Mathematische Grundlagen der Kryptografie (1321)SoSe 05

Nachklausur am 1.10.2005:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe I.1

Das Wort GAUSS verschlüsselt mit

(a) dem Permutationskryptosystem und dem Schlüsselwort HAGEN und dem Schlüsselbuchstaben L ergibt VPIDD.

(b) dem Hill-Kryptosystem und dem Schlüssel $\begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 4 \\ 0 & 1 & 1 \end{pmatrix}$ wird zu GAUKHP (dabei wurde GAUSS hinten mit einem X aufgefüllt, also GAUSSX verschlüsselt).

(c) dem Vigenère-Kryptosystem und dem Schlüssel ROT ergibt XONJG.

zu Aufgabe I.2

(a) Die zyklische Gruppe $\mathbb{F}_{11}^{\times}$ besitzt 4 Elemente der Ordnung 5.

(b) Die Gruppe $\{4, 5, 9, 3, 1\}$ ist die Untergruppe von $\mathbb{F}_{11}^{\times}$ mit 5 Elementen.

zu Aufgabe I.3

Sei $G = S_3$ und $S = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$. Dann ist S kein Normalteiler von G.

zu Aufgabe I.4

Das diskreter-Logarithmus-Problem für elliptische Kurven: Gegeben seien eine elliptische Kurve $E(a, b, \mathsf{IK})$ und ein Punkt $P \in E(a, b, \mathsf{IK})$. Sei Q ein Vielfaches von P. Finde den diskreten Logarithmus von Q zur Basis P, das heißt, eine Zahl $x \in \mathbb{Z}$ mit $Q = xP$.

zu Aufgabe I.5

Der Wert $2^{200} \bmod p$ lässt sich mit 9 Multiplikationen in $\mathbb{F}_p$ berechnen (nämlich 7 Multiplikationen, um $2^2 \bmod p$, $2^4 \bmod p$, $2^8 \bmod p$, $2^{16} \bmod p$, $2^{32} \bmod p$, $2^{64} \bmod p$ und $2^{128} \bmod p$ zu berechnen, und dann noch einmal 2 Multiplikationen, um $2^{200} \bmod p = 2^{128} \cdot 2^{64} \cdot 2^8 \bmod p$ zu berechnen).

zu Aufgabe II.1

Sei p eine ungerade Primzahl und g ein primitives Element in $\mathbb{F}_p$.

(a) **Behauptung** Gilt $p \equiv 1(\text{mod}4)$, dann ist auch $(-g)$ ein primitives Element in $\mathbb{F}_p$.

Beweis Sei $p = 4k + 1$ mit $k \in \mathbb{N}$. Angenommen, $-g$ ist kein primitives Element in $\mathbb{F}_p$. Dann existiert also ein $x \in \mathbb{N}$ mit $(-g)^x = 1$ in $\mathbb{F}_p$ und $x < p - 1$. Mit dem Satz von Lagrange gilt $x \mid p - 1 = 4k$. Ist x gerade, dann gilt $(-g)^x = g^x = 1$, ein Widerspruch dazu, dass g ein erzeugendes Element von $\mathbb{F}_p^\times$ ist. Ist x ungerade, dann ist x ein echter Teiler von k, also ist $2x < p - 1$ und $1 = (-g)^{2x} = g^{2x}$, ebenfalls ein Widerspruch dazu, dass g ein primitives Element ist. □

(b) Für $p = 3$ ist 2 ein primitives Element in $\mathbb{F}_p$, aber $-2 = 1$ ist kein primitives Element in $\mathbb{F}_3$.

zu Aufgabe II.2

Behauptung Die Menge $\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ ist mit der Matrizenaddition und -multiplikation ein Integritätsbereich.

Beweis Wir zeigen zunächst, dass $R = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ ein Ring ist: Da $R \subseteq \mathrm{M}_{22}(\mathbb{Z})$ gilt, reicht es zu zeigen, dass $(R, +)$ eine Untergruppe von $\mathrm{M}_{22}(\mathbb{Z})$ ist. Dazu benutzen wir das Untergruppenkriterium. Zunächst einmal ist R nicht leer. Seien weiter $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R$. Dann ist $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} - \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & -b+d \\ b-d & a-c \end{pmatrix} = \begin{pmatrix} a-c & -(b-d) \\ b-d & a-c \end{pmatrix} \in R$, also ist $(R, +)$ eine Untergruppe von $\mathrm{M}_{22}(\mathbb{Z})$.

