

# IT-Sicherheit

Kryptographie

Version vom 07.11.2017

# Kryptographie ist überall

- sichere Kommunikation

- web: HTTPS

- Funkübertragungen: WPA2, GSM, Bluetooth

- Verschlüsselte Datenträger: EFS, LUKS, BitLocker, VeraCrypt, ...

- Content Protection: BlueRay, DVD

- Nutzerauthentifizierung

- ...

Ziele:

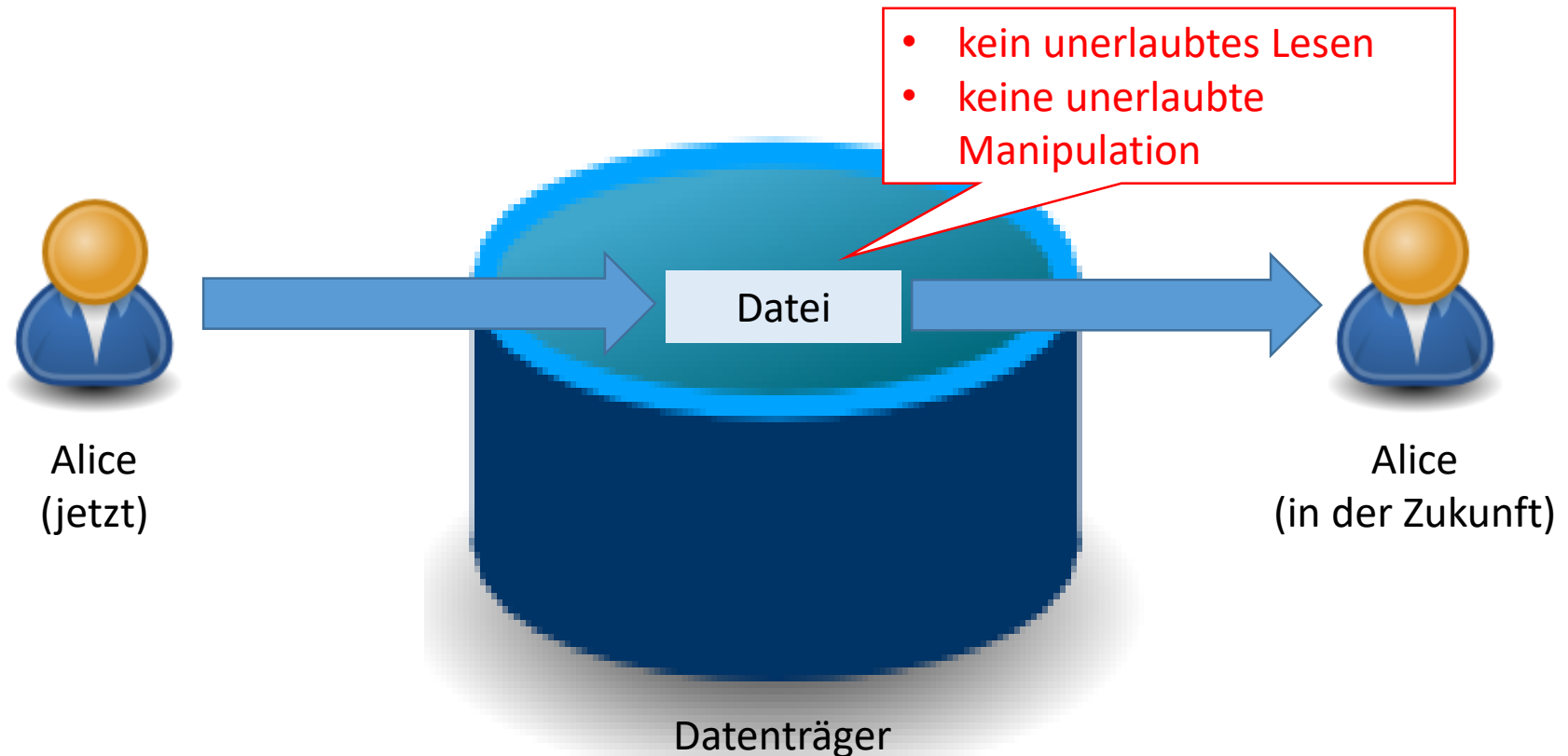
- Integrität
- Vertraulichkeit

# Secure Sockets Layer / Transport Layer Security

SSL / TLS teilt die Kommunikation in zwei Hauptteile auf:

