Mathematische Grundlagen der Kryptografie (1321) SoSe 04

Klausur am 21.08.2004:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe 1

Zunächst streichen wir doppelte Buchstaben im Wort Klausur und erhalten KLAUSR. Diese Buchstabenfolge wird beim Schlüsselbuchstaben J beginnend unter das Klartextalphabet geschrieben. Anschliessend werden die restlichen Buchstaben in der normalen Reihenfolge angeschlossen, wobei die Buchstaben aus dem Schlüsselwort ausgelassen werden. Dies ergibt

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

Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	M	N.

Nun ergibt sich, dass der Geheimtextbuchstabe F dem Klartextbuchstaben T entspricht, der Geheimtextbuchstabe R dem Klartextbuchstaben O entspricht und der Geheimtextbuchstabe Z dem Klartextbuchstaben I entspricht. Der Klartext lautet also TOITOITOI.

zu Aufgabe 2

In $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ gilt $\alpha^2 = \alpha + 1$, $\alpha(\alpha+1) = 1$ und $(\alpha+1)^2 = \alpha$. Weiter gilt

$$E(1, \alpha, \mathbb{F}_4) = \{(x, y) \mid y^2 + xy = x^3 + x^2 + \alpha\} \cup \{\mathcal{O}\}.$$

Wir probieren nun für jedes $x \in \mathbb{F}_4$ aus, ob es ein $y \in \mathbb{F}_4$ gibt mit $(x, y) \in E(1, \alpha, \mathbb{F}_4)$.

$x = 0$**:** Es folgt $y^2 = \alpha$. Wegen $0^2 = 0$, $1^2 = 1$, $\alpha^2 = \alpha + 1$ und $(\alpha+1)^2 = \alpha$ folgt $y = \alpha + 1$.

$x = 1$**:** Es folgt $y^2 + y = \alpha$. Wegen $0^2+0 = 0$, $1^2+1 = 0$, $\alpha^2+\alpha = 1$ und $(\alpha+1)^2+\alpha+1 = 1$ gibt es kein $y \in \mathbb{F}_4$ mit $(1, y) \in E(1, \alpha, \mathbb{F}_4)$.

$x = \alpha$**:** Es folgt $y^2 + \alpha y = 0$, also $y(y + \alpha) = 0$, das heißt, $y = 0$ oder $y = \alpha$.

$x = \alpha + 1$**:** Es folgt $y^2 + (\alpha + 1)y = 1$. Wegen $0^2 + (\alpha + 1)0 = 0$, $1^2 + (\alpha + 1)1 = \alpha$, $\alpha^2 + (\alpha+1)\alpha = \alpha$ und $(\alpha+1)^2 + (\alpha+1)^2 = 0$ gibt es kein $y \in \mathbb{F}_4$ mit $(\alpha+1, y) \in E(1, \alpha, \mathbb{F}_4)$.

Es gilt also $E(1, \alpha, \mathbb{F}_4) = \{(0, \alpha + 1), (\alpha, 0), (\alpha, \alpha), \mathcal{O}\}$.

zu Aufgabe 3

Dass n eine Eulersche Pseudoprimzahl zur Basis b ist, bedeutet, dass $b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\text{mod } n)$ gilt. Ist also $(\frac{b}{n}) = -1$, dann ist $b^{\frac{n-1}{2}} \equiv -1(\text{mod}n)$ und damit auch $b^{n-1} \equiv 1(\text{mod } n)$. Für $n - 1 = 2^r s$, wobei s ungerade ist, gilt also $b^{2^{r-1}s} \equiv b^{\frac{n-1}{2}} \equiv -1(\text{mod}n)$ und $b^{2^r s} \equiv b^{n-1} \equiv 1(\text{mod}n)$. Also ist n nach Definition eine starke Pseudoprimzahl zur Basis b. □

zu Aufgabe 4

(a) Der öffentliche Schlüssel beim RSA-Kryptosystem ist ein Paar (m, e), wobei m das Produkt von zwei verschiedenen Primzahlen ist, und e eine ganze Zahl mit der Eigenschaft $\text{ggT}(e, \varphi(m)) = 1$ ist.

