AN INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY
ERRATA FOR THE FIRST EDITION

JEFFREY HOFFSTEIN, JILL PIPHER, JOSEPH H. SILVERMAN

Acknowledgements
We would like to thank the following people who have sent us comments and corrections: Stefanos Aivazidis, John B. Baena, Robert Bond, Reinier Broker, Rebecca Constantine, Stephen Constantine, Christopher Davis, Steven Galbraith, Motahhareh Gharahi, David Hartz, Jeremy Huddleston, Calvin Jongsma, Maya Kaczorowski, Yamamoto Kato, Jonathan Katz, Ariella Kirsch, Ryo Masuda, Shahab Mirzadeh, Kenneth Ribet, Ghassan Sarkis, Frederick Schmitt, Christine Schwartz, David Singer, Michael Soltys, Bruce Stephens, Paulo Tanimoto, Ralph Wernsdorf, Sebastian Welsch, Ralph Wernsdorf, Edward White, Pomona College Math 113 (Spring 2009), University of California at Berkeley Math 116 (Spring 2009, 2010).

Page xiv, Line 7
Vigénere should be Vigenère. (The accent should be on the second e, not the first e.)

Page xiv
In the last line of the summary of Chapter 6, "covereed" has an extra "e".

Page 4, lines 2 and 11
The last part of the ciphertext should be SCVKC B, instead of SCVKV B, and the plaintext is `caesar`, not `caeser`. (But note that it has been corrected on line 14!).

Page 10, Line -13
Add commas to improve readability. Thus:

If a and b are integers, then we can add them, $a + b$, subtract them, $a - b$, and multiply them, $a \cdot b$. In each case, we get an integer as the result.

Page 12, Definition (Division Algorithm)
This is the definition of *division with remainder*, so it is not really an algorithm. Further, for a given a and b, it is not entirely clear that q and r exist. The existence is easy to prove, of course, for example by taking r to be the smallest positive element in the set $\{a - bn : n \in \mathbb{Z}\}$ and proving by contradiction that $r < b$. The uniqueness also needs to be proved. Might be best to note that the statements need to be proved, and make the proofs an exercise.

Date: June 27, 2012.

Page 13, Statement of Theorem 1.7

The conclusion of Theorem 1.7 (the Euclidean algorithm) should be that the division step is execuated at most $2\log_2(b)+2$ times. Of course, one can replace this with $\lfloor 2\log_2(b)+2\rfloor$. But in view of Remark 1.8, the real interest in the bound is that it is just a small multiple of $\log_2(b)$, and hence the Euclidean algorithm terminates quite rapidly, even when b is quite large.

Page 20, Proof of Proposition 1.13

The proof of (b) does not include a proof that the inverse is unique modulo m. A quick proof is to assume that b_1 and b_2 are both inverses of a modulo m and then compute

$$b_1 \equiv b_1 \cdot 1 \equiv \beta_1 \cdot (a \cdot b_2) \equiv (b_1 \cdot a) \cdot b_2 \equiv 1 \cdot b_2 \equiv b_2 \pmod{m}.$$

Page 21, Line 17

The text says here that the Euclidean algorithm takes $2\log_2(b)+3$ steps, but Theorem 1.7 on page 13 should state (and does prove) that the Euclidean algorithm takes at most $\lfloor 2\log_2(b)+2\rfloor$ steps.

Page 21, Definition of $\mathbb{Z}/m\mathbb{Z}$

The book says "Note that whenever we perform an addition or multiplication in $\mathbb{Z}/m\mathbb{Z}$, we always divide the result by m and take the remainder in order to obtain an element in $\mathbb{Z}/m\mathbb{Z}$." This is a bit confusing. Really, we add or multiply elements of $\mathbb{Z}$ and then divide in $\mathbb{Z}$ and take the remainder.

Page 22, Definition of $(\mathbb{Z}/m\mathbb{Z})^*$

Again, if $\mathbb{Z}/m\mathbb{Z}$ is defined to be $\{0,1,\ldots,m-1\}$, then the notion of an inverse is confusing. Of course, the elements of $\mathbb{Z}/m\mathbb{Z}$ are really equivalence classes, but that introduces an entire extra level of complexity.

Page 27, Line -6

In the reference to [126, Chatper 7], the word Chapter is misspelled.

Page 28, Line -11

"described in Exercise 1.28" should be "described in Exercise 1.29"

Page 32, Line 8

The book says that "In practice, the two algorithms tend to take about the same amount of time." This is true in the sense that naive implementations of each have run time of $O((\log p)^3)$. However, "Lehmer's variant" of Euclid's algorithm has a run time of $O((\log p)^2)$. So it might be worth putting in a footnote indicating that the run time issue is somewhat subtle.

Page 33, Line 6
The chain of congruences

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^r \cdot a^r \equiv 1^r \cdot a^r \equiv a^r \pmod{p}.$$

should be

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{p}.$$

(In the middle formula, $(a^k)^r$ is changed to $(a^k)^q$, and in the next formula, 1^r is changed to 1^q.)

Page 36, Line 19
"Germany introduced a new Enigama machine". The name of the machine has an extra "a", it should be "Enigma".

Page 38, Property 4 in the middle of the page
What is described is actually a *known plaintext attack* (KPA), not a *chosen plaintext attack* (CPA). In a CPA, the attacker is allowed to chose any plaintext and be given the corresponding ciphertext. For example, an attacker can always mount a CPA against a public key cryptosystem, since he can encrypt any plaintext that he desires. It is clear that if a system is secure against CPA, then it is secure against KPA.

Pages 38, 42, 43, 44, 56, 57
All of the references to "chosen plaintext attack" should be changed to "known plaintext attack".

Page 47, Problem 1.1(b)
There is an extra "L" in the ciphertext. The block in the middle that currently reads "`ZLJYL ALZAO`" should read "`ZLJYL AZAO`".

Page 53, Exercise 1.32(e)
The problem says to "verify that there are exactly $\phi(229)$ of them," but it should say to "verify that there are exactly $\phi(228)$ of them."

Page 53, Exercise 1.33
Also need to specify that $g \not\equiv 0 \pmod{p}$.

Page 58, Line 3
"(For example, if $k = 23$ and $d = 6$, then..." should be "(For example, if $k = 87$ and $d = 6$, then..."

