

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 2 / 27. und 29. April 2011

AUFGABE 1. Goodbye, Perfekte Sicherheit.

Sei $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ ein Public-Key Verschlüsselungsverfahren für 1-Bit Nachrichten $m \in \{0, 1\}$. Zeigen Sie, dass ein unbeschränkter Angreifer zur Eingabe pk und $c \leftarrow \text{Enc}_{\text{pk}}(m)$ stets mit Wahrscheinlichkeit 1 den Plaintext m bestimmen kann. (Insbesondere folgt hieraus, dass perfekte Sicherheit in der Public-Key Kryptographie ausgeschlossen ist).

Sei im Folgenden $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ ein Public-Key Verschlüsselungsverfahren und $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ ein symmetrisches Verschlüsselungsverfahren mit n -Bit Schlüsseln $k \in \{0, 1\}^n$. Sei außerdem $\Pi^{\text{hy}} = (\text{Gen}^{\text{hy}}, \text{Enc}^{\text{hy}}, \text{Dec}^{\text{hy}})$ das hybride Verfahren (siehe Folie 32f).

AUFGABE 2. Hybrides: Effizienz.

Zeigen Sie, dass die hybride Verschlüsselung für große Nachrichten m (d.h. $|m| \gg n$) effizienter ist als die direkte Anwendung der *mehrfachen Verschlüsselung* (siehe Folie 25f). Betrachten Sie hierzu die „Kosten“ der Verschlüsselung pro Eingabebit. Definieren Sie hierzu α als die Kosten von $\text{Enc}_{\text{pk}}(k)$ für $k \in \{0, 1\}^n$ und β als die Kosten von Enc' je Plaintextbit. Zeigen Sie, dass für $|m| \rightarrow \infty$ die Kosten von Π^{hy} gegen die Kosten von Π' konvergieren.

Wir wollen nun Punkt 2 der Beweisskizze zur Sicherheit von Π^{hy} formal beweisen (siehe Folie 35). Wir erinnern uns, dass wir hierzu Π als CPA-sicher und Π' als KPA-sicher annehmen.

AUFGABE 3. Hybrides: Sicherheit.

Beweisen Sie, dass

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

gilt.

Gehen Sie hierbei wie folgt vor: Sei $\mathcal{D}$ ein Algorithmus, der die obigen Verteilungen mit Vorteil $\varepsilon_{\mathcal{D}}(n)$ unterscheidet, d.h.

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

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

AUFGABE 4. Algebraisches.

Sei $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N : \text{ggT}(x, N) = 1\}$ die Einheitengruppe von $(\mathbb{Z}_N, \cdot)$ und sei $\phi(N) = |\mathbb{Z}_N^*|$ die Eulersche Phi-Funktion. Zeigen Sie:

- a) $\phi(p) = p - 1$ für jede Primzahl p
- b) $\phi(pq) = (p - 1)(q - 1)$ für zwei Primzahlen $p \neq q$
- c) Zeigen Sie, dass die Textbook-RSA Verschlüsselung *korrekt* ist für jede Nachricht $m \in \mathbb{Z}_N^*$. Was passiert, wenn $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$?