Universität Potsdam – Institut für Informatik

Seminar Kryptographie und Datensicherheit

Datensicherheit und Shannons Theorie

Marco Michael

2. November 2006

Inhalt

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Sicherheit?

Definitionsansätze für Sicherheit von Kryptosystemen

Kryptosysteme haben . . .

Definitionsansätze für Sicherheit von Kryptosystemen

Kryptosysteme haben . . .

- rechenbetonte Sicherheit (*computational security*)
  - Mindestens N Rechenoperationen notwendig (N sehr groß)
  - Kann nur auf spezifische Attacken gezeigt werden

Definitionsansätze für Sicherheit von Kryptosystemen

Kryptosysteme haben . . .

- rechenbetonte Sicherheit (*computational security*)
  - Mindestens N Rechenoperationen notwendig (N sehr groß)
  - Kann nur auf spezifische Attacken gezeigt werden
- beweisbare Sicherheit (*provable security*)
  - Reduzierung auf gut untersuchtes schweres Problem
  - Kein direkter Beweis für Sicherheit, da nur relativ zu einem anderen Problem

Definitionsansätze für Sicherheit von Kryptosystemen

Kryptosysteme haben . . .

- rechenbetonte Sicherheit (*computational security*)
  - Mindestens N Rechenoperationen notwendig (N sehr groß)
  - Kann nur auf spezifische Attacken gezeigt werden
- beweisbare Sicherheit (*provable security*)
  - Reduzierung auf gut untersuchtes schweres Problem
  - Kein direkter Beweis für Sicherheit, da nur relativ zu einem anderen Problem
- unbedingte Sicherheit (*unconditional security*)
  - Keine Bedingung an Rechenoperationen
  - Selbst mit unbegrenzter Rechenkapazität nicht zu knacken

Definitionsansätze für Sicherheit von Kryptosystemen

Kryptosysteme haben . . .

- rechenbetonte Sicherheit (*computational security*)
  - Mindestens N Rechenoperationen notwendig (N sehr groß)
  - Kann nur auf spezifische Attacken gezeigt werden
- beweisbare Sicherheit (*provable security*)
  - Reduzierung auf gut untersuchtes schweres Problem
  - Kein direkter Beweis für Sicherheit, da nur relativ zu einem anderen Problem
- unbedingte Sicherheit (*unconditional security*)
  - Keine Bedingung an Rechenoperationen
  - Selbst mit unbegrenzter Rechenkapazität nicht zu knacken

Untersuchung von Kryptosystemen auf unbedingte Sicherheit $\longrightarrow$ Wahrscheinlichkeitstheorie

Wahrscheinlichkeitstheorie

Einführung

Definition 1: Eine *diskrete Zufallsgröße* $\mathbf{X}$ besteht aus einer endlichen Menge X und einer auf X definierten *Wahrscheinlichkeitsverteilung*. Die Wahrscheinlichkeit, dass die Zufallsgröße $\mathbf{X}$ den Wert x annimmt wird mit $\mathbf{Pr}[\mathbf{X} = x]$ bezeichnet (kurz $\mathbf{Pr}[x]$, falls $\mathbf{X}$ fest). Weiterhin muss gelten $0 \leq \mathbf{Pr}[x], \forall x \in X$, und $\sum_{x \in X} \mathbf{Pr}[x] = 1$.

Einführung

Definition 1: Eine *diskrete Zufallsgröße* $\mathbf{X}$ besteht aus einer endlichen Menge X und einer auf X definierten *Wahrscheinlichkeitsverteilung*. Die Wahrscheinlichkeit, dass die Zufallsgröße $\mathbf{X}$ den Wert x annimmt wird mit $\mathbf{Pr}[\mathbf{X} = x]$ bezeichnet (kurz $\mathbf{Pr}[x]$, falls $\mathbf{X}$ fest). Weiterhin muss gelten $0 \leq \mathbf{Pr}[x], \forall x \in X$, und $\sum_{x \in X} \mathbf{Pr}[x] = 1$.

Definition 2: Sei $\mathbf{X}$ eine Zufallsgröße definiert auf X. Dann heißt $E \subseteq X$ *Ereignis*. Die Wahrscheinlichkeit, dass $\mathbf{X}$ einen Wert aus E annimmt, berechnet sich durch $\sum_{x \in E} \mathbf{Pr}[x]$.

Einführung

Definition 1: Eine *diskrete Zufallsgröße* $\mathbf{X}$ besteht aus einer endlichen Menge X und einer auf X definierten *Wahrscheinlichkeitsverteilung*. Die Wahrscheinlichkeit, dass die Zufallsgröße $\mathbf{X}$ den Wert x annimmt wird mit $\mathbf{Pr}[\mathbf{X} = x]$ bezeichnet (kurz $\mathbf{Pr}[x]$, falls $\mathbf{X}$ fest). Weiterhin muss gelten $0 \leq \mathbf{Pr}[x], \forall x \in X$, und $\sum_{x \in X} \mathbf{Pr}[x] = 1$.

Definition 2: Sei $\mathbf{X}$ eine Zufallsgröße definiert auf X. Dann heißt $E \subseteq X$ *Ereignis*. Die Wahrscheinlichkeit, dass $\mathbf{X}$ einen Wert aus E annimmt, berechnet sich durch $\sum_{x \in E} \mathbf{Pr}[x]$.

