Mathematische Grundlagen der Kryptografie (01321) SS 08

Klausur am 27.09.2008:

Musterlösungen

Aufgabe 1

(a) Das numerische Äquivalent zum Wort R H E I N ist $[17, 7, 4, 8, 13]$. Nun muss zu jeder Zahl der Schlüssel 5 in $\mathbb{Z}/26\mathbb{Z}$ addiert werden. Dies ergibt $[22, 12, 9, 13, 18]$, also W M J N S.

(b) Wenn im Permutations-Kryptosystem das Schlüsselwort N E B E N F L U S S verwendet wird, dann müssen zunächst die doppelten Buchstaben gestrichen werden. Dies ergibt N E B F L U S. Dieses Wort wird nun, beginnend beim Schlüsselbuchstaben R unter das Alphabet geschrieben und dann in alphabetischer Reihenfolge aufgefüllt. Dies ergibt

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

R	S	T	U	V	W	X	Y	Z
N	E	B	F	l	U	S	A	C

Damit wird der Geheimtext V D P W zu M A I N entschlüsselt.

(c) Das numerische Äquivalent zum Wort D O N A U ist $[3, 14, 13, 0, 20]$, das zum Wort K A N A L ist $[10, 0, 13, 0, 11]$. Da beide Wörter die selbe Länge haben, kann einfach komponentenweise in $\mathbb{Z}/26\mathbb{Z}$ addiert werden. Es ergibt sich also $[13, 14, 0, 0, 5]$ oder N O A A F.

(d) Das numerische Äquivalent zu L P M F ist $[11, 15, 12, 5]$. Wenn der Schlüssel beim Selbstschlüssel-Kryptosystem 7 ist, dann muss dieser vom ersten Element in $\mathbb{Z}/26\mathbb{Z}$ subtrahiert werden. Dies ergibt 4. Diese 4 wird nun vom zweiten Element subtrahiert, also 11. Das nächste Element ist dann $12-11=1$ und das letzte $5-1=4$. Insgesamt ergibt sich $[4, 11, 1, 4]$ oder E L B E.

(e) Das numerische Äquivalent zu O D E R ist $[14, 3, 4, 17]$. Also wird der Klartext verschlüsselt zu

$$\begin{pmatrix} 14 & 3 \\ 4 & 17 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 17 & 20 \\ 21 & 12 \end{pmatrix}$$

oder R U V M.

Aufgabe 2

(a) Ein Beispiel für einen Ring der Charakteristik 5, der kein Körper ist, ist $\mathbb{F}_5[T]$.

(b) Ein Element aus $\mathbb{C}$, dessen Minimalpolynom über $\mathbb{Q}$ den Grad 3 hat, ist $\sqrt[3]{2}$.

(c) $\mathbb{Z}$ ist eine unendliche abelsche Gruppe.

(d) $Gl_2(\mathbb{R})$, der Ring der invertierbaren 2×2-Matrizen über $\mathbb{R}$ ist eine unendliche Gruppe, die nicht abelsch ist.

(e) Die Carmichael-Zahl 561 ist eine Pseudoprimzahl zur Basis 2.

Aufgabe 3

(a) Es gilt $|(\mathbb{Z}/7\mathbb{Z})^\times| = \varphi(7) = 7 - 1 = 6 = \varphi(9) = |(\mathbb{Z}/9\mathbb{Z})^\times|$ und $|(\mathbb{Z}/5\mathbb{Z})^\times| = \varphi(5) = 4 = \varphi(8) = |(\mathbb{Z}/8\mathbb{Z})^\times|$.

(b) Beide Gruppen sind zyklisch, und zwar gilt $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3\rangle$ und $(\mathbb{Z}/9\mathbb{Z})^\times = \langle 2\rangle$. Da die Gruppen zyklisch sind und die gleiche Ordnung haben, sind sie isomorph. Ein Isomorphismus wäre zum Beispiel, die erzeugenden Elemente aufeinander abzubilden. Das ergibt dann $f : (\mathbb{Z}/7\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/9\mathbb{Z})^\times$ mit $3 \mapsto 2$ (und entsprechend $3^2 = 2 \mapsto 2^2 = 4$, $3^3 = 6 \mapsto 2^3 = 8$, $3^4 = 4 \mapsto 2^4 = 7$, $3^5 = 5 \mapsto 2^5 = 5$ und $3^6 = 1 \mapsto 2^6 = 1$).

