Mathematische Grundlagen der Kryptografie (1321) SS 04

Nachklausur am 2.10.2004:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe 1

Beim Verschiebe-Kryptosystem wird zunächst die übliche Identifizierung der Buchstaben A,...,Z mit den Zahlen $0, \ldots, 25$ vorgenommen:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25.

Der Geheimtext entspricht dann der Zahlenfolge $[23, 4, 11, 2, 6, 1, 5, 11, 5, 6, 17, 25]$. Die Zahlen werden aufgefasst als Elemente von $\mathbb{Z}/26\mathbb{Z}$. Zum Entschlüsseln (mit dem Schlüssel 13) bildet man nun für jede Zahl y aus der Zahlenfolge $y - 13 \bmod 26$ bzw. $y + 13 \bmod 26$. Dies ergibt die Zahlenfolge $[10, 17, 24, 15, 19, 14, 18, 24, 18, 19, 4, 12]$. In Buchstaben zurück übersetzt lautet das:

KRYPTOSYSTEM

zu Aufgabe 2

Behauptung Die Zahl $\sqrt{i + \sqrt{3}}$ ist algebraisch über $\mathbb{Q}$.

Beweis Die Zahl $a = \sqrt{i + \sqrt{3}}$ ist genau dann algebraisch über $\mathbb{Q}$, wenn es ein Polynom $f \in \mathbb{Q}[T]$ gibt mit $f(a) = 0$. Ein solches Polynom ist also zu suchen: Für $a = \sqrt{i + \sqrt{3}}$ ist $a^2 = i + \sqrt{3}$. Es gilt also $a^2 - i = \sqrt{3}$ und damit $(a^2 - i)^2 = a^4 - 2ia^2 - 1 = 3$. Es folgt $a^4 - 4 = 2ia^2$. Quadrieren ergibt $a^8 - 8a^4 + 16 = -4a^4$. Also ist $a^8 - 4a^4 + 16 = 0$, und a ist Nullstelle des Polynoms $T^8 - 4T^4 + 16 \in \mathbb{Q}[T]$. □

zu Aufgabe 3

Behauptung Ist $(G, *)$ eine Gruppe und U eine Untergruppe von G mit $[G : U] = 2$, dann ist U ein Normalteiler in G.

Beweis Die Untergruppe U ist ein Normalteiler in G, wenn $g * U = U * g$ für alle $g \in G$ gilt. Die Tatsache, dass $[G : U] = 2$ gilt, bedeutet, dass es nur zwei Linksnebenklassen und damit auch nur zwei Rechtsnebenklassen gibt. Eine davon ist jeweils U, die andere ist dann $G \setminus U$, denn G ist ja die disjunkte Vereinigung der Linksnebenklassen und auch der Rechtsnebenklassen. Sei nun $g \in U$. Dann gilt $g * U = U = U * g$. Gilt $g \notin U$, dann gilt $g * U \neq U$, also $g * U = G \setminus U$. Analog gilt $U * g = G \setminus U$. In beiden Fällen ist $g * U = U * g$, also ist U ein Normalteiler. □

zu Aufgabe 4

Behauptung Ist $(R, +, \cdot)$ ein Integritätsbereich und R' eine Teilmenge von R mit mindestens zwei Elementen, die mit den Verknüpfungen von R ebenfalls ein Ring ist, dann ist das neutrale Element der Multiplikation e' von R' gleich dem neutralen Element der Multiplikation e von R.

Beweis Da e das neutrale Element der Multiplikation in R ist, gilt $ee' = e'$. Andererseits gilt aber auch $e'e' = e'$, denn e' ist ja das neutrale Element der Multiplikation in R'. Es folgt also $ee' = e' = e'e'$, das heißt, $ee' - e'e' = 0$. Klammert man e' aus, ergibt sich $(e - e')e' = 0$. Da $R' \neq \{0\}$ gilt, ist $e' \neq 0$. Weil R nach Voraussetzung ein Integritätsbereich ist, folgt $e - e' = 0$, also $e = e'$. □

zu Aufgabe 5

Behauptung Ist $n = p_1 \cdots p_r$ für r verschiedene Primzahlen $p_1, \ldots, p_r$, dann gibt es genau 2^r verschiedene Elemente $a \in (\mathbb{Z}/n\mathbb{Z})$ mit $a^2 \bmod n = 1$.