Definition 3: Seien $\mathbf{X}$ und $\mathbf{Y}$ Zufallsgrößen auf den Mengen X bzw. Y. Die *Verbundwahrscheinlichkeit* $\mathbf{Pr}[x, y]$ (oder $\mathbf{Pr}[x \cap y]$) ist die Wahrscheinlichkeit, dass $\mathbf{X}$ den Wert x annimmt und $\mathbf{Y}$ den Wert y. Die *bedingte Wahrscheinlichkeit* $\mathbf{Pr}[x|y]$ bezeichnet die Wahrscheinlichkeit, dass $\mathbf{X}$ den Wert x annimmt unter der Vorraussetzung, dass $\mathbf{Y}$ den Wert y hat.
Die Zufallsgrößen $\mathbf{X}$ und $\mathbf{Y}$ heißen *unabhängig*, falls $\mathbf{Pr}[x, y] = \mathbf{Pr}[x]\mathbf{Pr}[y]$ für alle $x \in X, y \in Y$.

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\mathbf{Pr}[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\mathbf{Pr}[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Neue Zufallsgröße $\mathbf{Y}$ für Pasch oder Kein Pasch

$\hookrightarrow \mathbf{Pr}[P] = \frac{1}{6}$ und $\mathbf{Pr}[K] = \frac{5}{6}$

$\hookrightarrow \mathbf{Pr}[P,4] = \mathbf{Pr}[4,P] =$

$\hookrightarrow \mathbf{Pr}[P|4] =$ und $\mathbf{Pr}[4|P] =$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\mathbf{Pr}[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Neue Zufallsgröße $\mathbf{Y}$ für Pasch oder Kein Pasch

$\hookrightarrow \mathbf{Pr}[P] = \frac{1}{6}$ und $\mathbf{Pr}[K] = \frac{5}{6}$

$\hookrightarrow \mathbf{Pr}[P,4] = \mathbf{Pr}[4,P] = \frac{1}{36}$

$\hookrightarrow \mathbf{Pr}[P|4] =$ und $\mathbf{Pr}[4|P] =$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\mathbf{Pr}[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Neue Zufallsgröße $\mathbf{Y}$ für Pasch oder Kein Pasch

$\hookrightarrow \mathbf{Pr}[P] = \frac{1}{6}$ und $\mathbf{Pr}[K] = \frac{5}{6}$

$\hookrightarrow \mathbf{Pr}[P,4] = \mathbf{Pr}[4,P] = \frac{1}{36}$

$\hookrightarrow \mathbf{Pr}[P|4] = \frac{1}{3}$ und $\mathbf{Pr}[4|P] =$

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße $\mathbf{Z}$ definiert auf $Z = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$

$\hookrightarrow \mathbf{Pr}[(i,j)] = \frac{1}{36}$ für alle $(i,j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

$\hookrightarrow S_4 = \{(1,3),(2,2),(3,1)\}$ dann ist $\mathbf{Pr}[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\mathbf{Pr}[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Neue Zufallsgröße $\mathbf{Y}$ für Pasch oder Kein Pasch

$\hookrightarrow \mathbf{Pr}[P] = \frac{1}{6}$ und $\mathbf{Pr}[K] = \frac{5}{6}$

$\hookrightarrow \mathbf{Pr}[P,4] = \mathbf{Pr}[4,P] = \frac{1}{36}$

$\hookrightarrow \mathbf{Pr}[P|4] = \frac{1}{3}$ und $\mathbf{Pr}[4|P] = \frac{1}{6}$

Satz von Bayes

- Frage: Zusammenhang zwischen Verbund- und bedingter Wahrscheinlichkeit?

Satz von Bayes

- Frage: Zusammenhang zwischen Verbund- und bedingter Wahrscheinlichkeit?
- Antwort: Ja:

Satz von Bayes

- Frage: Zusammenhang zwischen Verbund- und bedingter Wahrscheinlichkeit?
- Antwort: Ja:

$$\mathbf{Pr}[x, y] = \mathbf{Pr}[x|y]\mathbf{Pr}[y] \quad \text{bzw.} \quad \mathbf{Pr}[x, y] = \mathbf{Pr}[y|x]\mathbf{Pr}[x]$$

Satz von Bayes

- Frage: Zusammenhang zwischen Verbund- und bedingter Wahrscheinlichkeit?
- Antwort: Ja:

$$\mathbf{Pr}[x,y] = \mathbf{Pr}[x|y]\mathbf{Pr}[y] \quad \text{bzw.} \quad \mathbf{Pr}[x,y] = \mathbf{Pr}[y|x]\mathbf{Pr}[x]$$

- Durch Umformung der Gleichungen erhält man

Satz von Bayes: Falls $\mathbf{Pr}[y] > 0$, dann

$$\mathbf{Pr}[x|y] = \frac{\mathbf{Pr}[x]\mathbf{Pr}[y|x]}{\mathbf{Pr}[y]}.$$

Perfekte Sicherheit

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße $\mathbf{K}$ und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\mathbf{Pr}[\mathbf{K} = K]$

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße $\mathbf{K}$ und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\mathbf{Pr}[\mathbf{K} = K]$
- $\mathbf{x}$ und $\mathbf{K}$ unabhängige Zufallsgrößen

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße $\mathbf{K}$ und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\mathbf{Pr}[\mathbf{K} = K]$
- $\mathbf{x}$ und $\mathbf{K}$ unabhängige Zufallsgrößen
- Zufallsgröße $\mathbf{y}$ auf $\mathcal{C}$ mit $\mathbf{Pr}[\mathbf{y} = y]$:

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße $\mathbf{K}$ und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\mathbf{Pr}[\mathbf{K} = K]$
- $\mathbf{x}$ und $\mathbf{K}$ unabhängige Zufallsgrößen
- Zufallsgröße $\mathbf{y}$ auf $\mathcal{C}$ mit $\mathbf{Pr}[\mathbf{y} = y]$:
  - Menge möglicher Chiffretexte, wenn K Schlüssel:

$$C(K) = \{e_K(x) | x \in \mathcal{P}\}$$

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf $\mathcal{P}$ mit Zufallsgröße $\mathbf{x}$, *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\mathbf{Pr}[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße $\mathbf{K}$ und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\mathbf{Pr}[\mathbf{K} = K]$
- $\mathbf{x}$ und $\mathbf{K}$ unabhängige Zufallsgrößen
- Zufallsgröße $\mathbf{y}$ auf $\mathcal{C}$ mit $\mathbf{Pr}[\mathbf{y} = y]$:
  - Menge möglicher Chiffretexte, wenn K Schlüssel:

$$C(K) = \{e_K(x) | x \in \mathcal{P}\}$$

  - Für alle $y \in \mathcal{C}$ gilt

$$\mathbf{Pr}[\mathbf{y} = y] = \sum_{\{K | y \in C(K)\}} \mathbf{Pr}[\mathbf{K} = K] \mathbf{Pr}[\mathbf{x} = d_K(y)]$$

