

Johannes Buchmann

Korrekturen zu “Einführung
in die Kryptographie, dritte
Auflage”

11. April 2005

Springer-Verlag

Berlin Heidelberg New York

London Paris Tokyo

Hong Kong Barcelona

Budapest

- p. 35** Beweis von Theorem 3.9.5: Theorem 3.9.2 statt Theorem 3.9.3 (Zweimal)
- p. 38** Beweis von Korollar 3.11.3: Theorem 3.9.2 statt Theorem 3.9.3.
- p. 49** Lemma 3.19.1: Lies K statt \mathbb{K} .
- p. 57** Übung 3.22.12: d_i fehlt in der Summe.
- p. 85** Zeile 2 von 4.13: Der Name lautet Blaise *de* Vigenère.
- p. 86** Letzte Zeile von Abschnitt 4.2: $\Pr(a)$ statt $P(a)$.
- p. 106** Abb. 6.1: Ersetze $f(R, K)$ durch $f(K, R)$.
- p. 111** Mitte: Ersetze $f(R_0, K_1)$ durch $f(K_1, R_0)$.
- p. 111** viert- und zweitletzte Zeile von Abschnitt 5.3: In beiden Strings muss das 3. und 16. Bit (von links) geändert werden. (der Fehler entsteht wegen dem Fehler in der P-Tabelle).
- p. 132** In Tabelle 5.3, Beschreibung der Funktion P müssen 10 und 20 vertauscht werden. Wo jetzt 10 steht, gehört 20 hin. Wo jetzt 20 steht, gehört 10 hin.
- p. 140** Beispiel 9.3.5: Ersetze 119 (zweimal) durch 110, und 26 durch 165.
- p. 155** Letzte Zeile des zweiten Absatzes: $g^c \equiv g^{ab} \text{ mod.}$
- p. 192** Zeile 3 von Abschnitt 9.6.3: $b \in \{0, 1, \dots, p-2\}$.
- p. 183** In Gleichung (11.4) fehlt ein +:

$$p^{e-1}x = x_0p^{e-1} + p^e(x_1 + x_2p + \dots + x_{e-1}p^{e-2}). \quad (0.1)$$

statt

$$p^{e-1}x = x_0p^{e-1} + p^e(x_1 + x_2p + \dots + x_{e-1}p^{e-2}). \quad (0.2)$$

- p. 198** Zeile 5 von unten. In der Definition von SHA-1 muss

$$C = S^{30}(B)$$

statt

$$C = S^{36}(B).$$

stehen.

- p. 218** Übung 13.7.5: Im ElGamal-Signaturverfahren werde die Primzahl p , $p \equiv 1 \pmod{4}$ und die Primitivwurzel $g \pmod{p}$ benutzt. Angenommen, g hat nur kleine Primfaktoren. Sei A der öffentliche Schlüssel von Alice.

1. Zeigen Sie, dass sich eine Lösung z der Kongruenz $A^q = g^{qz} \pmod{p}$ effizient finden läßt.
2. Sei x ein Dokument und sei h der Hashwert von x . Zeigen Sie, dass $(q, (p-3)(h-qz)/2)$ eine gültige Signatur von x ist.

- p. 236** Die korrekte Formel für die Determinante der Vandermonde-Matrix ist

$$\det U = \prod_{1 \leq i < j \leq \ell} (x_j - x_i).$$

- p. 250** Übung 4.16.1: Der Schlüssel ist 3.

p. 252 Übung 4.8.5: Die Menge A ist $\{12, 13, 14, 15, 16, 21, 23, \dots, 65\}$. Die zweite Menge ist $B = \{11, \dots$

p. 253 Zeilen 1, 3, und 6 nach der ersten Tabelle: das 3. und 16. Bit muss geändert werden.

p. 253 , die letzten drei Zeilen von Übung 5.5.1: x

0011 1100 1010 1011 1000 0111 1010 0011

1110 1111 0100 1010 0110 0101 0100 0100

1100 1100 0000 0001 0111 0111 0000 1001

p. 257 Zeile 1 von Übung 13.4.1: Grad 2.