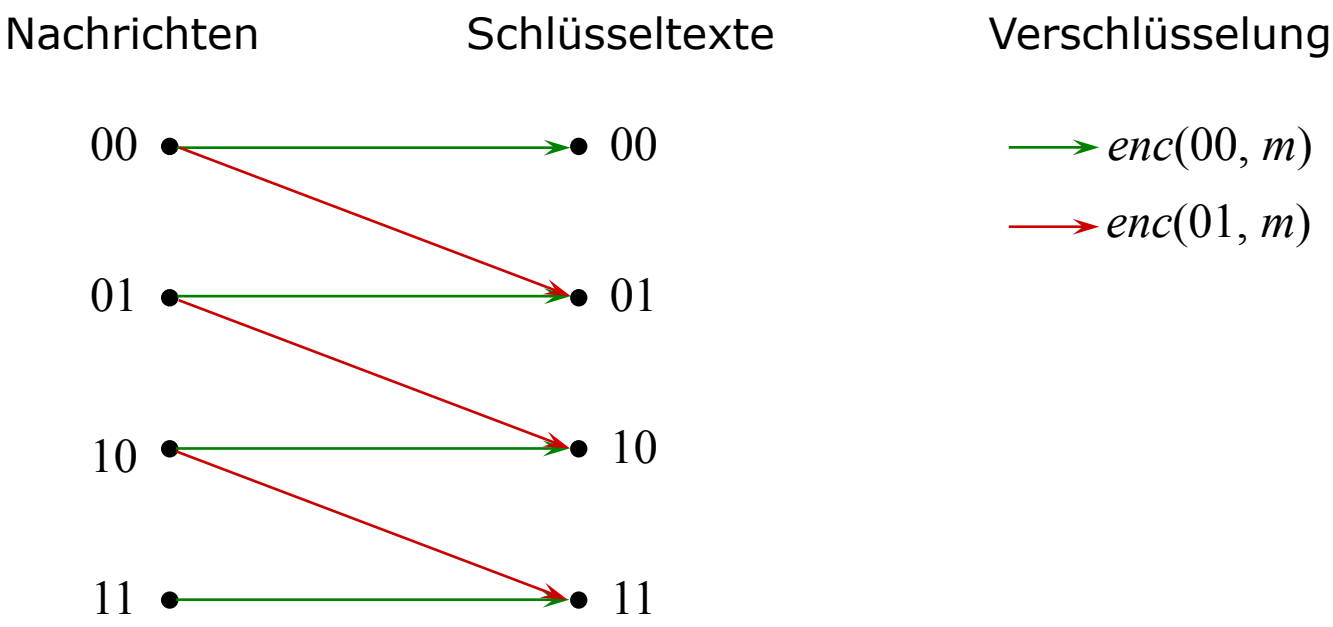
→ Notwendige und hinreichende Bedingung für informationstheoretische Sicherheit:

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

→ 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

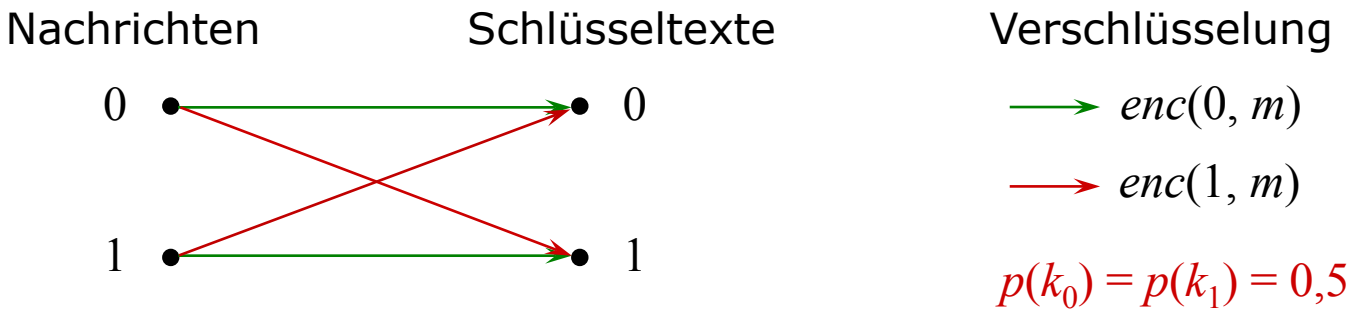
## Vernam-Chiffre (one-time pad)

