

## Prinzip 1 Sicherheitsziel

Die Sicherheitsziele müssen präzise definiert werden.

### Beispiele für ungenügende Definitionen von Sicherheit

- *Kein Angreifer kann  $k$  finden.* Betrachte  $Enc_k(\cdot)$ , das die Identität berechnet:  $k$  wird zum Entschlüsseln nicht benötigt.
- *Kein Angreifer kann die zugrundeliegende Nachricht bestimmen.* Möglicherweise können 90% der Nachricht bestimmt werden.
- *Kein Angreifer kann einen Buchstaben des Klartexts bestimmen.* Möglicherweise kann der Angreifer zwischen zwei Nachrichten – z.B. JA und NEIN – unterscheiden.
- *Kein Angreifer erhält Information über den Klartext vom Chiffretext.* Gut, erfordert aber Spezifikation des Begriffs Information.

**Alternative Definition:** *Kein Angreifer kann für einen Chiffretext eine Funktion auf dem zugrundeliegenden Klartext berechnen.*

# Prinzip 2 – Präzisierung der Annahmen

## Prinzip 2 Komplexitätsannahme

Es muss spezifiziert werden, unter welchen Annahmen das System als sicher gilt.

### Eigenschaften:

- Annahmen sollten unabhängig von der Kryptographie sein. Bsp: Das Faktorisierungsproblem ist nicht in polynomial-Zeit lösbar.
- Angriffsszenario KO, KP, CPA oder CCA muss definiert werden.
- Wir müssen das Berechnungsmodell des Angreifers definieren, z.B. eine Beschränkung auf ppt Angreifer.

# Prinzip 3 – Reduktionsbeweis der Sicherheit

## Prinzip 3 Beweis der Sicherheit

Wir beweisen, dass unter den gegebenen Annahmen *kein* Angreifer die Sicherheit brechen kann.

### Anmerkungen:

- D.h. wir beweisen, dass das System gegen **alle** Angreifer sicher ist, unabhängig von der Herangehensweise des Angreifers!
- Typische Beweisaussage: “Unter Annahme  $X$  folgt die Sicherheit von Konstruktion  $Y$  bezüglich der Sicherheitsdefinition  $Z$ ”.
- Der Beweis erfolgt per Reduktion: Ein erfolgreicher Angreifer  $\mathcal{A}$  für  $Y$  bezüglich  $Z$  wird transformiert in einen Algorithmus  $\mathcal{B}$ , der Annahme  $X$  verletzt.

**Bsp:** Angreifer  $\mathcal{A}$  auf die CCA-Sicherheit einer Verschlüsselung liefert einen Algorithmus  $\mathcal{B}$  zum Faktorisieren.

# Perfekte Sicherheit

## Szenario:

- Angreifer besitzt *unbeschränkte* Berechnungskraft.
- Seien  $\mathcal{M}, \mathcal{K}, \mathcal{C}$  versehen mit Ws-Verteilungen.
- Sei  $M$  eine Zufallsvariable für die Ws-Verteilung auf  $\mathcal{M}$ , d.h. wir ziehen ein  $m \in \mathcal{M}$  mit  $\text{Ws}[M = m]$ .
- Analog definieren wir Zufallsvariablen  $K$  für  $\mathcal{K}$  und  $C$  für  $\mathcal{C}$ .
- Es gelte oBdA  $\text{Ws}[M = m] > 0$  und  $\text{Ws}[C = c] > 0$  für alle  $m \in \mathcal{M}, c \in \mathcal{C}$ . (anderenfalls entferne  $m$  aus  $\mathcal{M}$  bzw.  $c$  aus  $\mathcal{C}$ )

## Definition Perfekte Sicherheit

Ein Verschlüsselungsverfahren  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  heißt *perfekt sicher*, falls  $\text{Ws}[M = m \mid C = c] = \text{Ws}[M = m]$  für alle  $m \in \mathcal{M}, c \in \mathcal{C}$ .

**Interpretation:**  $c$  liefert dem Angreifer keine Informationen über  $m$ .

# Verteilung auf Chiffretexten unabhängig vom Plaintext

## Satz Chiffretext-Verteilung

Ein Verschlüsselungsverfahren  $\Pi$  ist perfekt sicher gdw  $W_s[C = c \mid M = m] = W_s[C = c]$  für alle  $m \in \mathcal{M}, c \in \mathcal{C}$ .

### Beweis:

- " $\Rightarrow$ ": Sei  $\Pi$  perfekt sicher. Nach dem Satz von Bayes gilt

$$\frac{W_s[C = c \mid M = m] \cdot W_s[M = m]}{W_s[C = c]} = W_s[M = m \mid C = c] = W_s[M = m].$$

- Daraus folgt  $W_s[C = c \mid M = m] = W_s[C = c]$ .
- " $\Leftarrow$ ": Aus  $W_s[C = c \mid M = m] = W_s[C = c]$  folgt mit dem Satz von Bayes  $W_s[M = m] = W_s[M = m \mid C = c]$ .
- Damit ist  $\Pi$  perfekt sicher.

# Ununterscheidbarkeit von Verschlüsselungen

## Satz Ununterscheidbarkeit von Verschlüsselungen

Ein Verschlüsselungsverfahren  $\Pi$  ist perfekt sicher gdw für alle  $m_0, m_1 \in \mathcal{M}$ ,  $c \in \mathcal{C}$  gilt  $\text{Ws}[C = c \mid M = m_0] = \text{Ws}[C = c \mid M = m_1]$ .

