4. Übungsblatt
Diskrete Strukturen (WS 14/15)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Christian Forler, Eik List
URL: `https://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/ws-2014/diskrete-strukturen-vorlesung/`

Abgabe und Besprechung: 02.12.2014 (13:30 Uhr) in der Übung

Aufgabe 1 (4 Punkte) Restklassen
Berechnen Sie mit Stift und Papier für die folgenden Elemente/Zahlen aus. Geben Sie den Rechenweg mit an.

a) $9^{114} \bmod 113$

b) $27^{105} \bmod 53$

c) Geben Sie einen Fermat-Zeugen für $n = 15$ an

d) Geben Sie einen nicht trivialen Fermat-Lügner für $n = 15$ an

Aufgabe 2 (2+1+2+1 Punkte) RSA Kryptosystem
Gegeben ist ein RSA Kryptosystem mit $p = 13$ und $q = 11$ und $e = 7$. Begründen Sie Ihre Antworten und verwenden Sie nur Stift und Papier.

a) Verschlüsseln Sie den Wert 10

b) Berechnen Sie den geheimen Exponenten d

c) Welche Werte aus der Menge $S = \{3, 4, 5, 6, 9, 10, 11, 12, 13\}$ sind sinnvolle Alternativen für $e = 7$.

d) Faktorisieren Sie den RSA-Modulus $n = 899$.
(Hinweis: Der Abstand zwischen p und q ist sehr klein.)

Aufgabe 3 (1+2+1+2 Punkte) RSA Sicherheit
Das RSA Kryptosystem aus der Vorlesung (Kapitel 3.2) wird häufig mit kleinem öffentlichen Exponent e verwendet, um eine möglichst effiziente Verschlüsselungsoperation zu gewährleisten. Im Folgenden betrachten wir die Wahl $e = 3$ für den RSA Modulus $n = p \cdot q$.

a) Begründen Sie kurz weshalb $e = 3$ die kleinste sinnvolle Wahl ist.

b) Zeigen Sie, dass ein Angreifer ohne Kenntniss von p, q oder d einen Chiffretext $C = M^3 \bmod n$ für $M < \sqrt[3]{n}$ effizient berechnen kann.

c) Wie groß muss e mindestens sein, damit der Angriff aus b) nicht mehr funktioniert.

d) Angenommen e wurde entsprechend groß gewählt. Gibt es dann einen einen effizienten Angreifer der aus dem Chiffretext $C = M^e \bmod n$ die Nachricht M mit $M < 500.000$ berechnen kann. Sie können davon ausgehen, dass dem Angreifer weder p und q noch d bekannt sind.

Aufgabe 4 (4 Punkte) Größter gemeinsamer Teiler (Satz 42)
Zeigen Sie, dass gilt:

a) Aus $b|a$ folgt $b = \mathrm{ggT}(a, b) = 0a + 1b$.

b) Aus $z = a$ div b und $\mathrm{ggT}(a, b) = xb + yr$ folgt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r) = ya + (x - zy)b.$$

Aufgabe 5 (4 Punkte) Fermat Zeuge (Programmieraufgabe)
Implementieren Sie ein ein Skript in Python welches per Kommandozeileinparameter eine ungerade Zahl $n > 1$ engegennimmt. Das Programm soll die Anzahl aller Fermat-Zeugen und Fermat-Lügner berechnen.

Bevor Sie Ihre Implementation einreichen sollten sie die folgenden Tests korrekt beantworten.

Testfall	**(# Zeugen, # Lügner)**
3	$(0, 0)$
9	$(6, 2)$
31	$(0, 0)$
33	$(28, 4)$
437	$(432, 4)$
12345	$(12328, 16)$

Beispielaufruf:

```
# python3 fermat_123456.py 437
(432, 4)
```

(*Abgabe:* Schicken Sie Ihre Lösung als Anhang einer E-Mail `fermat_<MatrNr>.py` an `christian.forler@uni-weimar.de` mit dem Betreff "`[DS] Fermat`"