Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Felix Heuer

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 2 / 20. April 2010 / Abgabe 4. Mai, 08:30 Uhr, Kasten NA 02

AUFGABE 1. Konstruktives. (5 Punkte)
Zeigen Sie, dass jedes 2-Runden-Schlüsselaustauschprotokoll Π, welches sicher gegen passive Angreifer ist, in ein CPA-sicheres Public-Key Verfahren $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ transformiert werden kann, d.h. zeigen Sie sowohl die Korrektheit Ihres Verfahrens als auch die CPA-Sicherheit.

Hinweis: Benutzen Sie bei Ihrer Lösung folgende Notation: Seien msg_1 und msg_2 die Nachrichten im Protokoll Π und sei s_A der geheime Zustand (State) von Partei A. Ferner bezeichne $\mathsf{Derive}^{\mathsf{A}}(\mathsf{s}_{\mathsf{A}}, \mathsf{msg}_1, \mathsf{msg}_2)$ die Schlüsselableitungsfunktion der Partei A und $\mathsf{Derive}B(\mathsf{msg}_1, s_B)$ die Schlüsselableitungsfunktion von B. Geben Sie nun an, wie Sie diese Elemente als Public Key bzw. Secret Key in Ihrem Verschlüsselungsverfahren benutzen können und definieren Sie konkret Enc und Dec. (Wenn man bspw. den Diffie-Hellman Schlüsselaustausch betrachtet, so ist $\mathsf{msg}_1 = g^x$, $\mathsf{msg}_2 = g^y$ und $s_A = x$ sowie $\mathsf{Derive}(g^x, g^y, x) = g^{xy}$.)

In der nächsten Aufgabe wollen wir formal den 1. Punkt der Beweisskizze zur Sicherheit der hybriden Verschlüsselung beweisen (siehe Folie 35 und Präsenzübungsblatt für die verwendete Notation).

AUFGABE 2. Hybrides: Sicherheit. (5 Punkte)
Beweisen Sie, dass

$$(\mathsf{Enc}_{\mathsf{pk}}(k), \mathsf{Enc}'_k(m_0)) \equiv (\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_0))$$

gilt. Betrachten Sie hierzu einen Algorithmus $\mathcal{D}$, welcher obige Verteilungen mit Vorteil $\varepsilon_{\mathcal{D}}(n)$ unterscheidet, d.h.

$$\varepsilon_{\mathcal{D}}(n) = |\mathbf{Pr}\left[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(k), \mathsf{Enc}'_k(m_0)) = 1\right] - \mathbf{Pr}\left[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_0)) = 1\right]| \ ,$$

und zeigen Sie, dass $\varepsilon_{\mathcal{D}}(n) \leq \mathsf{negl}(n)$. Konstruieren Sie hierzu einen CPA-Angreifer $\mathcal{A}$ auf Π, welcher $\mathcal{D}$ benutzt.

AUFGABE 3. Faktorisieren. (5 Punkte)
Sei $N = pq$ ein RSA-Modul und sei $(N, e, d) \leftarrow \mathsf{GenRSA}$. Wir wollen für den Spezialfall $e = 3$ zeigen, dass das Berechnen von d äquivalent zum Faktorisieren von N ist. Beweisen Sie hierzu folgende Aussagen:

a) Wenn man N effizient faktorisieren kann, so kann man d effizient berechnen.
Bemerkung: Das zeigt die Rückrichtung der Äquivalenz für allgemeines e.

b) Sind $\phi(N)$ und N bekannt, so kann man p und q berechnen.

c) Seien $e = 3$ und $d \in \mathbb{N}$ mit $ed \equiv 1 \bmod \phi(N)$ bekannt. Zeigen Sie, dass man dann effizient p und q berechnen kann.

Zur Lösung von Teil c) ist es hilfreich, Teil b) zu benutzen.

AUFGABE 4. Padding. (5 Punkte)
Sei GenRSA ein Algorithmus zur RSA-Schlüsselerzeugung (siehe auch Folie 36). Betrachten Sie das folgende Experiment $\mathsf{PAD}_{\mathcal{A},\mathsf{GenRSA},\ell}$ für einen ppt-Algorithmus $\mathcal{A}$ und eine Funktion $\ell(n) \leq 2n - 2$ (für alle $n \in \mathbb{N}$):

i) $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$

ii) $m \leftarrow \mathcal{A}(N, e)$ wobei $m \in \{0,1\}^{\ell(n)}$

iii) Wähle $y_0 \in_R \mathbb{Z}_N^*$ und $r \in_R \{0,1\}^{\log_2 N - \ell(n) - 1}$ und setze $y_1 := (r||m)^e \mod N$

iv) Wähle $b \in_R \{0,1\}$ und sende y_b an $\mathcal{A}$. Sei $b' \leftarrow \mathcal{A}(N, e, y_b)$

v) Gib 1 aus genau dann, wenn $b = b'$

Wir sagen, dass das ℓ-padded-RSA Problem hart ist bezüglich GenRSA, wenn für jeden ppt-Angreifer $\mathcal{A}$ gilt

$$\mathbf{Pr}\left[\mathsf{PAD}_{\mathcal{A},\mathsf{GenRSA},\ell}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n)$$

Zeigen Sie: Wenn das ℓ-padded RSA Problem hart ist bzgl. GenRSA, so ist auch das padded RSA-Verschlüsselungsverfahren (siehe Folie 39) CPA-sicher (wobei obiges ℓ verwendet wird).