Page 62, Line 1
"probem" should be "problem"

Page 64, Line 11
$\log_p(h) = 11235$ should be $\log_2(h) = 11235$. (The base of the logarithm is 2.)

Page 68 and following
Tahir ElGamal now prefers that his name be spelled Tahir Elgamal (according to Wikipedia).

Page 68, Middle Displayed Computation
Mention that the quantity $(c_1^a)^{-1}$ can be efficently computed as c_1^{p-1-a}.

Page 69, line -13
The text says that "If Eve can solve the discrete logarithm problem, she can find a and decrypt the message. Otherwise it appears difficult for Eve to find the plaintext,...." In fact, it is enough for her to be able to solve the DHP, which was introduced on page 67. Mention this in the text, and add an exercise to prove that solving DHP breaks ElGamal. Note that this provides a converse to Proposition 2.10.

Page 73, Example (f)
Although the group G is noncommutative, the matrices used as an example actually commute. The example should read

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} \neq \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}.$$

Page 74, Proof of Proposition 2.13
There is some confusion with i and j in the first paragraph of the proof. It should read as follows:

Proof. Since G is finite, the sequence

$$a, a^2, a^3, a^4, \ldots$$

must eventually contain a repetition. That is, there exist positive integers i and j with $j < i$ such that $a^i = a^j$. Multiplying both sides by a^{-j} and applying the group laws leads to $a^{i-j} = e$. Since $i - j > 0$, this proves that some power of a is equal to e. We let d be the smallest positive exponent satisfying $a^d = e$.

Page 74, Proof of Proposition 2.13
The last line of the proof should be "Therefore $k = dq$, so $d \mid k$." (It currently says $d \mid q$.)

Page 74, First Paragraph
What is said is correct, but if one were really going to use a brute force method to solve the DLP, one could do it in fewer steps by computing successively $g, g^2, g^3, \ldots$, where computing g^{i+1} is done by multiplying the previously computed g^i by g.

Page 80, Line -10
The books says that "Step (3) takes $\mathcal{O}(\log n)$ steps," but it should say that "Step (3) takes $\mathcal{O}(n \log n)$ steps." (One can't even sort n elements in fewer than n steps, since each element must be examined at least once!)

Page 87, Line 4
"supppose" should be "suppose".

Page 94, Part (c)
We should say that R is always a ring, and it is a field precisely when n is prime.

Page 102, Line -13
"we can create new finite fields with a prime number of elements" should be we can create new finite fields with a prime power number of elements.

Page 104, Line -2
"The primitive element theorem" should be "The primitive root theorem", which is how Theorem 1.31 is labeled.

Page 106, Line 2
"if and only if its discrete logarithm $\log_g(a)$ modulo p" should be "if and only if its discrete logarithm $\log_g(a)$ modulo $p-1$".

Page 106 and elsewhere
In some places it is called the "decision Diffie–Hellman problem" and in other places it's called the "Diffie–Hellman decision problem". Probably this should be made consistant, with the former being the more common usage.

Page 107, Exercise 2.11
The second displayed equation should say $\tau^2 = e$, not $\tau^2 = 1$.

Page 109, Exercise 2.20
$x = a + cn$ should be $x = a + cm$ in line 3, and $x = a + cn + ymn$ should be $x = a + cm + ymn$ in line 5.

Page 109, Exercise 2.22
This exercise says that it is "non-constructive," but in principle the proof is constructive, since the rings are finite, so one can always compute the inverse to the map by trying all possible inverse images. What the proof does not give is an efficient way to compute the inverse map.

Page 109, Exercise 2.22, displayed equation
There should be ellipses between the $\frac{\mathbb{Z}}{m_2\mathbb{Z}}$ and the $\frac{\mathbb{Z}}{m_k\mathbb{Z}}$. Thus it should read

$$\begin{array}{ccc} \dfrac{\mathbb{Z}}{m\mathbb{Z}} & \longrightarrow & \dfrac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m_2\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{m_k\mathbb{Z}} \\ a \bmod m & \longmapsto & (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k) \end{array} \tag{2.25}$$

Page 109, Exercise 2.24
The exercise should specify that a is an integer that is not divisible by p.

Page 110, Exercise 2.25
In this problem, p and q should be *odd* primes.

Page 115, Proposition 3.2
Add an exercise for Section 3.1 that describes what happens when $\gcd(e, p-1) > 1$, and in the text refer the reader to the exercise. In particular, point out that in this case, the solution x is not uniquely determined. (For the exercise, refer the reader to Theorem 1.11, the extended Euclidean algorithm, as the key to solving the problem.)

Page 116, Line 3
"$z^{de} \equiv z \pmod{z}$" should be "$z^{de} \equiv z \pmod{p}$".

Page 121, Line 17
"since it takes only four squarings and one multiplication to compute m^{65537}" should be "since it takes only sixteen squarings and one multiplication to compute m^{65537}".

Page 126
Alford, Granville, and Pomerance proved that there were infinitely many Carmichael number in 1994, not in 1984. (More precisely, their paper appeared in 1994.)

Page 127, Table 3.2
The loop in Steps 5–8 is somewhat confusing. The idea is that Steps 6 and 7 are repeated exactly k times. But Step 5 says that i runs from 0 to $k-1$, while Step 8 increments i. It might be clearer if Step 8 simply said:
8. End i-loop

Page 130, Line 16
"To do this,, he first…" has a double comma.

Page 132, Lines 2–3
Put in a note that running time $O(\sqrt{n})$ is exponential because $\sqrt{n}$ is exponential in the *number of bits* required to write down the number n. Refer the reader back to Section 2.6 for the formal definitions of exponential-time and polynomial-time.

Page 132, Line 3
There is a missing period at the end of this sentence.

Page 147, Theorem 3.42
It would make more sense to say that $0 < \epsilon < \frac{1}{2}$. If $\epsilon > \frac{1}{2}$, then the lower bound on B is larger than the upper bound, so there are no allowable values of B.

Page 171, Proposition 3.64
The two parts of the proposition are both labeled (a).

Page 176, Exercise 3.2
Should specify that the integers e and f are positive.

Page 178, Exercise 3.10
In the second displayed equation, it says $c_1 =\equiv mg_1^{s_1} \pmod{N}$. The equal sign is extraneous, it should read $c_1 \equiv mg_1^{s_1} \pmod{N}$.