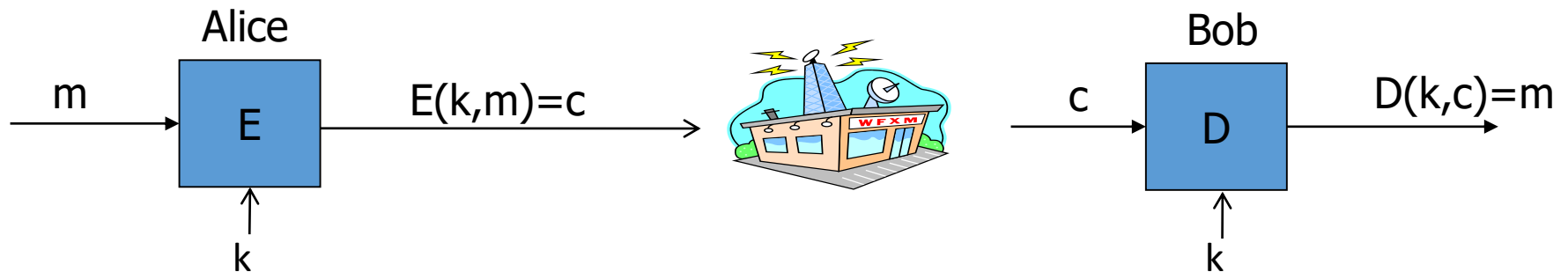
1. Handshake  
Es wird ein **gemeinsamer Schlüssel über ein Public-Key-Verfahren** ausgehandelt.
2. Record Layer  
Daten werden mit diesem **gemeinsamen Schlüssel verschlüsselt** ausgetauscht.  
➔ Vertraulichkeit und Integrität werden sichergestellt.

# Schutz von Dateien auf Datenträgern



Datenträgerschutz analog zu sicherer Kommunikation:  
Nachricht wird in die Zukunft gesendet.

# Symmetrische Verschlüsselung



E: Verschlüsselungsalgorithmus  
 D: Entschlüsselungsalgorithmus

m: Klartext

c: Ciphertext

k: geheimer Schlüssel

Chiffren (engl. Ciphers)

**Immer öffentlich bekannt!**

**Verwenden Sie niemals einen nicht-öffentlichen Verschlüsselungsalgorithmus!**

[Grafik: Dan Boneh, Cryptography I, Stanford University]

# „One time key“ vs. „Multi use key“

## Single use key (one time key)

- Schlüssel wird nur für eine einzelne Nachricht verwendet.
- Beispiel:  
Verschlüsselte E-Mail → neuer Schlüssel für jede Mail

## Multi use key

- Schlüssel wird für mehrere Nachrichten verwendet
- Beispiel:  
Verschlüsselte Dateien → gleicher Schlüssel für alle Dateien eines verschlüsselten Laufwerks
- etwas aufwendiger zu implementieren