(b) Der geheime Schlüssel besteht aus der Faktorisierung $m = pq$ in das Produkt von zwei Primzahlen und einer ganzen Zahl d mit $ed \equiv 1(\text{mod}\varphi(m))$.

(c) Möchte Bob eine Nachricht $N \in \mathbb{Z}/m\mathbb{Z}$ an Alice schicken, dann berechnet er $N^e \bmod m$ und schickt diese Zahl.

(d) Wenn Alice eine Nachricht M empfängt, dann berechet sie $M^d \bmod m$.

(e) Das RSA-Kryptosystem ist sicher, weil vermutet wird, dass man ganze Zahlen faktorisieren können muss, um das Kryptosystem brechen zu können. Weiter wird vermutet, dass es keinen effizienten Algorithmus gibt, um ganze Zahlen zu faktorisieren.

(f) Das RSA-Kryptosystem ist ein effizientes Verfahren, weil die beiden Primzahlen p und q, die zur Schlüsselerzeugung benötigt werden, mit einem effizienten Primzahltest gefunden werden können. Diese beiden Zahlen müssen dann multipliziert werden, was ebenfalls effizient möglich ist. Anschließend wird $\varphi(m) = (p-1)(q-1)$ berechnet, und auch das ist effizient möglich. Die Zahl e wird zufällig gewählt, und dann wird mit dem Euklidischen Algorithmus überprüft, ob $\text{ggT}(e, \varphi(m)) = 1$

gilt. Die Zahl d wird mit dem erweiterten Euklidischen Algorithmus berechnet. Sowohl der Euklidische Algorithmus als auch der erweiterte Euklidische Algorithmus sind effiziente Algorithmen. Das Chiffrieren und Dechiffrieren sind dann nur noch Potenzieren in $\mathbb{Z}/m\mathbb{Z}$, und das ist mit Wiederholtem Quadrieren effizient möglich.

zu Aufgabe 5

Ist a ein quadratischer Rest, dann gibt es ein $b \in \mathbb{F}_p^\times$ mit $b^2 = a$ in $\mathbb{F}_p$. Angenommen, a ist ein primitives Element von $\mathbb{F}_p^\times$. Dann gibt es ein $n \in \mathbb{N}$ mit $1 \leq n \leq p-1$ und $a^n = b$ in $\mathbb{F}_p$. Damit folgt $a = b^2 = a^{2n}$ in $\mathbb{F}_p$ oder $a^{2n-1} = 1$. Da a nach Annahme ein primitives Element ist, ist die Ordnung von a gerade gleich der Ordnung der Gruppe $(\mathbb{F}_p^\times, \cdot)$, also $p-1$. Es folgt also $p-1 \mid 2n-1$. Andererseits ist $n \leq p-1$, das heißt, $2n-1 \leq 2(p-1)-1 = 2p-3 < 2(p-1)$. Damit folgt $p-1 = 2n-1$ und $p = 2n$, ein Widerspruch zur Voraussetzung, dass p ungerade ist. □

zu Aufgabe 6

Um zu zeigen, dass M ein Unterkörper von IK ist, zeigen wir zunächst, dass $(M, +)$ eine Untergruppe von $(\mathsf{IK}, +)$ ist. Wir wenden das Untergruppenkriterium an: Seien $a, b \in M$, das heißt, $\sigma(a) = a$ und $\sigma(b) = b$. Dann ist $\sigma(a-b) = \sigma(a) - \sigma(b) = a - b$. Also folgt $a - b \in M$, und $(M, +)$ ist eine Untergruppe von $(\mathsf{IK}, +)$. Nun zeigen wir, ebenfalls mit dem Untergruppenkriterium, dass $(M\backslash\{0\}, \cdot)$ eine Untergruppe von $(\mathsf{IK}\backslash\{0\}, \cdot)$ ist. Dazu seien $a, b \in M\backslash\{0\}$. Wir zeigen nun zunächst, dass dann auch $b^{-1} \in M$ gilt. Da σ ein Körperautomorphismus ist, gilt nämlich $1 = \sigma(1) = \sigma(bb^{-1}) = \sigma(b)\sigma(b^{-1}) = b\sigma(b^{-1})$. Also folgt $\sigma(b^{-1}) = b^{-1}$ und $b^{-1} \in M$. Insgesamt gilt nun $\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = ab^{-1}$, also $ab^{-1} \in M\backslash\{0\}$. Da M eine Teilmenge des Körpers IK ist, gelten auch die Distributivgesetze in M, und damit ist M ein Körper. □