Page 178, Line 12 of Exercise 3.10
"Alice use the Chinese remainder theorem to solve the pair of congruences" should be "Alice uses the Chinese remainder theorem to solve the pair of congruences". (Missing "s".)

Page 179, Exercise 3.14(c)
Parts (b) and (c) are the same. The correct value for (c) is
(c) n = 294439.

Page 184, Exercise 3.34(c)
The definition of u should have a β^2 terms, instead of two β^3 terms. So this exercise should read:
(c) $u = 6 - 5\beta + 3\beta^2 + 3\beta^3$ and $v = -2 + 7\beta + 6\beta^2$.

Page 186, Last line of Exercise 3.38(a)
" that are congruent to 3 modulo p" should be " that are congruent to 3 modulo 4".

Page 186, Exercise 3.40
This problem should specify that the prime p satisfies $p \equiv 1 \pmod 3$. It might be worth adding the following part (d) to the problem:
(d) Suppose instead that $p \equiv 2 \pmod 3$. Prove that for every integer a there is an integer c satisfying $a \equiv c^3 \pmod p$. In other words, if $p \equiv 2 \pmod 3$, show that every number is a cube modulo p.

This may be further generalized as follows: if $\gcd(m, p-1) = 1$, then every number is an m^{th}-power modulo p.

Pages 190–191, Examples 4.1 and 4.2
The phrasing of these examples is somewhat ambiguous, especially in Example 4.1 where it says "How many possibilities are there?" This could be interpreted as the number of (ordered) pairs of classes, which would be $20 \cdot 20$. It might be clearer to ask "How many student–class possibilities are there?" Or change the examples to, say, ordering food at a restaurant, where there are (say) two appetizers and 20 entrées pm the menu, and the example computes how many different meals are possible.

Page 205, Line 17–19
"Similarly, if the keyword happens to start with `B`, then its second letter would be `B` shifted by γ_2, its third letter would be `A` shifted by γ_3, etc." should be "Similarly, if the keyword happens to start with `B`, then its second letter would be `B` shifted by γ_2, its third letter would be `B` shifted by γ_3, etc." (The reference to `A` in this sentence should be to `B`.)

Page 217, Example 4.26
The Prisoner Paradox can be confusing for students, but since it is not a fundamental part of the course, the authors do not feel it deserves more than half a page. The following material is thus made available as a supplement for instructors and students:

Before Alice gets any information from the jailer, there are three outcomes, each of which has equal probability, so

$$\begin{aligned} \Pr(\text{Alice released}) &= 1/3, \\ \Pr(\text{Bob released}) &= 1/3, \\ \Pr(\text{Carl released}) &= 1/3. \end{aligned}$$

Next suppose that the jailer tells Alice the name of someone who will stay jailed, but when the jailer has a choice, i.e., when both Bob and Carl will stay jailed, he picks one at random. Then

$$\begin{aligned}\Pr(\text{Alice released and jailer says ``Bob''}) &= 1/6,\\ \Pr(\text{Alice released and jailer says ``Carl''}) &= 1/6,\\ \Pr(\text{Bob released and jailer says ``Carl''}) &= 1/3,\\ \Pr(\text{Carl released and jailer says ``Bob''}) &= 1/3.\end{aligned}$$

So the fact that the jailer told Alice that Bob will stay jailed means that

$$\Pr(\text{Alice released} \mid \text{jailer says ``Bob''}) = \frac{1/6}{1/6+1/3} = \frac{1}{3},$$

so Alice's chances of being released are still $\frac{1}{3}$.

Finally, suppose that the jailer tells Alice the name of someone who will stay jailed, but when the jailer has a choice, he always chooses Bob. Then

$$\begin{aligned}\Pr(\text{Alice released and jailer says ``Bob''}) &= 1/3,\\ \Pr(\text{Alice released and jailer says ``Carl''}) &= 0,\\ \Pr(\text{Bob released and jailer says ``Carl''}) &= 1/3,\\ \Pr(\text{Carl released and jailer says ``Bob''}) &= 1/3.\end{aligned}$$

So the fact that the jailer told Alice that Bob will stay jailed means that

$$\Pr(\text{Alice released} \mid \text{jailer says ``Bob''}) = \frac{1/3}{1/3+1/3} = \frac{1}{2},$$

so in this scenario Alice's probability of being released has increased to $\frac{1}{2}$.

Page 220, Section 4.3.4

This section can be difficult for students (and instructors) who have not previously studied probability. It has been suggested that in each of the examples, we explicitly describe the sample space Ω, although once one becomes familiar with the language of probability, this is seldom done. In particular, note that the sample space in Example 4.31 is an infinite set.

Here is expanded text for Examples 4.29 and 4.31.

Example 4.29. The sample space Ω consists of all binary strings $\omega = b_1 b_2 \ldots b_n$ of length n, where $b_i = 0$ if the i'th experiment is a failure and $b_i = 1$ if the i'th experiment is a success. The value of the random variable X at ω is simply $X(\omega) = b_1 + b_2 + \cdots + b_n$, which is the number of successes. Using the random variable X, we can express the probability of the event ω as

$$\Pr(\{\omega\}) = p^{X(\omega)}(1-p)^{n-X(\omega)}.$$

(Do you see why this is the correct formula?)

Example 4.31. The sample space Ω consists of all binary strings $\omega = b_1b_2b_3\ldots$, where $b_i = 0$ if the i'th toss is tails and $b_i = 1$ if the i'th toss is heads. This is an example of an infinite probability space. The way in which we assign probabilities to events is by specifying a certain number of initial tosses. So for any given finite binary string $\beta_1\beta_2\ldots\beta_n$, we assign a probability

$$\Pr\bigl(\{\omega \in \Omega : \omega \text{ starts } \beta_1\beta_2\ldots\beta_n\}\bigr) = p^{(\#\text{ of }\beta_i\text{ equal to }1)}(1-p)^{(\#\text{ of }\beta_i\text{ equal to }0)}.$$

The random variable X is defined by

$$X(\omega) = X(b_1b_2b_3\ldots) = (\text{smallest } i \text{ such that } b_i = 1).$$

Then

$$\{X = n\} = \bigl\{\omega \in \Omega : X(\omega) = n\bigr\} = \bigl\{\underbrace{000\ldots00}_{n-1\text{ zeros}}1b_{n+1}b_{n+2}\ldots\bigr\}.$$

Hence

$$f_X(n) = \Pr(X = n) = (1-p)^{n-1}p.$$

Page 221 and following

On page 221 the balls in the urns are black and white, while later in the chapter (e.g., page 228) they are red and blue. Maybe it would be best to make the colors consistant.

