Errata/Typos for "Introduction to Modern Cryptography"

(Last updated February, 2015)

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 13, Figure 1.2: The values for the average letter frequencies of 'x' and 'y' should be swapped.
- Page 16: There are typos in the displayed example of encryption using the key beads. Under the plaintext the letter it should read ead sbeads; the corresponding ciphertext should then be YII EGYUIK. Under the plaintext office the key should be eadsbe; the corresponding ciphertext should then be TGJBEJ.
- Page 16: In the example, the distance between the two appearances of `MJJ` is 30, which is 6 times the period.
- 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 35, line -13: In the sentence beginning on this line, it is *not* the case that "every plaintext is equally likely to have been encrypted"; instead it is the case that, for every plaintext, the likelihood that it was encrypted is exactly the same as the a priori likelihood that it would be encrypted.
- Page 41, Exercise 2.4: Vigenére 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 52, Example 3.3: The calculation in the 3rd paragraph is incorrect. In fact, the adversary runs for the same amount of time as before (though the honest parties still run faster).
- Page 62, line -18: "to denote the probability that $\mathcal{A}$ outputs 1" should be "to denote the probability that the experiment evaluates to 1."
- Page 65, line -4: missing Pr.
- Page 66, line 12: missing Pr (twice).
- Page 71, line 18: The "=" in the displayed equation should be "$\geq$" instead.
- Page 74, line -13: $m \in \ell(n)$ should be $m \in \{0,1\}^{\ell(n)}$.
- Page 81: In Figure 3.3, synchronized mode should not use an IV.
- Page 81: The "augmented pseudorandomness" property referred to here is (informally) that for *any* polynomial ℓ and randomly chosen $IV_1, \ldots, IV_\ell$, the streams $G(s, IV_1), \ldots, G(s, IV_\ell)$ should look jointly pseudorandom even given $IV_1, \ldots, IV_\ell$.
- Page 113, line -15:

$$m_1 := F_k(c_1) \oplus IV' \quad \text{should be} \quad m_1 := F_k^{-1}(c_1) \oplus IV'.$$

- Page 132, line -5: Our discussion of small-space birthday attacks is incorrect: 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 (they could be equal). A revised algorithm and analysis are posted on `http://www.cs.umd.edu/~jkatz/imc.html`
- 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 140, line -13: "Theorem 4.18" should be "Theorem 4.16".
- Page 143, Equation (4.4): Security of HMAC can be proved based on the assumption that

$$G(s,k) = s \| h^s(IV \| (k \oplus \mathsf{opad})) \| h^s(IV \| (k \oplus \mathsf{ipad}))$$

  is a pseudorandom generator. (The above assumes that keys for h are chosen uniformly.)
- Page 151, line -9: Π should be Π'.
- Page 156, Exercise 4.7: Add the additional requirement that all messages must have length that is an integer multiple of $n/2 - 1$.
- 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 157, Exercise 4.15(c): This exercise should be omitted, since hash functions are required to be deterministic.

- Page 157, Exercise 4.15(e): Instructors, please be aware that the solution given in the *Solutions Manual* is incorrect.
- Page 158, Exercise 4.18: For this problem, assume that the underlying fixed-length MAC used in Construction 4.5 *does* have unique tags. (Note that Construction 4.5 does not have unique tags even if this is the case.)
- page 211, line -21: $\mathcal{A}(x, r \oplus e^i)$ should be $\mathcal{A}(f(x), r \oplus e^i)$.
- Page 213, first displayed equation: the second equal sign should instead be a greater-than-or-equal sign.
- Page 216, line -1: "H_n^1, H_n^2, and H_n^3" should be "H_n^0, H_n^1, and H_n^2".
- Page 237, Exercise 6.3. The function f' in the hint is *length-regular* (i.e., has the property that $|f'(x)| = |f'(y)|$ for all $|x| = |y|$); it is not length-preserving.
- Page 239, Exercise 6.15: "$x \in \{0,1\}^{1 \leq n}$" should be "$x \in \{0,1\}^{\leq n} \setminus \{\varepsilon\}$". (The meaning is unchanged, however: we still mean that x is any non-empty string of length at most n.)
- Page 239, Exercise 6.20: Should read "Let G be a pseudorandom *generator*..."
- Page 294, Exercise 7.4(b): The question is significantly easier if use of the Chinese remainder theorem is allowed.
- Page 295, Exercise 7.14: Add the requirement that $d \in \{1, \ldots, \varphi(N)\}$.
- Page 302: Claim 8.2 only holds for F satisfying