Annahmen

Es lassen sich nun folgende bedingte Wahrscheinlichkeiten für jedes $y \in \mathcal{C}$ und $x \in \mathcal{P}$ berechnen:

Annahmen

Es lassen sich nun folgende bedingte Wahrscheinlichkeiten für jedes $y \in \mathcal{C}$ und $x \in \mathcal{P}$ berechnen:

- $\mathbf{Pr}[\mathbf{y} = y | \mathbf{x} = x]$:

$$\mathbf{Pr}[\mathbf{y} = y | \mathbf{x} = x] = \sum_{\{K | x = d_K(y)\}} \mathbf{Pr}[\mathbf{K} = K]$$

Annahmen

Es lassen sich nun folgende bedingte Wahrscheinlichkeiten für jedes $y \in \mathcal{C}$ und $x \in \mathcal{P}$ berechnen:

- $\mathbf{Pr}[\mathbf{y} = y|\mathbf{x} = x]$:

$$\mathbf{Pr}[\mathbf{y} = y|\mathbf{x} = x] = \sum_{\{K|x=d_K(y)\}} \mathbf{Pr}[\mathbf{K} = K]$$

- $\mathbf{Pr}[\mathbf{x} = x|\mathbf{y} = y]$ (mittels Satz von Bayes):

$$\mathbf{Pr}[\mathbf{x} = x|\mathbf{y} = y] = \frac{\mathbf{Pr}[\mathbf{x} = x] \times \mathbf{Pr}[\mathbf{y} = y|\mathbf{x} = x]}{\mathbf{Pr}[\mathbf{y} = y]}$$

Annahmen

Es lassen sich nun folgende bedingte Wahrscheinlichkeiten für jedes $y \in \mathcal{C}$ und $x \in \mathcal{P}$ berechnen:

- $\mathbf{Pr}[\mathbf{y} = y | \mathbf{x} = x]$:

$$\mathbf{Pr}[\mathbf{y} = y | \mathbf{x} = x] = \sum_{\{K | x = d_K(y)\}} \mathbf{Pr}[\mathbf{K} = K]$$

- $\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y]$ (mittels Satz von Bayes):

$$\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y] = \frac{\mathbf{Pr}[\mathbf{x} = x] \times \mathbf{Pr}[\mathbf{y} = y | \mathbf{x} = x]}{\mathbf{Pr}[\mathbf{y} = y]}$$

. . . oder ausführlicher . . .

$$\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y] = \frac{\mathbf{Pr}[\mathbf{x} = x] \times \sum_{\{K | x = d_K(y)\}} \mathbf{Pr}[\mathbf{K} = K]}{\sum_{\{K | y \in C(K)\}} \mathbf{Pr}[\mathbf{K} = K] \mathbf{Pr}[\mathbf{x} = d_K(y)]}$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

Beispiel

$$\mathcal{P} = \{a, b\} \quad \text{mit} \quad \mathbf{Pr}[a] = \tfrac{1}{4}, \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathcal{K} = \{K_1, K_2, K_3\} \quad \text{mit} \quad \mathbf{Pr}[K_1] = \tfrac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \tfrac{1}{4}$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$\mathbf{Pr}[1] =$ $\mathbf{Pr}[2] =$

$\mathbf{Pr}[3] =$ $\mathbf{Pr}[4] =$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$\mathbf{Pr}[1] = \frac{1}{8}$ $\quad$ $\mathbf{Pr}[2] =$

$\mathbf{Pr}[3] =$ $\quad$ $\mathbf{Pr}[4] =$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$\mathbf{Pr}[1] = \frac{1}{8}$ $\quad$ $\mathbf{Pr}[2] = \frac{3}{8} + \frac{1}{16} = \frac{7}{16}$

$\mathbf{Pr}[3] =$ $\quad$ $\mathbf{Pr}[4] =$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$\mathbf{Pr}[1] = \frac{1}{8}$ $\quad$ $\mathbf{Pr}[2] = \frac{3}{8} + \frac{1}{16} = \frac{7}{16}$

$\mathbf{Pr}[3] = \frac{3}{16} + \frac{1}{16} = \frac{1}{4}$ $\quad$ $\mathbf{Pr}[4] =$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$$\mathbf{Pr}[1] = \tfrac{1}{8} \qquad \mathbf{Pr}[2] = \tfrac{3}{8} + \tfrac{1}{16} = \tfrac{7}{16}$$

$$\mathbf{Pr}[3] = \tfrac{3}{16} + \tfrac{1}{16} = \tfrac{1}{4} \qquad \mathbf{Pr}[4] = \tfrac{3}{16}$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$$\mathbf{Pr}[1] = \tfrac{1}{8} \qquad \mathbf{Pr}[2] = \tfrac{3}{8} + \tfrac{1}{16} = \tfrac{7}{16}$$

$$\mathbf{Pr}[3] = \tfrac{3}{16} + \tfrac{1}{16} = \tfrac{1}{4} \qquad \mathbf{Pr}[4] = \tfrac{3}{16}$$

