Mathematische Grundlagen der Kryptografie (1321) SS 05

Nachklausur am 1.10.2005:

Aufgabenstellungen

I. Die Lösungen der folgenden fünf Aufgaben brauchen Sie nicht zu begründen.

Aufgabe I.1

Verschlüsseln Sie das Wort GAUSS mit

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

(b) dem Hill-Kryptosystem und dem Schlüssel $\begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 4 \\ 0 & 1 & 1 \end{pmatrix}$ (füllen Sie das Wort bei Bedarf mit X auf).

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

[2 + 2 + 2 = 6 Punkte]

Aufgabe I.2

(a) Wie viele Elemente der Ordnung 5 hat $\mathbb{F}_{11}^{\times}$?

(b) Welches ist die Untergruppe der Ordnung 5 von $\mathbb{F}_{11}^{\times}$?

[2 + 2 = 4 Punkte]

Aufgabe I.3

Geben Sie ein Beispiel für eine Gruppe G und eine Untergruppe S, die kein Normalteiler von G ist.

[4 Punkte]

Aufgabe I.4

Was ist das Diskreter-Logarithmus-Problem für elliptische Kurven?

[*4 Punkte*]

Aufgabe I.5

Sei p eine große Primzahl. Mit wie vielen Multiplikationen $\bmod p$ lässt sich $2^{200} \bmod p$ berechnen?

[*4 Punkte*]

II. Die Lösungen der folgenden sechs Aufgaben sollen begründet werden.

Aufgabe II.1

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

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

(b) Geben Sie ein Beispiel für eine Primzahl p und ein primitives Element g in $\mathbb{F}_p$, so dass $(-g)$ kein primitives Element in $\mathbb{F}_p$ ist.

[*6 + 4 = 10 Punkte*]

Aufgabe II.2

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

[*10 Punkte*]

Aufgabe II.3

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

[*10 Punkte*]

Aufgabe II.4

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

(a) Zeigen Sie: Es gibt ein $k \geq 1$ mit $n^{(e^k)} \equiv n(\text{mod}m)$.

(b) Zeigen Sie für das k aus Teil (a): $c^{(e^{k-1})} \equiv n(\text{mod}m)$.

(c) Ist dies eine Bedrohung für RSA?

[4 + 3 + 3 = 10 Punkte]

Aufgabe II.5

Beschreiben Sie das Knapsack-Kryptosystem:

(a) Wie erzeugt Alice den öffentlichen und den geheimen Schlüssel?

(b) Wie wird eine Nachricht verschlüsselt?

(c) Wie wird die Nachricht von Alice entschlüsselt?

(d) Auf welcher Vermutung beruhte die Annahme, dass das Knapsack-Kryptosystem sicher ist?

(e) Beschreiben Sie ganz kurz, wie das Knapsack-Kryptosystem gebrochen wurde.

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

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. Zeigen Sie: $(\frac{a}{p}) = 1$.

[8 Punkte]