Seien nun $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R$. Dann ist $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix} \in R$, also ist die Matrizenmultiplikation eine Verknüpfung in R. Weiter ist $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$ und die Matrizenmultiplikation ist assoziativ, also ist $(R, \cdot)$ eine Halbgruppe mit Einselement. Da die Distributivgesetze in ganz $\mathrm{M}_{22}(\mathbb{Z})$ erfüllt sind, gelten sie auch in R, das heißt, R ist ein Ring.

R ist kommutativ, denn $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ für alle $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R$. Es ist also nur noch zu zeigen, dass R nullteilerfrei ist. Seien also $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R$ mit $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Dann gilt also $ac-bd = 0$ und $ad+bc = 0$. Angenommen, es gilt $a = 0$. Dann gilt entweder $b = 0$, also $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ oder $c = d = 0$, also $\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Ist $a \neq 0$, dann folgt aus der ersten Gleichung $c = \frac{bd}{a}$ und damit $ad + b\frac{bd}{a} = ad + \frac{b^2d}{a} = 0$. Es folgt $a^2d + b^2d = (a^2+b^2)d = 0$. Da $a \neq 0$ gilt, ist auch $a^2 + b^2 \neq 0$, und damit ist dann $d = 0$. Wegen $c = \frac{bd}{a}$, folgt dann auch $c = 0$, also $\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Damit ist R ein nullteilerfreier, kommutativer Ring und damit ein Integritätsbereich. □

zu Aufgabe II.3

Sei $\mathbb{F}_{27} = \mathbb{F}_3[T]/(T^3 + 2T + 1)$. Sei $[T] = T \bmod (T^3 + 2T + 1)$.

Behauptung Das Minimalpolynom von $[T]^2$ ist $T^3 + T^2 + T + 2$.

Beweis Da $[\mathbb{F}_{27} : \mathbb{F}_3] = 3$ und $[T]^2 \in \mathbb{F}_{27}$ gilt, ist der Grad des Minimalpolynoms von $[T]^2$ über $\mathbb{F}_3$ ein Teiler von 3, also 1 oder 3. Da $[T]^2 \notin \mathbb{F}_3$ gilt, wissen wir schon, dass der Grad des Minimalpolynoms 3 sein muss.

Weiter ist $([T]^2)^2 = [T]^4 = [T][T]^3 = [T][T+2] = [T]^2 + 2[T]$. Dabei gilt $[T^3 + 2T + 1] = [T]^3 + 2[T] + 1 = [0]$, also $[T]^3 = [T] + 2 = [T+2]$. Nun ist $([T]^2)^3 = [T]^6 =$

$([T]^3)^2 = ([T]+2)^2 = [T^2]+[T]+1$. Also ist

$$\begin{aligned}([T]^2)^0 &= 1\\ ([T]^2)^1 &= [T]^2\\ ([T]^2)^2 &= [T]^2+2[T]\\ ([T]^2)^3 &= [T]^2+[T]+1.\end{aligned}$$

Also folgt $([T]^2)^3+([T]^2)^2+[T]^2+2=0$, das heißt, $[T]^2$ ist Nullstelle des Polynoms $T^3+T^2+T+2 \in \mathbb{F}_3[T]$. Dieses Polynom ist dann auch das Minimalpolynom von $[T]^2$. □

zu Aufgabe II.4

Sei (m,e) ein öffentlicher RSA-Schlüssel. Sei $n \in \mathbb{Z}/m\mathbb{Z}$ mit $\mathrm{ggT}(n,m)=1$ ein Klartext und und sei $c = n^e \bmod m$ der zugehörige Schlüsseltext.

(a) **Behauptung** Es gibt ein $k \geq 1$ mit $n^{(e^k)} \equiv n(\mathrm{mod} m)$.