. . . nun lässt sich $\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y]$ bestimmen

$$\mathbf{Pr}[a|1] = \qquad \mathbf{Pr}[b|1] =$$

$$\mathbf{Pr}[a|2] = \qquad \mathbf{Pr}[b|2] =$$

$$\mathbf{Pr}[a|3] = \qquad \mathbf{Pr}[b|3] =$$

$$\mathbf{Pr}[a|4] = \qquad \mathbf{Pr}[b|4] =$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$$\mathbf{Pr}[1] = \tfrac{1}{8} \qquad \mathbf{Pr}[2] = \tfrac{3}{8} + \tfrac{1}{16} = \tfrac{7}{16}$$

$$\mathbf{Pr}[3] = \tfrac{3}{16} + \tfrac{1}{16} = \tfrac{1}{4} \qquad \mathbf{Pr}[4] = \tfrac{3}{16}$$

...nun lässt sich $\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y]$ bestimmen

$$\mathbf{Pr}[a|1] = 1 \qquad \mathbf{Pr}[b|1] =$$

$$\mathbf{Pr}[a|2] = \qquad \mathbf{Pr}[b|2] =$$

$$\mathbf{Pr}[a|3] = \qquad \mathbf{Pr}[b|3] =$$

$$\mathbf{Pr}[a|4] = \qquad \mathbf{Pr}[b|4] =$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$$\mathbf{Pr}[1] = \tfrac{1}{8} \qquad \mathbf{Pr}[2] = \tfrac{3}{8} + \tfrac{1}{16} = \tfrac{7}{16}$$

$$\mathbf{Pr}[3] = \tfrac{3}{16} + \tfrac{1}{16} = \tfrac{1}{4} \qquad \mathbf{Pr}[4] = \tfrac{3}{16}$$

...nun lässt sich $\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y]$ bestimmen

$$\mathbf{Pr}[a|1] = 1 \qquad \mathbf{Pr}[b|1] =$$

$$\mathbf{Pr}[a|2] = \tfrac{1}{7} \qquad \mathbf{Pr}[b|2] =$$

$$\mathbf{Pr}[a|3] = \qquad \mathbf{Pr}[b|3] =$$

$$\mathbf{Pr}[a|4] = \qquad \mathbf{Pr}[b|4] =$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ ist daher:

$$\mathbf{Pr}[1] = \tfrac{1}{8} \qquad \mathbf{Pr}[2] = \tfrac{3}{8} + \tfrac{1}{16} = \tfrac{7}{16}$$

$$\mathbf{Pr}[3] = \tfrac{3}{16} + \tfrac{1}{16} = \tfrac{1}{4} \qquad \mathbf{Pr}[4] = \tfrac{3}{16}$$

...nun lässt sich $\mathbf{Pr}[\mathbf{x} = x | \mathbf{y} = y]$ bestimmen

$$\mathbf{Pr}[a|1] = 1 \qquad \mathbf{Pr}[b|1] = 0$$

$$\mathbf{Pr}[a|2] = \tfrac{1}{7} \qquad \mathbf{Pr}[b|2] = \tfrac{6}{7}$$

$$\mathbf{Pr}[a|3] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|3] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|4] = 0 \qquad \mathbf{Pr}[b|4] = 1$$

Definition

Definition: Ein Kryptosystem hat *perfekte Sicherheit*, falls
$\mathbf{Pr}[x|y]=\mathbf{Pr}[x]$ für alle $x \in \mathcal{P}, y \in \mathcal{C}$.

Definition

Definition: Ein Kryptosystem hat *perfekte Sicherheit*, falls
$\mathbf{Pr}[x|y]=\mathbf{Pr}[x]$ für alle $x \in \mathcal{P}, y \in \mathcal{C}$.

Am Beispiel:

$$\mathbf{Pr}[a|1] = 1 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|1] = 0 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|2] = \tfrac{1}{7} \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|2] = \tfrac{6}{7} \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|3] = \tfrac{1}{4} = \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|3] = \tfrac{3}{4} = \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|4] = 0 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|4] = 1 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

Definition

Definition: Ein Kryptosystem hat *perfekte Sicherheit*, falls
$\mathbf{Pr}[x|y]=\mathbf{Pr}[x]$ für alle $x \in \mathcal{P}, y \in \mathcal{C}$.

Am Beispiel:

$$\mathbf{Pr}[a|1] = 1 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|1] = 0 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|2] = \tfrac{1}{7} \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|2] = \tfrac{6}{7} \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|3] = \tfrac{1}{4} = \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|3] = \tfrac{3}{4} = \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|4] = 0 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|4] = 1 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$\hookrightarrow$ Dieses Kryptosystem erfüllt die Vorraussetzung für perfekte Sicherheit nur für den Chiffretext $y = 3$, daher insgesamt keine perfekte Sicherheit.

Definition

Definition: Ein Kryptosystem hat *perfekte Sicherheit*, falls $\mathbf{Pr}[x|y]=\mathbf{Pr}[x]$ für alle $x \in \mathcal{P}, y \in \mathcal{C}$.

Am Beispiel:

$$\mathbf{Pr}[a|1] = 1 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|1] = 0 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|2] = \tfrac{1}{7} \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|2] = \tfrac{6}{7} \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|3] = \tfrac{1}{4} = \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|3] = \tfrac{3}{4} = \mathbf{Pr}[b] = \tfrac{3}{4}$$

$$\mathbf{Pr}[a|4] = 0 \neq \mathbf{Pr}[a] = \tfrac{1}{4} \qquad \mathbf{Pr}[b|4] = 1 \neq \mathbf{Pr}[b] = \tfrac{3}{4}$$

$\hookrightarrow$ Dieses Kryptosystem erfüllt die Vorraussetzung für perfekte Sicherheit nur für den Chiffretext $y = 3$, daher insgesamt keine perfekte Sicherheit.

