Universität Wien
Prof. Dr. D. Burde

Kryptographie
— Test-Examen —

Sommersemester 2003

---

1. Teilbarkeit und Kongruenzen.

(a) Bestimmen Sie den größten gemeinsamen Teiler d von $a = 903$ und $b = 701$ und stellen Sie ihn als ganzzahlige Linearkombination von a und b dar.
(b) Berechnen sie die Eulersche φ-Funktion $\varphi(n)$ für $n = 999$.
(c) Welche Zahl in $\{0, 1, \ldots, 16\}$ ist 2^{40} modulo 17 ?

(6 Punkte)

2. Das RSA-Verfahren. Alice verschlüsselt die Nachricht (m_1, m_2) mit Bobs öffentlichem Schlüssel $(n, e) = (119, 55)$. Der Schlüsseltext ist $(m_1^e \mod n, m_2^e \mod n) = (2, 3)$. Bestimmen Sie den Klartext. Erklären Sie, wie die Entschlüsselung funktioniert.

(6 Punkte)

3. Primitivwurzeln und Primzahltests.

(a) Bestimmen Sie alle Primitivwurzeln modulo 14 und alle modulo 16.
(b) Formulieren Sie die Primitivwurzelvermutung von Artin.
(c) Zeigen Sie mit dem Primzahltest von Fermat, daß 111 keine Primzahl ist.

(6 Punkte)

4. Diskreter Logarithmus. Mit dem Baby-Step-Giant-Step Verfahren löse man das diskrete Logarithmus Problem

$$2^x \equiv 3 \mod 53$$

Berechnen Sie dazu zuerst die Baby-Steps und dann die Giant-Steps nur soweit wie nötig.

(6 Punkte)

Besprechung: Mittwoch, 11 Juni 2003