Mathematische Grundlagen der Kryptografie (01321) SoSe 09

Klausur am 29.08.2009:

Musterlösungen

Aufgabe 1

(a) Das numerische Äquivalent zum Wort O R A N G E ist $[14, 17, 0, 13, 6, 4]$. Der Schlüssel, mit dem verschlüsselt werden soll, ist 17, also muss zu jeder der Zahlen 17 in $\mathbb{Z}/26\mathbb{Z}$ addiert werden. Dies ergibt $[5, 8, 17, 4, 23, 21]$ oder F I R E X V.

(b) Der Schlüssel zum Verschlüsseln ist $(21, 21)$. Die Entschlüsselungsabbildung ist also $y \mapsto 21^{-1}(y-21)$. Entweder sehen wir sofort, was 21^{-1} in $\mathbb{Z}/26\mathbb{Z}$ ist, oder wir müssen den erweiterten Euklidischen Algorithmus verwenden:

$$\begin{aligned} 26 &= 21 + 5 \\ 21 &= 4 \cdot 5 + 1 \end{aligned}$$

Es ist also $1 = 21 - 4 \cdot 5 = 21 - 4(26 - 21) = (-4)26 + 5 \cdot 21$ und damit $21^{-1} = 5$. Die Entschlüsselungsabbildung ist also $y \mapsto 5(y + 5)$. Das numerische Äquivalent zu R B S Q ist $[17, 1, 18, 16]$. Es ist

$$\begin{aligned} 5(17+5) &\equiv 5 \cdot 22 \equiv 110 \equiv 6 (\mathrm{mod} 26) \\ 5(1+5) &\equiv 5 \cdot 6 \equiv 30 \equiv 4 (\mathrm{mod} 26) \\ 5(18+5) &\equiv 5 \cdot 23 \equiv 115 \equiv 11 (\mathrm{mod} 26) \\ 5(16+5) &\equiv 5 \cdot 21 \equiv 105 \equiv 1 (\mathrm{mod} 26). \end{aligned}$$

Der Klartext ist also $[6, 4, 11, 1]$ oder G E L B.

(c) Aus dem Schlüsselwort M A R I N E B L A U werden die doppelten Buchstaben gestrichen. Dies ergibt M A R I N E B L U. Dieses Wort wird nun beginnend beim Schlüsselbuchstaben P unter das Alphabet geschrieben und anschließend mit den restlichen Buchstaben in alphabetischer Reihenfolge aufgefüllt.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
F	G	H	J	K	O	P	Q	S	T	V	W	X	Y	Z	M	A	R	I

T	U	V	W	X	Y	Z
N	E	B	L	U	C	D

Das Wort R O T wird also zu R Z N verschlüsselt.

(d) Um die Nachricht zu entschlüsseln, muss die Matrix $K = \begin{pmatrix} 5 & 16 \\ 11 & 5 \end{pmatrix}$ invertiert werden. Es gilt $\det(K) = 5 \cdot 5 - 11 \cdot 16 = 25 - 176 = -151 \equiv 5 (\mathrm{mod} 26)$. Damit ist

$$K^{-1} = \frac{1}{5} K^{\mathrm{Ad}} = \frac{1}{5} \begin{pmatrix} 5 & 10 \\ 15 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}.$$

Das numerische Äquivalent zur Nachricht N I D U ist $[13, 8, 3, 20]$. Zum Entschlüsseln rechnen wir also

$$\begin{pmatrix} 13 & 8 \\ 3 & 20 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 11 & 0 \end{pmatrix}.$$

Dies entspricht dem Klartext L I L A.

Aufgabe 2

(a) Ein Beispiel für ein Kryptosystem, dessen Sicherheit auf der Schwierigkeit beruht, Zahlen zu faktorisieren, ist das RSA-Kryptosystem.

(b) Ein Beispiel für ein Kryptosystem, das auch über elliptischen Kurven verwendet werden kann, ist das ElGamal-Kryptosystem.

(c) Ein Beispiel für ein Kryptosystem, auf das man den Kasiski-Test anwenden kann, um es zu brechen, ist das Vigenère-Kryptosystem.

(d) Ein Beispiel für ein Kryptosystem, dessen Sicherheit bewiesen ist, ist das One-time Pad.

(e) Ein Beispiel für ein Kryptosystem, bei dem der Sender eine doppelt so lange Nachricht wie die Ursprungsnachricht schickt, ist das ElGamal-Kryptosystem.