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Dann bietet es perfekte Sicherheit, gdw. jeder Schlüssel mit gleicher Wahrscheinlichkeit $\frac{1}{|\mathcal{K}|}$ benutzt wird und $\forall x \in \mathcal{P}, y \in \mathcal{C}$ ein eindeutiger Schlüssel K existiert, so dass $e_K(x) = y$.

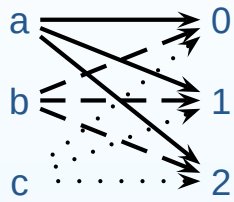
Beispiele für perfekt sichere Kryptosysteme

1. Exemplarisch (nach [1])

	a	b	c
K_1	0	1	2
K_2	1	2	0
K_3	2	0	1

$$|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}| = 3$$

$$\mathbf{Pr}[K_i] = \tfrac{1}{3}$$



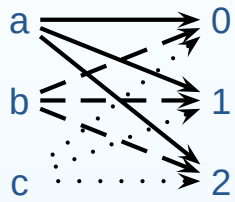
Beispiele für perfekt sichere Kryptosysteme

1. Exemplarisch (nach [1])

	a	b	c
K_1	0	1	2
K_2	1	2	0
K_3	2	0	1

$|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}| = 3$

$\mathbf{Pr}[K_i] = \frac{1}{3}$



2. One-Time Pad (Beispielrealisierung)

- $n \in \mathbb{Z}, n \geq 1$ und $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$
- $x = (x_1, \ldots, x_n), K = (K_1, \ldots, K_n), y = (y_1, \ldots, y_n)$
- $e_K(x) = (x_1 + K_1, \ldots, x_n + K_n) \mod 2$ *(entspricht $\otimes$)*
- $d_K(y) = (y_1 + K_1, \ldots, y_n + K_n) \mod 2$ *(entspricht $\otimes$)*

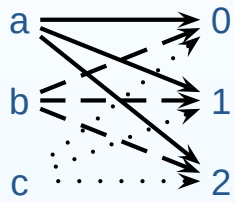
Beispiele für perfekt sichere Kryptosysteme

1. Exemplarisch (nach [1])

	a	b	c
K_1	0	1	2
K_2	1	2	0
K_3	2	0	1

$|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}| = 3$

$\mathbf{Pr}[K_i] = \frac{1}{3}$



2. One-Time Pad (Beispielrealisierung)

- $n \in \mathbb{Z}, n \geq 1$ und $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$
- $x = (x_1, \ldots, x_n), K = (K_1, \ldots, K_n), y = (y_1, \ldots, y_n)$
- $e_K(x) = (x_1 + K_1, \ldots, x_n + K_n) \mod 2$ *(entspricht $\otimes$)*
- $d_K(y) = (y_1 + K_1, \ldots, y_n + K_n) \mod 2$ *(entspricht $\otimes$)*
- Sicherheit begründet durch:
  - Zufälligkeit (unvorhersagbar!) der Schlüssel
  - Geheimhaltung der Schlüssel
  - Schlüssel nur *einmal* benutzen

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext								
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1							
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0						
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0					
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1				
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1			
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0		
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel								
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext								

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:
  - Schlüssellänge und -anzahl

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:
  - Schlüssellänge und -anzahl
  - Zufälligkeit der Schlüssel

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:
  - Schlüssellänge und -anzahl
  - Zufälligkeit der Schlüssel
  - Synchronisationsproblem bei verschollenen Nachrichten

One-Time Pad – Beispiel

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
  - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
  - Kein ausreichend zufälliger Schlüssel
  - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:
  - Schlüssellänge und -anzahl
  - Zufälligkeit der Schlüssel
  - Synchronisationsproblem bei verschollenen Nachrichten
  - Kollisionssproblem bei gleichzeitigen Nachrichten A$\leftrightarrow$B

Entropie

Definition

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie
- Informationstheorie: Ungewissheit über einen Versuchsausgang, (mittlerer) Informationsgehalt einer Nachricht

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie
- Informationstheorie: Ungewissheit über einen Versuchsausgang, (mittlerer) Informationsgehalt einer Nachricht

Definition: Sei $\mathbf{X}$ eine diskrete Zufallsgröße, die die Werte einer endlichen Menge X annimmt. Dann ist die *Entropie* von $\mathbf{X}$ definiert als die Größe

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie
- Informationstheorie: Ungewissheit über einen Versuchsausgang, (mittlerer) Informationsgehalt einer Nachricht

Definition: Sei $\mathbf{X}$ eine diskrete Zufallsgröße, die die Werte einer endlichen Menge X annimmt. Dann ist die *Entropie* von $\mathbf{X}$ definiert als die Größe

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

Anmerkung 1: Da $\log_2 y$ undefiniert für $y = 0$, aber $\lim_{y \to \infty} y \log_2 y = 0$ kann $\mathbf{Pr}[x] = 0$ für einige x angenommen werden.

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie
- Informationstheorie: Ungewissheit über einen Versuchsausgang, (mittlerer) Informationsgehalt einer Nachricht

Definition: Sei $\mathbf{X}$ eine diskrete Zufallsgröße, die die Werte einer endlichen Menge X annimmt. Dann ist die *Entropie* von $\mathbf{X}$ definiert als die Größe

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

Anmerkung 1: Da $\log_2 y$ undefiniert für $y = 0$, aber $\lim_{y \to \infty} y \log_2 y = 0$ kann $\mathbf{Pr}[x] = 0$ für einige x angenommen werden.

Anmerkung 2: Wenn $|X| = n$ und $\mathbf{Pr}[x] = \frac{1}{n}, \forall n \in X$, dann ist $H(\mathbf{X}) = \log_2 n$.