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

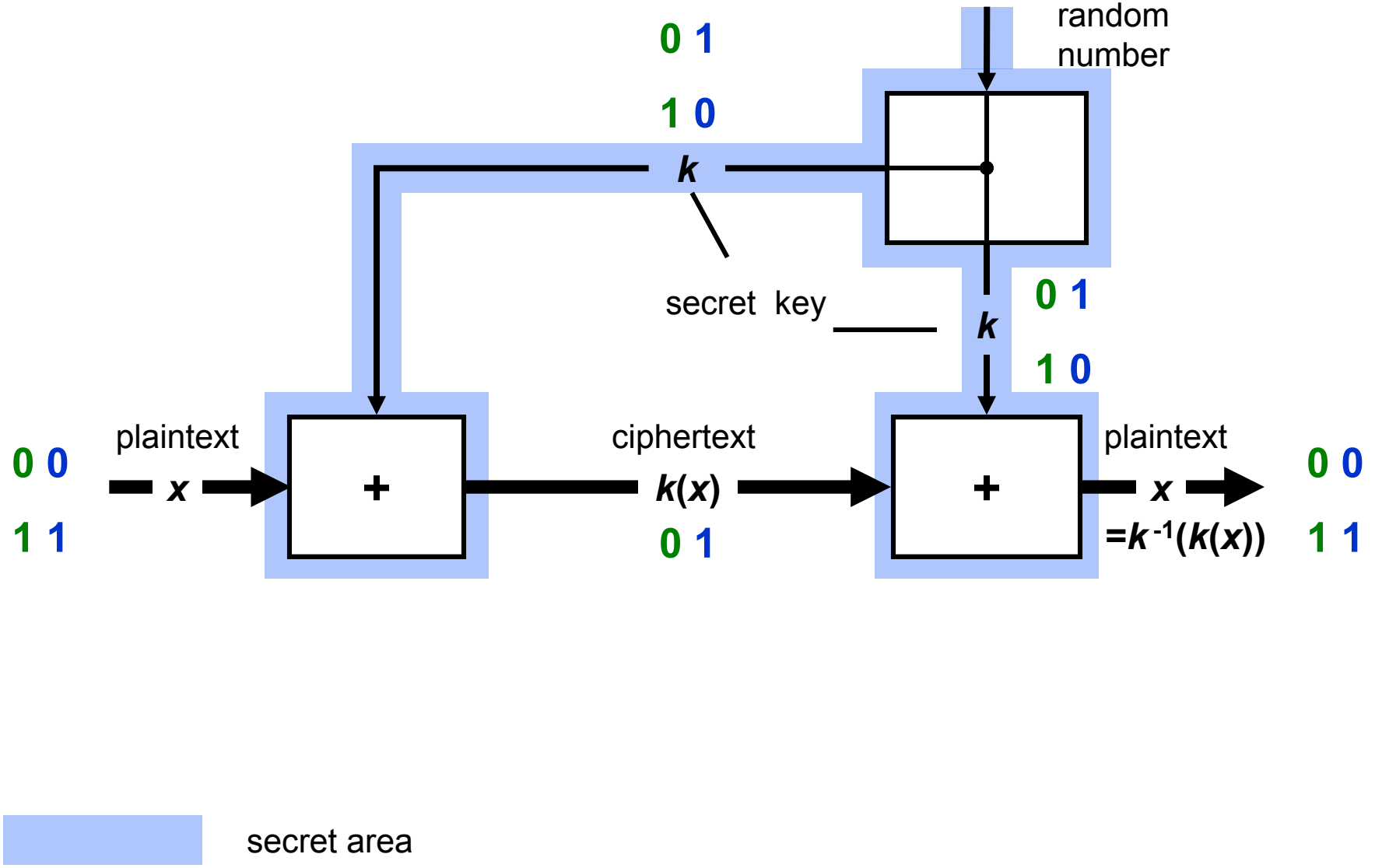
→ Einzige informationstheoretisch sichere Chiffre.