Aufgabe 3

Sei $E(1,1,\mathbb{F}_4) = \{(x,y) \mid x,y \in \mathbb{F}_4 \text{ und } y^2+xy = x^3+x^2+1\} \cup \{\mathcal{O}\}$, $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2+T+1)$ und $\alpha = T \bmod (T^2+T+1)$. Ist nun $P = (x,y)$ ein Punkt auf $E(1,1,\mathbb{F}_4)$ mit x-Koordinate $\alpha+1$, dann muss die y-Koordinate die Gleichung $y^2+(\alpha+1)y = (\alpha+1)^3+(\alpha+1)^2+1$ erfüllen. Wegen $\alpha^2+\alpha+1 = 0$ und damit $\alpha^2 = \alpha+1$ gilt $(\alpha+1)^2 = \alpha^2+1 = \alpha+1+1 = \alpha$. Wegen $|\mathbb{F}_4^\times| = 3$ ist mit dem Satz von Lagrange weiter $(\alpha+1)^3 = 1$. Es muss also für y die Bedingung $y^2+(\alpha+1)y = 1+\alpha+1 = \alpha$ oder

$$y^2+(\alpha+1)y+\alpha = 0$$

erfüllt sein. Wir setzen in diese Bedingung nun einfach alle Elemente aus $\mathbb{F}_4$ ein.

$y = 0$**:** Es ist $0^2+(\alpha+1)0+\alpha = \alpha \neq 0$, also ist $(\alpha+1,0)$ kein Punkt auf der Kurve.

$y = 1$**:** Es ist $1^2+(\alpha+1)1+\alpha = 1+\alpha+1+\alpha = 0$, also ist $(\alpha+1,1)$ ein Punkt auf der Kurve.

Hier sind wir fertig, denn wir haben mit $(\alpha+1,1)$ einen Punkt auf der Kurve mit x-Koordinate $\alpha+1$ gefunden.

Aufgabe 4

Sei $(G,\cdot) = \langle a \rangle$ eine zyklische Gruppe.

Behauptung: Es gilt $\phi \circ \psi = \psi \circ \phi$ für alle $\phi, \psi \in \mathrm{Aut}(G)$.

Beweis: Seien $\phi, \psi \in \mathrm{Aut}(G)$. Da $G = \langle a \rangle$ gilt, gibt es ein $z_1 \in \mathbb{Z}$ mit $\phi(a) = a^{z_1}$. Ebenso gibt es ein $z_2 \in \mathbb{Z}$ mit $\psi(a) = a^{z_2}$. Sei nun g ein beliebiges Element aus G. Dann gibt es ein $z \in \mathbb{Z}$ mit $g = a^z$. Es folgt

$$\phi \circ \psi(g) = \phi(\psi(g)) = \phi(\psi(a^z)) = \phi(\psi(a)^z) = \phi(\psi(a))^z = \phi(a^{z_2})^z = \phi(a)^{zz_2} = a^{zz_1z_2}$$

und

$$\psi \circ \phi(g) = \psi(\phi(g)) = \psi(\phi(a^z)) = \psi(\phi(a)^z) = \psi(\phi(a))^z = \psi(a_1^z)^z = \psi(a)^{zz_1} = a^{zz_1z_2}.$$

Es gilt also $\phi \circ \psi(g) = \psi \circ \phi(g)$ für alle $g \in G$ und damit $\phi \circ \psi = \psi \circ \phi$. □

Aufgabe 5

Sei $n \in \mathbb{N}$.

Behauptung: Wenn es ein $a \in \mathbb{N}$ mit $1 \leq a \leq n-1$ und $a^{\frac{n-1}{2}}(\frac{a}{n}) \not\equiv 1(\mathrm{mod} n)$ gibt, dann ist n zusammengesetzt.

Beweis: Ist n eine Primzahl und $a \in \mathbb{N}$ mit $1 \leq a \leq n-1$, dann gilt $\mathrm{ggT}(a,n) = 1$ und deshalb mit dem Satz von Euler

$$a^{\frac{n-1}{2}} \equiv (\frac{a}{n})(\mathrm{mod} n).$$

Damit folgt

$$a^{\frac{n-1}{2}}(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} a^{\frac{n-1}{2}} \equiv a^n \equiv 1(\mathrm{mod} n)$$

mit dem kleinen Satz von Fermat. Ist also n eine Primzahl, dann gilt immer $a^{\frac{n-1}{2}}(\frac{a}{n}) \equiv 1(\mathrm{mod} n)$. Ist also $a^{\frac{n-1}{2}}(\frac{a}{n}) \not\equiv 1(\mathrm{mod} n)$, dann muss n zusammengesetzt sein. □

Aufgabe 6

Wir betrachten das RSA-Kryptosystem mit öffentlichem Schlüssel $(n = pq, e)$ und geheimem Schlüssel d.