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ mit $\mathbf{Pr}[1] = \frac{1}{8}, \mathbf{Pr}[2] = \frac{7}{16}, \mathbf{Pr}[3] = \frac{1}{4}, \mathbf{Pr}[4] = \frac{3}{16}$

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ mit $\mathbf{Pr}[1] = \frac{1}{8}, \mathbf{Pr}[2] = \frac{7}{16}, \mathbf{Pr}[3] = \frac{1}{4}, \mathbf{Pr}[4] = \frac{3}{16}$

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

$$H(\mathbf{P}) = -\left(\frac{1}{4}\log_2\frac{1}{4} + \frac{3}{4}\log_2\frac{3}{4}\right)$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ mit $\mathbf{Pr}[1] = \frac{1}{8}, \mathbf{Pr}[2] = \frac{7}{16}, \mathbf{Pr}[3] = \frac{1}{4}, \mathbf{Pr}[4] = \frac{3}{16}$

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

$$H(\mathbf{P}) \approx 0{,}81$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ mit $\mathbf{Pr}[1] = \frac{1}{8}, \mathbf{Pr}[2] = \frac{7}{16}, \mathbf{Pr}[3] = \frac{1}{4}, \mathbf{Pr}[4] = \frac{3}{16}$

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

$$H(\mathbf{P}) \approx 0{,}81$$

$$H(\mathbf{K}) = 1{,}5$$

Beispiel

$\mathcal{P} = \{a, b\}$ mit $\mathbf{Pr}[a] = \frac{1}{4}, \mathbf{Pr}[b] = \frac{3}{4}$

$\mathcal{K} = \{K_1, K_2, K_3\}$ mit $\mathbf{Pr}[K_1] = \frac{1}{2}, \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \frac{1}{4}$

$\mathcal{C} = \{1, 2, 3, 4\}$ mit $\mathbf{Pr}[1] = \frac{1}{8}, \mathbf{Pr}[2] = \frac{7}{16}, \mathbf{Pr}[3] = \frac{1}{4}, \mathbf{Pr}[4] = \frac{3}{16}$

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x]$$

$$H(\mathbf{P}) \approx 0{,}81$$

$$H(\mathbf{K}) = 1{,}5$$

$$H(\mathbf{C}) \approx 1{,}85$$

Entropieeigenschaften I

Satz: Sei $\mathbf{X}$ eine Zufallsgröße mit einer Wahrscheinlichkeitsverteilung, die die Werte $p_1, \ldots, p_n (p_i > 0, 1 \leq i \leq n)$ annimmt. Dann gilt $H(\mathbf{X}) \leq \log_2 n$ mit Gleichheit gdw. $p_i = \frac{1}{n}, 1 \leq i \leq n$.

Folgerung: Die *maximale Entropie* $H(\mathbf{X})$ beträgt $\log_2 n$.

Satz: $H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$, mit Gleichheit gdw. $\mathbf{X}$ und $\mathbf{Y}$ unabhängige Zufallsgrößen sind.

Definition (a): Seien $\mathbf{X}$ und $\mathbf{Y}$ zwei Zufallsgrößen. Dann erhält man für jeden Wert y aus $\mathbf{Y}$ eine (bedingte) Wahrscheinlichkeitsverteilung auf X. Die zugehörige Zufallsgröße wird mit $(\mathbf{X}|y)$ bezeichnet. Offensichtlich gilt

$$H(\mathbf{X}|y) = -\sum_x \mathbf{Pr}[x|y] \log_2 \mathbf{Pr}[x|y]$$

Entropieeigenschaften II

Definition (b): Die *bedingte Entropie* $H(\mathbf{X}|\mathbf{Y})$ ist das gewichtete Mittel (bezüglich der Wahrscheinlichkeiten der $\mathbf{Pr}[y]$) der Entropien $(\mathbf{X}|y)$ über allen möglichen Werten von y. Sie wird wie folgt berechnet

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y}\sum_{x}\mathbf{Pr}[y]\mathbf{Pr}[x|y]\log_2\mathbf{Pr}[x|y]$$

Satz: $H(\mathbf{X},\mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$

Folgerung: $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$ mit Gleichheit gdw. $\mathbf{X}$ und $\mathbf{Y}$ unabhängig.

Gute Schlüssel

Schlüsselmehrdeutigkeit

Es existiert ein fundamentaler Zusammenhang zwischen den Entropien der einzelnen Komponenten eines Kryptosystems. Die bedingte Entropie $H(\mathbf{K}|\mathbf{C})$ heißt *Schlüsselmehrdeutigkeit* (key equivocation) und ist ein Maß dafür, wieviel Information über den Schlüssel durch den Chiffretext offengelegt wird. Es gilt hierbei folgender

Schlüsselmehrdeutigkeit

Es existiert ein fundamentaler Zusammenhang zwischen den Entropien der einzelnen Komponenten eines Kryptosystems. Die bedingte Entropie $H(\mathbf{K}|\mathbf{C})$ heißt *Schlüsselmehrdeutigkeit* (key equivocation) und ist ein Maß dafür, wieviel Information über den Schlüssel durch den Chiffretext offengelegt wird. Es gilt hierbei folgender

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem. Dann gilt

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$$

Schlüsselmehrdeutigkeit

Es existiert ein fundamentaler Zusammenhang zwischen den Entropien der einzelnen Komponenten eines Kryptosystems. Die bedingte Entropie $H(\mathbf{K}|\mathbf{C})$ heißt *Schlüsselmehrdeutigkeit* (key equivocation) und ist ein Maß dafür, wieviel Information über den Schlüssel durch den Chiffretext offengelegt wird. Es gilt hierbei folgender

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem. Dann gilt

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$$

Am Beispiel:

$$H(\mathbf{K}) = 1{,}5 \quad , \quad H(\mathbf{P}) \approx 0{,}81 \quad , \quad H(\mathbf{C}) \approx 1{,}85$$

$$H(\mathbf{K}|\mathbf{C}) = 1{,}5 + 0{,}81 - 1{,}85 = 0{,}46$$

Schlüsselkandidaten

- Annahmen: Eve
  - hört Chiffretext ab
  - weiß, dass Klartext eine „natürliche“ Sprache
  - hat Wissen um Verschlüsselungsmethode
  - hat unbegrenzte Rechenressourcen

