



Präsenzübungen zur Vorlesung  
Kryptographie  
WS 2013/14  
Blatt 1 / 14. Oktober 2013

**AUFGABE 1:**

Bilden Sie die Kontraposition der folgenden Aussagen:

- (a) Wenn es regnet, ist die Straße nass.
- (b) Wenn das Auto fährt, ist der Tank nicht leer.
- (c) Wenn  $p$  eine Primzahl ist, dann gilt  $p = 2$  oder  $p$  ist ungerade.
- (d) Wenn Annahme  $X$  gilt, ist Verfahren  $Y$  sicher.
- (e) Wenn man effizient faktorisieren kann, ist RSA nicht sicher.

**AUFGABE 2:**

In einer Schuhfabrik sei die Wahrscheinlichkeit, dass ein Schuh **bunt** ist, 95% und die Wahrscheinlichkeit, dass ein Schuh **klein** ist, 10%. Schätzen Sie möglichst genau die Wahrscheinlichkeit dafür ab, dass ein Schuh sowohl **klein** als auch **bunt** ist. Wann nimmt die Wahrscheinlichkeit die obere Schranke Ihrer Abschätzung an? Wann ist die Wahrscheinlichkeit 9,5%?

**AUFGABE 3:**

Die Wahrscheinlichkeit, dass ein Zeitungsartikel das Wort **Bundeskanzlerin** enthält sei 20%. Die Wahrscheinlichkeit, dass das Wort **Bundeskanzlerin** enthalten ist, wenn bereits das Wort **Merkel** enthalten ist, sei 35%. Die Wahrscheinlichkeit, dass das Wort **Bundeskanzlerin** enthalten ist, wenn das Wort **Merkel** nicht enthalten ist, sei 5%.

Wie groß ist die Wahrscheinlichkeit, dass ein Zeitungsartikel das Wort **Merkel** enthält?

**AUFGABE 4:**

Sei  $\text{Ws}[E_2] \neq 0$ . Zeigen Sie, dass dann gilt:

$$\text{Ws}[E_1 | E_2] = \frac{\text{Ws}[E_1] \cdot \text{Ws}[E_2 | E_1]}{\text{Ws}[E_2]}$$