Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 3
31. Oktober 2018

Übungen zur Kryptographie
Lösung

Aufgabe 9

a) Wir berechnen

$$\mathbb{P}_{plain,cipher}(a,A) = \sum_{\substack{k\in\mathcal{K}\\ E_k(a)=A}} \mathbb{P}_{plain}(a)\mathbb{P}_{key}(k) = \frac{1}{3}\cdot\frac{1}{4} = \frac{1}{12}$$

$$\mathbb{P}_{plain,cipher}(a,B) = \frac{1}{12}, \quad \mathbb{P}_{plain,cipher}(a,C) = \frac{1}{6}, \quad \mathbb{P}_{plain,cipher}(a,D) = 0$$

$$\mathbb{P}_{plain,cipher}(b,A) = \mathbb{P}_{plain,cipher}(b,B) = \mathbb{P}_{plain,cipher}(b,C) = \mathbb{P}_{plain,cipher}(b,D) = \frac{1}{12}$$

$$\mathbb{P}_{plain,cipher}(c,A) = \mathbb{P}_{plain,cipher}(c,B) = \frac{1}{12}, \quad \mathbb{P}_{plain,cipher}(c,C) = 0, \quad \mathbb{P}_{plain,cipher}(c,D) = \frac{1}{6}.$$

Da jeder Wert in der Tabelle 3-fach vorkommt gilt weiter $\mathbb{P}_{cipher}(y) = \sum_{\substack{x\in\mathcal{P},k\in\mathcal{K}\\ E_k(x)=y}} \mathbb{P}_{plain}(x)\mathbb{P}_{key}(k) = \frac{3}{12} = \frac{1}{4}, \forall y \in \mathcal{C}$ und weiter

$$\mathbb{P}_{plain|cipher}(a|A) = \frac{\mathbb{P}_{plain,cipher}(a,A)}{\mathbb{P}_{cipher}(A)} = \frac{1}{12}\cdot\frac{1}{4} = \frac{1}{3}$$

$$\mathbb{P}_{plain|cipher}(a|B) = \frac{1}{3}, \quad \mathbb{P}_{plain|cipher}(a|C) = \frac{2}{3}, \quad \mathbb{P}_{plain|cipher}(a|D) = 0$$

$$\mathbb{P}_{plain|cipher}(b|A) = \mathbb{P}_{plain|cipher}(b|B) = \mathbb{P}_{plain,cipher}(b|C) = \mathbb{P}_{plain,cipher}(b|D) = \frac{1}{3}$$

$$\mathbb{P}_{plain|cipher}(c|A) = \mathbb{P}_{plain|cipher}(c|B) = \frac{1}{3}, \quad \mathbb{P}_{plain,cipher}(c|C) = 0, \quad \mathbb{P}_{plain|cipher}(c|D) = \frac{2}{3}.$$

Da aber z.B.

$$\mathbb{P}_{plain|cipher}(a|D) = \frac{\mathbb{P}_{plain,cipher}(a,D)}{\mathbb{P}_{cipher}(A)} = 0 \neq \frac{1}{3} = \mathbb{P}_{plain}(a)$$

ist das System nicht perfekt im Sinne von Shannon.

b) Notwendige und hinreichende Bedingung, dass das System für jede Verteilung der Klartexte sicher ist, ist dass in jeder Zeile nur verschiedene Buchstaben auftreten. Tritt in jeder Zeile jeder Buchstabe einfach auf, so gilt $\mathbb{P}_{plain,cipher}(x,y) = \frac{1}{4}\mathbb{P}_{plain}(x)$ und $\mathbb{P}_{cipher}(y) = \frac{1}{4}\sum_{\substack{x\in\mathcal{P},\exists k\in\mathcal{K}\\ E_k(x)=y}} \mathbb{P}_{plain}(x) = \frac{1}{4}$, also

$$\mathbb{P}_{plain|cipher}(x|y) = \frac{\mathbb{P}_{plain,cipher}(x,y)}{\mathbb{P}_{cipher}(y)} = \mathbb{P}_{plain}(x).$$

Angenommen ein Buchstabe $\overline{y}$ tritt nicht auf, dann gilt $\mathbb{P}_{plain,cipher}(x,\overline{y}) = 0 \neq \mathbb{P}_{plain}(x)$ für mindestens ein x.

Bemerkung. Man beachte, dass man nur ein Kryptosystem erhält, wenn in jeder Spalte verschiedene Buchstaben stehen.

Aufgabe 10

Man beachte

$$\mathbb{P}_{plain_i,cipher_i}(x_i, y_i) = \sum_{\substack{k_i \in \mathcal{K}_i \\ E_{k_i}(x_i)=y_i}} \mathbb{P}_{plain_i}(x_i)\mathbb{P}_{key_i}(k_i).$$

Für das Produktsystem gilt

$$\begin{aligned}
&\mathbb{P}_{plain_\times,cipher_\times}(x_1 \times x_2, y_1 \times y_2) \\
&= \sum_{\substack{i=1,2: k_i \in \mathcal{K}_i \\ E_{k_i}(x_i)=y_i}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_1}(k_1)\mathbb{P}_{key_2}(k_2) \\
&= \left(\sum_{\substack{k_1 \in \mathcal{K}_1 \\ E_{k_1}(x_1)=y_1}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{key_1}(k_1) \right) \left(\sum_{\substack{k_2 \in \mathcal{K}_2 \\ E_{k_2}(x_2)=y_2}} \mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_2}(k_2) \right)
\end{aligned}$$

und

$$\begin{aligned}
&\mathbb{P}_{cipher_\times}(y_1 \times y_2) \\
&= \sum_{\substack{i=1,2: x_i \in \mathcal{P}_i \\ k_i \in \mathcal{K}_i, E_{k_i}(x_i)=y_i}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_1}(k_1)\mathbb{P}_{key_2}(k_2) \\
&= \left(\sum_{\substack{x_1 \in \mathcal{P}_1, k_1 \in \mathcal{K}_1 \\ E_{k_1}(x_1)=y_1}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{key_1}(k_1) \right) \left(\sum_{\substack{x_2 \in \mathcal{P}_2, k_2 \in \mathcal{K}_2 \\ E_{k_2}(x_2)=y_2}} \mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_2}(k_2) \right).
\end{aligned}$$