- Binäre Vernam-Chiffre

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



# Example: Vernam cipher (=one-time pad)



## Anmerkungen zur informationstheoretischen Sicherheit

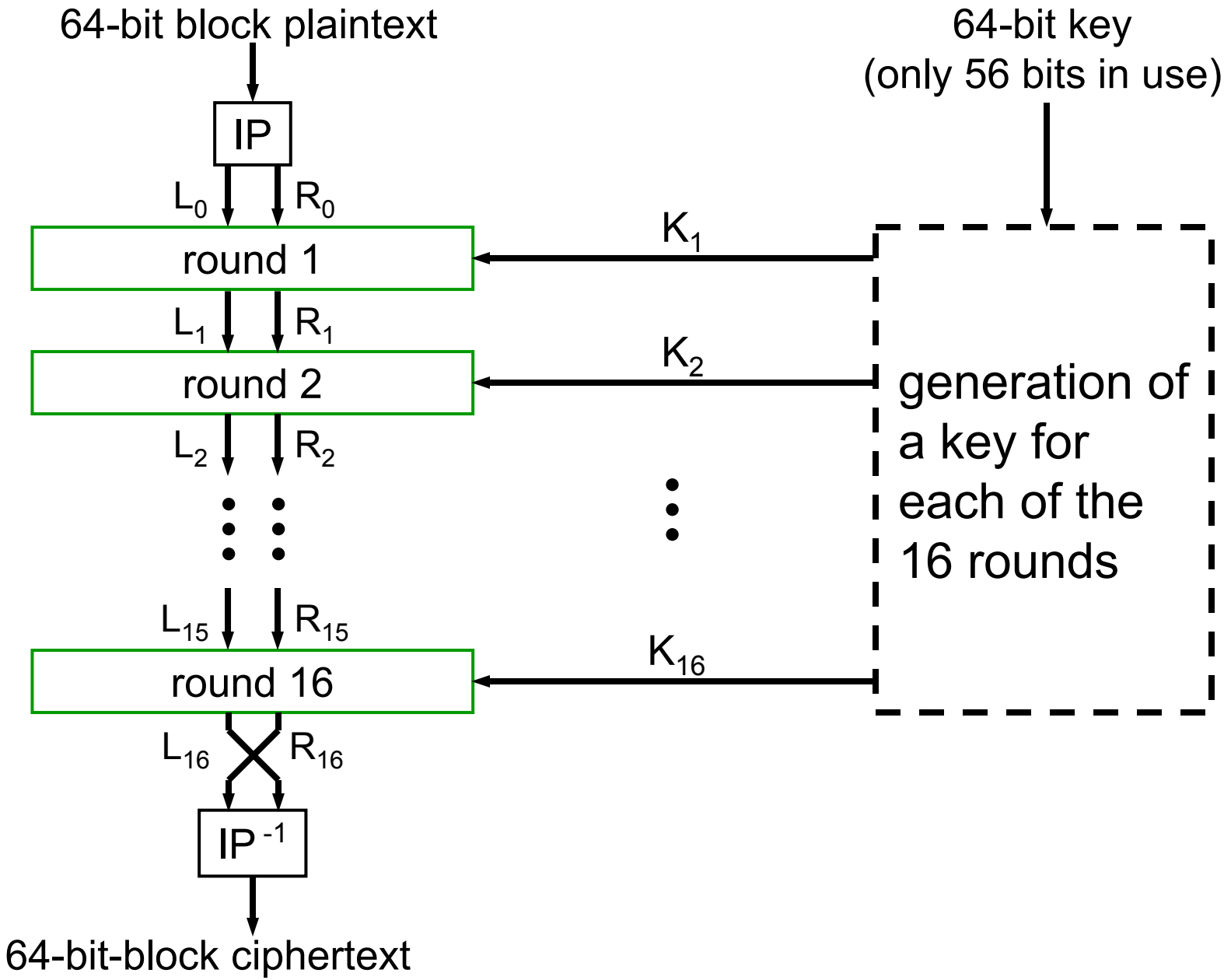
- Informationstheoretische Sicherheit kann nur von symmetrischen Systemen erreicht werden
- Systeme, die ein und denselben Schlüssel mehrfach verwenden, können nicht informationstheoretisch sicher sein