Schlüsselkandidaten

- Annahmen: Eve
  - hört Chiffretext ab
  - weiß, dass Klartext eine „natürliche“ Sprache
  - hat Wissen um Verschlüsselungsmethode
  - hat unbegrenzte Rechenressourcen
- Eve kann einige Schlüssel verwerfen (Klartext ist unbrauchbar)
- Verbleibende „mögliche“ Schlüssel unterteilt in
  - Korrekter Schlüssel
  - Falsche Schlüssel

Schlüsselkandidaten

- Annahmen: Eve
  - hört Chiffretext ab
  - weiß, dass Klartext eine „natürliche“ Sprache
  - hat Wissen um Verschlüsselungsmethode
  - hat unbegrenzte Rechenressourcen
- Eve kann einige Schlüssel verwerfen (Klartext ist unbrauchbar)
- Verbleibende „mögliche“ Schlüssel unterteilt in
  - Korrekter Schlüssel
  - Falsche Schlüssel

Beispiel:

- Sprache Englisch, Chiffretext *WNAJW*, Methode Verschiebungschiffre
- nur zwei „sinnvolle“ Klartexte möglich: *RIVER* und *ARENA*
  $\hookrightarrow$ mögliche Schlüssel F (5) und W (22)

Untersuchung von Spracheigenschaften

Ziel: Anzahl falscher Schlüssel eingrenzen

Untersuchung von Spracheigenschaften

Ziel: Anzahl falscher Schlüssel eingrenzen

- Entropie (pro Buchstabe) einer natürlichen Sprache (H_L) misst die durchschnittliche Information pro Buchstabe in einem „sinnvollen“ natürlichsprachigem Text
- n-Gram: Wort der Länge n über einem Alphabet, $\mathbf{P}^n$ Zufallsgröße mit Wahrscheinlichkeitsverteilung aller n-Gramme eines Klartextes

Untersuchung von Spracheigenschaften

Ziel: Anzahl falscher Schlüssel eingrenzen

- Entropie (pro Buchstabe) einer natürlichen Sprache (H_L) misst die durchschnittliche Information pro Buchstabe in einem „sinnvollen“ natürlichsprachigem Text
- n-Gram: Wort der Länge n über einem Alphabet, $\mathbf{P}^n$ Zufallsgröße mit Wahrscheinlichkeitsverteilung aller n-Gramme eines Klartextes

Definition: Sei L eine natürliche Sprache. Die *Entropie von* L ist definiert als die Größe

$$H_L = \lim_{n\to\infty} \frac{H(\mathbf{P}^n)}{n}$$

und die *Redundanz von* L ist definiert durch

$$R_L = 1 - \frac{H_L}{\log_2 |\mathcal{P}|}$$

Beispiel

- L ist englische Sprache

Beispiel

- L ist englische Sprache
- Durch Untersuchungen: $1{,}0 \leq H_L \leq 1{,}5$ also rund $1{,}25$

Beispiel

- L ist englische Sprache
- Durch Untersuchungen: $1{,}0 \leq H_L \leq 1{,}5$ also rund $1{,}25$
- Redundanz:

$$R_L = 1 - \frac{1{,}25}{\log_2 26} \approx 0{,}734$$

Beispiel

- L ist englische Sprache
- Durch Untersuchungen: $1{,}0 \leq H_L \leq 1{,}5$ also rund $1{,}25$
- Redundanz:

$$R_L = 1 - \frac{1{,}25}{\log_2 26} \approx 0{,}734$$

$\hookrightarrow$ ca. 75% der englischen Sprache redundant

Eliminierung falscher Schlüssel

Redundanz

- gibt Aufschluss über effektive Codierungsmöglichkeit
- erlaubt Anzahl falscher Schlüssl zu minimieren

Eliminierung falscher Schlüssel

Redundanz

- gibt Aufschluss über effektive Codierungsmöglichkeit
- erlaubt Anzahl falscher Schlüssl zu minimieren

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit $|\mathcal{C}| = |\mathcal{P}|$ und gleichwahrscheinlicher Schlüsselverteilung. R_L sei die Redundanz der zu Grunde liegenden Sprache. Mit gegebenen Chiffretext der Länge n, mit n hinreichend groß, erfüllt die erwartete Anzahl falscher Schlüssel $\overline{s}_n$ die Formel

$$\overline{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

Eliminierung falscher Schlüssel

Redundanz

- gibt Aufschluss über effektive Codierungsmöglichkeit
- erlaubt Anzahl falscher Schlüssl zu minimieren

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit $|\mathcal{C}| = |\mathcal{P}|$ und gleichwahrscheinlicher Schlüsselverteilung. R_L sei die Redundanz der zu Grunde liegenden Sprache. Mit gegebenen Chiffretext der Länge n, mit n hinreichend groß, erfüllt die erwartete Anzahl falscher Schlüssel $\overline{s}_n$ die Formel

$$\overline{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

Definition: Die *Eindeutigkeitsdistanz* eines Kryptosystems ist definiert durch den Wert n, bezeichnet als n_0, bei dem die Anzahl erwarteter falscher Schlüssel Null wird. D.h. die durchschnittliche Menge an Chiffretext, die ein Angreifer benötigt, um den Schlüssel eindeutig zu bestimmen.

