TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
www.math.tu-berlin.de/∼hess/krypto-ws2007

Abgabe: 12.02.2008
in der Sprechstunde im MA-811

13. Übung Kryptographie

(Schlüsselaustausch, Identifikationsprotokolle, Zero-Knowledge Beweise)

---

1. Aufgabe

3-Move Identifikationsverfahren:

Ein 3-Move Identifikationsverfahren ist ein interaktives, korrektes und vollständiges Verfahren besteht aus folgendem Ablauf:

- **Commit:** Der Beweiser P berechnet ein w_1 und schickt es an Verifizierer V.
- **Challenge:** V berechnet ein w_2 und schickt es an P.
- **Response:** P berechnet ein w_3 und schickt es an V.
- V verifiziert w_1 und w_3 und liefert $\{0, 1\}$.

Fiat-Shamir Transformation:

Jedes korrekte und vollständige 3-Move Identifikationsverfahren kann folgendermassen in ein Signatur Verfahren umgewandelt werden, welches im Zufallsorakelmodell bezüglich existenzieller Fälschung unter adaptivem chosen-message Angriff sicher ist:

- P berechnet w_1 wie oben.
- P berechnet $w_2 = h(M, w_1)$, wobei h eine öffentlich bekannte Hashfunktion ist.
- P berechnet w_3 wie oben. Die Signatur ist (M, w_1, w_3).
- V verifiziert den Signatur wie oben unter Verwendung von $w_2 = H(M, w_1)$.

Ein konkretes Identifikationsverfahren:

Sei $(G, \cdot)$ eine zyklische Gruppe der Ordnung $l \in \mathbb{P}$ mit dem Erzeuger g. Ferner sei $y = g^x \in G$.

- P waehlt $k \in \mathbb{Z}/l\mathbb{Z}$ zufällig und schickt $w_1 = g^k$ an V.
- V waehlt $w_2 \in \mathbb{Z}/l\mathbb{Z}$ zufällig und schickt an P.
- P berechnet $w_3 = w2 \cdot x + k$ und schickt w_3 an V.
- V überprüft, ob $g^{w_3} = y^{w_2} \cdot w_1$ gilt.

(a) Zeigen Sie, dass das obige Verfahren ein 3-Move Identifikationsverfahren ist.

(b) Welches Sigverfahren erhalten wir aus obigem Identifikationsverfahren nach Anwenundg von Fiat-Shamir Transformation?

(c) Zeigen Sie, dass das obige Identifikationsverfahren zero-knowledge ist.

(8 Punkte)

2. Aufgabe

Sei n ein RSA-Modul, x zufällig und $y = x^2 \mod n$. Person P soll die Kenntnis von x beweisen ohne etwas über x zu verraten. Im Skript wird dazu eine Vorgehensweise angegeben. Die Bezeichnungen sind hier wie im Skript. Angenommen es gibt ein schummelndes B mit Erfolgswahrscheinlichkeit $> \frac{1}{2}$. Zeigen Sie, dass dann B Wurzeln b, r mit $b^2 = ay^e$ und $r^2 = ay^{e'}$ und $e \neq e'$ berechnen kann.

(5 Punkte)

3. Aufgabe

Seien G_1, G_2, G_I zyklische Gruppen von Primzahlordunung p. Eine Paarung ist eine nicht-degenerierte bilineare Abbildung

$$e : G_1 \times G_2 \longrightarrow G_I.$$

Die Gruppen G_1, G_2 und G_I sollen sicheres DLP und CDH haben. Zeigen Sie, dass wenn $G_1 = G_2$ gilt dann das DDH in G_1 mit Hilfe von e leicht zu lösen ist.

(5 Punkte)

4. Aufgabe

Auf der Vorlesungsseite finden Sie eine kurze Einführung in GPG in der Datei gpg-2.pdf. Erklären Sie wie A und B miteinander verschlüsselte Nachrichten austauschen und entschlüsseln können.

(5 Punkte)

Hinweis: Die praktische Aufgabe des 12. Übungsblatts kann auch bis 12.02.2008 abgegeben werden.