Errata/Typos for “Introduction to Modern Cryptography, second edition”

(Last updated May 11, 2018)

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

• Page 5, line 12: The reference to Figure 1.2 should be to Figure 1.1 instead.
• page 11, Figure 1.3: The percentage listed for the letter ‘o’ should be 7.5, not 1.5.
• page 102, Exercise 3.6(a): \( \lfloor n/2 \rfloor \) should be \( \lceil n/2 \rceil \).
• page 103, Exercise 3.9: the output length of \( F \) should be one bit.
• page 129, line 12: \( X \) and \( X' \) should be \( X_i \) and \( X_j \), respectively.
• page 129, equation (4.6) should read:

\[
\Pr[\text{Coll}] \leq \sum_{i,j:i<j} \Pr[\text{Coll}_{i,j}] < \frac{q^2}{2} \cdot \max_{i<j} \{\Pr[\text{Coll}_{i,j}]\}.
\]

• page 129, line 15: \( \text{Coll}_{i,j} \) should be \( \max_{i<j} \{\Pr[\text{Coll}_{i,j}]\} \).
• page 129, line -12: \( 2^\ell - 2 \) should be \( 2^\ell - t - 2 \), and this change should be propagated throughout the rest of the proof.
• page 146, second displayed equation: \( K(m_0, t_0) \) should be \( K(t_0) \).
• page 149, Exercise 4.11: the question assumes that \( \Pi' \) is a secure MAC that uses canonical verification.
• page 149, Exercise 4.14(b) should read as follows:

A random initial block is used each time a message is authenticated. That is, change Construction 4.11 by choosing uniform \( t_0 \in \{0,1\}^n \), computing \( t_\ell \) as before, and then outputting the tag \( \langle t_0, t_\ell \rangle \); verification is done in the natural way.

• page 150, Exercise 4.20: the question assumes that \( \Pi' \) is strongly secure.
• page 210: In the second and third paragraphs on that page, the roles of \( k_1 \) and \( k_2 \) were confused. These paragraphs should read as follows:
A better attack is possible by noting that individual bits of the output depend on only part of the master key. Fix some given input/output pair \((x, y)\) as before. Now, the adversary will enumerate over all possible values for the first byte of \(k_1\). It can XOR each such value with the first byte of \(x\) to obtain a candidate value for the input of the first \(S\)-box. Evaluating this \(S\)-box, the attacker learns a candidate value for the output of that \(S\)-box. Since the output of that \(S\)-box is XOR’d with 8 bits of \(k_2\) to give 8 bits of \(y\) (where the positions of those bits depend on the mixing permutation and are known to the attacker), this yields a candidate value for 8 bits of \(k_2\).

To summarize: for each candidate value for the first byte of \(k_1\), there is a unique possible corresponding value for some 8 bits of \(k_2\). . . .

(The rest is the same, exact that \(k_2\) should be replaced with \(k_1\).)

- page 237, Exercise 6.4: the attack in the text already considers \(S\)-boxes with 8-bit input. So the first part of the question should instead consider a block length of 64 bits and 16 \(S\)-boxes taking 4-bit input.
- page 240, Exercise 6.16: there is in fact an attack taking time \(2^{56}\) and using only constant space.
- page 255, line -12: \(A(x, r \oplus e^i)\) should be \(A(f(x), r \oplus e^i)\).
- page 326, line -16: This sentence should read: “. . . every line intersecting \(E(\mathbb{Z}_p)\) at two points must also intersect it at a third point . . . ”
- page 358, Exercise 9.2: show instead that the algorithm outputs \(p\) with overwhelming probability.
- page 424, last line of Construction 11.36: \(\hat{m}\) should be \(m'\).
- page 434, Exercise 11.7: \(m\) should be in \(\mathbb{Z}_p\), not \(\mathbb{Z}_q\).
- page 455, line -13: \(\text{Sig-Forge}_{A^{'}, \Pi^{'}}(n)\) should be \(\Pr[\text{Sig-Forge}_{A^{'}, \Pi^{'}}(n) = 1]\).
- page 459, line -9: \(h\) should be \(y\) (twice).
- page 460, line 3: \(Gm\) should be \(G\).
- page 484, Exercise 12.5(c): the encoding should be \(\text{enc}(m) = 0^{\kappa/10} \| m \| 0^{\kappa/10}\).
- page 490, last line of Construction 13.4: \(\text{Inv}_I(c)\) should be \(\text{Inv}_{\mathbb{G}}(c)\).