Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 13.06.2005, 14h

Kryptografie
Übungsblatt 8

Aufgabe 25:

Ist $p > 2$ eine Primzahl und $a \in \mathbb{Z}$, so ist das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a, \\ 1 & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist}, \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

a) Beweisen Sie die folgenden Rechenregeln für das Legendre-Symbol:

1. $\left(\frac{a}{p}\right)$ hängt nur von der Restklasse von a modulo p ab.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ für alle $a, b \in \mathbb{Z}$
3. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ für $b \in \mathbb{Z}$ mit $p \nmid b$
4. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$

Ist $n \in \mathbb{N}_+$ eine ungerade Zahl mit Primfaktorzerlegung $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, so definieren wir das *Jacobi-Symbol* $\left(\frac{a}{n}\right)$ durch

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

b) Schreiben Sie eine Funktion `Jacobi(...)`, die für zwei gegebene Zahlen $a \in \mathbb{Z}$, $n \in \mathbb{N}_+$ ungerade das Jacobi-Symbol $\left(\frac{a}{n}\right)$ berechnet. Verwenden Sie dabei (ohne Beweis) die Formel $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ und das *quadratische Reziprozitätsgesetz* $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \cdot \left(\frac{p}{q}\right)$ für ungerade Primzahlen p, q. Vermeiden Sie es, die Zahlen a und n in ihre Primfaktoren zu zerlegen.

c) Sei nun $n = pq$ das Produkt zweier ungerader Primzahlen. Zeigen Sie, dass jeder quadratische Rest modulo n ein quadratischer Rest modulo p und modulo q ist. Folgern Sie ein Verfahren für die Erzeugung einer Zahl $y \in \{1, \ldots, n-1\}$ mit $\mathrm{ggT}(y, n) = 1$, die ein quadratischer Nichtrest modulo n ist und $\left(\frac{y}{n}\right) = 1$ erfüllt.

d) Implementieren Sie die Hashfunktion aus Beispiel 3.2 in einem Programm `Muenzwurf(...)`, das als Eingabe ein Element von $\{0, 1\}$ und eine geeignete Zufallszahl erwartet und als Ausgabe eine große (ca. 20-stellige) Zahl liefert. Beschreiben Sie nochmals ausführlich, wie zwei Anwender mit Hilfe dieses Programms den Münzwurf über das Internet bewerkstelligen können. (Die Kommunikation soll per E-Mail erfolgen.)

Für die Aufgabe gibt es 8 Punkte.

Aufgabe 26:

a) Zeigen Sie, wie man das Feige-Fiat-Shamir-Protokoll (Beispiel 3.20) knacken kann, wenn man die Primfaktorzerlegung von n kennt.

b) Seien $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ zwei Graphen mit Eckenmenge V_i und Kantenmenge E_i. Ein Isomorphismus von G_1 nach G_2 ist eine biijektive Abbildung $\sigma : V_1 \to V_2$ derart, dass $E_2 = \{(\sigma(v_i), \sigma(v_j)) \mid (v_i, v_j) \in E_1\}$. Zu gegebenen isomorphen Graphen ist es „schwierig“, einen

Isomorphismus zwischen diesen zu bestimmen. Beweisen Sie, dass das folgende Protokoll einen Zero-Knowledge-Beweis dafür liefert, dass A den Isomorphismus zwischen G_1 und G_2 kennt:
Schlüsselerzeugung: A wählt einen Graphen $G_1 = (V, E_1)$ und bildet diesen mittels einer Bijektion $\sigma : V \to V$ isomorph auf einen Graphen $G_2 = (V, E_2)$ ab. Öffentlich sind die Graphen G_1, G_2, geheim ist der Isomorphismus σ.

1. A bildet mittels einer weiteren (geheimen) Bijektion $\tau : V \to V$ einen weiteren isomorphen Graphen $H = (V, E_3)$ und sendet diesen an B.

2. B fragt zufällig nach dem Isomorphismus zwischen G_1 und H oder dem Isomorphismus zwischen G_2 und H.

3. A beantwortet die Frage von B.

4. B überprüft die Korrektheit der Antwort.

5. Das Verfahren (die Schritte 1 bis 4) wird wiederholt, bis B sicher ist, dass A das Geheimnis σ kennt.