(c) Die Gruppe $(\mathbb{Z}/5\mathbb{Z})^\times$ ist zyklisch. In $(\mathbb{Z}/8\mathbb{Z})^\times$ gilt jedoch $1^2 = 3^2 = 5^2 = 7^2 = 1$. Da die Gruppe die Ordnung 4 hat, jedes Element jedoch nur die Ordnung 2, kann die Gruppe nicht zyklisch sein. Damit können $(\mathbb{Z}/5\mathbb{Z})^\times$ und $(\mathbb{Z}/8\mathbb{Z})^\times$ nicht isomorph sein.

Aufgabe 4

Sei R ein Ring und $a \in R$. Dann heißt a **Idempotent**, wenn $a^2 = a$ gilt.

(a) **Behauptung:** In einem Integritätsbereich sind 0 und 1 die einzigen Idempotente.

Beweis: Sei I ein Integritätsbereich und $a \in I$ ein Idempotent. Dann gilt $a^2 = a$, also $a^2 - a = a(a - 1) = 0$. In einem Integritätsbereich ist das Produkt von zwei Elementen nur dann 0, wenn einer der Faktoren 0 ist. Es folgt also $a = 0$ oder $a - 1 = 0$, das heißt, $a = 1$. □

(b) In $\mathbb{Z}/6\mathbb{Z}$ ist $4 \cdot 4 = 16 = 4$, also ist 4 ein Idempotent.

Aufgabe 5

Es sei (m, e) ein Schlüssel für das RSA-Kryptosystem. Weiter sei $s > 1$ mit $e^s \equiv 1 \pmod{\varphi(m)}$. Sei $x \in \mathbb{Z}/m\mathbb{Z}$ ein Klartext, und sei $y \in \mathbb{Z}/m\mathbb{Z}$ der zugehörige Geheimtext.

Behauptung: Es gilt $y^{e^{s-1}} = x$ in $\mathbb{Z}/m\mathbb{Z}$.

Beweis: In $\mathbb{Z}/m\mathbb{Z}$ ist $y = x^e$, also ist $y^{e^{s-1}} \equiv (x^e)^{e^{s-1}} \equiv x^{e^s} \pmod{m}$. Da $e^s \equiv 1 \pmod{\varphi(m)}$ gilt, gibt es ein $k \in \mathbb{Z}$ mit $e^s = 1 + k\varphi(m)$. Also ist $x^{e^s} = x^{1+k\varphi(m)} =$

$x \cdot (x^{\varphi(m)})^k \equiv x \cdot 1^k \equiv x \pmod{m}$, denn $x^{\varphi(m)} \equiv 1 \pmod{m}$ mit dem Satz von Euler. □

Aufgabe 6

Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$ mit $(\frac{a}{p}) = (\frac{b}{p}) = 1$.

Behauptung: Die Kongruenz $ax^2 \equiv b \pmod{p}$ besitzt eine Lösung.

Beweis: Da $(\frac{a}{p}) = 1$ gilt, ist $\mathrm{ggT}(a, p) = 1$, das heißt, a ist invertierbar modulo p. Es gibt also ein $c \in \mathbb{Z}$ mit $ac \equiv 1 \pmod{p}$. Für dieses c gilt damit ebenfalls $\mathrm{ggT}(c, p) = 1$. Die Kongruenz $ax^2 \equiv b \pmod{p}$ ist damit genau dann erfüllbar, wenn die Kongruenz $cax^2 \equiv cb \pmod{p}$, also $x^2 \equiv cb \pmod{p}$ erfüllbar ist. Dies ist genau dann der Fall, wenn cb ein quadratischer Rest modulo p ist, wenn also $(\frac{cb}{p}) = 1$ gilt.

Es ist

$$\begin{aligned}
(\frac{cb}{p}) &= (\frac{c}{p})(\frac{b}{p}) = (\frac{c}{p}), \text{ denn } (\frac{b}{p}) = 1 \\
&= (\frac{c}{p})(\frac{a}{p}), \text{ denn } (\frac{a}{p}) = 1 \\
&= (\frac{ca}{p}) = (\frac{1}{p}), \text{ denn } ca \equiv 1 \pmod{p} \\
&= 1.
\end{aligned}$$

Also ist cb ein quadratischer Rest modulo p, und die Kongruenz besitzt eine Lösung. □

Aufgabe 7

Alice und Bob möchten mit dem Diffie-Hellman-System einen gemeinsamen Schlüssel vereinbaren. Sie wählen sich als endlichen Körper $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$ und als erzeugendes Element $g = [T+1] = T+1 \pmod{T^3+T+1}$. Alice wählt $e_A = 3$ und Bob wählt $e_B = 4$.