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

→ Verwendung von nicht informationstheoretisch sicheren Systemen notwendig

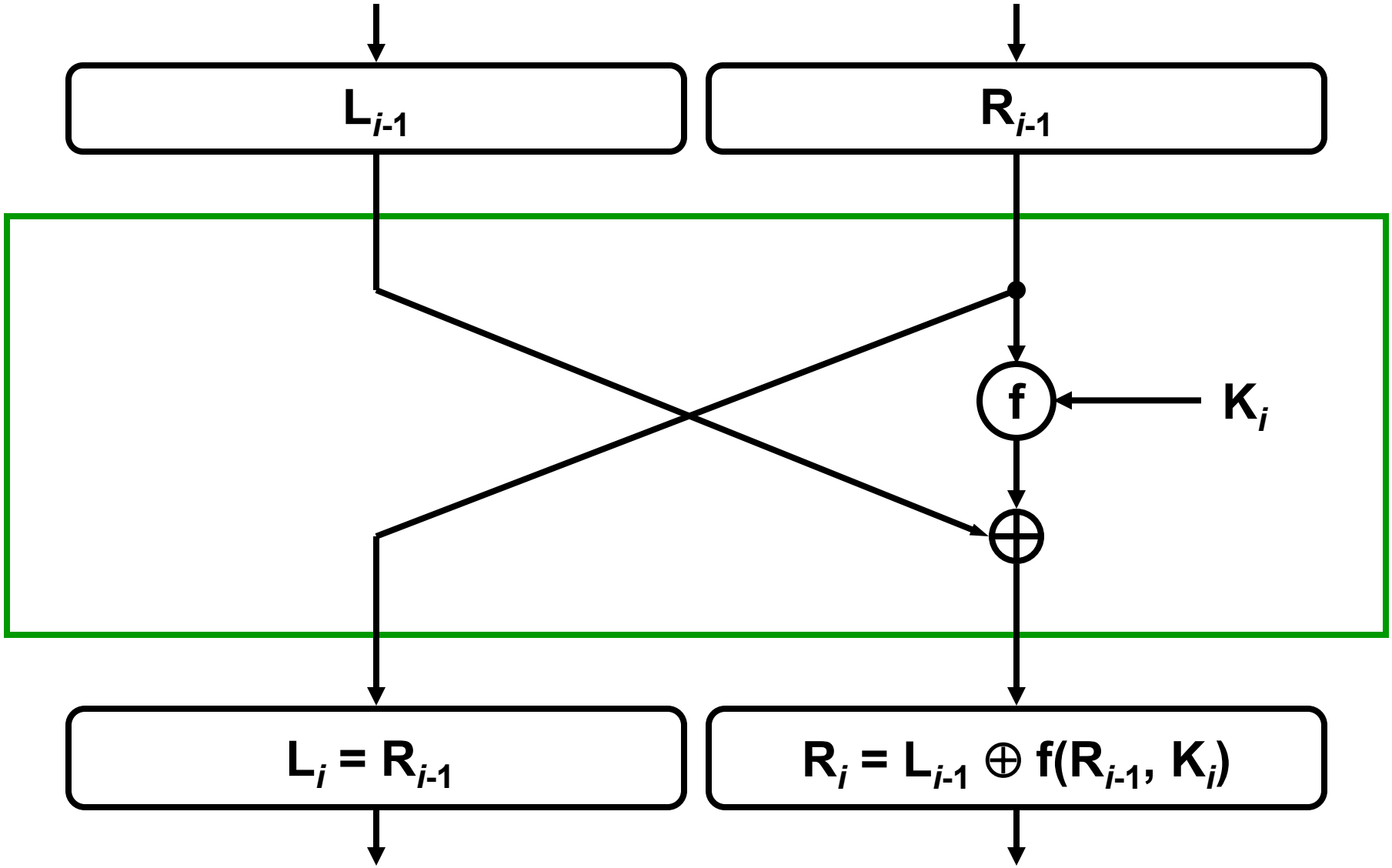
→ Annahmen über den Angreifer notwendig (notwendige Berechnungen des Angreifers sind *nicht effizient* möglich)