# Fazit

## Kryptographie ist

- ein mächtiges Werkzeug
- die Grundlage vieler Sicherheitsmechanismen

## Kryptographie ist nicht

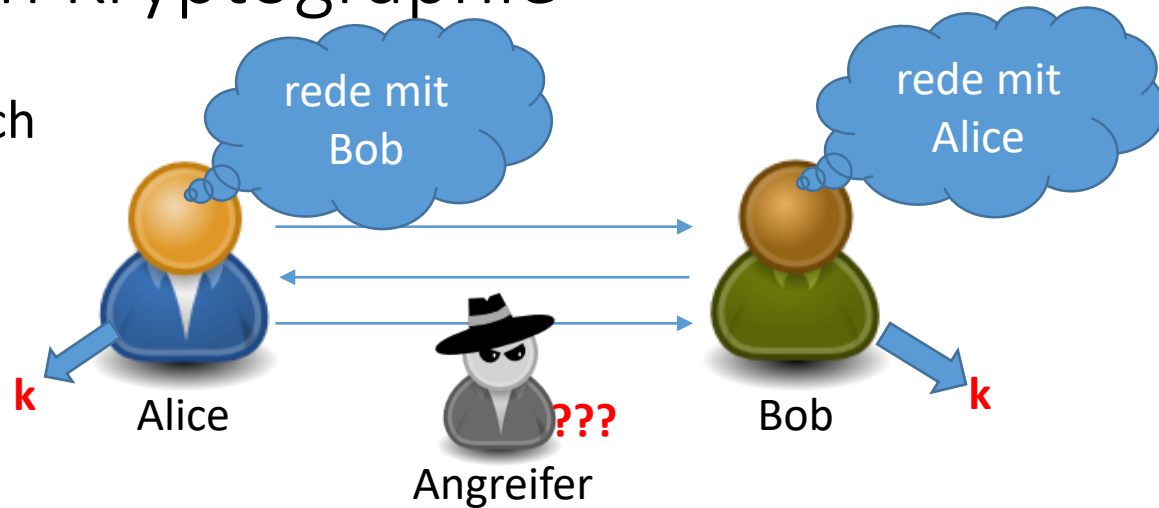
- die Lösung aller Sicherheitsprobleme
- verlässlich, wenn sie nicht sauber implementiert und angewendet wird
- **etwas, das Sie selbst neu erfinden sollten!**  
Es gibt zu viele Beispiele, in denen das schief ging (vgl. PC-Wahl).

# Was ist Kryptographie?



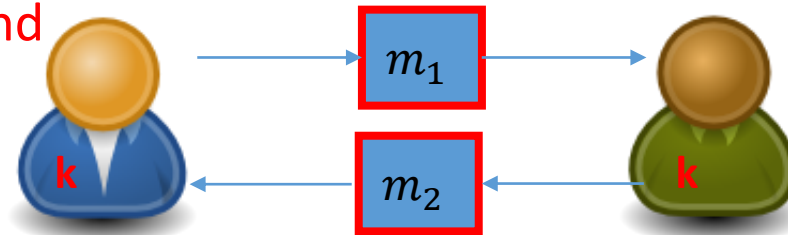
# Kernaufgaben von Kryptographie

## Sicherer Schlüsselaustausch



## Sichere Kommunikation

Ziel: **Vertraulichkeit und Integrität**



# Weitere Aufgaben von Kryptographie

- Digitale Signaturen und Unterschriften
- Anonyme Kommunikation
- Anonyme (pseudonyme) Währungen
  - Ausgeben von Kryptogeld ohne Identität zu verraten
  - Doppeltes Ausgeben vermeiden
- geheime Wahlen (Gewinner: Mehrheit der Stimmen)
- geheime Auktionen (Gewinner: Höchstes Gebot, Preis: zweithöchstes Gebot)
- sichere Gruppenkommunikation
- sicheres Outsourcing von Rechenleistung (Stichwort: homomorphe Chiffren), noch Gegenstand der Forschung
- Zero Knowledge Protokoll



# Grundsätzliche, wissenschaftliche Vorgehensweise

Entwicklung und Implementierung von Kryptographie bzw. kryptographischen Verfahren folgt i.A. folgenden Schritten:

1. Exakte Definition und Modellierung der Bedrohung
2. Vorschlag einer Konstruktion (Algorithmus, Protokoll, Nachrichten)
3. Beweis, dass der Bruch der Konstruktion bei der Bedrohung aus (1) identisch ist mit der Lösung eines zugrundeliegenden, schwierigen Problems

# Historische Kryptoverfahren

# Historische Verfahren

## 1. Ersetzungstabelle

$$c := E(k, \text{"text"}) = \text{"jkwj"}$$

$$D(k, C) = \text{"text"}$$

mit einfacher Häufigkeitsanalyse zu brechen  
→ unsicher

$$k := \begin{bmatrix} a \rightarrow x \\ \vdots \\ t \rightarrow j \\ \vdots \\ x \rightarrow w \\ y \rightarrow a \\ z \rightarrow l \end{bmatrix}$$

Wie viele Schlüssel existieren bei 26 verschiedenen Zeichen?

$$26! = 403291461126605635584000000 \approx 2^{88}$$

# Historische Verfahren

## 2. Caesar-Chiffre

Verschieben um ein konstantes Offset im Alphabet.