(a) Alice muss g^{e_A}, also $[T+1]^3$ berechnen. Es ist $[T+1]^3 = [T^3 + 3T^2 + 3T + 1] = [T^3 + T^2 + T + 1] = [T^2]$, denn $[T^3 + T + 1] = 0$. Das heißt, Alice schickt $[T^2]$ an Bob.

(b) Bob berechnet $g^{e_B} = [T+1]^4$. Aus (a) wissen wir, dass $[T+1]^3 = [T^2]$ gilt. Also ist $[T+1]^4 = [T^2][T+1] = [T^3 + T^2] = [T^2 + T + 1]$, denn in $\mathbb{F}_2[T]/(T^3 + T + 1)$ ist $[T^3] = [T+1]$. Also schickt Bob $[T^2 + T + 1]$ an Alice.

(c) Der geheime Schlüssel ist $g^{e_A e_B} = [T+1]^{12}$. Da $a^8 = a$ für jedes Element $a \in \mathbb{F}_8$ gilt, folgt $[T+1]^{12} = [T+1]^8[T+1]^4 = [T+1][T+1]^4 = [T+1]^5$. Mit (b) gilt $[T+1]^4 = [T^2+T+1]$. Also folgt $[T+1]^5 = [T+1][T^2+T+1] = [T^3+2T^2+2T+1] = [T^3+1] = [T]$, denn $[T^3] = [T+1]$ in $\mathbb{F}_2[T]/(T^3+T+1)$. Damit ist $[T]$ der geheime Schlüssel.

Aufgabe 8

Sei $q = p^n$ eine Primzahlpotenz, und sei $f \in \mathbb{F}_q[T]$ mit $\text{Grad}(f) = m \geq 1$.

Behauptung: f besitzt genau dann m verschiedene Nullstellen in $\mathbb{F}_q$, wenn f ein Teiler des Polynoms $T^q - T \in \mathbb{F}_q[T]$ ist.

Beweis: Wie wir im Kurs gezeigt haben, gilt $T^q - T = \prod_{a \in \mathbb{F}_q} (T - a)$.

Angenommen, f besitzt genau m verschiedene Nullstellen in $\mathbb{F}_q$. Dann zerfällt f also in $f = a \prod_{i=1}^{m} (T - a_i)$, wobei die a_i aus $\mathbb{F}_q$ und alle verschieden sind. Außerdem ist $a \neq 0$. Damit ist also f ein Teiler von $T^q - T$.

Ist f ein Teiler von $T^q - T$, dann gilt $f \mid \prod_{a \in \mathbb{F}_q} (T - a)$, das heißt, f zerfällt über $\mathbb{F}_q$ in ein Produkt von m verschiedenen Linearfaktoren. Damit hat f also m verschiedene Nullstellen in $\mathbb{F}_q$. □

Aufgabe 9

(a) Dem Knapsack-Kryptosystem liegt zugrunde, dass das Teilmengen-Summen-Problem vermutlich schwer zu lösen ist. Bei diesem Problem sind $a_1, \ldots, a_n, s \in \mathbb{N}$ gegeben, und das Problem ist, zu entscheiden, ob es $x_1, \ldots, x_n \in \{0, 1\}$ gibt, so dass $\sum_{i=1}^{n} x_i a_i = s$ gilt.

(b) Der geheime Schlüssel ist eine superaufsteigende Folge $(a_1, \ldots, a_n)$, ein $m \in \mathbb{N}$ mit $m > \sum_{i=1}^{n} a_i$, ein $a \in \mathbb{N}$ mit $\text{ggT}(a, m) = 1$ und ein $b \in \mathbb{N}$ mit $ab \equiv 1 \bmod m$.

(c) Der öffentliche Schlüssel ist eine Folge $(w_1, \ldots, w_n)$. Diese wird berechnet durch $w_i = aa_i \bmod m$ für alle $1 \leq i \leq n$.

(d) Die Klartexte sind $0-1$-Folgen $(x_1, \ldots, x_n)$ der Länge n. Verschlüsselt werden sie zu $\sum_{i=1}^{n} x_i w_i = s$.

(e) Um das Kryptosystem zu brechen, wird der LLL-Algorithmus benutzt. Er hat als Eingabe die Basis eines Gitters über $\mathbb{Q}^n$ und als Ausgabe eine reduzierte Basis des Gitters.