# Symmetric Cryptosystem DES

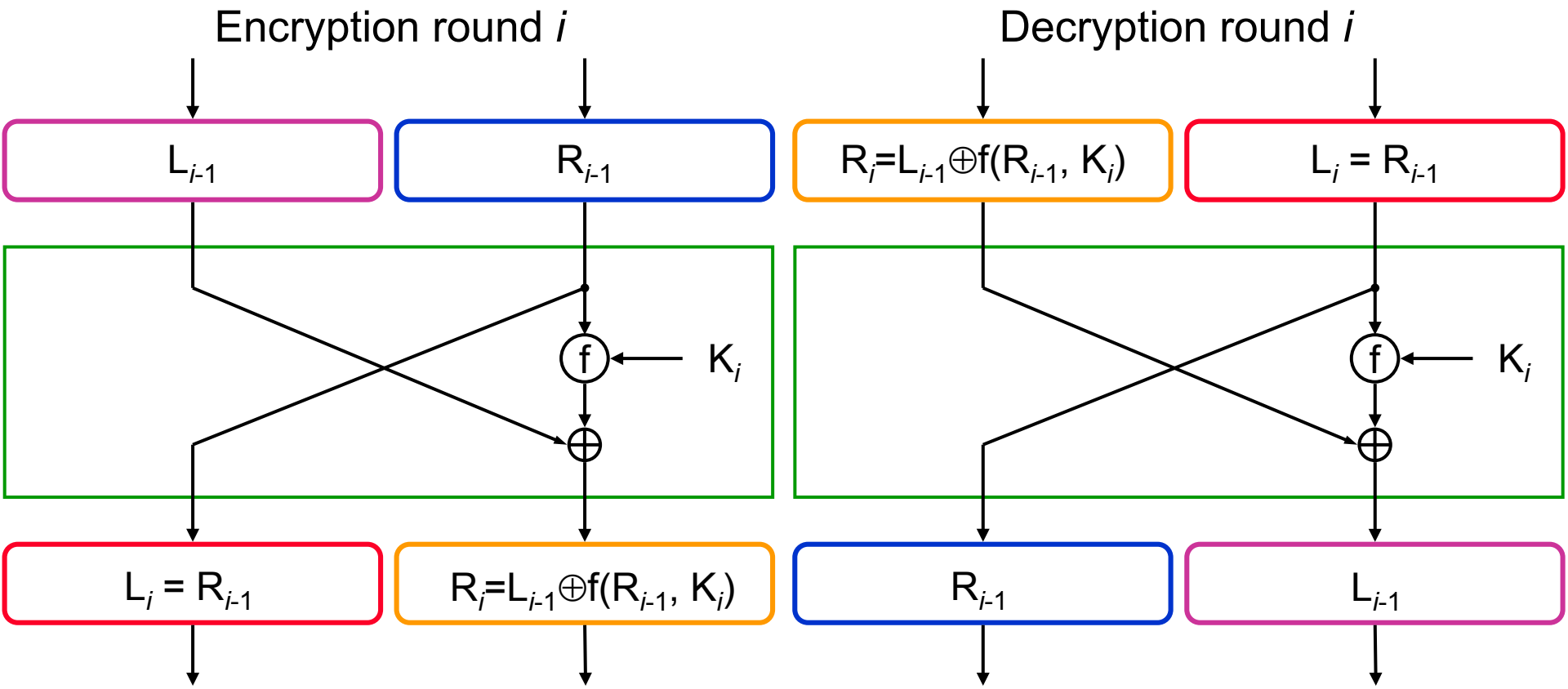


# One round

Feistel ciphers



# Why does decryption work?




Decryption

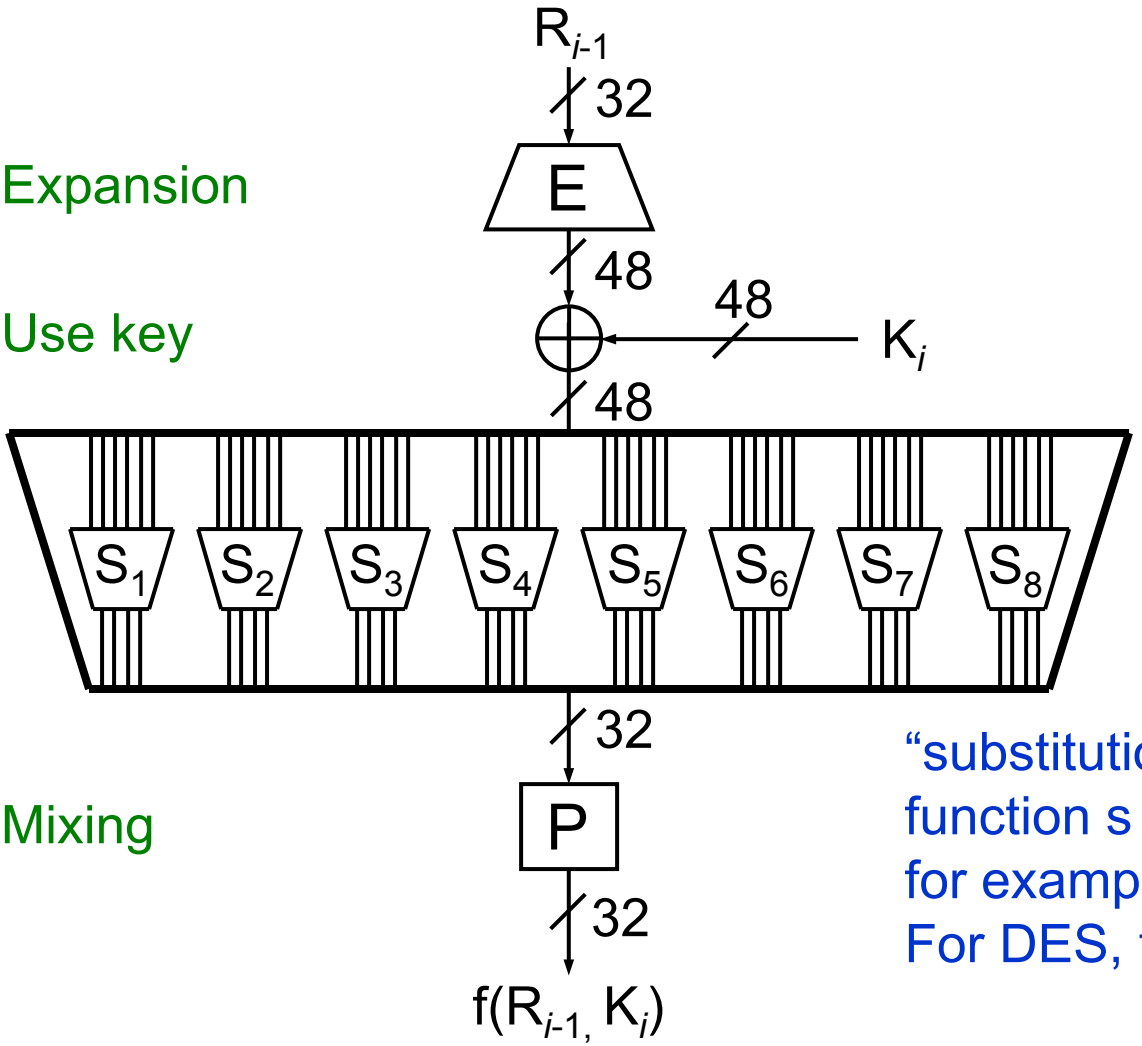
trivial

$L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(L_i, K_i) =$

