



## Einführung in Trusted Systems - WS07/08

### 4. Übung

#### Aufgabe 1 (Wurzel ziehen Modulo $n$ )

Berechnen Sie  $x \in \mathbb{Z}_n$  mit

- (a)  $x = \sqrt[5]{2} \bmod 10$
- (b)  $x = \sqrt[7]{5} \bmod 13$
- (c)  $x = \sqrt[3]{4} \bmod 22$
- (d)  $x = \sqrt[5]{23} \bmod 57$

*Hinweis:* Berechnen Sie zuerst das Inverse des Exponenten modulo  $\varphi(n)$ . Verwenden Sie schnelle Exponentiation.

#### Aufgabe 2 (Der kleine Fermat)

Sei  $p$  eine Primzahl. Dann gilt nach dem kleinen Satz von Fermat  $a^{p-1} \equiv 1 \pmod p$ , falls  $\gcd(p, a) = 1$ . Für ein beliebiges  $n \in \mathbb{N}$  gilt  $a^{\varphi(n)} \equiv 1 \pmod n$ , falls  $\gcd(n, a) = 1$ . Berechnen Sie  $x \in \mathbb{Z}_n$  mit

- (a)  $x = 2^3 \bmod 3$
- (b)  $x = 5^{957} \bmod 10$
- (c)  $x = 8^{9381280} \bmod 41$

#### Aufgabe 3 (RSA)

Lösen Sie diese Aufgabe mit Hilfe der schnellen Exponentiation und des erweiterten Euklidischen Algorithmus. Seien  $p = 11$  und  $q = 13$ .

- (a) Wählen Sie  $e > 1$  so klein wie möglich und berechnen Sie den öffentlichen RSA Schlüssel.
- (b) Berechnen Sie den privaten RSA-Schlüssel  $d$ .
- (c) Verschlüsseln Sie  $m = 34$ .
- (d) Entschlüsseln Sie  $c = 21$ .

#### Hausaufgabe 1 (RSA mit kleinem Exponenten)

RSA-Implementierungen, die in der Praxis eingesetzt werden, sind oft dann besonders schnell, wenn der öffentliche Exponent  $e$  eine kleine Zahl ist. Die kleinste sinnvolle Möglichkeit,  $e$  zu wählen, ist  $e = 3$ . Wir wollen in dieser Aufgabe die Sicherheit von RSA im Spezialfall  $e = 3$  etwas genauer betrachten. Zeigen Sie: Wird eine Nachricht  $m$  mit  $m < \sqrt[3]{n}$  mit dem öffentlichen RSA-Schlüssel  $(n, 3)$  verschlüsselt, so kann ein Angreifer effizient aus  $c$  und  $n$  den Klartext  $m$  berechnen.

**Plagiarismus** *Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Zu diesen gehört auch die strikte Verfolgung von Plagiarismus. Mit der Abgabe einer Lösung (Hausaufgabe, Programmierprojekt, Diplomarbeit, etc. ) bestätigen Sie, dass (Sie/Ihre Gruppe) (der alleinige Autor/die alleinigen Autoren) des gesamten Materials sind. Falls Ihnen die Verwendung von Fremdmaterial gestattet war, so müssen Sie dessen Quellen deutlich zitiert haben. Bei Unklarheiten zu diesem Thema finden Sie weiterführende Informationen unter <http://www.informatik.tu-darmstadt.de/Plagiarism>.*