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

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 2 / 03. Mai 2013

AUFGABE 1:

Beweisen Sie, dass

$$(\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_0)) \equiv (\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_1))$$

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

$$|\mathsf{Ws}[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_0)) = 1] - \mathsf{Ws}[\mathcal{D}(\mathsf{Enc}_{\mathsf{pk}}(0^n), \mathsf{Enc}'_k(m_1)) = 1]| = \varepsilon(n),$$

und zeigen Sie, dass $\varepsilon(n) \leq \mathsf{negl}(n)$ gilt. Konstruieren Sie hierzu einen KPA-Angreifer $\mathcal{A}'$ für das *symmetrische* Verfahren Π', welcher $\mathcal{D}$ benutzt.

AUFGABE 2:

Sei $\mathcal{G}$ ein ppt-Algorithmus, der bei Eingabe 1^n eine n-Bit Primzahl p ausgibt, welche die zyklische Gruppe $\mathbb{Z}_p^*$ definiert, sowie einen Generator g für $\mathbb{Z}_p^*$.

Zeigen Sie, dass das ElGamal-Verschlüsselungsverfahren Π nicht CPA-sicher bzgl. $\mathcal{G}$ ist.

AUFGABE 3:

Sei $\mathcal{G}$ ein Algorithmus, der eine zyklische Gruppe G der bekannten Ordnung q und einen Generator g für G erzeugt. In der Vorlesung wurde gezeigt, dass ElGamal bzgl. $\mathcal{G}$ CPA-sicher unter der DDH-Annahme ist. Zeigen Sie, dass diese Annahme auch notwendig ist, indem Sie zeigen:

ElGamal ist CPA-sicher bzgl. $\mathcal{G} \Longrightarrow$ Das DDH-Problem ist hart bzgl. $\mathcal{G}$

Bitte wenden!

AUFGABE 4:

Sei $N = pq$ ein RSA-Modul und sei $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$. Wir wollen für den Spezialfall $e = 3$ zeigen, dass das Berechnen von d äquivalent zum Faktorisieren von N ist. Beweisen Sie hierzu folgene Aussagen:

(a) Wenn man N effizient faktorisieren kann, so kann man d effizient berechnen.

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

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