Page 223, Line 17, Example 4.32

"Further the events F and S are independent" should be "Further the random variables F and S are independent"

Page 223, Line -9

"easy because X and Y are independent" should be "easy because F and S are independent". (The events X and Y are not independent since $X + Y = 2$.)

Page 223, Example 4.32

It could be mentioned that the second part of this example (picking two coins without replacement) is a special case of Example 4.30 (hypergeometric distribution) that starts on the bottom of page 221. Thus the $\frac{4}{7}$ appearing as the last line of page 223 is the formula (4.24) on page 222 evaluated with $N = 7$, $m = 4$, $n = 2$, $i = 1$, which yields

$$\frac{\binom{4}{1}\binom{3}{1}}{\binom{7}{2}} = \frac{4}{7}.$$

Page 225, Line 3

"The prompts" should be "This prompts".

Page 230, Lines 13–15
"the "red balls" are the eight marked cards in the second deck, and the "blue balls" are the other 48 cards in the second deck" should be "the "red balls" are the eight marked cards in the second deck, and the "blue balls" are the other 44 cards in the second deck". (If we take 8 card away from 52 cards, there are 44 cards left, not 48!)

Page 230, Example 4.40
The previous discussion and Theorem 4.38 deal with probabilities of selection with replacement, but this example is different. From the way it is phrased, Bob selects $100,000$ elements, puts them back into the set, and then selects another $100,000$ elements. It is actually not clear if either or both subsets are selected with replacement. In order for the formula to be exactly correct, the first set should be chosen without replacement, the second with replacement.

Of course, since the set has 10 billion elements and the sample sets only have $100,000$ elements, the issue of replacement should not greatly affect the answer. The same applies to Example 4.41, as long as n is small compared to N. But this should be explained.

Page 230, Line -14
"Theorem 4.38(a)says" needs a space between (a) and "says".

Page 232 and Elsewhere
The discrete logarithm problem is stated using different notations in different parts of the book. Thus:

Section 2.7: $g^x = h$.
Section 4.4.3: $h^x = b$.
Section 4.5.2: $g^t = a$.

To the extent possible, it would be good to use a consistant notation.

Page 232 Proposition 4.44
This proposition is included to illustrate the running time of a randomized algorithm and as a warm-up for Pollard's rho algorithm. But it is also true that the babystep-giantstep algorithm described in Proposition 2.22 accomplishes the same task and is guaranteed to have $O(\sqrt{N})$ running time. It might be worth making an explicit comment to this effect.

Page 233, First displayed equation
The middle term should be $1-(1-n/N)^n$, not $(1-n/N)^n$. Thus the entire line should read

$$\operatorname{Prob}\begin{pmatrix}\text{at least one match}\\ \text{between (4.31) and (4.32)}\end{pmatrix} \approx 1-\Bigl(1-\frac{n}{N}\Bigr)^n \approx 1-e^{-n^2/N}.$$

Page 233, Line 6–7
The text currently says: "then our probability of getting a match is approximately 99.98%." It has been pointed out that taking $n = 3\sqrt{N}$ gives a probability of 99.987659%, which is closer to 99.99%. So change it to "then our probability of getting a match is greater than 99.98%."

Page 233, Line -5
"moduluo" should be "modulo".

Page 240, Line 4
$g^{i-j} = a^{\ell-j}$ should be $g^{i-k} = a^{\ell-j}$.

Page 243, Line 15
In the list of powers of 19, the quantity 19^{135645} should be 44690, not 23894.

Page 244, Section 4.6.1
This section may be difficult for students whose first introduction to probability theory was reading Section 4.3. In particular, the definition of a random variable on page 220 says that a random variable is a function $X : \Omega \to \mathbb{R}$, while the random variables M, K, and C used in Section 4.6.1 do not have this form. Thus if we let $\mathcal{M}$, $\mathcal{K}$, and $\mathcal{C}$ denote the sets of plaintexts, keys, and ciphertexts, then there we start with a probability space $(\Omega, \Pr)$ and define random variables M, K, and C to be functions

$$M : \Omega \to \mathcal{M}, \qquad K : \Omega \to \mathcal{K}, \qquad C : \Omega \to \mathcal{C}.$$

Then for any particular plaintext $m \in \mathcal{M}$, we have

$$f_M(m) = \Pr(M = m) = \Pr\bigl(\{\omega \in \Omega : M(\omega) = m\}\bigr),$$

and similarly for K and C. The distribution functions f_M, f_K, and f_C are related to one another via the encryption/decryption formula $d_k(e_k(m)) = m$, which is what leads to formula (4.47) on page 245.

Page 245, Formula (4.47)
This formula is not correct if there are some keys k such that c is not the encryption of any plaintext. The correct formula is

$$f_C(c) = \sum_{\substack{k\in\mathcal{K}\\ \text{such that}\\ c\in e_k(\mathcal{M})}} f_K(k) f_M\bigl(d_k(c)\bigr). \tag{4.47}$$

In other words, we should sum only over those keys k for which c is a possible ciphertext. A more detailed derivation of (4.47) goes as follows and reveals the problem:

$$\begin{aligned} f(c) &= \sum_{k\in\mathcal{K}} f(k) f(c \mid k) \\ &\qquad\qquad \text{(using the decomposition formula, Exercise 4.23)} \\ &= \sum_{k\in\mathcal{K}} f(k) \sum_{m\in\mathcal{M}} f(m) f(c \mid k \text{ and } m) \\ &\qquad\qquad \text{(using the decomposition formula again)} \\ &= \sum_{k\in\mathcal{K}} f(k) \sum_{\substack{m\in\mathcal{M}\\ e_k(m)=c}} f(m). \qquad (*) \end{aligned}$$

The last equality follows from the fact that

$$f(c \mid k \text{ and } m) = \begin{cases} 1 & \text{if } c = e_k(m), \\ 0 & \text{if } c \ne e_k(m). \end{cases}$$

Now consider the set

$$S = \bigl\{m \in \mathcal{M} : e_k(m) = c\bigr\}.$$

If $c \notin e_k(\mathcal{M})$, then it is clear that $S = \emptyset$. On the other hand, if $c \in e_k(\mathcal{M})$, say $c = e_k(m')$, then

$$e_k(d_k(c)) = e_k(d_k(e_k(m'))) = e_k(m') = c,$$

so $d_k(c) \in S$. Conversely, if $m \in S$, then $d_k(c) = d_k(e_k(m)) = m$. This proves that

$$S = \begin{cases} \bigl\{d_k(c)\bigr\} & \text{if } c \in e_k(\mathcal{M}), \\ \emptyset & \text{if } c \notin e_k(\mathcal{M}). \end{cases}$$

Hence the inner sum in $(*)$ equals $f(d_k(c))$ if $c \in e_k(\mathcal{M})$, and it equals 0 otherwise. This gives the corrected version of formula (4.47).