→ 25 verschiedene Schlüssel möglich (ca. 5 Bit)

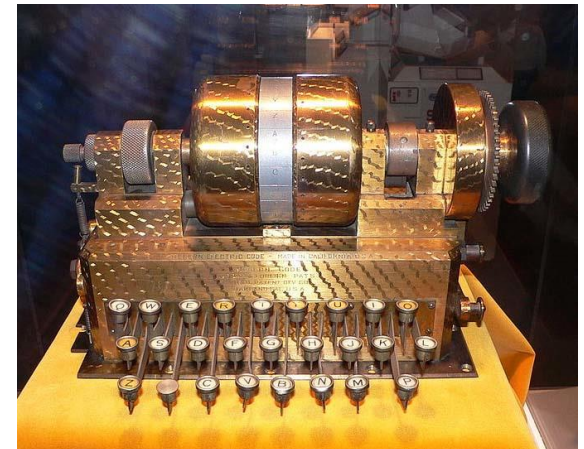
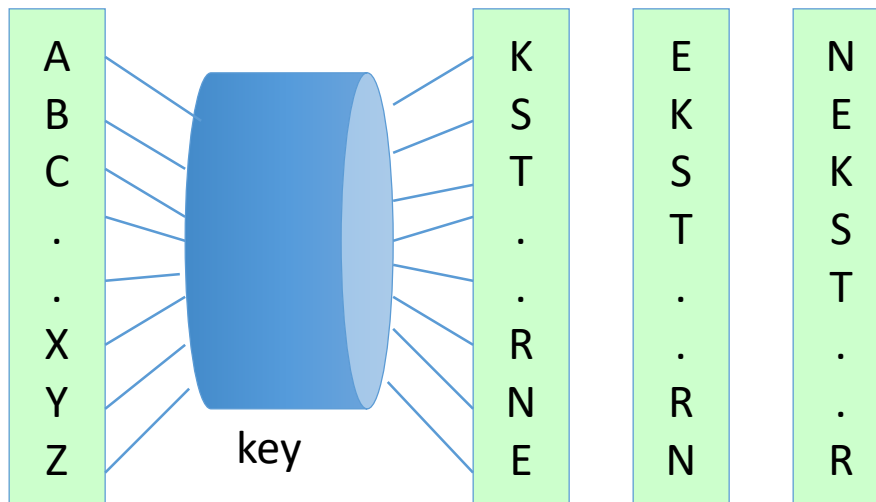
# Historische Verfahren

## 3. Vigenere Chiffre (ca. 16. Jahrhundert, Rom)



# Historische Verfahren

## 4. Rotor-basierte Maschinen: Hebern-Maschine

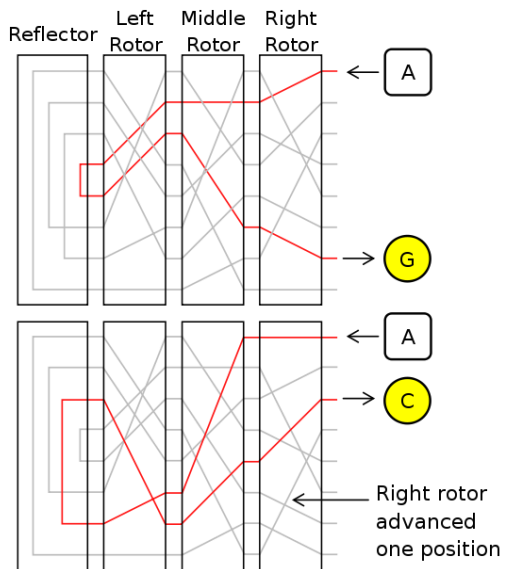


[Grafik: Dan Boneh, Cryptography I, Stanford University]



# Historische Verfahren

- Rotor-Maschinen: Enigma (3 bis 5 Rotoren)



Anzahl möglicher Schlüssel:  $26^4 = 2^{18}$

[Grafik: Dan Boneh, Cryptography I, Stanford University]

# Historische Verfahren

- DES (Data Encryption Standard)

