Mathematische Grundlagen der Kryptografie (01321) SoSe 09

Klausur am 29.08.2009:

Aufgabenstellungen

Aufgabe 1

(a) Verschlüsseln Sie das Wort O R A N G E mit dem Verschiebe-Kryptosystem und dem Schlüssel 17.

(b) Entschlüsseln Sie den Geheimtext R B S Q, der mit dem affinen Kryptosystem und dem Schlüssel $(21, 21)$ verschlüsselt wurde.

(c) Verschlüsseln Sie das Wort R O T mit dem Permutationskryptosystem, dem Schlüsselwort M A R I N E B L A U und dem Schlüsselbuchstaben P.

(d) Entschlüsseln Sie den Geheimtext N I D U, der mit dem Hill-Kryptosystem und dem Schlüssel $\begin{pmatrix} 5 & 16 \\ 11 & 5 \end{pmatrix}$ verschlüsselt wurde.

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

$[2 + 3 + 2 + 3 = 10 \ \textit{Punkte}]$

Aufgabe 2

Geben Sie jeweils ein Beispiel (ohne Begründung) für ein Kryptosystem aus dem Kurstext,

(a) dessen Sicherheit darauf beruht, dass es wahrscheinlich keine effizienten Faktorisierungsalgorithmen gibt.

(b) das auch über elliptischen Kurven verwendet werden kann.

(c) auf das man den Kasiski-Test anwenden kann, um es zu brechen.

(d) dessen Sicherheit bewiesen ist und nicht nur vermutet wird.

(e) bei dem der Sender dem Empfänger eine Nachricht schickt, die die doppelte Länge der eigentlichen Nachricht hat.

$[2 + 2 + 2 + 2 + 2 = 10 \ \textit{Punkte}]$

Aufgabe 3

Gibt es auf der elliptischen Kurve

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

einen Punkt mit x-Koordinate $\alpha + 1$? Dabei sei $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2 + T + 1)$ und $\alpha = T \bmod (T^2 + T + 1)$.

[*10 Punkte*]

Aufgabe 4

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

$$\mathrm{Aut}(G) = \{\phi : G \longrightarrow G \mid \phi \text{ ist ein bijektiver Gruppenhomomorphismus}\}.$$

Zeigen Sie, dass für alle $\phi, \psi \in \mathrm{Aut}(G)$ gilt: $\phi \circ \psi = \psi \circ \phi$. (Sie dürfen ohne Beweis verwenden, dass für alle $\phi \in \mathrm{Aut}(G)$, alle $g \in G$ und alle $z \in \mathbb{Z}$ gilt $\phi(g^z) = \phi(g)^z$.)

[*10 Punkte*]

Aufgabe 5

Sei $n \in \mathbb{N}$. Zeigen Sie: 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.

[*10 Punkte*]

Aufgabe 6

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

(a) Berechnen Sie alle möglichen Werte für n mit $\varphi(n) = 24$ und die Primzahlen p und q, so dass $n = pq$ gilt.

(b) Bestimmen Sie für alle Werte n aus Teil (a) und für den öffentlichen Schlüssel $e = 5$ den Klartext zum Geheimtext 3.

[*5 + 5 = 10 Punkte*]

Aufgabe 7

Sei R ein kommutativer Ring. Sei $a \in R$ nilpotent, das heißt, es gibt ein $n \in \mathbb{N}$ mit $a^n = 0$. Sei P ein Primideal in R. Zeigen Sie, dass $a \in P$ gilt.

[*10 Punkte*]

Aufgabe 8

Beantworten Sie kurz (in 1-2 Sätzen) die folgenden Fragen:

(a) Wann ist ein Algorithmus **effizient**?

(b) Seien $b, n, m \in \mathbb{N}$. Warum ist die Berechnung von $b^n \bmod m$ als $\underbrace{b \cdot b \cdots b}_{n \text{ Mal}} \bmod m$ nicht effizient?

[*5 + 5 = 10 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