

Errata/Typos for “Introduction to Modern Cryptography”

(Last updated November 6, 2008)

Note: negative line numbers correspond to counting from the bottom of the page.

- Page 10. The quote regarding Caesar’s cipher in fact indicates that *decryption* involved rotating letters of the alphabet forward 3 positions, implying that *encryption* required rotation *backward* 3 positions.
- Page 17, line 9: The displayed equation should read:

$$S_\tau \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 \approx 0.038,$$

- Page 41, Exercise 2.4: Vigenère should be Vigenère (both times).
- Page 43, Exercise 2.13: The hint is misleading; ignore it.
- Page 49, last paragraph: We were a bit too pessimistic regarding available computing power. The paragraph, from the 3rd sentence on, should be changed to say:

Computation on the order of 2^{60} is difficult for desktop computers, but within reach of powerful computers today. Indeed, running on a 1GHz computer (that executes 10^9 cycles per second), 2^{60} CPU cycles require $2^{60}/10^9$ seconds, or about 35 years. However, the fastest existing supercomputer at the time of this writing can execute roughly 4.78×10^{14} floating point operations per second, and 2^{60} such operations would require only about 40 minutes on such a machine. Taking $t = 2^{80}$ is therefore a more prudent choice; even the supercomputer thus mentioned would require about 80 years to carry out this many operations.

- Page 74, line -13: $m \in \ell(n)$ should be $m \in \{0, 1\}^{\ell(n)}$.
- Page 132, line -5: Even when $x_i = x_{2i}$, it is not necessarily the case that x_{i-1} and $H(x_{2(i-1)})$ are a collision (the issue is that they could also be equal). The algorithm needs to be modified so that once it finds $x_i = x_{2i}$, it then finds the *first* index j where $x_j = x_{j+i}$. Then x_{j-1} and x_{j+i-1} are a collision unless $j = 0$, but the latter occurs with small probability.
- Page 135, line -16: z_{B+1} should be $z'_{B'+1}$. Also, in the analysis of Case 1 every instance of $z_{B'}$ should instead be $z'_{B'}$.
- Page 151, line -9: Π should be Π' .
- Page 157, line 7: Should read: “Then define $H^{s_1, s_2}(x) = H_1^{s_1}(x) \| H_2^{s_2}(x)$ ”.

- Page 213, first displayed equation: the second equal sign should instead be a greater-than-or-equal sign.
- Page 294, Exercise 7.4(b): The question is significantly easier if using the Chinese remainder theorem is allowed.
- Page 295, Exercise 7.14: Add the requirement that $d \in \{1, \dots, \varphi(N)\}$.
- Page 380, line 16: \mathcal{A} should be \mathcal{A}' .
- Page 416, line -3: $\text{Dec}_{sk}(C_2)$ should be $\text{Dec}_{sk}(c_2)$.
- Pages 430–431: Throughout the proof, $\overline{\text{coll}}_{\mathcal{A}, \Pi'}(n)$ should be replaced with $\overline{\text{coll}}_{\mathcal{A}', \Pi'}(n)$.
- Page 442, line 13: π^* should be Π^* .

The following errata were corrected in the second printing:

- Page 41: Remove the hint in Exercise 2.6.
- Page 42, line -15 (Exercise 2.10): Should read $\Pr[C = c \wedge C' = c'] > 0$. A similar typo occurs in Exercise 2.9.
- Page 50, line 10: $t = 80$ should be $t = 2^{80}$.
- Page 85, line -9: “Proposition 3.19” should be “Proposition 3.22”.
- Page 101, line -20 (the last displayed equation on the page): Should be “ \leq ” instead of “ \geq ”.
- Page 106: In Exercise 3.6, the condition on G should be that $|G(s)| > 2 \cdot |s|$.
- Page 108: In Exercise 3.20(b), line -8 on the page, the question should be referring to F (not F').
- Page 125: In Construction 4.9, Gen should choose $k \leftarrow \{0, 1\}^n$.
- Page 153, lines 12–13: “flips the first two bits of c ...” should be “flips the first two bits of the second block of c (recall that the first block of c is simply the initial counter value ctr)...”.
- Page 154, line 21: $F_k(r||m)$ should be $F_k(m||r)$.
- Page 166, Figure 5.2: The arrow labelled “Loop for R rounds” should go to the top-most oval in the figure.
- Page 168, line 9: “ S -boxed” should be “ S -boxes”.
- Page 176, line 4: “property 4” should be “property 3”.
- Page 189: The displayed equation should read

$$DESX_{k_i, k, k_o}(x) = k_o \oplus DES_k(x \oplus k_i).$$

- Page 259: In Example 7.27, the reference to “Exercise 7.25” should instead be to “Example 7.25”.
- Page 284, line 4: This should read:

$$f(1) = 0 \pmod{7}, \text{ so we obtain the point } (1, 0) \in E(\mathbb{Z}_7).$$

- Page 382, Exercise 10.14. The message m should have length *exactly* $\|N/2\|$.
- Page 414, line -3: The displayed equation should read

$$\hat{m} := (25620 - 1)/187 = 137.$$

- Page 488, Construction 13.12: On line -2, ak should be sk . On line -1, $\text{Dec}(c_1)$ should be $\text{Dec}_{sk}(c_1)$.
- Page 521: The authors of reference [62] are E.-J. Goh, S. Jarecki, J. Katz, and N. Wang.

Thanks to Richard Chang, Claude Crépeau, Michael Fuhr, Eyal Kushilevitz, Steve Myers, Ruy de Queiroz, Eli Quiroz, and Arkady Yerukhimovich for sending us some of the above corrections.