Page 246, Line -13
" the number of keys must also be at least as large as the number of ciphertexts" should be " the number of keys must also be at least as large as the number of plaintexts". Note that this is what we prove, $\#\mathcal{K} \ge \#\mathcal{M}$.

Page 246, Proposition 4.54
It should be stated explicitly in Proposition 4.54 that we assume that $f(m) > 0$ for all plaintexts $m \in \mathcal{M}$. Note that this is a reasonable assumption, since there is no practical reason to include plaintexts in $\mathcal{M}$ that are never used. Further, Proposition 4.54 is false without this assumption, since we can always make $\mathcal{M}$ arbitrarily large by adjoining plaintexts that cannot occur (and thus that have no associated ciphertexts). The proof breaks down at the line $f(c \mid m) = f(c) > 0$, since the conditional probability $f(c \mid m)$ is not defined if $f(m) = 0$. As an alternative, we could define $\mathcal{M}^+ = \{m \in \mathcal{M} : f(m) > 0\}$, and then the conclusion of Proposition 4.54 is $\#\mathcal{K} \ge \#\mathcal{M}^+$.

Page 252, Definition of Concavity and Theorem 4.59
The definition of concave (4.52) is a non-strict inequality, which it must be if we allow α in the closed interval $[0,1]$. But then a linear function is concave, in which case Theorem 4.59 is not correct, since if F is a linear function, then equality in (4.53) holds for all values of $t_1, \dots, t_n$. So either change the definition to use strict concavity, i.e., make (4.52) a strict inequality that is supposed to hold for all $0 < \alpha < 1$, or in Theorem 4.59 say that equality holds in (4.53) if and only if either F is a linear function or $t_1 = \cdots = t_n$.

Page 253, Corollary 4.60
The wording of Corollary 4.60 should be changed, since a random variable is not an experiment and the x_i are real numbers, not events. The event is $\{\omega : X(\omega) = x_i\}$, which can be abbreviated $X = x_i$. Here is a reformulation of the corollary.

Corollary 4.6. *Let X be a random variable that takes on finitely many possible values $x_1, \dots, x_n$.*
(a) $H(X) \le \log_2(n)$.
(b) $H(X) = \log_2(n)$ *if and only if every event $X = x_i$ occurs with the same probability $1/n$.*

Page 254, Lines 4–7
The displayed equation ends with $\frac{3}{2} \approx 0.585$. This should read $\frac{3}{2} = 1.5$. The following line says: “Notice that $H(M)$ is considerably smaller than $\log_2(3) \approx 1.585, \ldots$”. This should be replaced with: “Notice that $H(M)$ is somewhat smaller than $\log_2(3) \approx 1.585, \ldots$”.

Page 255, Line 4
The value at the end of this displayed equation is incorrect. It should read

$$H(C) = -\frac{1}{4}\log_2\left(\frac{1}{4}\right) - 2\cdot\frac{3}{8}\log_2\left(\frac{3}{8}\right) = \frac{1}{2} + \frac{3}{4}\log_2\left(\frac{8}{3}\right) \approx 1.56,$$

Page 255, Lines 6–8
Due to the correction on Line 4, we need to change Line 6 to read:

$$H(K \mid C) = H(K) + H(M) - H(C) \approx 1 + 1.5 - 1.56 \approx 0.94.$$

The next two lines say “This is quite low, which confirms our intuition that in this cryptosystem, an average ciphertext reveals a significant amount of information about the key.” Either remove these lines, or change them to reflect the fact that the entropy is not particularly low.

Page 256, Definition of $H(\mathsf{L})$
The entropy of L is defined as the limit

$$H(\mathsf{L}) = \lim_{n\to\infty} \frac{H(L^n)}{n},$$

but it's not clear that the limit exists. In practice, one should probably define upper and lower entropies $\overline{H}(\mathsf{L})$ and $\underline{H}(\mathsf{L})$ using a limsup and liminf, and then the inequality at the bottom of page 256 would be written as

$$1.0 \le \underline{H}(\mathsf{L}) \le \overline{H}(\mathsf{L}) \le 1.5,$$

but it's probably not worth going into such detail. Instead, can just say that $H(\mathsf{L})$ is the limit, if the limit exists, and that experimentally it appears that

$$1.0 \le \frac{H(L^n)}{n} \le 1.5$$

as n increases.

Page 257, Line -13
This displayed equation should read

$$e : \mathcal{M} \to \mathcal{C} \qquad \text{and} \qquad e' : \mathcal{M}' \to \mathcal{C}'$$

(In the text there is a missing prime on the second $\mathcal{M}$.)

Page 258, Middle
The description of Post's correspondence problem is incorrect. In the correct description, one is allowed to use pairs an unlimited number of times. Here is the corrected description of that paragraph.

There are uncountably many undecidable problems in mathematics, some of which have simple and interesting formulations. Here is an example of an easy to state undecidable problem called *Post's correspondence problem* [96]. Suppose that you are given a sequence of pairs of strings,

$$(s_1, t_1),\ (s_2, t_2),\ (s_3, t_3),\ \ldots,\ (s_k, t_k),$$

where a string is simply a list of characters from some alphabet containing at least two letters. The correspondence problem asks you to decide whether there is an integer $r \geq 1$ and a list of indices

$$i_1, i_2, \ldots, i_r \quad \text{between 1 and } k \tag{4.55}$$

such that the concatenations

$$s_{i_1} \parallel s_{i_2} \parallel \cdots \parallel s_{i_r} \qquad \text{and} \qquad t_{i_1} \parallel t_{i_2} \parallel \cdots \parallel t_{i_r} \qquad \text{are equal.} \tag{4.56}$$

Note that if we bound the value of r, say $r \leq r_0$, then the problem becomes decidable, since there are only a finite number of concatentations to check. The problem with r restricted in this way is called the *bounded Post correspondence problem.*

Page 259, Line 7
The quote marks before ”nondeterministic” are backwards, it should be “nondeterministic”.

