Übungen zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Dr. Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte, alles Zusatzpunkte
Abgabe: Freitag, 13. Februar 2015, vor den Übungen

1. Es sei K ein endlicher Körper mit q Elementen und $C \subset K^n$ ein linearer Code.

   (a) Wieviele Kontrollmatrizen hat der Code C?

   (b) Gib eine Kontrollmatrix für den $(7, 4)$- Hammingcode an, die von der Matrix

   $$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

   verschieden ist. (6 Punkte)

2. Wir wollen nun eine Methode finden, um Lösungen einer Kongruenz $x^k \equiv b \bmod m$ zu bestimmen, wobei wir nun auf die Voraussetzung $ggT(k, \varphi(m)) = 1$ verzichten wollen. Wir beschränken uns dabei aber auf Primzahlmoduln.

   (a) Es sei $p \in \mathbb{P}$ und r eine Primitivwurzel modulo p.
   Wir definieren die Exponentialfunktion $\exp_r \colon (\mathbb{Z}/(p-1)\mathbb{Z}, +) \to ((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ über $g \to r^g$.
   Zeige, dass dann $\exp_r(g + h) = \exp_r(g) \cdot \exp_r(h)$ für alle $g, h \in (\mathbb{Z}/(p-1)\mathbb{Z}, +)$ gilt.

   (b) Zeige, dass die Exponentialfunktion bijektiv ist und deren Umkehrfunktion über den diskreten Logarithmus $\operatorname{dlog}_r \colon ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \to (\mathbb{Z}/(p-1)\mathbb{Z}, +)$ über $r^g \to g$ gegeben ist.

   (c) Zeige, dass die Kongruenz $x^k \equiv b \bmod p$ zur linearen Kongruenz $kg \equiv h \bmod (p-1)$ mit $g = \operatorname{dlog}_r x$ und $h = \operatorname{dlog}_r b$ äquivalent ist.

   (d) Bestimme die Anzahl der Lösungen der Kongruenz $x^7 \equiv 17 \bmod 29$.

   (e) Gib alle Lösungen der Kongruenz aus Teilaufgabe d) an. (8 Punkte)

3. Der diskrete Logarithmus aus Aufgabe 2 lässt sich in der Kryptographie beim sogenannten Diffie-Hellman- Schlüsselaustauschverfahren anwenden. Zwei Teams, Team I, bestehend aus Artur, Bastian, Marc und Viet, und Team II, bestehend aus Chris, Marcus, Philipp und Tizian, wollen über eine unsichere Leitung vertrauliche Nachrichten austauschen. Dazu benutzen sie ein symmetrisches Verschlüsselungsverfahren, wozu sie aber erst einen geheimen Schlüssel austauschen müssen. Hierfür steht aber auch nur eine unsichere Leitung zur Verfügung. Sie gehen nun folgendermaßen vor:

   - Die beiden Teams wählen $p \in \mathbb{P}$ und eine Primitivwurzel $r \bmod p$ als öffentlichen Schlüssel.
   - Team I wählt eine Zahl $a \in \{1, \ldots, p-1\}$, berechnet $A \equiv r^a \bmod p$ und sendet A an Team II.
   - Team II wählt eine Zahl $b \in \{1, \ldots, p-1\}$, berechnet $B \equiv r^b \bmod p$ und sendet B an Team I.
   - Beide Teams können nun beide das Element $k \equiv A^b \equiv r^{ab} \equiv B^a \bmod p$ berechnen.
     Dies ist der private Schlüssel, den folglich beide kennen.

Julia und Tabea haben den unsicheren Kanal abgehört, weswegen sie ebenfalls p, r, A und B kennen. Um aber den privaten Schlüssel k berechnen zu können, müssen sie aber entweder a oder b kennen. Dies lässt sich zwar mit dem diskreten Logarithmus bewerkstelligen, doch wenn die Primzahlen groß genug gewählt sind, können Julia und Tabea dieses Problem nicht mehr effizient lösen, und die zwei Teams können sicher Nachrichten verschicken.

(a) Die zwei Teams wählen nun als öffentlichen Schlüssel die kleinstmögliche Primzahl p, die eine Mersenne- Primzahl, aber keine Fermatzahl ist und $\varphi(p)$ mindestens drei verschiedene Primfaktoren besitzt. Weiter nutzen sie die kleinste Primitivwurzel r modulo p.
Team I wählt $a \in \{1, \dots, p-1\}$ und Team II $b \in \{1, \dots, p-1\}$, wonach sie dann $A \equiv r^a \bmod p$ und $B \equiv r^b \bmod p$ berechnen, wobei A eine vollkommene Zahl ist, die nicht durch 3 teilbar ist und B sich über

$$\frac{A+B+p}{2} = \min_{p \in S(\mathbb{P})} \{p \equiv 1 \bmod 10 \colon p \neq 11\}$$

bestimmen lässt, wobei $S(\mathbb{P})$ die Streichungmenge von Übungsblatt 6 bezeichne.
Bestimme die Werte p, r, A und B, um auf dem gleichen Wissensstand wie Julia und Tabea zu sein.

(b) Berechne daraus mit dem diskreten Logarithmus a und b.

(c) Wie lautet der private Schlüssel k?

Die zwei Teams wissen nun aber nicht, dass ihr Code geknackt wurde.
Team I schickt Team II unter Verwendung des öffentlichen Schlüssels (p, r, B) und der Zuordnung jedes Buchstaben mit einer Zahl, was über

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	ß
16	17	18	19	20	21	22	23	24	25	26	27	28	29	00

vonstatten geht, eine "geheime" Nachricht mittels des privaten Schlüssels k und des sogenannten ElGamal- Kryptoverfahrens, welches auf dem Diffie- Hellman- Verfahren beruht und dies zum Ver- und Entschlüsseln anstatt zum Schlüsselaustausch nutzt. Das ElGamal- Verfahren funktioniert so: Team I wählt eine Nachricht $m \in \{0, \dots, p-1\}$ und berechnet nun mit dem öffentlichem Schlüssel (p, r, B) die Werte $c_1 \equiv r^k \bmod p$ und $c_2 \equiv mB^k \bmod p$.

(d) Zeige, dass $m \equiv (c_1^b)^{-1} \cdot c_2 \bmod p$ gilt.

(e) Team I schickt Team II die Botschaft $(c_1, [c_{2_1}, c_{2_2}, c_{2_3}, c_{2_4}, c_{2_5}, c_{2_6}, c_{2_7}, c_{2_8}, c_{2_9}, c_{2_{10}}, c_{2_{11}}])$ mit

c_{2_1}	c_{2_2}	c_{2_3}	c_{2_4}	c_{2_5}	c_{2_6}	c_{2_7}	c_{2_8}	c_{2_9}	$c_{2_{10}}$	$c_{2_{11}}$
1	18	25	8	9	18	17	4	26	7	19

Wie lautet die Nachricht? (10 Punkte)