

11. November 2010

## 9. Übungsblatt Kryptologie

### Aufgabe 1: (9 Punkte)

- a) Beweisen Sie den kleinen Satz von FERMAT als Korollar des Lemmas von LAGRANGE!
- b) 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  $3^x \equiv 2007 \pmod{F_4}$  nach der Methode von POHLIG und HELLMAN!
- d) Bestimmen Sie die Ordnung von 2007 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  $g^x \equiv 100 \pmod{131}$  !

### Aufgabe 3: (4 Punkte)

Bestimmen Sie nach der *baby step - giant step* Methode eine Lösung der Gleichung  $3^x \equiv 200 \pmod{257}$  !

### 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

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