Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 2 /
Abgabe: 10. Mai 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (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 Unterscheider $\mathcal{D}$, welcher obige Verteilungen mit Vorteil $\varepsilon(n)$ unterscheidet, d.h.

$$|\mathsf{Ws}[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(k), \mathsf{Enc}'_k(m_0)) = 1] - \mathsf{Ws}[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_0)) = 1]| = \varepsilon(n)$$

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

AUFGABE 2 (5 Punkte)**:**

Betrachten Sie das folgende Public Key Verschlüsselungsverfahren. Der öffentliche Schlüssel (q, g, h) und der private Schlüssel x werden analog zur ElGamal Verschlüsselung mit Hilfe eines Algorithmus $\mathcal{G}$ generiert. Um ein Bit b zu verschlüsseln, berechnet der Sender den Chiffretext folgendermaßen:

1. Falls $b = 0$ ist, dann wählt er $y \in_R \mathbb{Z}_q$ und berechnet $c = (c_1, c_2) := (g^y, h^y)$.
2. Falls $b = 1$ ist, dann wählt er unabhängig gleichverteilt $y, z \in_R \mathbb{Z}_q$ und berechnet $c = (c_1, c_2) := (g^y, g^z)$.

(a) Zeigen Sie, dass mit Hilfe des privaten Schlüssels x eine effiziente Entschlüsselung möglich ist (hierbei darf es zu Entschlüsselungsfehlern kommen, Sie sollten aber begründen, warum diese nur mit vernachlässigbarer Wahrscheinlichkeit auftreten).

(b) Beweisen Sie, dass das Verschlüsselungsverfahren CPA-sicher ist, falls das DDH-Problem hart bzgl. $\mathcal{G}$ ist.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Zeigen Sie, dass jedes 2-Runden-Schlüsselaustauschprotokoll Π' (für Schlüssel $K \in \{0,1\}^n$), welches sicher gegen passive Angreifer ist, in ein CPA-sicheres Public Key Verfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 p_A (von Alice nach Bob) und p_B (von Bob nach Alice) die öffentlich übertragenen Parameter im Protokoll Π' und seien s_A (von Alice) und s_B (von Bob) die geheimen Zustände der Parteien. Ferner bezeiche $\mathsf{Derive}^A(s_A, p_B)$ die Schlüsselableitungsfunktion von Alice, $\mathsf{Derive}^B(s_B, p_A)$ die Schlüsselableitungsfunktion von Bob. Geben Sie an, wie Sie diese Elemente als Public Key bzw. Secret Key in Ihrem Verschlüsselungsverfahren benutzen können und definieren Sie konkret Enc und Dec.

Alice		Bob
s_A	$\xrightarrow{p_A}$	
	$\xleftarrow{p_B}$	s_B
$K := \mathsf{Derive}^A(s_A, p_B)$		$K := \mathsf{Derive}^B(s_B, p_A)$

AUFGABE 4 (5 Punkte)**:**

Ein Unternehmen verwendet den öffentlichen RSA-Schlüssel (N, e). Bei einem Sicherheitsupdate wird der Schlüssel auf (N, e') aktualisiert, d.h. der Modulus N bleibt erhalten, lediglich der Exponent e wird geändert. Dabei wird darauf geachtet, dass e und e' keine gemeinsamen Teiler haben, d.h. $\mathrm{ggT}(e, e') = 1$ gilt.

Ein Kunde schickt eine verschlüsselte Nachricht m, noch unter dem alten öffentlichen Schlüssel, an das Unternehmen. Nachdem er auf den Fehler hingewiesen wurde, schickt er die Nachricht erneut, nun verschlüsselt mit dem neuen öffentlichen Schlüssel. Ein Angreifer liest beide Übertragungen mit und erhält $x = m^e \bmod N$ sowie $y = m^{e'} \bmod N$.

(a) Zeigen Sie (allgemein), wie der Angreifer die Nachricht m in Zeit polynomiell in $\log(N)$ bestimmen kann. Nehmen Sie dazu an, dass $e, e' < N$ sind.

(b) Bestimmen Sie für $N = 221, e = 7, e' = 11, x = 178$ und $y = 94$ die Nachricht m.