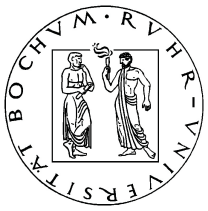
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Hausübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 3 / 14. Mai 2009 / Abgabe spätestens 27. Mai, 8:30 Uhr

AUFGABE 1 (5 Punkte)**:**
Sei $GenRSA$ der Schlüsselerzeugungsalgorithmus von Textbook RSA. Betrachten Sie das folgende Spiel für einen Angreifer $\mathcal{A}$ und eine Funktion ℓ mit $\ell(n) \leq 2n - 2$:

Spiel $PAD_{\mathcal{A},GenRSA,\ell}(n)$:

1. $GenRSA(1^n)$ liefert (N, e, d)
2. Der Angreifer $\mathcal{A}$ erhält (N, e) und gibt einen String $m \in \{0,1\}^{\ell(n)}$ zurück.
3. Wähle zufällig $y_0 \leftarrow \mathbb{Z}_N^*$ und zufällig $r \leftarrow \{0,1\}^{||N||-\ell(n)-1}$ und setze $y_1 := [(r||m)^e \bmod N]$.
4. Wähle ein zufälliges Bit $b \leftarrow \{0,1\}$. Der Angreifer erhält y_b und gibt ein Bit b' zurück.
5. $PAD_{\mathcal{A},GenRSA,\ell}(n) = \begin{cases} 1 & \text{if } b' = b \\ 0 & \text{else} \end{cases}$

Wir sagen das ℓ-padded RSA Problem ist hart bzgl. GenRSA, falls für alle ppt Angreifer gilt:

$$Pr[PAD_{\mathcal{A},GenRSA,\ell} = 1] \leq \frac{1}{2} + \text{negl.}$$

Zeigen Sie, dass falls das ℓ-padded RSA Problem hart bzgl. GenRSA ist, dann ist das Padded RSA Verschlüsselungsverfahren aus der Vorlesung CPA-sicher.

AUFGABE 2 (5 Punkte)**:**
ElGamal Hybrid Verfahren Auf natürliche Art erzeugen wir aus der ElGamal Verschlüsselung das folgende Hybride Verfahren. Der öffentliche Schlüssel ist wie bei ElGamal $pk = (\mathbb{G}, q, g, h)$ mit $h = g^x$, wobei x der geheime Schlüssel ist. Zur Verschlüsselung einer Nachricht m wählt der Sender zufällig $k \leftarrow \{0,1\}^n$ und sendet den Chiffretext

$$\langle g^r, h^r \cdot k, Enc_k(m)\rangle, \qquad r \leftarrow \mathbb{Z}_q \text{ zufällig.}$$

$Enc_k()$ ist die Verschlüsselungsfunktion des symetrischen Verfahrens.
Schlagen Sie eine Verbesserung vor, die zu einem kürzeren Chiffretext führt. Der Chiffretext soll dabei aus einem einzigen Gruppenelement und der symetrischen Verschlüsselung der Nachricht bestehen.

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie das folgende Public Key Verschlüsselungsverfahren. Der öffentliche Schlüssel $(\mathbb{G}, g, q, h)$ und der private Schlüssel x werden analog zur ElGamal Verschlüsselung generiert. Um ein Bit b zu verschlüsseln berechnet der Sender den Chiffretext folgendermaßen:

1. Falls $b = 0$ ist, dann wählt er $y \leftarrow \mathbb{Z}_q$ und berechnet $c = \langle c_1, c_2\rangle = \langle g^y, h^y\rangle$.
2. Falls $b = 1$ ist, dann wählt er zufällig und unabhängig $y, z \leftarrow \mathbb{Z}_q$ und berechnet $c = \langle c_1, c_2\rangle = \langle g^y, g^z\rangle$.

Zeigen Sie, dass mit Hilfe des privaten Schlüssels x eine effiziente Dechiffrierung möglich ist. Beweisen Sie, dass das Verschlüsselungsschema CPA-sicher ist, falls das *Decisional Diffie Hellman Problem* schwer bzgl. der Gruppe $\mathbb{G}$ ist.

AUFGABE 4 (5 Punkte)**:**
Sei $\mathcal{G}$ ein Algorithmus der bei Eingabe 1^n eine n-bit Primzahl p, die multiplikative Gruppe der Ordnung $q = p - 1$ und einen Generator g ausgibt.
Zeigen Sie, dass die Schwierigkeit des diskreten Logarithmus Problems bezüglich $\mathcal{G}$ die Existenz einer Einwegfunktion impliziert.