Also

$$\begin{aligned}
&\mathbb{P}_{plain_\times,cipher_\times}(x_1 \times x_2 | y_1 \times y_2) \\
&= \frac{\mathbb{P}_{plain_\times,cipher_\times}(x_1 \times x_2, y_1 \times y_2)}{\mathbb{P}_{cipher_\times}(y_1 \times y_2)} \\
&= \frac{\left(\sum_{\substack{k_1 \in \mathcal{K}_1 \\ E_{k_1}(x_1)=y_1}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{key_1}(k_1) \right) \left(\sum_{\substack{k_2 \in \mathcal{K}_2 \\ E_{k_2}(x_2)=y_2}} \mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_2}(k_2) \right)}{\left(\sum_{\substack{x_1 \in \mathcal{P}_1, k_1 \in \mathcal{K}_1 \\ E_{k_1}(x_1)=y_1}} \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{key_1}(k_1) \right) \left(\sum_{\substack{x_2 \in \mathcal{P}_2, k_2 \in \mathcal{K}_2 \\ E_{k_2}(x_2)=y_2}} \mathbb{P}_{plain_2}(x_2)\mathbb{P}_{key_2}(k_2) \right)} \\
&= \frac{\mathbb{P}_{plain_1,cipher_1}(x_1, y_1)}{\mathbb{P}_{cipher_1}(y_1)} \cdot \frac{\mathbb{P}_{plain_2,cipher_2}(x_2, y_2)}{\mathbb{P}_{cipher_2}(y_2)} \\
&= \mathbb{P}_{plain_1}(x_1)\mathbb{P}_{plain_2}(x_2) = \mathbb{P}_{plain_\times(x_1 \times x_2)}
\end{aligned}$$

und wir erhalten perfekte Sicherheit auch im Produktsystem.

Aufgabe 11

Ist z.B. $y = 0$ gegeben, dann folgt daraus $x = 0$ und somit $\mathbb{P}_{plain|cipher}(x = 0|y = 0) = 1 \neq \mathbb{P}_{plain}(x = 0) = 1 - \sum_{x \neq 0} \mathbb{P}_{plain}(x) < 1$. Oder umgekehrt $\mathbb{P}_{plain|cipher}(x|y = 0) = 0 < \mathbb{P}_{plain}(x)$ für alle $x \neq 0$.

Aufgabe 12

a) Wir haben $\binom{N}{n}$ Möglichkeiten die verschwindenden Stellen auszuwählen. Offensichtlich bleibt die Anzahl der verschwindenden Stellen unter Permutation gleich, also $E_\pi(\mathcal{P}_1) = \mathcal{C}_1 = \mathcal{P}_1$.

b) Sei $x = (x_1, \ldots, x_N) \in \mathcal{P}_1, y = (y_1, \ldots, y_N) \in \mathcal{C}_1$. Man beachte, es gibt (unabhängig von $x \in \mathcal{P}_1$ und $y \in \mathcal{C}_1$) genau $(n!)^2$ Permutationen, die die Menge $\{1 \leq i \leq N : x_i \neq 0\}$ auf die Menge $\{1 \leq j \leq N : y_j \neq 0\}$ abbilden. Wir müssen $\mathbb{P}_{plain|cipher}(x|y)$ berechnen. Es ist

$$\mathbb{P}_{plain,cipher}(x,y) = \sum_{\substack{\sigma \in S_N \\ \sigma(x)=y}} \mathbb{P}_{plain}(x)\mathbb{P}_{key}(\sigma) = \frac{1}{N!} \sum_{\substack{\sigma \in S_N \\ \sigma(x)=y}} \mathbb{P}_{plain}(x) = \frac{(n!)^2}{N!}\mathbb{P}_{plain}(x)$$

und

$$\mathbb{P}_{cipher}(y) = \sum_{\substack{x \in \mathcal{P}_1, \sigma \in S_N \\ \sigma(x)=y}} \mathbb{P}_{plain}(x)\mathbb{P}_{key}(\sigma) = \frac{1}{N!} \sum_{\substack{x \in \mathcal{P}_1, \sigma \in S_N \\ \sigma(x)=y}} \mathbb{P}_{plain}(x) = \frac{(n!)^2}{n!} \underbrace{\sum_{x \in \mathcal{P}_1} \mathbb{P}_{plain}(x)}_{=1}.$$

Folglich erhalten wir perfekte Sicherheit:

$$\mathbb{P}_{plain|cipher}(x|y) = \frac{\mathbb{P}_{plain,cipher}(x,y)}{\mathbb{P}_{cipher}(y)} = \frac{\frac{(n!)^2}{N!}\mathbb{P}_{plain}(x)}{\frac{(n!)^2}{N!}} = \mathbb{P}_{plain}(x).$$

Man beachte, dass das Ergebnis unabhängig von der auf $\mathcal{P}_1$ gewählten Verteilung gilt.