Mathematisches Institut
Abt. für Reine Mathematik 22.05.2007
Dr. K. Halupczok

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2007

Blatt 6

Abgabe: Dienstag, den 05.06.2007, zu Beginn der Vorlesung

Aufgabe 1.

(a) Elisabeth will Patrick eine Nachricht senden. Öffentlich sind Patricks RSA-Modul $N = 15229$ und der Schlüssel $t = 5$. Elisabeth sendet ihm die chiffrierte Nachricht $v(k) = 100$. Berechne den Klartext k.

(b) Betrachtet wird die RSA-Chiffre mit Modul N und öffentlichem Schlüssel t. Es sei $v(k)$ die bekannte chiffrierte Nachricht und k der Klartext. Zeige, dass es eine natürliche Zahl m gibt mit $k^{t^m} \equiv k(N)$ und $v(k)^{t^{m-1}} \equiv k(N)$.

(c) Kann man auf Teilaufgabe b) einen erfolgversprechenden Angriff auf die RSA-Chiffre aufbauen? *(Freiwillige Zusatzfrage)*

Aufgabe 2.

Sei $\alpha \in \mathbb{R}$ gegeben und es existiere ein $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) \to \infty$ für $n \to \infty$, sowie eine Folge $\frac{a_n}{b_n}$ rationaler Zahlen mit $(a_n, b_n) = 1$ und $b_n \to \infty$ für $n \to \infty$, sodass für alle $n \in \mathbb{N}$: $\left|\alpha - \frac{a_n}{b_n}\right| < \frac{1}{b_n \cdot f(n)}$. Zeige: α ist irrational.

Aufgabe 3.

Beweise das folgende Primzahlkriterium: Sei $N \geq 3$ eine ungerade Zahl und sei $N - 1 = \prod_{i=1}^{r} p_i^{k_i}$ die Primfaktorzerlegung von $N - 1$ mit paarweise verschiedenen p_i. N ist genau dann eine Primzahl, wenn es eine Zahl a gibt mit den Eigenschaften:

(a) $a^{N-1} \equiv 1(N)$

(b) $a^{\frac{N-1}{p_i}} \not\equiv 1(N)$ für alle $i = 1, \ldots, r$.

bitte wenden

Aufgabe 4. (RSA-Verfahren)

Die Buchstaben des Alphabets A bis Z werden mit den Zahlen 0 bis 25 identifiziert, das Leerzeichen mit der Zahl 26. Klartexte werden zu Blöcken aus je drei Zahlen von 0 bis 26 zusammengefaßt, also z. B. „KLARTEXT_“$=$ $10, 11, 0/17, 19, 4/23, 19, 26$. Jedem Block k_1, k_2, k_3 wird die Zahl $k = k_1 \cdot 27^2 + k_2 \cdot 27 + k_3$ zugeordnet, die beim RSA-Verfahren gemäß $k \mapsto v(k) = k^t \ (N)$ verschlüsselt wird. Die Zahl $v(k)$ wird durch $v(k) = v_1 \cdot 29^2 + v_2 \cdot 29 + v_3$ mit einen Geheimtextblock aus drei Zeichen $v_1, v_2, v_3 \in \{0, \ldots, 28\}$ beschrieben, die auch die zusätzlichen Zeichen „.“$= 27$ und „,“$= 28$ sein können.

(a) Sei $N = 22499$, $t = 1291$. Verschlüssle damit die Klartextnachricht „ZAHLEN“.

(b) Knack den Code: Faktorisiere N und berechne den Schlüssel s, für den $st \equiv 1 \ \ (\varphi(N))$ gilt. Entschlüssle damit den Geheimtext „JI.FTJ“.

(c) Warum ist $N = 22499$ – abgesehen davon, daß N sehr klein gewählt ist – eine besonders schlechte Wahl für N? Welche N sind generell eher ungeeignet?

(d) Hier kann $(k, N) > 1$ sein. Warum arbeitet das angegebene RSA-Verfahren trotzdem korrekt? *(Freiwillige Zusatzfrage)*