Übungen zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 8. Februar 2013, vor den Übungen

1. Zeige Lemma 3.8:
   Es seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ Zahlen mit $ggT(a, m) = 1$. Dann gilt für alle $k \in \mathbb{N}$
   $$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m\, a}{ggT(\mathrm{ord}_m\, a, k)}.$$
   (4 Punkte)

2. Es sei $(\mathbb{Z}/17\mathbb{Z})^*$ gegeben.
   (a) Finde eine Primitivwurzel in $(\mathbb{Z}/17\mathbb{Z})^*$.
   (b) Stelle jedes $g \in (\mathbb{Z}/17\mathbb{Z})^*$ als Potenz der in Teilaufgabe a) gefundenen Primitivwurzel dar.
   (c) Löse die Kongruenz $x^{11} \equiv 4 \bmod 17$. (7 Punkte)

3. Melanie schickt Immanuel eine Nachricht.
   Dazu wählen sie als öffentlichen Schlüssel die kleinstmögliche Primzahl p, die eine Mersenne- Primzahl, aber keine Fermatzahl ist und die regelmäßigen Polygone mit $p \pm 1$ Ecken mit Zirkel und Lineal konstruierbar sind, die mit p und $p \pm 2$ Ecken dagegen nicht. Weiter nutzen sie die kleinste Primitivwurzel r modulo p. Immanuel wählt $a \in \{1, \ldots, p-1\}$, Melanie $b \in \{1, \ldots, p-1\}$ und berechnen dann $A \equiv r^a \bmod p$ und $B \equiv r^b \bmod p$, wobei A eine vollkommene Zahl ist, die nicht durch 3 teilbar ist und B sich als Summe einer Fermatzahl und einer vollkommenen Zahl darstellen lässt, eine Primzahl aber kein Bestandteil eines Primzahlzwillingspaares ist.
   So kennen beide ihren geheimen Schlüssel k.
   Achim und Marcel, den Melanie nicht kennt, haben den Kanal abgehört, kennen damit ebenfalls die Werte p, r, A und B und knacken daraufhin mittels folgender Vorgehensweise den Code:
   (a) Bestimme selbst die Werte p, r, A und B.
   (b) Berechne daraus mit dem diskreten Logarithmusproblem a und b.
   (c) Wie lautet der geheime Schlüssel k?

   Melanie und Immanuel wissen nicht, dass ihr Code geknackt wurde. Immanuel nutzt Melanies öffentlichen Schlüssel (p, r, B) und schickt ihr eine "geheime" Nachricht, in der er jedem Buchstaben eine Zahl gemäß Schema (3.1) aus dem Skript zuordnet und mittels des Elgamal- Kryptoverfahrens und dem privaten Schlüssel k codiert. Somit bestimmt er für die achtstellige Nachricht $c_1 = 20$ und

c_{2_1}	c_{2_2}	c_{2_3}	c_{2_4}	c_{2_5}	c_{2_6}	c_{2_7}	c_{2_8}
9	23	7	2	25	25	2	24

   und schickt die Botschaft $(c_1, [c_{2_1}, c_{2_2}, c_{2_3}, c_{2_4}, c_{2_5}, c_{2_6}, c_{2_7}, c_{2_8}])$ an Melanie.
   (d) Wie lautet die Nachricht? (13 Punkte)