Beweis Es gilt $n \in \mathbb{Z}/m\mathbb{Z}$ und $\mathrm{ggT}(n,m)=1$, also $n \in (\mathbb{Z}/m\mathbb{Z})^\times$ und $n^{\varphi(m)} \equiv 1(\bmod m)$. Weiter gilt $\mathrm{ggT}(\varphi(m),e)=1$. Es ist also $e \in (\mathbb{Z}/\varphi(m)\mathbb{Z})^\times$. Sei k die Ordnung von e in $(\mathbb{Z}/\varphi(m)\mathbb{Z})^\times$, dann gilt $e^k \equiv 1(\bmod \varphi(m))$. Es gibt also ein $x \in \mathbb{Z}$ mit $e^k = 1+x\varphi(m)$. Dann ist

$$n^{(e^k)} \equiv n^{1+x\varphi(m)} \equiv n \cdot (n^{\varphi(m)})^x \equiv n \cdot 1^x \equiv n(\mathrm{mod} m).$$

□

(b) **Behauptung** Für das k aus Teil (a) gilt $c^{(e^{k-1})} \equiv n(\mathrm{mod} m)$.

Beweis Mit dem k aus Teil (a) gilt $c = n^e \bmod m$ und $n^{e^k} \equiv n(\mathrm{mod} m)$, also $n \equiv n^{e^k} \equiv (n^e)^{e^{k-1}} \equiv c^{e^{k-1}}(\mathrm{mod} m)$. □

(c) Dies ist keine Bedrohung für RSA, weil man das k aus Teil (a) (wahrscheinlich) nur berechnen kann, wenn man $\varphi(m)$ kennt. Und dies ist Teil des privaten Schlüssels.

zu Aufgabe II.5

Bechreibung des Knapsack-Kryptosystems:

(a) Alice wählt eine superaufsteigende Folge $(a_0,\ldots,a_{n-1})$ und $m \in \mathbb{N}$ mit $m > \sum_{i=0}^{n-1} a_i$ und $a \in \mathbb{N}$ mit $\mathrm{ggT}(a,m)=1$. Sie berechnet $b \in \mathbb{Z}/m\mathbb{Z}$

mit $ab \bmod m = 1$. Der geheime Schlüssel ist dann $(a_0, \ldots, a_{n-1})$ zusammen mit a, b und m. Der öffentliche Schlüssel ist $(aa_0 \bmod m, \ldots, aa_{n-1} \bmod m) = (w_0, \ldots, w_{n-1})$.

(b) Nachrichten sind n-Bit Zahlen $(x_0, \ldots, x_{n-1})$. Bob bildet $s = \sum_{i=0}^{n-1} x_i w_i$ und schickt s an Alice.

(c) Alice entschlüsselt die Nachricht s, indem sie $bs \equiv \sum_{i=0}^{n-1} x_i a_i (\mathrm{mod} m)$ bildet und dieses Teilmengen-Summen-Problem löst.

(d) Die Vermutung, dass das Knapsack-Kryptosystem sicher ist, beruhte auf der Annahme, dass ein Teilmengen-Summen-Problem gelöst werden muss, um das Knapsack-Kryptosystem zu brechen.

(e) Das Knapsack-Kryptosystem wurde gebrochen, indem in einem bestimmten, zum Kryptosystem gehörenden Gitter mit dem LLL-Algorithmus eine reduzierte Basis gesucht wurde. Aus dem ersten Vektor dieser Basis kann mit großer Wahrscheinlichkeit eine Lösung des zum Kryptosystem gehörenden Teilmengen-Summen-Problems abgelesen werden.

zu Aufgabe II.6

Sei p eine Primzahl mit $p \equiv 1(\mathrm{mod}4)$. Es gelte $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ und a ist ungerade.

Behauptung $(\frac{a}{p}) = 1$.

Beweis Da $p \equiv 1(\mathrm{mod}4)$ gilt und a ungerade ist, ist $(\frac{a}{p}) = (\frac{p}{a})$. Weiter ist $(\frac{p}{a}) = (\frac{p \bmod a}{a}) = (\frac{b^2}{a}) = (\frac{b}{a})^2 = 1$. □