Beweis Sei $a \in (\mathbb{Z}/n\mathbb{Z})$ mit $a^2 \bmod n = 1$. Dann gilt auch $a^2 \mod p_i = 1$ für alle $1 \leq i \leq r$. In $\mathbb{Z}/p_i\mathbb{Z}$ gibt es genau zwei Elemente b, so dass $b^2 \bmod p_i = 1$ gilt, nämlich $b \equiv 1 (\mathrm{mod} p_i)$ oder $b \equiv -1 \bmod p_i$. Es folgt also $a \equiv \pm 1 (\mathrm{mod} p_i)$ für alle $1 \leq i \leq r$. Es gibt 2^r Möglichkeiten, wie die $\pm 1 \bmod p_i$ verteilt sind, und mit dem chinesischen Restsatz gehört zu jedem a mit $a \equiv \pm 1 (\mathrm{mod} p_i)$ genau ein $a \in (\mathbb{Z}/n\mathbb{Z})$, das diese Eigenschaft erfüllt. Damit ist gezeigt, dass es höchstens 2^r Elmente in $(\mathbb{Z}/n\mathbb{Z})^\times$ gibt mit $a^2 \bmod n = 1$. Andererseits erfüllt aber auch jedes $a \in (\mathbb{Z}/n\mathbb{Z})$ mit $a \equiv \pm 1 (\mathrm{mod} p_i)$ für alle $1 \leq i \leq r$ die Bedingung $a^2 \bmod p_i = 1$ für alle $1 \leq i \leq r$, und dann folgt, wieder mit dem Chinesischen Restsatz $a^2 \bmod n = 1$. Dies zeigt, dass es mindestens 2^r Elemente a in $(\mathbb{Z}/n\mathbb{Z})$ gibt mit $a^2 \bmod n = 1$. □

zu Aufgabe 6

Beschreibung des Diffie-Hellman-Schlüsselaustauschverfahrens über endlichen Körpern.

(a) Der öffentliche Schlüssel bei diesem Verfahren sind ein endlicher Körper $\mathbb{K}$ und ein primitives Element $g \in \mathbb{K}$.

(b) Alice' geheimer Schlüssel ist ein zufällig gewähltes $a \in \mathbb{Z}$, und sie schickt g^a an Bob.

(c) Bobs geheimer Schlüssel ist ein zufällig gewähltes $b \in \mathbb{Z}$, und er schickt g^b an Alice.

(d) Der gemeinsame Schlüssel ist dann g^{ab}.

(e) Die Sicherheit des Verfahrens beruht auf der Annahme, dass diskrete Logarithmen in endlichen Körpern schwer zu berechnen sind, das heißt, dass es keinen effizienten Algorithmus gibt, um diskrete Logarithmen in endlichen Körpern zu berechnen. Weiterhin wird angenommen, dass jeder, der das Diffie-Hellman-System brechen kann, auch diskrete Logarithmen in endlichen Körpern berechnen kann.

(f) Das Verfahren ist effizient, weil Alice und Bob nur Potenzen in endlichen Körpern berechnen müssen. Dies ist mit Wiederholtem Quadrieren effizient möglich.

zu Aufgabe 7

Es sollen alle Punkte von $E(1, 1, \mathbb{F}_7) = \{(x, y) \mid y^2 = x^3 + x + 1\} \cup \{\mathcal{O}\}$ berechnet werden. Schauen wir uns zunächst die Quadrate in $\mathbb{F}_7$ an:

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

Nun berechnen wir für jedes $x \in \mathbb{F}_7$ den Wert $x^3 + x + 1$ und schauen nach, ob es ein $y \in \mathbb{F}_7$ gibt mit $y^2 = x^3 + x + 1$.

x	x^3+x+1	y
0	1	1,6
1	3	-
2	4	2,5
3	3	-
4	6	-
5	5	-
6	6	-

Die elliptische Kurve besteht also aus den Punkten

$$E(1,1,\mathbb{F}_7) = \{(0,1),(0,6),(2,2),(2,5),\mathcal{O}\}.$$

zu Aufgabe 8

Behauptung Die Menge $L = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}^3 \mid 2x_1 + x_3 \equiv 0(\text{mod}3)\}$ ist ein Gitter.

Beweis Seien $b_1 = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$, $b_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ und $b_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Wir zeigen, dass $L = L(b_1,b_2,b_3)$ gilt. Sei $A = (b_1|b_2|b_3)$. Dann ist $\det(A) = \det \begin{pmatrix} 3 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3 \neq 0$, also sind die Vektoren b_1, b_2, b_3 linear unabhängig, und $L(b_1,b_2,b_3)$ ist ein Gitter. Jeder der Vektoren b_1, b_2, b_3 liegt in L. Sei nun $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = a_1b_1 + a_2b_2 + a_3b_3$ mit $a_1, a_2, a_3 \in \mathbb{Z}$ ein beliebiger Vektor aus $L(b_1,b_2,b_3)$. Dann gilt

$$2x_1 + x_3 = 2(3a_1 + a_3) + a_3 = 6a_1 + 3a_3 \equiv 0(\text{mod}3).$$

Also gilt $L(b_1,b_2,b_3) \subseteq L$.

Sei nun $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in L$. Dann gilt $2x_1 + x_3 \equiv 0(\text{mod}3)$, das heißt, $2x_1 \equiv 2x_3(\text{mod}$ 3) oder $x_1 \equiv x_3(\text{mod}3)$. Also folgt $x_1 = x_3 + 3a$ mit $a \in \mathbb{Z}$. Damit lässt sich x

schreiben als $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3a + x_3 \\ x_2 \\ x_3 \end{pmatrix} = ab_1 + x_2b_2 + x_3b_3$ mit $a, x_2, x_3 \in \mathbb{Z}$. Also ist $x \in L(b_1, b_2, b_3)$, und es gilt $L = L(b_1, b_2, b_3)$. □

Die Determinante des Gitters $L = L(b_1, b_2, b_3)$ ist der Betrag der Determinante der Matrix $A = (b_1|b_2|b_3)$, also $\det(L) = 3$.