**Dozent:** Prof. Dr. Johannes Blömer
**Tutoren:** Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
**Ausgabedatum:** 29.1.2016

# Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 7

**AUFGABE 1:**
Zeigen Sie, dass die folgenden Modifikationen von CBC-MAC aus der Vorlesung *jeweils* nicht zu einem sicheren MAC führen:

a) Statt der festen Initialisierung $z_0 = 0^n$ wählen Sie $z_0$ zufällig gleichverteilt in $\{0,1\}^n$ und geben für $x$ den MAC $h_k(x) = (z_0, z_b)$ aus.

b) Statt als MAC $h_k(x) = z_b$ auszugeben, geben Sie $h_k(x) = (z_1, \ldots, z_b)$ als MAC für $x$ aus.

*Hinweis:* Beschreiben Sie einen Angreifer, der ohne Kenntnis des geheimen Schlüssels $k$, aber unter Kenntnis eines MACs zu einer Nachricht $m$ einen gültigen MAC zu einer weiteren Nachricht $m' \neq m$ erstellen kann.

**AUFGABE 2:**
Gegeben sei ein beliebiges Signaturverfahren $(P, U, K, S, V)$ mit Klartextraum $P = \{0,1\}^n$ für ein $n \in \mathbb{N}$. Wir wandeln die Verifikationsfunktionen $v_{pk} \in V$ nun folgendermaßen ab: $v'_{pk}(m,s) = 1$ falls $m = 0^n$ und $v'_{pk}(m,s) = v_{pk}(m,s)$ falls $m \neq 0^n$ für eine Signatur $(m,s) \in P \times S$. Für die Nachricht $0^n$ wird also jedes Element aus $S$ als gültige Signatur akzeptiert.

a) Handelt es sich noch um ein Signaturverfahren?

b) Angenommen das ursprüngliche Signaturverfahren ist sicher im Chosen-Message-Modell. Ist das neue Signaturverfahren immer noch sicher im Chosen-Message-Modell?

**AUFGABE 3:**
Betrachten Sie das RSA-Signaturverfahren. Geben Sie einen Angreifer an, der zu einer gegebenen Signatur $s$ eine Nachricht $m$ berechnet, so dass $s$ eine gültige Signatur für $m$ ist.

**AUFGABE 4:**
Alice und Bob benutzen das folgende Protokoll, um einen Schlüssel $k \in \{0,1\}^n$ auszutauschen:

1 Alice wählt $k, r \in \{0,1\}^n$ zufällig gleichverteilt und schickt $s := k \oplus r$ an Bob.
2 Bob wählt $t \in \{0,1\}^n$ zufällig gleichverteilt und schickt $u := s \oplus t$ an Alice.
3 Alice berechnet $w := u \oplus r$ und sendet $w$ an Bob.
4 Alice gibt $k$ als gemeinsamen Schlüssel aus.
5 Bob gibt $w \oplus t$ als gemeinsamen Schlüssel aus.

a) Zeigen Sie, dass Alice und Bob den selben Schlüssel ausgeben.

b) Handelt es sich um ein *interaktives Schlüsselaustauschprotokoll* gemäß der Definition aus der Vorlesung?

c) Analysieren Sie die Sicherheit des Protokolls gegen passive Angreifer. Falls das Protokoll sicher ist zeigen Sie dazu, dass die Verteilung der ausgetauschten Nachrichten unahbhängig von $k$ ist: $\Pr(s, u, w|k) = \Pr(s, u, w)$. Falls das Protokoll nicht sicher ist geben Sie einen passiven Angreifer an, der bei Eingabe von $s, u, w$ den Schlüssel $k$ ausgibt.