Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

# Einführung IT Security

# Paradigmenwechsel der Kryptologie



Die Enigma markierte das Ende der klassischen Kryptologie und den Beginn der modernen Kryptologie.

1910er & 1920er (elektro-)mechanische Chiffriermaschinen

1920er & 1930er Kommerzialisierung & zivile Nutzung

1930er & 1940er Kryptoanalyse: Linguisten $\rightarrow$ Mathematiker

# Moderne Kryptologie



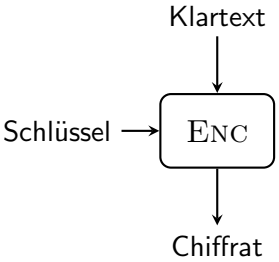
| | **symmetrische Kryptologie** | **asymmetrische Kryptologie** |
|---|---|---|
| **Vertraulichkeit** | symmetrische Verschlüsselung | asymmetrische Verschlüsselung |
| **Integrität** | MAC | Signaturen |
| **Schlüsselaustausch** | symmetrischer Schlüsselaustausch | asymmetrischer Schlüsselaustausch |
| **Kryptoanalyse** | symmetrische Kryptoanalyse | Mathematik |
| | Implementierungsangriffe | |
| | Seitenkanalanalyse | |
| **Bausteine** | Hashfunktionen<br>⋮ | <br>⋮ |

# Moderne Kryptologie

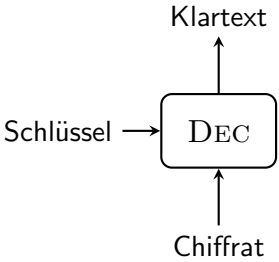


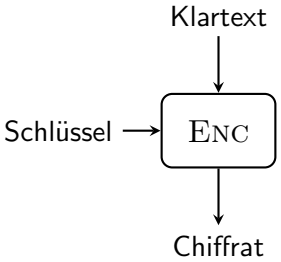
| | **symmetrische Kryptologie** | **asymmetrische Kryptologie** |
|---|---|---|
| **Vertraulichkeit** | symmetrische Verschlüsselung | asymmetrische Verschlüsselung |
| **Integrität** | MAC | Signaturen |
| **Schlüsselaustausch** | symmetrischer Schlüsselaustausch | asymmetrischer Schlüsselaustausch |
| **Kryptoanalyse** | symmetrische Kryptoanalyse | Mathematik |
| | Implementierungsangriffe | |
| | Seitenkanalanalyse | |
| **Bausteine** | Hashfunktionen | |
| | ⋮ | ⋮ |

## Verschlüsselung




## Entschlüsselung



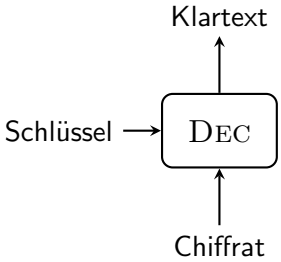



## Verschlüsselung

- kombiniert Klartext mit Schlüssel
- erzeugt Chiffrat (oder Chiffretext)

## Entschlüsselung

- kombiniert Chiffrat mit Schlüssel
- erzeugt Klartext
- Entschlüsselung ohne Schlüssel ist schwer



## Schlüssel

- gleicher Schlüssel für Ver- und Entschlüsselung
- unstrukturierter Bitstring
- (fast) jeder Bitstring (entsprechender Länge) ist gültiger Schlüssel
- Länge entspricht Komplexität

Image by 8385 from Pixabay

# Entropie

## Logarithmus

$$\log_2 16 = 4$$

$$2^4 = 16$$

$$\log_n x = a \iff n^a = x$$

$n = 10$

$\log_n x$

$\log_{10} 10.000 = 4 \quad \Leftrightarrow \quad 10^4 = 10.000$

0 - 9.999

Wie viele Stellen (Ziffern) braucht man, um Zahlen 1 - 10.000 darzustellen?

