Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 06.11.2015

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 2

AUFGABE 1:
Gegeben sei eine Nachricht $m = 1011\ 1001\ 0100\ 1010 \in \{0,1\}^*$ und der Initialvektor $IV = 1001$. Verschlüsseln Sie die Nachricht m mittels der *Permutationschiffre* unter Verwendung des *CBC-Modus*. Der Schlüssel sei $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$.

AUFGABE 2:
Die Verschlüsselung $c_0c_1c_2\cdots c_t$ einer Nachricht $m_1m_2m_3\cdots m_t$ im *Output-Feedback-Modus (OFB)* ist formal beschrieben durch $c_0 = z_0 = IV$ und für alle $1 \leq i \leq t$:

$$z_i = E_k(z_{i-1}) \qquad \text{und} \qquad c_i = m_i \oplus z_i.$$

a) Wie lautet die formale Beschreibung der Entschlüsselung einer Nachricht im OFB-Modus?

b) Geben Sie außerdem ein Netzwerkdiagramm für die Ver- und die Entschlüsselung im OFB-Modus an.

AUFGABE 3:
Es wird mit zwei fairen sechsseitigen Würfeln gewürfelt. Sei A das Ereignis, dass beide Würfel das gleiche Ergebnis zeigen und sei B das Ereignis, dass die Summe der Würfe ungerade ist.

a) Geben Sie den Wahrscheinlichkeitsraum S an und modellieren Sie die Ereignisse A und B als Teilmengen von S.

b) Bestimmen Sie die Wahrscheinlichkeiten für A und für B.

c) Bestimmen Sie die bedingte Wahrscheinlichkeit, dass die Summe der Würfe ungerade ist, wenn die beiden Würfel das gleiche Ergebnis zeigen.

d) Bestimmen Sie die bedingte Wahrscheinlichkeit, dass die beiden Würfel verschiedene Ergebnisse zeigen, wenn die Summe der Würfe gerade ist.

e) Bestimmen Sie die bedingte Wahrscheinlichkeit, dass die die Summe der Würfe gerade ist, wenn beiden Würfel verschiedene Ergebnisse zeigen.