TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Dr. J. Zumbrägel, Dr. C. Zschalig

Mathematik für Informatiker, Teil Diskrete Strukturen, Wintersemester 2016/17

8. Übungsblatt für die Übungen vom 5.12.-9.12.2016

Anwendungen von square & multiply

V54. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**

(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

$$\text{(i) } (n, e) = (33, 3), \qquad \text{(ii) } (n, e) = (15, 5)$$

(b) Alice hat Ben eine RSA-verschlüsselte Nachricht geschickt. Eva hat die Nachricht `QUTCIM` mitgehört (die Buchstaben sind wie in V54a durch Zahlen codiert). Außerdem kennt sie den öffentlichen Schlüssel $(21, 5)$ von Ben. Wie kann Eva die Nachricht entschlüsseln? Wie lautet die gesendete Nachricht?

Ü55. (a) Beweisen Sie: Gilt $n = pq$ für zwei Primzahlen p und q, dann folgt $\varphi(n) = (p-1)(q-1)$. Wie können p und q aus n und $\varphi(n)$ berechnet werden?

(b)* Zeigen Sie, dass $e = \frac{1}{2}\varphi(n) + 1$ eine schlechte Wahl für den öffentlichen Schlüssel ist, da dann (für $p, q \neq 2$) jeder Buchstabe auf sich selbst abgebildet wird.

Ü56. Welche der folgenden Zahlen n bestehen den Fermat-Test zu den angegebenen Basen a?

(a) $n = 73,\ a = 2$ (b) $n = 15,\ a = 11$ (c) $n = 91,\ a = 29$ (d) $n = 341,\ a = 2$

Ü57. Alice und Bob wollen mit dem Diffie-Hellman-Verfahren einen geheimen Schlüssel erzeugen. Dabei einigen sie sich auf den Modul 101.

(a) Alice schickt an Bob die Zahl 53 (mit $2^a \equiv 53 \pmod{101}$). Bob verwendet $b = 65$. Wie lautet der gemeinsame Schlüssel?

(b) Bei einem neuerlichen Schlüsselaustausch lauscht Eva den gemeinsamen Kommunikationskanal ab. Dabei erfährt sie $2^a = 96 \pmod{101}$ und $2^b = 66 \pmod{101}$. Wie lauten der geheime Schlüssel von Alice und der geheime Schlüssel von Bob?

A58. **Hausaufgabe, bitte zu Beginn der 9. Übung oder im Lernraum unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

(a) 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.

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

H59. Zeigen Sie: Wenn $2^n + 1$ eine Primzahl ist ($n \in \mathbb{N}$), so ist n eine Zweierpotenz.

Hinweis: Zeigen Sie zuerst, dass folgendes gilt: Sind $a, k \in \mathbb{N}$ und k ungerade, so ist $a+1$ ein Teiler von $a^k + 1$. Zerlegen Sie dann $n = k \cdot l$ mit ungeradem $k \in \mathbb{N}$ und betrachten Sie $a = 2^l$.

H60. 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 ($A \to 0, B \to 1, \ldots, Z \to 25$). 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.