### Beweis:

- " $\Rightarrow$ ": Mit dem Satz auf voriger Folie gilt für perfekt sichere  $\Pi$   
 $\text{Ws}[C = c \mid M = m_0] = \text{Ws}[C = c] = \text{Ws}[C = c \mid M = m_1]$ .
- " $\Leftarrow$ ": Sei  $m' \in \mathcal{M}$  beliebig. Es gilt

$$\begin{aligned}\text{Ws}[C = c] &= \sum_{m \in \mathcal{M}} \text{Ws}[C = c \mid M = m] \cdot \text{Ws}[M = m] \\ &= \text{Ws}[C = c \mid M = m'] \cdot \sum_{m \in \mathcal{M}} \text{Ws}[M = m] \\ &= \text{Ws}[C = c \mid M = m'].\end{aligned}$$

- Die perfekte Sicherheit von  $\Pi$  folgt mit dem Satz auf voriger Folie.

# Das One-Time Pad (Vernam Verschlüsselung)

## Definition One-Time Pad (1918)

Sei  $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^\ell$ .

- 1 **Gen:** Ausgabe  $k \in_R \{0, 1\}^\ell$
- 2 **Enc:** Für  $m \in \{0, 1\}^\ell$  Ausgabe  $c = \text{Enc}_k(m) := m \oplus k$ .
- 3 **Dec:** Für  $c \in \{0, 1\}^\ell$  Ausgabe  $m = \text{Dec}_k(c) := c \oplus k$ .

## Satz Sicherheit des One-Time Pads

Das One-Time Pad ist perfekt sicher.

### Beweis:

- Wegen  $C = M \oplus K$  gilt für alle  $m_0, m_1 \in \mathcal{M}$  und  $c \in \mathcal{C}$

$$\begin{aligned} \text{Ws}[C = c \mid M = m_0] &= \text{Ws}[M \oplus K = c \mid M = m_0] = \text{Ws}[K = m_0 \oplus c] \\ &= \frac{1}{2^\ell} = \text{Ws}[C = c \mid M = m_1]. \end{aligned}$$

- Damit ist das One-Time Pad perfekt sicher.

# Beschränkungen perfekter Sicherheit

## Satz Größe des Schlüsselraums

Sei  $\Pi$  perfekt sicher. Dann gilt  $|\mathcal{K}| \geq |\mathcal{M}|$ .

**Beweis:** Angenommen  $|\mathcal{K}| < |\mathcal{M}|$ .

- Für  $c \in \mathcal{C}$  definiere  $D(c) = \{m \mid m = Dec_k(c) \text{ für ein } k \in \mathcal{K}\}$ .
- Es gilt  $|D(c)| \leq |\mathcal{K}|$ , da jeder Schlüssel  $k$  genau ein  $m$  liefert.
- Wegen  $|\mathcal{K}| < |\mathcal{M}|$  folgt  $|D(c)| < |\mathcal{M}|$ . D.h. es gibt ein  $m \in \mathcal{M}$  mit
$$\text{Ws}[M = m \mid C = c] = 0 < \text{Ws}[M = m].$$
- Damit ist  $\Pi$  nicht perfekt sicher.

# Satz von Shannon (1949)

## Satz von Shannon

Sei  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  mit  $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$ .  $\Pi$  ist perfekt sicher gdw

- 1  $\text{Gen}$  wählt alle  $k \in \mathcal{K}$  gleichverteilt mit Ws  $\frac{1}{|\mathcal{K}|}$ .
- 2 Für alle  $m \in \mathcal{M}, c \in \mathcal{C}$  existiert genau ein  $k \in \mathcal{K}$ :  $c = \text{Enc}_k(m)$ .

## Beweisidee:

- " $\Leftarrow$ ": Jedes  $c \in \mathcal{C}$  korrespondiert zu genau einem  $m \in \mathcal{M}$  via  $k$ .
- D.h.  $c$  wird zu  $m$  entschlüsselt, falls  $k$  verwendet wird.
- Dies geschieht gleichverteilt mit Ws  $\frac{1}{|\mathcal{K}|}$ . Damit gilt

$$\text{Ws}[\mathbf{C} = c \mid \mathbf{M} = m] = \frac{1}{|\mathcal{K}|} \text{ für alle } m \in \mathcal{M}.$$

- Es folgt  $\text{Ws}[\mathbf{C} = c \mid \mathbf{M} = m_0] = \frac{1}{|\mathcal{K}|} = \text{Ws}[\mathbf{C} = c \mid \mathbf{M} = m_1]$ .

# Satz von Shannon (1949)

## Beweisidee (Fortsetzung):

- " $\Rightarrow$ ": Sei  $\Pi$  perfekt sicher mit  $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$ .
- Ann:  $\exists(m, c)$  mit  $c \neq \text{Enc}_k(m)$  für alle  $k \in \mathcal{K}$ . Dann gilt  $\text{Ws}[M = m | C = c] = 0 < \text{Ws}[M = m]$ . (Widerspruch)
- Ann:  $\exists(m, c)$  mit  $c = \text{Enc}_k(m)$  für mehrere  $k \in \mathcal{K}$ . Dann existiert ein  $(m', c')$  mit  $c' \neq \text{Enc}_k(m')$  für alle  $k \in \mathcal{K}$ . (Widerspruch)
- Damit gibt es für jedes feste  $c$  und jedes  $m$  genau einen Schlüssel  $k_m$  mit  $c = \text{Enc}_{k_m}(m)$ .
- Daraus folgt für alle  $m, m'$

$$\begin{aligned}\text{Ws}[K = k_m] &= \text{Ws}[C = c | M = m] \\ &= \text{Ws}[C = c | M = m'] = \text{Ws}[K = k_{m'}].\end{aligned}$$

- D.h. es gilt  $\text{Ws}[K = k] = \frac{1}{|\mathcal{K}|}$  für alle  $k \in \mathcal{K}$ .