Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 09.05.2005, 10h

Kryptografie
Übungsblatt 4

Aufgabe 13:
Es sei n eine quadratfreie Zahl (d.h. Produkt von paarweise verschiedenen Primzahlen). Zeigen Sie, dass für *alle* ganzen Zahlen a und b mit $b \equiv 1 \pmod{\varphi(n)}$ gilt $a^b \equiv a \pmod{n}$.

Aufgabe 14:
Sei $p \geq 17$ eine Fermatsche Primzahl, d.h. eine Primzahl der Form $p = 2^{2^k} + 1$ mit $k \geq 2$.

a) Beweisen Sie, dass die Restklasse von 5 die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ erzeugt. (Hinweis: Verwenden Sie (ohne Beweis), dass es keine Zahl $a \in \mathbb{Z}$ gibt mit $a^2 \equiv 5 \pmod{p}$.)

b) Zeigen Sie, dass man das ElGamal-Kryptosystem in $\mathbb{Z}/p\mathbb{Z}$ wie folgt knacken kann. Gegeben sei $a \in \mathbb{Z}$ und ein $g \in \mathbb{N}_+$, so dass die Restklasse von g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Gesucht sei ein $x \in \{0, \ldots, p-1\}$ mit $g^x \equiv a \pmod{p}$.

1. Sei $l = 2^k$ und sei a_0 die Restklasse von $a \in \mathbb{Z}/p\mathbb{Z}$, $g_0 = g$.
2. Für $j = 1, \ldots, l$ berechne $b_j = a_{j-1}^{2^{l-j}} \bmod p \in \{1, p-1\}$ und setze $x_{j-1} = 0$, falls $b_j = 1$ bzw. $x_{j-1} = 1$, falls $b_j = p-1$. Ferner setze $g_j = g_{j-1}^2 \bmod p$ und $a_j = a_{j-1} \cdot g_{j-1}^{x_{j-1}} \bmod p$.
3. Gib das Ergebnis $x = p - 1 - (x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1})$ aus.

Tipp: Zeigen Sie $g_j = g^{2^j}$ und $a_j = g^{x_0 + 2x_1 + \cdots + 2^{j-1}x_{j-1}} \cdot a$ für $j = 0, \ldots, l$.

c) Bei einem ElGamal-Kryptosystem mit $p = 65537$ und öffentlichem Schlüssel $5^a = 27849$ erreicht uns die Nachricht

$$(5660, 28471),\ (17747, 6537),\ (26694, 32563),\ (32609, 35447)$$

Dabei entspreche $A \hat{=} 0$, $B \hat{=} 1, \ldots$, und ein Block von drei Buchstaben abc mit entsprechenden Nummern α, β, γ werde in die Zahl $\alpha \cdot 26^2 + \beta \cdot 26 + \gamma$ umgewandelt. Entschlüsseln Sie die Nachricht.

Aufgabe 15: Sei $\alpha > 0$ und $a \in \mathbb{Z}$ nicht durch 3 teilbar. Zeigen Sie, dass man wie folgt x findet mit $2^x \equiv a \pmod{3^\alpha}$. Dass 2 die multiplikative Gruppe $(\mathbb{Z}/3^\alpha\mathbb{Z})^\times$ erzeugt, kann vorausgesetzt werden.

1. Zeigen Sie, dass man obiges x finden kann, wenn man die Kongruenz $2^x a \equiv 1$ lösen kann. Zeigen Sie weiterhin, dass man dieses Problem lösen kann, wenn man es für $a \equiv 1 \pmod{3}$ und gerades x lösen kann, so dass es genügt, die Kongruenz $4^x a \equiv 1 \pmod{3^\alpha}$ zu lösen.

2. Sei $x = x_0 + x_1 3 + \cdots + x_{\alpha-2}3^{\alpha-2}$ die 3-adische Darstellung von x, sei $a_j = 4^{x_0 + 3x_1 + \cdots + 3^{j-2}x_{j-2}} \cdot a \bmod 3^\alpha$ und $g_j = 4^{3^{j-1}} \bmod 3^\alpha$ für $j = 1, \ldots, \alpha$. Bestimme induktiv $x_0, \ldots, x_{\alpha-2}$ und $a_1, \ldots, a_\alpha$ wie folgt:
Setze $x_{-1} = 0$, $a_1 = a \bmod 3^\alpha$. Sei nun $j > 1$ und angenommen, $x_0, \ldots, x_{j-3}$ und $a_1, \ldots, a_{j-1}$ sind bestimmt. Berechne $x_{j-2} = (1 - a_{j-1})/3^{j-1} \bmod 3$ (warum geht das?). Berechne $a_j = g_{j-1}^{x_{j-2}} a_{j-1} \bmod 3^\alpha$.