Page 259, Paragraph after the Definition
Regarding the discussion of P versus NP, the book says that the Post's Correspondence Problem is in NP. That is not true. First, all languages in NP are decidable. Second, the book says that “given a subsequence of pairs (4.55) whose concatenations (4.56) are alleged to be the same, then it takes a polynomial number of steps to verify that the concatenations are indeed the same.” But it has to be polynomial in the size of the input problem, and the proof (or certificate) in the PCP problem (if it exists) can be very long. (The authors thank Michael Soltys and Christopher Davis for this correction.) What is true is that there is a variation of Post's problem which is NP complete. This is the bounded Post correspondence problem (see the correction for page 258). Here is the corrected version of this paragraph:

For example, the bounded Post correspondence problem is in $\mathcal{NP}$. It is clear that if you are given a list of indices (4.55) of bounded length such that the concatenations (4.56) are alleged to be the same, it takes a polynomial number of steps to verify that the concatenations are indeed the same. On the other hand, exhaustively checking all possible concatenations of length up to r_0 takes an exponential number of steps. It is less clear, but can be proven, that one cannot find a solution in a polynomial number of steps.

Page 259, Line -8
“inuuition” shoud be “intuition”.

Page 270, Exercise 4.27
The last sentence says that this exercise generalizes Section 4.3.3 with $\delta = 0.01$ and $p = \frac{1}{2}$. It should say with $\delta = 0.99$, since δ is the probability that m has property A, while in Section 4.3.3, E is the event that an integer does *not* have property A and we're given that $\Pr(E) = 0.01$. Alternatively, one can define δ to be the probability that m does not have property A.

Page 271, Exercise 4.31
Parts of this problem are easier using the operator $\Theta = x\dfrac{d}{dx}$, since $\Theta(x^n) = nx^n$. (So the monomials are eigenfunctions for Θ.) Then

$$\Theta^k\left(\frac{1}{1-x}\right) = \Theta^k\left(\sum_{n=0}^{\infty} x^n\right) = \sum_{n=0}^{\infty} n^k x^n,$$

valid for $|x| < 1$. It is not clear if it is worth introducing Θ in the text, but this material may be used by interested instructors or students.

Page 272, Exercise 4.32(d)
The hint should be to (4.29) on page 221, not (4.23) on page 221.

Page 286, Remark 5.7
Rather than first defining elliptic curves over $\mathbb{F}_p$ in general, and then excluding $p = 2$ and 3, it might be better to exclude them from the start.

Page 288, Line -9 and -7
There's an arithmetic error in these calculations, although it does not affect the final answer. (λ should be 12, not 1, although note that 12 is the same as -1, since we're working in $\mathbb{F}_{13}$.) These lines should read as follows:

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = \frac{246}{14} = 12 \quad \text{and} \quad \nu = y_1 - \lambda x_1 = 7 - 12 \cdot 9 = 3.$$

Then

$$x_3 = \lambda^2 - x_1 - x_2 = (12)^2 - 9 - 9 = 9 \quad \text{and} \quad y_3 = -(\lambda x_3 + \nu) = -(12 \cdot 9 + 3) = 6,$$

Page 288, Line -6
"for the X-and Y-coordinates" should have a space after the dash following the X. Thus it should read "for the X- and Y-coordinates."

Page 295, Line above equation (5.6)
Replace "for some $t \geq 1$" by "for some $t \geq 2$", since we want at least two consecutive ones.

Page 299, Last line of Section 5.4.1
" their shared secret value is the x-coordinate $x = 593$, which is the same for both points" should be " their shared secret value is the x-coordinate $x = 509$, which is the same for both points". Note that 509 is the x-coordinate of their shared point. The value 593 is the value of x_A.

Page 299, 338, 350, . . .
The use of the term *ephemeral key* in the text is somewhat non-standard. The usual definition of an ephemeral key in cryptography is a key that is generated for each execution of a key establishment process. In the text it is used to denote a quantity that is used for encryption, but that changes each time a new plaintext is encrypted, hence its "ephemeral" nature. The occurrences of the term "ephemeral key" in the text are listed in the index on page 508.

Page 300, Table 5.6 and in several other places
"ciphtertext" should be "ciphertext"

Page 312, Theorem 5.29
"Notice that Hasse's theorem (Theorem 5.11) says that $|t| \le \sqrt{p}$" should be "Notice that Hasse's theorem (Theorem 5.11) says that $|t| \le 2\sqrt{p}$". (There's a missing 2 in the upper bound for Hasse's theorem.)

Page 312, Line -4
This displayed equation should read

$$\tau^2(Q) - t \cdot \tau(Q) + p \cdot Q = \mathcal{O},$$

(The "zero" on the right-hand side is $\mathcal{O}$, not the number 0.)

Page 313, Line -1
This line says "equation $\tau^2 + \tau + 2$ when it acts on points of $E(\mathbb{F}_{2^k})$," but it should read "equation $\tau^2 + \tau + 2 = 0$ when it acts on points of $E(\mathbb{F}_{2^k})$," (an equation needs an equal sign!).

Page 316, Line 4
This displayed equation should read

$$E[m] = \bigl\{P \in E : mP = \mathcal{O}\bigr\}.$$

(The notation $[m]P$ is also a common notation, but it is not the notation used in this book.)

Page 317, Second Paragraph
The text says "In a similar manner, if E is an elliptic curve,

$$E : Y^2 = X^3 + AX + B,$$

and if $f(X, Y)$ is a rational function of two variables, then there are points of E where the numerator of f vanishes. . . " Add a sentence explaining that f defines a function on E in the sense that if $P = (x, y)$ is any point of E, then we define $f(P)$ to equal $f(x, y)$, i.e., evaluate the rational function $f(X, Y)$ as the point $(X, Y) = (x, y)$.

Page 317, Section 5.8.2
When discussing poles and zeros of rational functions on an elliptic curve, add a sentence to emphasize the fact that the coordinates of the poles and zeros may well lie in some extension field. In particular, if E is defined over $\mathbb{F}_p$, the poles and zeros of a rational function f have coordinates in $\mathbb{F}_{p^k}$ for some k, but the value of k will, in general, depend on the function f.