  $$x = x' \bmod p \Rightarrow F(x) = F(x') \bmod p.$$

  The F used in practice, which are polynomials, satisfy this condition.
- Page 352, line -2 (and similarly on page 354, line 18): $\mathsf{Enc}'(m_0)$ should be $\mathsf{Enc}'_k(m_0)$.
- Page 360, Algorithm 10.17, line 3: x_i should be x_r.
- Page 366, line 3: "Theorem 10.10" should be "Proposition 10.5".
- Page 380, line 16: $\mathcal{A}$ should be $\mathcal{A}'$.
- Page 381, Exercise 10.10: The Exercise should ask for a proof of Theorem 10.19 *for the case* $\ell = 1$. Also, in retrospect, this exercise is too difficult and should not be assigned.
- Page 382, Exercise 10.16(a): This should read "Argue that encryption can be performed in polynomial time, while ensuring that correctness holds with all but negligible probability."
- Page 416, line -3: $\mathsf{Dec}_{sk}(C_2)$ should be $\mathsf{Dec}_{sk}(c_2)$.
- Page 419, Exercise 11.9(a): The question should read "Show how the sender can generate a random element of $\mathcal{J}_N^{+1}$ in polynomial time, where it is allowed to fail with probability negligible in n."

- Page 420, Exercise 11.14(a): The range of the function should be $\mathcal{QR}_N \times \{-1, +1\} \times \{0, 1\}$. Also, Exercise 11.14(b) is ambiguous as currently written, and should be skipped.
- Page 420, Exercise 11.15: "Lemma 11.27" should be "Proposition 11.27".
- Pages 430–431: Throughout the proof, $\overline{\mathsf{coll}}_{\mathcal{A},\Pi'}(n)$ should be replaced with $\overline{\mathsf{coll}}_{\mathcal{A}',\Pi'}(n)$.
- Page 442, line 13: π^* should be Π^*.
- Page 454, Exercise 12.4: While the problem can be solved as stated, it becomes significantly easier if we assume that $e = 3$ in parts (c) and (d).
- Page 470, line -13: "Theorem 10.10" should be "Proposition 10.5".
- Page 515, Exercise B.3: The hint should read:

  > Let y denote the answer. Use auxiliary variables x (initialized to a) and t (initialized to 1), and maintain the invariant $t \cdot x^b = y \bmod N$ while decrementing b. The algorithm terminates when $b = 0$ and t is equal to the answer.

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 $\Pr[C = c \bigwedge C' = c'] > 0$. 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:

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

- Page 382, Exercise 10.14. The message m should have length *exactly* $\|N/2\|$.
- Page 383, Exercise 10.17(b). In applying El Gamal encryption here, the bit b is first encoded as the group element $m := g^b$ and then this group element is encrypted in the usual way.
- 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, $\mathsf{Dec}(c_1)$ should be $\mathsf{Dec}_{sk}(c_1)$.
- Page 521: The authors of reference [62] are E.-J. Goh, S. Jarecki, J. Katz, and N. Wang.

Thanks to Gilad Asharov, Giuseppe Ateniese, Amir Azodi, Richard Chang, Qingfeng Cheng, Kwan Tae Cho, Kyliah Clarkson, Claude Crépeau, Michael Fuhr, Eyal Kushilevitz, Steve Lai, Ugo Dal Lago, Quentin Lefebvre, Steve Myers, Naveen Nathan, Ruy de Queiroz, Eli Quiroz, Yona Raekow, Tzachy Reinman, Joachim Schipper, Rupeng Yang, Arkady Yerukhimovich, Hila Zarosim, and Konstantin Ziegler for sending us some of the above corrections.