Wolfgang K. Seiler
Tel. 2515

A5, C201

7. November 2007

9. Übungsblatt Kryptologie

Aufgabe 1: (*4 Punkte*)
$p = 2^{16} + 1$ sei die vierte Fermat-Zahl.

a) Lösen Sie die Gleichung $3^x \equiv 2007 \bmod p$ nach der Methode von Pohlig und Hellman!

b) Bestimmen Sie die Ordnung von 2007 in der multiplikativen Gruppe modulo p !

Aufgabe 2: (*4 Punkte*)

a) Finden Sie die kleinste primitive Wurzel g modulo 131 !

b) Lösen Sie für diese die Gleichung $g^x \equiv 100 \bmod 131$!

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*)

a) Stellen Sie eine Tabelle der diskreten Logarithmen modulo 19 zur Basis zwei der Zahlen von 0 bis 18 zusammen!

b) Berechnen Sie mit Hilfe dieser Logarithmentafel die Zahlen

$$a = 13 \cdot 17 \bmod 19, \quad b = 13! \bmod 19 \quad \text{und} \quad c = 13^{100} \bmod 19\,!$$

Aufgabe 5: (*4 Punkte*)
Berechnen Sie über dem Körper $\mathbb{F}_2 = \{0, 1\}$ mit zwei Elementen der ggT der Polynome

$$f = x^8 + x^5 + x^2 + 1 \quad \text{und} \quad g = x^5 + x^3 + 1\,,$$

und stellen Sie ihn als Linearkombination dieser beiden Polynome dar!

Abgabe bis zum Dienstag, dem 13. November 2007, um 12.00 Uhr