Johannes A. Buchmann

Corrections to “Introduction to Cryptography, Second Edition”

April 11, 2005
p. 10 In the line before Example 1.7.4. replace $a_i$ by $\alpha_i$.

p. 29 last line of Definition 2.1.1: Delete “the” after “divides”.

p. 42 Proof of Theorem 2.9.5: Theorem 2.9.2 instead of Theorem 2.9.3 (Twice)

p. 45 Proof of Corollary 2.11.3: Theorem 2.9.2 instead of Theorem 2.9.3.

p. 59 Lemma 2.19.2: Use a “plain” $K$.

p. 68 Exercise 2.22.12: $d_i$ is missing in the sum.

p. 88 At the bottom the sequence reads $c_1, c_2, ..., c_n$. The last entry should be $c_u$ instead.

p. 93 Equation (3.3): replace $z_{i-j}$ by $s_{i-j}$.

p. 95 above example 3.9.3, the $p_i$ should be $c_i$.

p. 103 line 2 of 3.13: The name is Blaise de Vigenère.

p. 104/105 Example 3.14.1: The determinant of $A$ is even, and so the cipher is not allowable since it is not relatively prime to $m = 26$. Replace FUSS replaced by FOOT.

p. 117 line 2: $\Pr(a)$ instead of $P(a)$.

p. 117 p. 105, line 2 of Definition 4.2.2: The “end quote” should be placed after ‘occurs’ (and not after the $B$).

p. 118 line 1 of Example 4.2.3: Delete “probability of the”.

p. 123 line 9 from below: $m$ should be replaced by $p$ (3 times).

p. 131 Figure 5.1: replace “Expansionsfunktion” by “expansion function”, “S-Boxen” by “S-boxes” and $f(R, K)$ by $f(K, R)$.

p. 132 In Table 5.3, description of the function $P$ the positions for 10 and 20 must be switched.

p. 136 Replace $f(R_0, K_1)$ by $f(K_1, R_0)$.

p. 136 4th last and 2nd last lines of Section 5.3: In both strings, the 3rd and 16th bits (from the left) should be changed (that’s a result of the problem with the P-table).

p. 140 line 9: Those arrays have “four” rows ...x

p. 168 line 3 of Example 7.2.1: Read $\gcd(3, 220) = 1$. p. 145, line 3 of Example 7.2.5:

p. 171 Example 8.3.5: 119 should be replaced by 110 (twice), and 26 by 165.

p. 171 line 8 of 2nd paragraph: 1023 instead of 1024.

p. 189 line 7 of Section 8.5.4: Read $K = A^b \mod p$.

p. 190 last line of first paragraph: Read $g^c \equiv g^{ab} \mod p$.

p. 192 line 1: $b \in \{0, 1, \ldots, p - 2\}$.

p. 223 In equation (10.4) $a +$ is missing:

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

statt

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

p. 244 Line 15: In the definition of SHA-1 we have

$$C = S^{30}(B)$$
instead of 
\[ C = S^{36}(B). \]

**p. 279** Exercise 12.9.5: In the ElGamal signature scheme use the prime number \( p \) and the primitive root \( g \) mod \( p \). Suppose that \( p \equiv 1 \pmod{4} \) and that \( g \) has only small prime factors. Let \( A \) be Alice’s public key.

1. Show that a solution \( z \) of the congruence \( A^q = g^z \mod p \) can be found efficiently.
2. Let \( x \) be a document and let \( h \) be its hash value. Prove that \( (q, (p - 3)(h - qz)/2) \) is a valid signature of \( x \).

**p. 295** The correct formula for the determinant of the Vandermonde matrix is

\[ \det U = \prod_{1 \leq i < j \leq \ell} (x_j - x_i). \]
Introduction to Cryptography
Buchmann, J.
2004, XVI, 338 p., Hardcover