$L_{i-1} \oplus f(L_i, K_i) \oplus f(L_i, K_i) = L_{i-1}$

replace $R_{i-1}$ by $L_i$

# Encryption function f




Expansion

Use key

Mixing

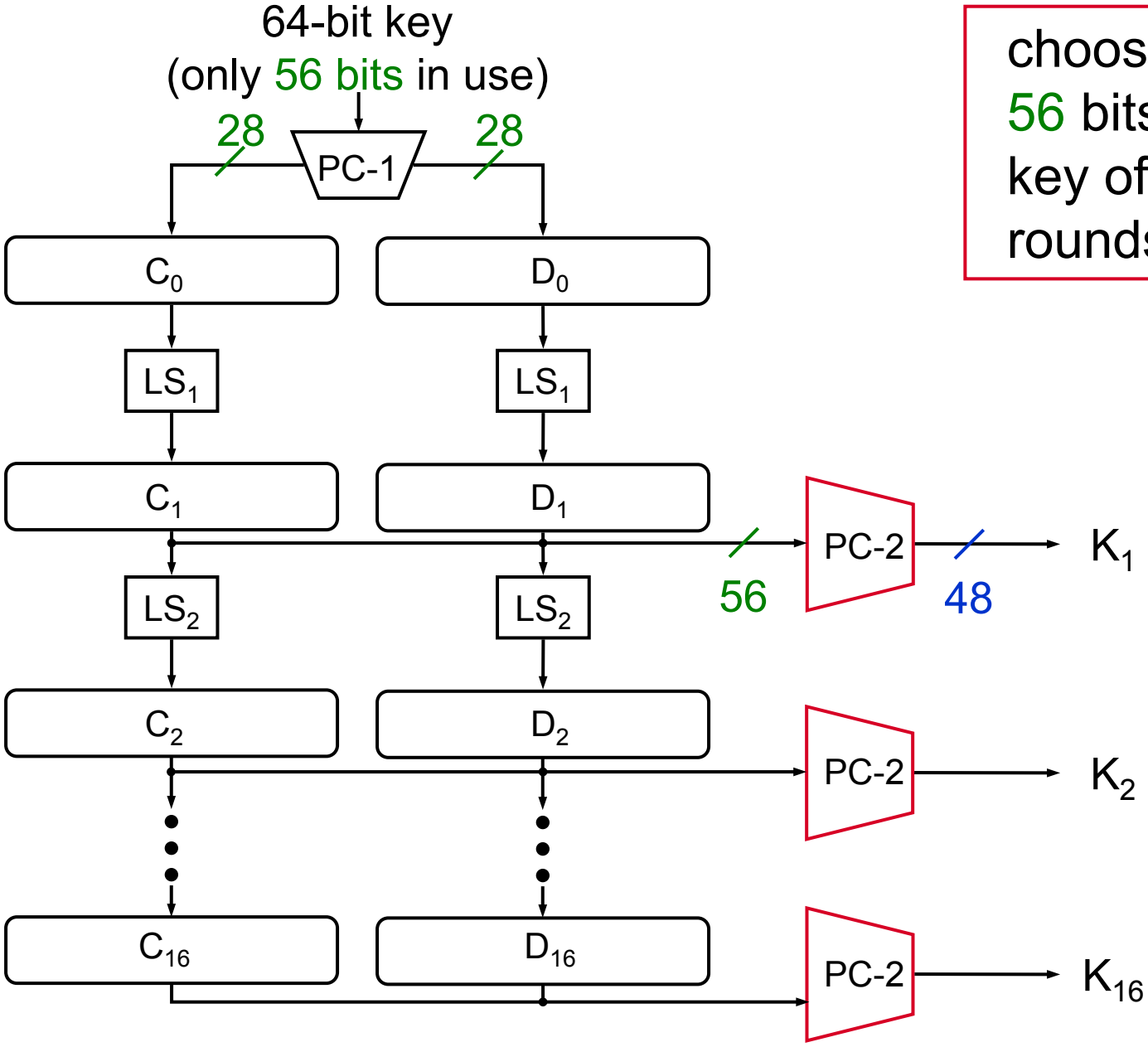
Make f (and DES) non-linear (permutations and $\oplus$ are linear)