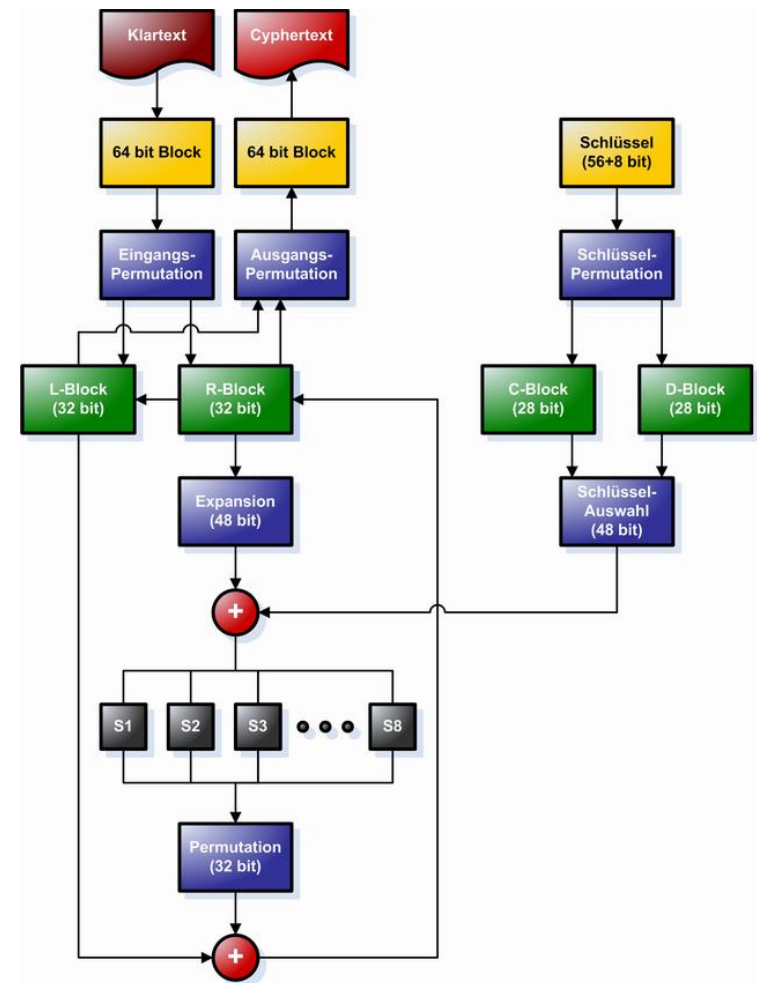
Symmetrische Verschlüsselung

arbeitet auf Blöcken von 64 bit

Anzahl möglicher Schlüssel:  $2^{56}$

1998 erstmals erfolgreich gebrochen.

Seit 11/2008 in weniger als einem Tag zu brechen.



[Grafik: Wikimedia]

# Diskrete Wahrscheinlichkeit

# Wahrscheinlichkeitsverteilung

Sei  $U$  eine endliche Menge (Beispiel:  $U = \{0,1\}^n$ ), dann

ist die **Wahrscheinlichkeitsverteilung**  $P$  über  $U$  eine Funktion  $P : U \rightarrow [0,1]$ , so dass  $\sum_{x \in U} P(x) = 1$

Beispiele:

1. Gleichverteilung:  $\forall x \in U: P(x) = \frac{1}{|U|}$
2. Punktverteilung bei  $x_0$ :  $P(x_0) = 1, \forall x \neq x_0: P(x) = 0$

Verteilungsvektor:  $(P(000), P(001), P(010), \dots, P(111))$

# Ereignis

- Für eine Teilmenge  $A \subseteq U$ :  $\Pr[A] := \sum_{x \in A} P(x) \in [0,1]$
- Die Menge  $A$  ist ein **Ereignis**.
- Hinweis:  $\Pr[U] = 1$
- Beispiel:
  - $U = \{0,1\}^8$  (Menge aller Bytewerte)
  - $A = \{x \in U, \text{so dass } \text{lsb}_2(x) = 11\} \subseteq U$
  - bei Gleichverteilung über  $\{0,1\}^8$  gilt  $\Pr[A] = ?$

