Wolfgang K. Seiler A5, C201
Tel. 2515

21. Dezember 2004

9. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)
Die n-te Fermat-Zahl ist $F_n = 2^{2^n} + 1$. Beweisen Sie, daß $F_4 = 65537$ eine Primzahl ist!
Hinweis: Zeigen Sie, daß 3 die multiplikative Gruppe modulo F_4 erzeugt!

Aufgabe 2: (*4 Punkte*)
Zerlegen Sie die Zahl 1 545 013 mit dem Fermatschen Verfahren in ein Produkt zweier Faktoren!

Aufgabe 3: (*5 Punkte*)
p sei eine Primzahl und $p \equiv 3 \bmod 4$.

a) Zeigen Sie: Falls die Gleichung $x^2 \equiv a \bmod p$ überhaupt eine Lösung hat, dann ist auch $x = a^{(p+1)/4}$ eine Lösung.

b) Welche anderen Lösungen gibt es?

c) Bestimmen Sie für $p = 2^{16} + 3$ die Lösungsmengen der Gleichungen

$$x^2 \equiv 2 \bmod p \quad \text{und} \quad x^2 \equiv 5 \bmod p\,!$$

Aufgabe 4: (*6 Punkte*)
Die fünfte Fermat-Zahl $F_5 = 2^{32} + 1$ soll nach dem quadratischen Sieb mit Hilfe des Polynoms

$$f(x) = (x + 2^{16})^2 - F_5$$

faktorisiert werden.

a) Geben Sie das Polynom in ausmultiplizierter Form explizit an!

b) Finden Sie alle $x \in \mathbb{Z}$, für die $f(x)$ durch 127 teilbar ist!

c) Zeigen Sie, daß $f(x)$ nie durch sieben teilbar ist!
Hinweis: Sie können das Ergebnis von Aufgabe 3*a)* verwenden.

IURKH ZHLKQ DFKWH QXQGD OOHVJ XWHIX HUGDV QHXHM DKU!

Abgabe bis zum Dienstag, dem 11. Januar 2005, um 12.00 Uhr