(a) Es gilt $n = pq$, also $\varphi(n) = (p-1)(q-1) = 24$. Wir betrachten alle Möglichkeiten, 24 in zwei Faktoren $p-1$ und $q-1$ zu zerlegen und schauen dann, ob p und q jeweils Primzahlen sind.

$24 = 1 \cdot 24$**:** Dann ist $p-1 = 1$ und $q-1 = 24$, also $p = 2$ und $q = 25$. Da 25 keine Primzahl ist, kommt diese Möglichkeit nicht in Betracht.

$24 = 2 \cdot 12$**:** Dann ist $p-1 = 2$ und $q-1 = 12$, also $p = 3$ und $q = 13$. Damit wäre $n = 39$ möglich.

$24 = 3 \cdot 8$**:** Dann ist $p-1 = 3$ und $q-1 = 8$, also $p = 4$ und $q = 9$. Da 4 und 9 keine Primzahlen sind, kommt diese Möglichkeit nicht in Betracht.

$24 = 4 \cdot 6$**:** Dann ist $p-1 = 4$ und $q-1 = 6$, also $p = 5$ und $q = 7$. Damit wäre $n = 35$ möglich.

Da sich ab hier die Faktorisierungen wiederholen, gibt es also zwei Möglichkeiten, nämlich $n = 39 = 3 \cdot 13$ und $n = 35 = 5 \cdot 7$.

(b) Da für beide n's gilt $\varphi(n) = 24$, ist auch der geheime Schlüssel d für beide gleich. Gesucht ist ein $d \in \mathbb{N}$ mit $ed \equiv 5d \equiv 1(\mathrm{mod} 24)$. Mit bloßem Auge sehen wir, dass $d = 5$ diese Eigenschaft besitzt. Um den Klartext zu bekommen, muss also 3^5 mod n gebildet werden. Es ist

$$3^5 \equiv 3^4 \cdot 3 \equiv 81 \cdot 3 \equiv 3 \cdot 3 \equiv 9(\mathrm{mod} 39),$$

also ist für $n = 39$ der Klartext 9. Weiter ist

$$3^5 \equiv 3^4 \cdot 3 \equiv 81 \cdot 3 \equiv 11 \cdot 3 \equiv 33 (\mathrm{mod} 35),$$

also ist für $n = 35$ der Klartext 33.

Aufgabe 7

Sei R ein kommutativer Ring. Sei $a \in R$ nilpotent und sei P ein Primideal in R.

Behauptung: Es gilt $a \in P$.

Beweis: Sei $n \in \mathbb{N}$ mit $a^n = 0$. Dann gilt $a^n = 0 \in P$, denn P ist bezgl. $+$ eine Untergruppe von R. Wir zeigen nun mit Induktion nach n, dass aus $a^n \in P$ schon $a \in P$ folgt.

Sei also $n = 1$. Dann gilt $a \in P$, und wir sind fertig. Nehmen wir nun an, dass $n \geq 1$ gilt und aus $a^n \in P$ schon $a \in P$ folgt. Wenn dann $a^{n+1} \in P$ gilt, dann ist also $a \cdot a^n \in P$, und weil P ein Primideal ist, folgt, dass entweder $a \in P$ oder $a^n \in P$ gilt. Ist $a \in P$, sind wir fertig. Ist $a^n \in P$, folgt $a \in P$ mit der Induktionsannahme. □

Aufgabe 8

(a) Ein Algorithmus ist effizient, wenn es ein $n_0 \in \mathbb{N}$ und ein Polynom f gibt, so dass die Anzahl der Schritte, die der Algorithmus bei einer Eingabe der Länge $n \geq n_0$ benötigt, höchstens $f(n)$ ist.

(b) Die Eingabegrößen der Werte b, n und m sind (in Binärdarstellung) $\log b$, $\log n$ und $\log m$. Multipliziert man b aber n-Mal mit sich selbst, dann sind das $n - 1$ Multiplikationen, und es gibt kein Polynom f und kein $n_0 \in \mathbb{N}$, so dass $n - 1 \leq f(\log n)$ für alle $n \geq n_0$ gilt.