

4. November 2010

## 8. Übungsblatt Kryptologie

### Aufgabe 1: (5 Punkte)

Finden Sie alle Primzahlen  $p \equiv 1 \pmod{41}$  zwischen 10 000 und 11 000.

*Hinweis:* Jede zusammengesetzte Zahl  $n \equiv 1 \pmod{41}$  zwischen 10 000 und 11 000 hat einen Primteiler kleiner zwanzig.

### Aufgabe 2: (5 Punkte)

Ihr geheimer ELGAMAL-Schlüssel ist 32; das System arbeitet mit der Basis  $a = 2$  und modulo der Primzahl  $p = 100\,003$ .

- a) Welchen öffentlichen Schlüssel müssen Sie bekanntgeben?
- b) Entschlüsseln Sie die an Sie gerichtete Nachricht (23 094, 72 676) !

### Aufgabe 3: (5 Punkte)

P.D.G. WICHTIG verwendet für seine elektronischen DSA-Unterschriften die Parameter  $q = 1\,009$ ,  $p = 1\,124\,027$  und  $g = 2\,952$ . Sein öffentlicher Schlüssel ist  $u = 9\,275$ . Er unterschreibt die Nachricht 456 mit (1006, 199), die Nachricht 789 mit (1006, 202). Berechnen Sie seinen geheimen Schlüssel!