Wolfgang K. Seiler
Tel. 2515

A5, C201

26. April 2013

9. Übungsblatt Kryptologie

Aufgabe 1: *(6 Punkte)*

a) Zeigen Sie, daß drei eine primitive Wurzel modulo der Fermat-Primzahl $F_4 = 2^{16}+1$ ist, daß sich also jede Zahl zwischen eins und 2^{16} modulo F_4 als Potenz von drei schreiben läßt!

c) Lösen Sie die Gleichung $3^x \equiv 2013 \bmod F_4$ nach der Methode von Pohlig und Hellman!

d) Bestimmen Sie die Ordnung von 2013 in der multiplikativen Gruppe modulo F_4 !

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: *(3 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: *(3 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 Freitag, dem 3. Mai 2013, um 11.55 Uhr