Should also mention that the zero function does not have a divisor, since it vanishes at every point.

Page 317, Example 5.35
Clarify that Y represents the function on the elliptic curve E defined by

$$Y(P) = (\text{the } y\text{-coordinate of the point } P).$$

So the function Y vanishes at the three points $(\alpha_i, 0)$, $i = 1, 2, 3$. That explains the positive part of the divisor $\operatorname{div}(Y)$. In order to get the negative part explicitly, one needs to change coordinates. But can mention that it follows from Theorem 5.36(b) on the next page. Thus Y clearly has no poles at the finite points of E, since $Y(x, y) = y$, so its only possible pole is at $\mathcal{O}$. Hence

$$\operatorname{div}(Y) = [P_1] + [P_2] + [P_3] - n[\mathcal{O}]$$

for some integer n. Now Theorem 5.36(b) tells us that $\deg(\operatorname{div}(Y)) = 0$, which gives $n = 3$.

Page 318, Theorem 5.36(a)
Say that f and f' are *nonzero* rational functions.

Page 318, Last Paragraph
It has been suggested that it would helpful to offer some explanation as to why the divisor of $X - \alpha$ is $2[P] - 2[O]$, and not $[P] - [O]$, or at least to add such an explanation to this errata sheet.

There are various ways to see that $\operatorname{div}(X - \alpha)$ is $2[P] - 2[O]$. In particular, the fact that $(\alpha, 0)$ is a point on E means that α is a root of the cubic used to define E, so the equation of E has the form

$$E : Y^2 = (X - \alpha)(X^2 + aX + b).$$

Further, the polynomials of $X - \alpha$ and $X^2 + aX + b$ have no common roots (this is where we use the nonsingularity of E), so they have no common zeros. And of course, their only pole is the point O. It follows that $\operatorname{div}(X-\alpha)$ and $\operatorname{div}(X^2+aX+b)$ have no points in common except for O. But

$$2\operatorname{div}(Y) = \operatorname{div}(X - \alpha) + \operatorname{div}(X^2 + aX + b),$$

which shows that the zeros of $X - \alpha$ appear with even multiplicity. Of course, the only zero of $X - \alpha$ is the point $P = (\alpha, 0)$, which shows that

$$\operatorname{div}(X - \alpha) = 2n[P] - 2n[O]$$

for some integer $n \geq 1$. (Note that the total number of zeros and poles sums to zero.)

There are various ways to prove that n equals 1. For example, we can prove that Y is a local uniformizer at P, i.e., it vanishes to order 1 at P. To do that, we consider the local ring at P, which is the ring

$$R = \left\{ \frac{f(X,Y)}{g(X,Y)} : Y^2 = X^3 + AX + B \text{ and } g(\alpha, 0) \neq 0 \right\}.$$

In other words, we take all rational functions whose denominator does not vanish at P. This is a local right whose maximal ideal is generated by $X - \alpha$ and Y. But since

$$X - \alpha = \frac{Y^2}{X^2 + aX + b} \quad \text{and} \quad X^2 + aX + b \text{ does not vanish at } P,$$

we see that $X - \alpha$ is in the ideal of R generated by Y, so Y is a uniformizer. Indeed, this shows that $X - \alpha$ generates the same ideal as Y^2, so

$$\operatorname{ord}_P(X - \alpha) = 2 \operatorname{ord}_P(Y) = 2.$$

Page 319, Section 5.8.3
Add [123, Section III.8] as a reference for the Weil pairing and for the proof of Theorem 5.38.

Page 321, Section 5.8.4
Add [123 (2nd edition, 2009), Section XI.8] as a reference for additional material on Miller's algorithm.

Page 324, Section 5.8.5
Add [123 (2nd edition, 2009), Section XI.9] as a reference for the Tate pairing.

Page 326 and 328
After Step 4 of the MOV algorithm, if it turns out that $\alpha = 1$, then one needs to go back to Step 2 and choose a new point T. This may happen even if $T' \neq \mathcal{O}$, e.g., if T' happens to be a multiple of P.

Page 328, Table 5.9, Step 2
It is natural to ask how one generates a random point $T \in E(\mathbb{F}_{p^k})$ with $T \notin E(\mathbb{F}_p)$. One method is to choose random values $x \in \mathbb{F}_{p^k}$ and check if $x^3 + Ax + B$ is a square in $\mathbb{F}_{p^k}$. An easy way to do this is

$$z \text{ is a square in } \mathbb{F}_{p^k} \quad \Longleftrightarrow \quad z^{(p^k-1)/2} = 1.$$

(We are assuming here that p is an odd prime, of course.) There then exist practical (i.e., polynomial time) algorithms to compute square roots in finite fields, but to describe them would take us too far afield. (See (26, §§1.5.1, 1.5.2) for the case $k = 1$.)

Page 332, Last displayed equation
This line is true, but the logic of the line is a bit confusing. It would be better to write: "Since P is a point of order ℓ, Proposition 5.51(b) says that

$$\ell\phi(P) = \phi(\ell P) = \phi(\mathcal{O}) = \mathcal{O},$$

so $\phi(P)$ is a point of order ℓ.

Page 337, Line -15
The book says: "Let $\hat{e}_\ell$ be the associated modified Weil height." First, it should be "Weil pairing," not "Weil height." Second, this is slightly different from the terminology on page 330, so change it to "Let $\hat{e}_\ell$ be the modified Weil pairing relative to the map."

Page 337–338
The hash function H_1 needs to select points of order ℓ, not arbitrary points in $E(\mathbb{F}_q)$. So H_1 should be defined by

$$H_1 : \{\text{User IDs}\} \longrightarrow E(\mathbb{F}_q)[\ell].$$

This needs to be changed on page 337, line -10 and page 338 line 5 of Table 5.11.

Page 337–338
It might be worthwhile to explain how to construct a hash function like H_1 that takes its values in $E(\mathbb{F}_q)[\ell]$. Here is one method. Note that Tom has already fixed a point in $P \in E(\mathbb{F}_q)[\ell]$ of order ℓ. So we can take the User ID, call it i, and use it as a seed for a pseudorandom number generator (see Section 8.2) to get a number m. Then we set $H_1(i) = mP$. (In practice, one needs to be a bit more careful so as to ensure that as i varies, the values of $m \bmod \ell$ are uniformly distributed modulo ℓ.)