"substitution box" S can implement any function $s : \{0,1\}^6 \rightarrow \{0,1\}^4$, for example as table.
For DES, the functions are fixed.

Terms

- Substitution-permutation networks
- Confusion - diffusion

# Generation of a key for each of the 16 rounds

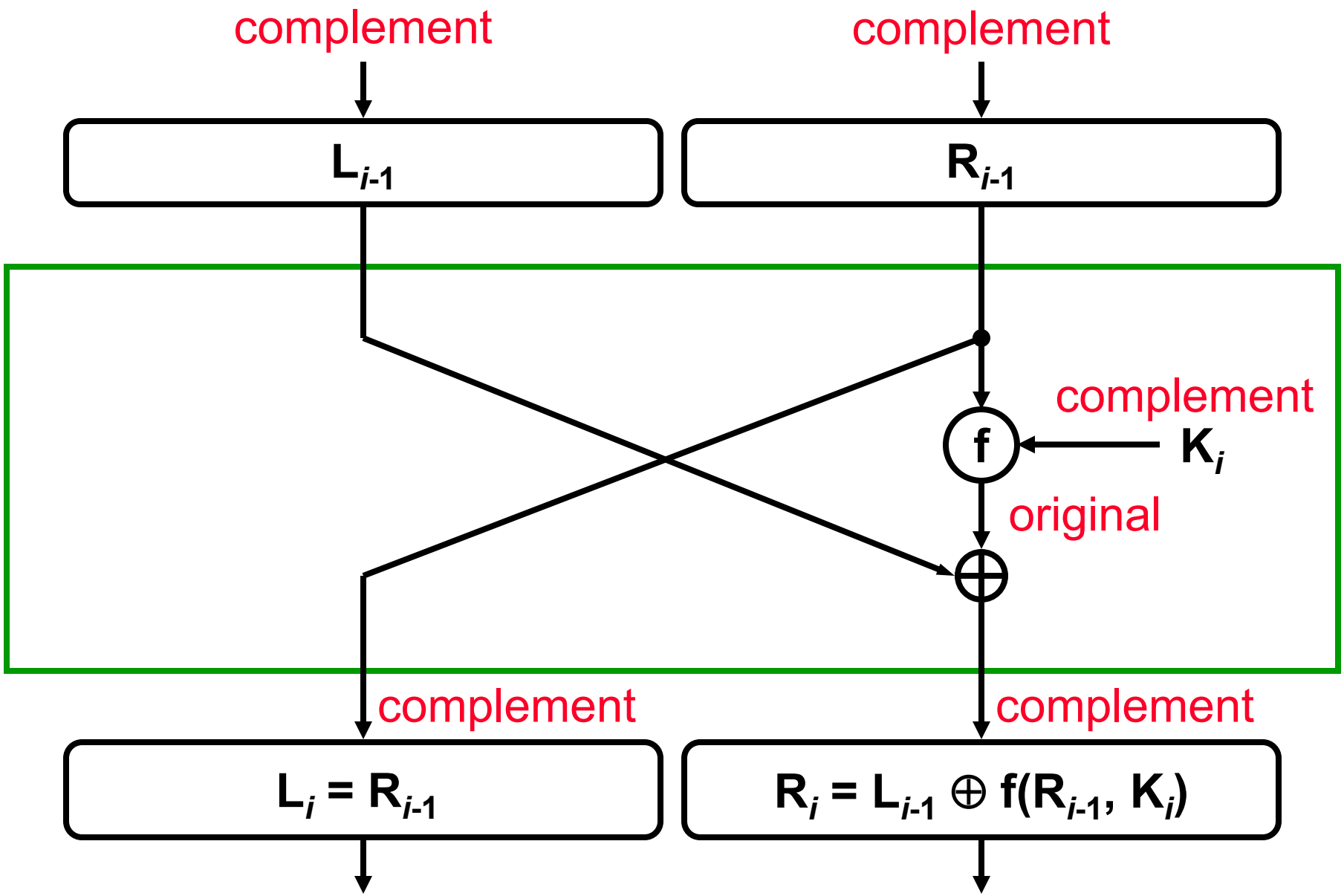



choose 48 of the 56 bits for each key of the 16 rounds

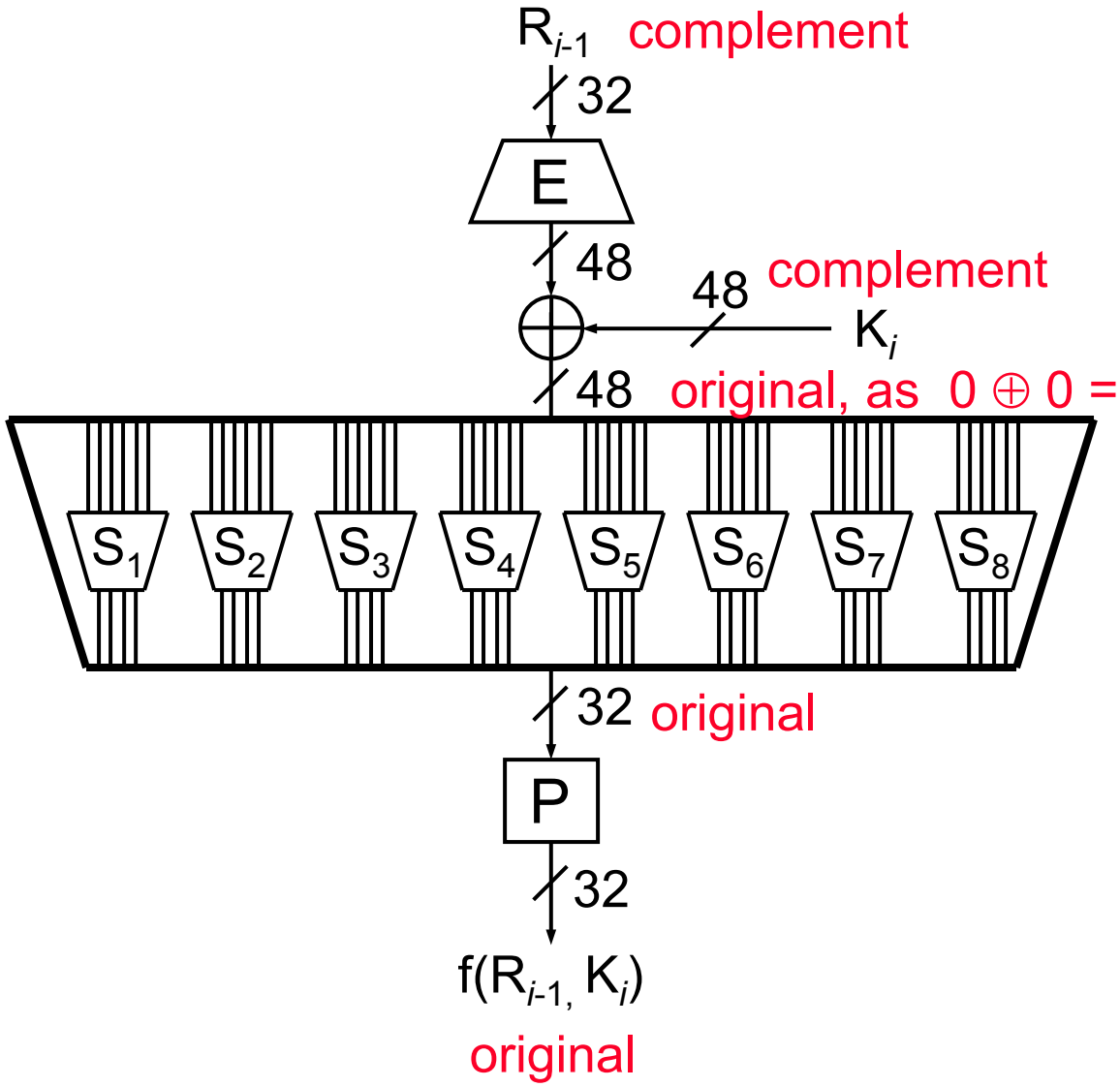
# The complementation property of DES

$$DES(\bar{k}, \bar{x}) = \overline{DES(k, x)}$$

# One round


complement
complement
$L_{i-1}$
$R_{i-1}$
complement
f
$K_i$
original
complement
complement
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

# Encryption function f



# Generalization of DES

1.) 56 $\Rightarrow$ 16 • 48 = 768 key bits

2.) variable substitution boxes

3.) variable permutations

4.) variable expansion permutation

5.) variable number of rounds