WOLFGANG K. SEILER
Tel. 2515

A5, C201

26. Januar 2005

12. Übungsblatt Kryptologie

Aufgabe 1: *(4 Punkte)*

a) Zeigen Sie, daß 3 eine primitive Wurzel modulo der FERMAT-Primzahl $p = F_4 = 2^{16} + 1$ ist!

b) Lösen Sie die Gleichung $3^x \equiv 2005 \bmod p$ nach der Methode von POHLIG und HELLMAN!

c) Bestimmen Sie die Ordnung von $2005 \in \mathbb{F}_p^\times$!

Aufgabe 2: *(4 Punkte)*

a) Finden Sie die kleinste primitive Wurzel g modulo 431 !

b) Lösen Sie für diese die Gleichung $g^x \equiv 100 \bmod 431$ nach der Methode von POHLIG und HELLMAN!

Aufgabe 3: *(4 Punkte)*

Bestimmen Sie nach der *baby step – giant step* Methode eine Lösung der Gleichung $3^x \equiv 200 \bmod 257$!

Aufgabe 4: *(4 Punkte)*

$G = Gl_2(\mathbb{R})$ sei die Gruppe aller invertierbarer 2×2-Matrizen mit reellen Einträgen, und $M = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$. Bestimmen Sie intelligenter als durch systematisches Ausprobieren den diskreten Logarithmus der Matrix

$$A = \begin{pmatrix} 241674213589320374544014751382329 7 & 170889475266934512278141228363815 2 \\ 341778950533869024556282456727630 4 & 241674213589320374544014751382329 7 \end{pmatrix}$$

zur Basis M !

Hinweis: Die Matrizen A und M sind auch auf dem Maple *worksheet* `blatt12.mws` zu finden.

Aufgabe 5: *(4 Punkte)*

Finden Sie ohne Computer die kleinste vierstellige Primzahl p der Form $2q + 1$ mit einer Primzahl q !

Hinweis: Es reicht, wenn Sie mit den Primzahlen ≤ 20 sieben.

Abgabe bis zum Dienstag, dem 1. Februar 2005, um 12.00 Uhr