Page 338, Table 5.11
In **Master Key Creation**, Tom should choose s modulo ℓ, not modulo m.

Page 338, Table 5.11
In **Decryption**, Alice should compute

$$C_2 \,\mathsf{xor}\, H_2(\hat{e}_\ell(Q^{\text{Alice}}, C_1)).$$

(The H_2 is missing in the text.)

Page 344, Exercise 5.22(b)
The displayed equation should read

$$t_k = t_1 t_{k-1} - 2t_{k-2} \qquad \text{for all } k \geq 3.$$

There are two corrections: the pt_{k-2} is changed to $2t_{k-2}$, and the condition $t \geq 3$ has been changed to $k \geq 3$.

Could add a part (e) to this problem (or create a new problem) to prove a similar recursion for general elliptic curves. Using the formula in Theorem 5.29 on page 312, let

$$t_k = p^k + 1 - \#E(\mathbb{F}_{p^k}).$$

Then one can show that

$$t_k = t_1 t_{k-1} - pt_{k-2} \qquad \text{for all } k \geq 3.$$

Page 339, Exercise 5.3
The equation should read

$$x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3).$$

(The text has a typo $(x - e_1)(x - e_2)(x - e_2)$.)

Page 344, Exercise 5.23
The upper bound on ℓ should be $\ell \le 2\lceil \log n \rceil + 1$. We say in the proof of Proposition 5.30 that it is possible to get $\ell \approx \log n$ and we give a reference. However, the algorithm given in Exercise 5.23 seems to only return an expansion with $\ell \le 2\lceil \log n \rceil + 1$.

Page 346, Exercise 5.32
The exercise says the formula is true "provided that the Tate pairings on the right-hand side are computed properly." This may cause some confusion. (How can they be computed "improperly"?) Instead say "provided that the Tate pairings on the right-hand side are computed consistently."

Page 347, Exercise 5.40
It should say to "Use the distortion map on E from Exercise 5.37 to compute. . . ," not the distortion map from Exercises 5.38 and 5.39. (Note that the curve in Exercises 5.38 and 5.39 is a different curve.)

Page 350, Line 1
Also need to require $\gcd(f, g) = 1$, since later in (6.1) we compute $f^{-1}a \pmod{g}$.

Page 351, Table 6.1
Line 3: Need to require that $\gcd(f, q) = 1$, as well as $\gcd(f, g) = 1$.
Line 10: It says $a \equiv fe \pmod{e}$, but it should be $a \equiv fe \pmod{q}$.
Line 6: It says $m < \sqrt{q/2}$, but it should be $m < \sqrt{q/4}$. (This is done correctly on page 350.)

Page 353, Example 6.2
It is not true that $S = 27$ has a unique representation, since it is also $4 + 23$. The problem is that 9, 14, and 23 are all in the set $\mathbf{M}$, and $23 = 9 + 14$. Could change change to $S = 21$, which has the unique representation $21 = 3 + 4 + 13$.

Page 365, Line 4
There is a typo in the definition of $\mathbf{w}_3$. It should be $\mathbf{w}_3 = \mathbf{v}_1 + 2\mathbf{v}_2$

Page 366, Line -2
"Then very vector" should be "Then every vector".

Page 373, Theorem 6.28
In the statement of Theorem 6.28 (Minkowski's theorem), add the assumption that S is bounded, since the proof uses this fact. (In fact, the first part of the theorem is true even if S is not bounded, since we can first replace S with $S \cap B$ for a sufficiently large ball centered at the origin. If B is large enough, we will have $\mathrm{Vol}(S \cap B) > 2^n \,\mathrm{Vol}(L)$. However, the second half of the theorem won't work, since if $\mathrm{Vol}(S) = 2^n \,\mathrm{Vol}(L)$, then $\mathrm{Vol}(S \cap B) < 2^n \,\mathrm{Vol}(L)$ for any ball B.)

Page 374, Fifth displayed equation
The end of this sentence is missing. It should read "We now observe that the vector

$$\underbrace{\frac{1}{2}\mathbf{a}_1 + \overbrace{\left(-\frac{1}{2}\mathbf{a}_2\right)}^{\substack{S \text{ is symmetric,} \\ \text{so } -\mathbf{a}_2 \text{ is in } S}}}_{\substack{\text{this is the midpoint of the line} \\ \text{segment from } \mathbf{a}_1 \text{ to } -\mathbf{a}_2\text{,} \\ \text{so it is in } S \text{ by convexity}}}$$

is in the set S."

Page 377, Line -12
The text reads "we use the estimate (6.30) from Theorem 6.19," but it should be "we use the estimate (6.19) from Theorem 6.30."

Page 385, Line 10
"he selects a small vector **m** as his plaintext" should be "he selects a small vector **m** with integer coordinates as his plaintext".

Page 386, Table 6.3
The Encryption part of the table says that Bob should compute

$$\mathbf{e} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n + \mathbf{r}.$$

This is not correct, he should compute

$$\mathbf{e} = x_1\mathbf{w}_1 + \cdots + x_n\mathbf{w}_n + \mathbf{r},$$

since Alice's public key is $\mathbf{w}_1, \ldots, \mathbf{w}_n$, not $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Page 379, Line -10
It reads "parallelepiped $L + \mathbf{v}$", but it should say "parallelepiped $\mathcal{F} + \mathbf{v}$".

Page 382, Line -1
The $\mathbf{v}_1$ and $\mathbf{v}_2$ in this formula should be $\mathbf{v}_1'$ and $\mathbf{v}_2'$.

Page 386, Table 6.3
Line 10: It says

$$\mathbf{e} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n + \mathbf{r},$$

but it should read

$$\mathbf{e} = m_1\mathbf{w}_1 + \cdots + m_n\mathbf{w}_n + \mathbf{r},$$

Line 11: "ciphtertext" should be "ciphertext".

Page 387, Line 7
Since $\mathbf{e} \approx 75.76\mathbf{w}_1 - \cdots$, when it is rounded, the vector $\mathbf{v}'$ should be $\mathbf{v}' = 76\mathbf{w}_1 + \cdots$.

Page 387, Remark 6.37
There are potential problems with choosing the ephemeral key deterministically as suggested in this remark. