TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. U. Baumann, Dr. C. Zschalig

Algebra für Informationssystemtechniker (Modul ET - 01 04 04), Wintersemester 2015/16

7. Übungsblatt für die Übung am 1.2.2016

Euler-Funktion, RSA-Verschlüsselung

Ü37. (a) Berechnen Sie zu den folgenden natürlichen Zahlen n den Wert $\varphi(n)$ der Eulerschen Funktion.

(i) $n = 30$, (ii) $n = 60$, (iii) $n = 100$, (iv) $n = 2520$.

(b) Beweisen Sie: Gilt $n = p^\alpha$ für eine Primzahl p und eine natürliche Zahl $\alpha > 0$, dann folgt $\varphi(n) = (p-1)p^{\alpha-1}$.

(c) Zeigen Sie: Ist n eine ungerade Zahl, dann gilt $\varphi(n) = \varphi(2n)$.

Ü38. Berechnen Sie die folgenden Potenzen. Benutzen Sie den Satz von Euler, falls möglich:

(i) $19^{289} \pmod{21}$, (ii) $13^{54} \pmod{32}$, (iii) $7^{27} \pmod{36}$, (iv) $15^{13} \pmod{18}$.

Ü39. (a) Zum Verschlüsseln eines Textes verwenden wir das RSA-Verfahren. Wir codieren die Buchstaben $\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}$ durch die Zahlen $0, 1, \ldots, 25$. Verschlüsseln Sie den Klartext `GEHEIM` mit dem öffentlichen Schlüssel

(i) $(n, e) = (33, 3)$, (ii) $(n, e) = (15, 5)$

(b) Alice hat Ben eine RSA-verschlüsselte Nachricht geschickt. Eva hat die Nachricht `QUTCIM` mitgehört (die Buchstaben sind wie in Ü39a durch Zahlen codiert). Außerdem kennt sie den öffentlichen Schlüssel $(21, 5)$ von Ben. Wie kann Eva die Nachricht entschlüsseln? Wie lautet die gesendete Nachricht?

H40. (a) (i) Verschlüsseln Sie Ihren Nachnamen mit dem RSA-Verfahren mit dem öffentlichen Schlüssel $(n, e) = (33, 13)$. Führen Sie dazu folgende Schritte aus:

(i) Codieren Sie die Buchstaben $A_1, \ldots, A_n$ Ihres Nachnamens durch Zahlen $m_1, \ldots, m_n$ ($A \to 2, B \to 3, \ldots, Z \to 27, \ddot{A} \to 28, \ddot{O} \to 29, \ddot{U} \to 30, ß \to 31$).

(ii) Bestimmen Sie zu jedem Klartextbuchstaben m_i den Schlüsseltextbuchstaben c_i.

(ii) Bestimmen Sie den privaten Schlüssel d mit Hilfe des erweiterten Euklidischen Algorithmus und entschlüsseln Sie den entstandenen Schlüsseltext.

(b) Zum Verschlüsseln eines Textes wurde das RSA-Verfahren mit $(n, e) = (671, 113)$ verwendet. Bestimmen Sie d und entschlüsseln Sie den Text KC EW OS WK UK.

Hinweis: Die Buchstaben $A_1, \ldots, A_{10}$ des Klartextes wurden durch Zahlen $a_1, \ldots, a_{10}$ ersetzt ($A \to 0, B \to 1, \ldots, Z \to 26$). Je zwei aufeinanderfolgende Zahlen a_i und a_{i+1} ($i \in \{1, 3, 5, 7, 9\}$) wurden zu der neuen Zahl $m_i := 26 \cdot a_i + a_{i+1}$ zusammengefasst und durch $c_i = m_i^{113} \pmod{671}$ verschlüsselt. Die c_i wurden schließlich wieder in die Form $c_i = 26 \cdot b_i + b_{i+1}$ zerlegt und den Zahlen $b_1, \ldots, b_{10}$ Buchstaben $B_1, \ldots, B_{10}$ zugeordnet.

H41. Von der Zahl 14803 ist bekannt, dass sie Produkt von genau zwei Primzahlen ist und dass $\varphi(14803) = 14560$ gilt. Wie können mit diesen Informationen die Primfaktoren von 14803 bestimmt werden?

H42. Auf einer Insel leben 13 rote, 15 grüne und 17 blaue Chamäleons. Treffen sich zwei verschiedenfarbige Chamäleons, ändern sie beide ihre Farbe in die dritte Farbe. Begegnen sich gleichfarbige Chamäleons, ändern sie ihre Farbe nicht. Ist es durch eine bestimmte Folge von Begegnungen möglich, dass alle Chamäleons die gleiche Farbe annehmen?