Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 1 / 14. Oktober 2013

Abgabe: 22. Oktober 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

In der Praxis sei die Wahrscheinlichkeit, dass ein Verschlüsselungsverfahren sicher und effizient ist, 10%. Die Wahrscheinlichkeit, dass es nicht sicher ist, wenn es effizient ist, sei 80%. Wie groß ist die Wahrscheinlichkeit, dass es

(a) sicher ist, wenn es effizient ist?

(b) effizient ist?

AUFGABE 2 (5 Punkte)**:**

Seien $E_1, \ldots, E_n$ beliebige Ereignisse. Zeigen Sie:

$$\mathsf{Ws}[E_1 \vee \ldots \vee E_n] \leq \mathsf{Ws}[E_1] + \ldots + \mathsf{Ws}[E_n]$$

Hinweis: Sie dürfen $\mathsf{Ws}[X \vee Y] \leq \mathsf{Ws}[X] + \mathsf{Ws}[Y]$ verwenden.

AUFGABE 3 (5 Punkte)**:**

Seien A_1, A_2 unabhängig. Zeigen Sie, dass dann $(A_1, \bar{A}_2)$, $(\bar{A}_1, A_2)$, $(\bar{A}_1, \bar{A}_2)$ ebenfalls unabhängig sind.

Hinweis: Sie dürfen $\mathsf{Ws}[X] = \mathsf{Ws}[X \wedge Y] + \mathsf{Ws}[X \wedge \bar{Y}]$ verwenden.

AUFGABE 4 (5 Punkte)**:**

Seien $E_1, \ldots, E_n$ beliebige Ereignisse mit $\mathsf{Ws}[E_1 \wedge \cdots \wedge E_n] > 0$. Zeigen Sie, dass dann

$$\mathsf{Ws}[E_1 \wedge \ldots \wedge E_n] = \mathsf{Ws}[E_1] \cdot \mathsf{Ws}[E_2 \mid E_1] \cdot \ldots \cdot \mathsf{Ws}[E_n \mid E_1 \wedge \ldots \wedge E_{n-1}]$$

gilt.