# Zufallsvariablen

- Definition:

Eine Zufallsvariable  $X$  ist eine Funktion  $X: U \rightarrow V$

- Beispiel:

$$X: \{0,1\}^n \rightarrow \{0,1\}; \quad X(y) := \text{lsb}(y)$$

Bei Gleichverteilung über  $U$  gilt damit

$$\Pr[X = 0] = \frac{1}{2}, \quad \Pr[X = 1] = \frac{1}{2}$$

- Allgemein:

Zufallsvariable  $X$  definiert eine Verteilung über  $V$ :

$$\Pr[X = v] := \Pr[X^{-1}(v)]$$

# Randomisierter Algorithmus

- Deterministischer Algorithmus:  $y \leftarrow A(m)$

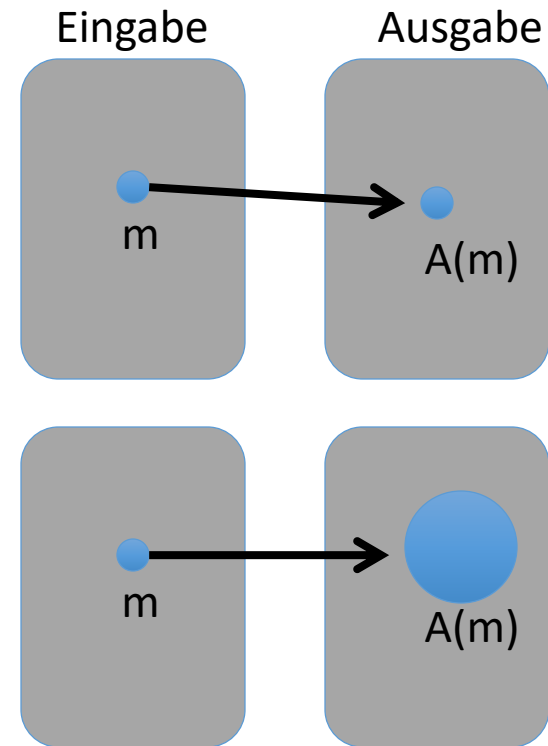
- Randomisierter Algorithmus  
 $y \leftarrow A(m; r)$  wobei  $r \xleftarrow{R} \{0,1\}^n$

Ausgabe ist eine Zufallsvariable:

$$y \xleftarrow{R} A(m)$$

- Beispiel Verschlüsselung

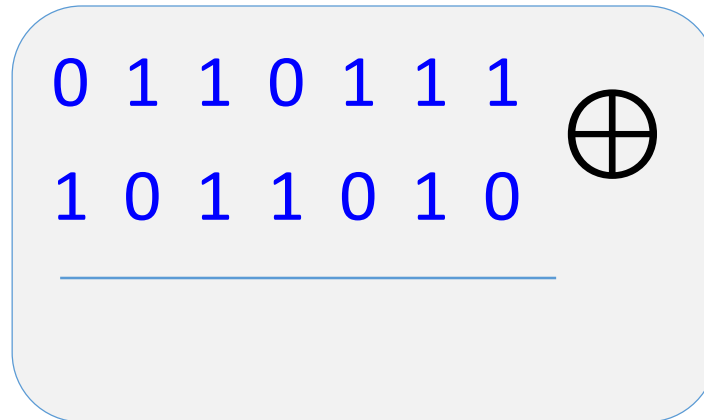
$$A(m; k) = E(k, m), \quad y \xleftarrow{R} A(m)$$



# XOR

XOR von zwei Elementen einer Menge  $\{0,1\}^n$  ist definiert als ihre bitweise Addition modulo 2:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0



$$\begin{array}{ccccccc}
 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
 \hline
 \end{array}
 \oplus$$



# Wichtige Eigenschaft von XOR

Sei

- $Y$  eine Zufallsvariable über  $\{0,1\}^n$  (Verteilung unbekannt!), und
- $X$  eine unabhängige, gleichverteilte Zufallsvariable über  $\{0,1\}^n$ , dann gilt
- $Z := X \oplus Y$  ist eine gleichverteilte Zufallsvariable über  $\{0,1\}^n$