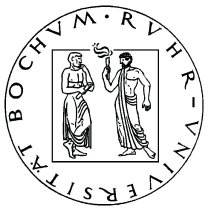
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Hausübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 1 / 04. Mai 2009 / Abgabe spätestens 13. Mai, 8:30 Uhr

AUFGABE 1:
Sicherheit hybrider Verfahren Sei $\mathcal{A}^{hy}$ ein Angreifer auf das Hybridverfahren Π^{hy} bestehend aus einem CPA-sicheren asymetrischen Verfahren Π (gegen passive Angreifer) und einem symetrischen Verfahren mit ununterscheidbaren Verschlüsselungen (gegen passive Angreifer).
Betrachten Sie den folgenden Angreifer $\mathcal{A}_1$ der Nachrichten des Public Key Verfahrens Π belauscht:

1. $\mathcal{A}_1$ erhält als Eingabe den öffentlichen Schlüssel pk. Er wählt zufällig $k \leftarrow \{0,1\}^n$ und gibt das Paar von Nachrichten $(k, 0^n)$ zurück. Anschließende erhält er einen Challenge-Ciphertext c_1.

2. $\mathcal{A}_1$ ruft $\mathcal{A}^{hy}(pk)$ auf und bekommt m_0, m_1 zurückgeliefert.

3. $\mathcal{A}_1$ berechnet $c_2 \leftarrow Enc'_k(m_0)$ und sendet die Challenge (c_1, c_2) an $\mathcal{A}^{hy}$. $\mathcal{A}_1$ gibt das Bit b' aus, welches von $\mathcal{A}^{hy}$ ausgegeben wird.

Zeigen Sie, falls Π ununterscheidbare Verschlüsselungen bzgl. eines passiven Angreifers hat, dann gilt:

$$\frac{1}{2}(Pr[\mathcal{A}^{hy}(Enc_{pk}(k), Enc'_k(m_0)) = 0] + Pr[\mathcal{A}^{hy}(Enc_{pk}(0^n), Enc'_k(m_0)) = 0]) \leq \frac{1}{2} + negl.$$

AUFGABE 2 (5 Punkte)**:**
Zeigen Sie, dass jedes 2 Runden Schlüsselaustauschprotokoll, welches sicher gegen passive Angreifer ist, in ein CPA-sicheres Public-Key Verfahren transformiert werden kann.

AUFGABE 3 (5 Punkte)**:**
Wir betrachten den Hastad-Angriff auf Textbook RSA. Sei dazu $pk_1 = (N_1, e) = (2501, 3)$, $pk_2 = (2537, 3)$ und $pk_3 = (2491, 3)$. Der Angreifer beobachtet die Chiffretexte $c_1 = m^3 = 2370 \bmod N_1$, $c_2 = 1059 \bmod N_2$ und $c_3 = 2277 \bmod N_3$.

1. Berechnen Sie m.

2. Funktioniert der Angriff auch für andere Werte von e?

AUFGABE 4:
Sei N fest und nehmen Sie an, dass es einen Angreifer $\mathcal{A}$ mit Laufzeit t gibt, so dass

$$Pr[\mathcal{A}(x^e \bmod N) = x] = 0.01,$$

wobei die Wahrscheinlichkeit über die zufällige Wahl $x \leftarrow \mathbb{Z}_N^*$ geht.
Zeigen Sie, dass es möglich ist einen Angreifer $\mathcal{A}'$ zu konstruieren für den gilt

$$Pr[\mathcal{A}'(x^e \bmod N) = x] = 0.99.$$

Für die Laufzeit t' von $\mathcal{A}'$ soll gelten $t' = poly(\log_2 N, t)$.