Mathematische Grundlagen der Kryptografie (1321) SS07

Klausur am 18.08.2007:

Aufgabenstellungen

Aufgabe 1

Verschlüsseln Sie

(a) das Wort F E R M A T mit dem Verschiebekryptosystem und dem Schlüssel K=(erste Ziffer Ihrer Matrikelnummer).

(b) das Wort E U L E R mit dem Permutationskryptosystem und dem Schlüsselwort = (Ihr Nachname) und dem Schlüssel = (erster Buchstabe Ihres Vornamens).

(c) das Wort R A B I N M I L L E R mit dem Vigenère-Kryptosystem und dem Schlüssel = (Ihr Vorname).

(d) das Wort S O L O V A Y mit dem Selbstschlüsselkryptosystem und dem Schlüssel K=(zweite Ziffer Ihrer Matrikelnummer).

(e) das Wort S T R A S S E N mit dem affinen Kryptosystem mit Schlüssel (a, b)=(dritte Ziffer Ihrer Matrikelnummer,vierte Ziffer Ihrer Matrikelnummer), wenn möglich. Wenn dies kein zulässiger Schlüssel ist, erhöhen Sie a solange um 1, bis Sie einen zulässigen Schlüssel erhalten.

(Hinweis: Die numerischen Äquivalente zu den Buchstaben finden Sie am Schluss der Klausur.)

[*2 + 2 + 2 + 2 + 2 = 10 Punkte*]

Aufgabe 2

(a) Führen Sie den Primzahltest von Fermat für $n = 21$ und $b = 2$ durch.

(b) Führen Sie den Primzahltest von Rabin-Miller für $n = 21$ und $b = 2$ durch.

(c) Führen Sie den Primzahltest von Solovay-Strassen für $n = 21$ und $b = 5$ durch.

[*3 + 3 + 4 = 10 Punkte*]

Aufgabe 3

Geben Sie jeweils ein Beispiel für

(a) ein Gitter im $\mathbb{R}^3$ mit Determinante 6, das die Vektoren $\begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}3\\3\\1\end{pmatrix}, \begin{pmatrix}6\\0\\0\end{pmatrix}$ enthält.

(b) eine Gruppe G und $n \in \mathbb{N}$ mit $\mathrm{ord}(g) \mid n$ für alle $g \in G$, aber $|G| \nmid n$.

(c) einen Ring R mit Primideal P, das kein maximales Ideal ist.

[*2 + 2 + 2 = 6 Punkte*]

Aufgabe 4

Geben Sie ein Beispiel für eine elliptische Kurve $E(a, b, \mathbb{F}_5)$, die mindestens einen Punkt der Ordnung 2 besitzt.

[*6 Punkte*]

Aufgabe 5

Bestimmen Sie die kleinste Zahl $\lambda \in \mathbb{N}$, so dass $n^\lambda \equiv 1 \pmod{100}$ für alle $n \in \mathbb{Z}$ mit $\mathrm{ggT}(n, 100) = 1$ gilt.

[*10 Punkte*]

Aufgabe 6

Sei $(G, \cdot)$ eine Gruppe. Zeigen Sie, dass G genau dann zyklisch ist, wenn es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \longrightarrow G$ gibt.

[*10 Punkte*]

Aufgabe 7

Welche Bedingung muss eine Primzahl $p \geq 3$ erfüllen, damit es ein $n \in \mathbb{N}$ gibt, so dass $p \mid n^2 + 1$ gilt?

[*8 Punkte*]

Aufgabe 8

Sei p eine Primzahl und $n \in \mathbb{N}$. Sei $G = \{f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} \mid f \text{ ist bijektiv}\}$. Dann ist G zusammen mit der Verknüpfung $\circ$ von Abbildungen eine Gruppe. Sei $\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ mit $\sigma(x) = x^p$ für alle $x \in \mathbb{F}_{p^n}$ der Frobenius-Automorphismus. Dann wissen wir schon, dass $\sigma \in G$ gilt.

Bestimmen Sie die Ordnung von σ in G.

[*8 Punkte*]

Aufgabe 9

Beschreiben Sie (jeweils kurz in 1-2 Sätzen) das Diffie-Hellman-Schlüsselaustauschverfahren über endlichen Körpern.

(a) Was ist der öffentliche Schlüssel?

(b) Woraus besteht Alice' geheimer Schlüssel, und welchen Wert schickt sie an Bob?

(c) Woraus besteht Bobs geheimer Schlüssel, und welchen Wert schickt er an Alice?

(d) Welches ist der gemeinsame Schlüssel, der mit dem Verfahren festgelegt wird?

(e) Warum ist das Verfahren sicher?

(f) Warum ist das Verfahren effizient?

$[2 + 2 + 2 + 2 + 2 + 2 = 12\ Punkte]$

Hinweis: Die Buchstaben A,..,Z entsprechen folgenden Elementen aus $\mathbb{Z}/26\mathbb{Z}$:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25