$\log_{10} 4.819 \approx 4$

$\log_2 1.000 \approx 10$

$2^{10} = 1.024$

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16$

$\vdots$

$2^8 = 256$

$2^9 = 512$

$2^{10} = 1.024 \approx 1.000$

$\log_2 2.000 \approx 11$

Was ist $\log_2 8$?

Eigenschaften den Logarithmus:

- $\log(a \cdot b) = \log a + \log b$
- $\log a^x = x \cdot \log a$
- $\log \frac{1}{a} = -\log a$

Was ist $\log_2 8$?

$\log_2 8 = 3$ denn $2^3 = 8$.

Eigenschaften den Logarithmus:

- $\log(a \cdot b) = \log a + \log b$
- $\log a^x = x \cdot \log a$
- $\log \frac{1}{a} = -\log a$

Wie viel Entropie enthält eine Zeichenkette?

- Was ist Entropie?
- Wie viel Entropie enthält ein Zeichen?
- Wie berechnet sich die Entropie einer Zeichenkette?

Image by OpenClipart-Vectors from Pixabay

Informationsgehalt $I$ eines Zeichens $z$

$I(z) = -\log_2 p_z$ $\quad$ $p_z$ : Wahrscheinlichkeit von $z$

$I(1) = -\log_2 1 = 0$ $\quad$ $z = 1$, $p_z = 1$

$\log_2 \frac{1}{2} = -1 \quad \Leftrightarrow \quad 2^{-1} = \frac{1}{2}$

Informationsgehalt $I$ eines Zeichens $z$

$$I(z) = -\log_2 p_z \qquad p_z : \text{ Wahrscheinlichkeit von } z$$

Beispiel: fairer Münzwurf $\rightarrow I(\text{'Zahl'}) = 1$ Bit

$I(\text{'Zahl'}) = -\log_2 \frac{1}{2} = -(-1) = 1$

W8 achtseitiger Würfel

Informationsgehalt $I$ eines Zeichens $z$

$$I(z) = -\log_2 p_z \qquad p_z : \text{ Wahrscheinlichkeit von } z$$

$$I('5') = -\log_2 \frac{1}{8} = 3 \text{ Bit}$$

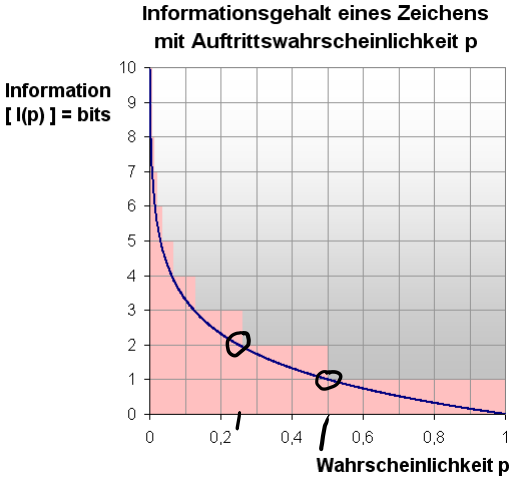
Informationsgehalt $I$ eines Zeichens $z$

$$I(z) = -\log_2 p_z \qquad p_z : \text{ Wahrscheinlichkeit von } z$$

Beispiel: fairer Münzwurf $\rightarrow I(\text{‘Zahl’}) = 1$ Bit

Beispiel: Würfelwurf $\rightarrow I(\text{‘6’}) \approx 2,6$ Bit

# Entropie




von Akribix - Eigenes Werk

1 € Kosten

1-4: 0€ Gewinn

5-6: 2€ Gewinn

1: $0€ \cdot \frac{1}{6}$ 5: $2€ \cdot \frac{1}{6}$

2: "

3: " 6: $2€ \frac{1}{6}$

4: "

$\mathbb{E}(\text{Gewinn}) = 0€ \cdot \frac{2}{3} + 2€ \cdot \frac{1}{3} = \frac{2}{3}€$