Eindeutigkeitsdistanz – Beispiel

- $\overline{s}_n = 0$ in Gleichung (letzter Satz) setzen und nach n umformen ergibt

$$n_0 \approx \frac{log_2|\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}$$

Eindeutigkeitsdistanz – Beispiel

- $\overline{s}_n = 0$ in Gleichung (letzter Satz) setzen und nach n umformen ergibt

$$n_0 \approx \frac{log_2|\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}$$

- Kryptosystem *Substitutions-Chiffre*: $|\mathcal{P}| = 26$ und $|\mathcal{K}| = 26!$, $R_L = 0{,}75$

$$n_0 \approx \frac{88{,}4}{0{,}75 \cdot 4{,}7} \approx 25$$

Eindeutigkeitsdistanz – Beispiel

- $\overline{s}_n = 0$ in Gleichung (letzter Satz) setzen und nach n umformen ergibt

$$n_0 \approx \frac{log_2|\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}$$

- Kryptosystem *Substitutions-Chiffre*: $|\mathcal{P}| = 26$ und $|\mathcal{K}| = 26!$, $R_L = 0{,}75$

$$n_0 \approx \frac{88{,}4}{0{,}75 \cdot 4{,}7} \approx 25$$

$\hookrightarrow$ Ein Chiffretext der Länge 25 ermöglicht (normalerweise) eine eindeutige Entschlüsselung.

Produktkryptosysteme

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit

Produktkryptosysteme

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit
- *endomorphe* Kryptosysteme notwendig ($\mathcal{P} = \mathcal{C}$)
  $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$
  $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$

Produktkryptosysteme

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit
- *endomorphe* Kryptosysteme notwendig ($\mathcal{P} = \mathcal{C}$)
  $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$
  $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$

$\hookrightarrow$ Produkt: $S_1 \times S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$

Produktkryptosysteme

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit
- *endomorphe* Kryptosysteme notwendig ($\mathcal{P} = \mathcal{C}$)
  $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$
  $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$

$\hookrightarrow$ Produkt: $S_1 \times S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$

- Schlüssel K hat die Form (K_1, K_2) mit $K_1 \in \mathcal{K}_1, K_2 \in \mathcal{K}_2$
- Verschlüsselungsfunktion: $d_{(K_1,K_2)}(y) = d_{K_1}(d_{K_2}(y))$
- Entschlüsselungsfunktion: $e_{(K_1,K_2)}(x) = e_{K_2}(e_{K_1}(x))$

Produktkryptosysteme

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit
- *endomorphe* Kryptosysteme notwendig ($\mathcal{P} = \mathcal{C}$)
  $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$
  $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$

$\hookrightarrow$ Produkt: $S_1 \times S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$

- Schlüssel K hat die Form (K_1, K_2) mit $K_1 \in \mathcal{K}_1, K_2 \in \mathcal{K}_2$
- Verschlüsselungsfunktion: $d_{(K_1,K_2)}(y) = d_{K_1}(d_{K_2}(y))$
- Entschlüsselungsfunktion: $e_{(K_1,K_2)}(x) = e_{K_2}(e_{K_1}(x))$
- Beachte umgekehrte Schlüsselfolge:

$$\begin{aligned} d_{(K_1,K_2)}(e_{(K_1,K_2)}(x)) &= d_{(K_1,K_2)}(e_{K_2}(e_{K_1}(x))) \\ &= d_{K_1}(d_{K_2}(e_{K_2}(e_{K_1}(x)))) \\ &= d_{K_1}(e_{K_1}(x)) \\ &= x \end{aligned}$$

Eigenschaften von Produktkryptosystemen

- Assoziativität: $S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$ gilt für alle Kryptosysteme

Eigenschaften von Produktkryptosystemen

- Assoziativität: $S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$ gilt für alle Kryptosysteme
- Kommutierende Kryptosysteme: $S_1 \times S_2 = S_2 \times S_1$ gilt nicht für alle Krytosysteme

Eigenschaften von Produktkryptosystemen

- Assoziativität: $S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$ gilt für alle Kryptosysteme
- Kommutierende Kryptosysteme: $S_1 \times S_2 = S_2 \times S_1$ gilt nicht für alle Krytosysteme
- Idempotenz: $S \times S = S^2 = S$
  $\hookrightarrow$ falls nicht idempotent Chance für höhere Sicherheit durch multiple Iterationen (DES = S^{16})

Eigenschaften von Produktkryptosystemen

- Assoziativität: $S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$ gilt für alle Kryptosysteme
- Kommutierende Kryptosysteme: $S_1 \times S_2 = S_2 \times S_1$ gilt nicht für alle Krytosysteme
- Idempotenz: $S \times S = S^2 = S$
  $\hookrightarrow$ falls nicht idempotent Chance für höhere Sicherheit durch multiple Iterationen (DES = S^{16})
- Beachte: S_1, S_2 idempotent und kommutierend $\Rightarrow S_1 \times S_2$ ebenso

$$\begin{aligned}(S_1 \times S_2) \times (S_1 \times S_2) &= S_1 \times (S_2 \times S_1) \times S_2 \\ &= S_1 \times (S_1 \times S_2) \times S_2 \\ &= (S_1 \times S_1) \times (S_2 \times S_2) \\ &= S_1 \times S_2\end{aligned}$$

Literatur

[1] BRACKMANN, Roland. *Shannons Theorie*. http://www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/shannons_theorie_brackmann.pdf

[2] HOPPE, Tobias. *Das One-Time-Pad und Chiffriermaschinen*. http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/choppe/choppe.html

[3] MENEZES, Alfred J. ; VAN OORSCHOT, Paul C. ; VANSTONE, Scott A.: *Handbook of Applied Cryptography*. CRC Press, Inc., 1996. – ISBN 0849385237

[4] SHANNON, Claude E. *Communication Theory of Secrecy Systems*. http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

[5] STINSON, Douglas R.: *Cryptography: Theory and Practice*. Second. CRC Press, Inc./Chapman&Hall, 2002. – ISBN 1584882069

[6] WIKIPEDIA. *Bayestheorem*. http://de.wikipedia.org/wiki/Bayestheorem

Vielen Dank für Ihre Aufmerksamkeit