Übungen zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte
Abgabe: Freitag, 11. Januar 2013, vor den Übungen

1. Ein Teilnehmer T eines RSA- Systems hat den öffentlichen Schlüssel (e, n) und erhält von einem anderen Teilnehmer S den Geheimtext C. Was war die ursprüngliche Botschaft?

   (a) $(e, n) = (11, 35)$ und $C = 22$

   (b) $(e, n) = (13, 77)$ und $C = 5$. (5 Punkte)

2. Entschlüssele die folgenden Geheimtexte:

   (a) 2846 0811 0105 1312 0001 2604 2435 1717 3045 2161 2405 mit $(e, n) = (17, 3127)$

   (b) 39568405 04669943 17207789 30043037 43138001 93572298 mit $(e, n) = (65537, 99799811)$.
   (10 Punkte)

3. Zeige Lemma 3.1, dass das Chiffrierverfahren (3.3) mit dem Schlüssel (a, d) genau dann bijektiv ist, wenn $ggT(a, 26) = 1$ ist. (4 Punkte)

4. Es sei $n = 2^{1001} \cdot 3^{1600} + 1$, eine Zahl mit 1165 Dezimalstellen.
   Man kann rechnerisch folgende Tatsachen beweisen:

$$5^{n-1} \equiv 1 \bmod n \quad (1)$$
$$5^{\frac{n-1}{2}} \not\equiv 1 \bmod n \quad (2)$$
$$5^{\frac{n-1}{3}} \not\equiv 1 \bmod n. \quad (3)$$

   Folgere aus (1), (2) und (3), dass n eine Primzahl ist.

   Hinweis:
   Betrachte $\mathrm{ord}_n 5$. (5 Punkte)

Wir wünschen Euch allen frohe Weihnachten und einen guten Rutsch ins Neue Jahr 2013!