1: $0€ \cdot \frac{1}{6}$ 5: $2€ \cdot \frac{1}{6}$

2: " 6: $2€ \cdot \frac{1}{6}$

3: "

4: "

$$\mathbb{E}(\text{Gewinn}) = \sum_{n=1}^{6} p_n \cdot \text{Gewinn}(n) =$$

$$= \underbrace{\frac{1}{6} \cdot 0€}_{n=1} + \underbrace{\frac{1}{6} \cdot 0€}_{n=2} + \underbrace{\frac{1}{6} \cdot 0€}_{n=3} + \underbrace{\frac{1}{6} \cdot 0€}_{n=4} + \underbrace{\frac{1}{6} \cdot 2€}_{n=5} + \underbrace{\frac{1}{6} \cdot 2€}_{n=6}$$

$$= 0€ \cdot \frac{2}{3} + 2€ \cdot \frac{1}{3} = \frac{2}{3}€$$

$$\sum_{n=1}^{15} n = 1 + 2 + 3 + \ldots + 15$$

$$\prod_{i=1}^{15} n = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 15$$

Entropie einer Quelle ist der erwartete (mittlere) Informationsgehalt eines Zeichens

$$H = \mathbb{E}[I] = \sum_z p_z \cdot I(z) = -\sum_z p_z \cdot \log_2 p_z$$

$$= \underbrace{(-\tfrac{1}{8}) \cdot \log_2 \tfrac{1}{8} + \ldots + (-\tfrac{1}{8}) \cdot \log_2 \tfrac{1}{8}}_{8\text{-mal}} = -8 \cdot \tfrac{1}{8} \cdot \log_2 \tfrac{1}{8}$$

$$= -(-3) = 3 \text{ Bit}$$

Entropie einer Quelle ist der erwartete (mittlere) Informationsgehalt eines Zeichens

$$H = \mathbb{E}[I] = \sum_z p_z \cdot I(z) = -\sum_z p_z \cdot \log_2 p_z$$

Sonderfall: alle $n$ Zeichen gleich wahrscheinlich:

$$H = -\log_2 \frac{1}{n} = \log_2 n$$

W4 fair: 2 Bit

$p_1 = \frac{1}{4}$

$p_2 = \frac{1}{2}$

$p_3 = \frac{1}{8}$

$p_4 = \frac{1}{8}$

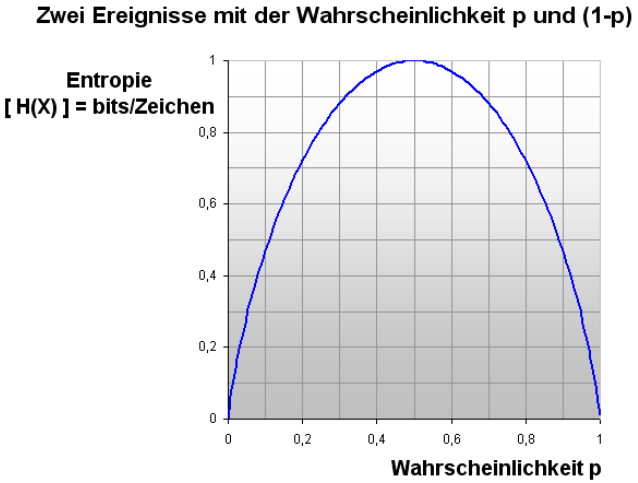
$$H = -\sum_{i=1}^{4} p_i \cdot \log_2 p_i$$

$$= \frac{1}{4} \cdot 2 + \frac{1}{2} \cdot 1 + \frac{1}{8} \cdot 3 + \frac{1}{8} \cdot 3$$

$p_a \cdot \log_2 p_a$

$$= \frac{1}{2} + \frac{1}{2} + \frac{3}{8} + \frac{3}{8} = 1 + \frac{3}{4} = 1{,}75 < 2$$

# Entropie




von Akribix - Eigenes Werk