zu Aufgabe 7

Ein Punkt der Ordnung 2 auf einer elliptischen Kurve über $\mathbb{F}_4$ ist ein Punkt der Form $(0, y)$ mit $y \in \mathbb{F}_4$. Für einen solchen Punkt gilt nämlich $-(0, y) = (0, y + 0) = (0, y)$, also $2(0, y) = \mathcal{O}$.

Es ist $E(a, b, \mathbb{F}_4) = \{(x, y) \mid y^2 + xy = x^3 + ax^2 + b\} \cup \{\mathcal{O}\}$, also folgt aus $x = 0$, dass $y^2 = b$ gilt. Wegen $0^2 = 0$, $1^2 = 1$, $\alpha^2 = \alpha + 1$ und $(\alpha + 1)^2 = \alpha$ gibt es genau eine Lösung für die Gleichung $y^2 = b$, also genau einen Punkt der Ordnung 2.

Angenommen, $E(a, b, \mathbb{F}_4)$ ist nicht zyklisch. Dann ist diese Gruppe von der Form $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, wobei $n \mid m$ und $n \geq 2$ gilt. Dabei muss n ungerade sein, denn wenn n gerade wäre, wäre auch m gerade, und dann gäbe es ein Element der Ordnung zwei in $\mathbb{Z}/n\mathbb{Z}$ und ein Element der Ordnung 2 in $\mathbb{Z}/m\mathbb{Z}$, also mindestens zwei Elemente der Ordnung 2 in $E(a, b, \mathbb{F}_4)$. Also folgt, dass $n \geq 3$ und ungerade ist. Außerdem ist m gerade, denn es gibt ein Element der Ordnung 2. Wegen $n \mid m$ folgt $m \geq 2n \geq 6$. Sei N die Anzahl der Punkte von $E(a, b, \mathbb{F}_4)$, dann ist also $N = nm \geq 18$. Andererseits ist mit dem Satz von Hasse

$$|N - 5| \leq 2\sqrt{4} = 4,$$

also $N \leq 9$, ein Widerspruch. Es folgt, dass $E(a, b, \mathbb{F}_4)$ zyklisch ist. □

zu Aufgabe 8

Sei $r \in R$, $r \neq 0$. Zu zeigen ist, dass r invertierbar ist. Da $r \neq 0$ gilt, ist $\{0\} \subsetneq (r)$, wobei $(r) = \{sr \mid s \in R\}$ das von r erzeugte Ideal bezeichnet.

Behauptung Für alle $i \in \mathbb{N}$ gilt $\{0\} \subsetneq (r^{i+1}) \subseteq (r^i)$.

Beweis Da R ein Integritätsbereich ist, ist $r^{i+1} \neq 0$ für alle $i \geq 1$, also gilt $(r^{i+1}) \neq \{0\}$. Außerdem ist $r^{i+1} = rr^i \in (r^i)$, also ist $(r^{i+1}) \subseteq (r^i)$ für alle $i \geq 1$. □

Es gibt in R also eine Kette von Idealen $\{0\} \subsetneq \ldots (r^{i+1}) \subseteq (r^i) \subseteq \ldots \subseteq (r^3) \subseteq (r^2) \subseteq (r)$. Da es in R nach Voraussetzung aber nur endlich viele Ideale gibt, muss es ein $i \geq 1$ geben mit $(r^{i+1}) = (r^i)$. Es gibt also ein $s \in R$ mit $sr^{i+1} = r^i$, das heißt, $(sr - 1)r^i = 0$. Da R ein Integritätsbereich ist, folgt $r^i = 0$ oder $sr - 1 = 0$. Da $r \neq 0$ ist, ist auch $r^i \neq 0$, denn R ist ein Integritätsbereich, also folgt $sr - 1 = 0$ oder $sr = 1$. Also ist r invertierbar. □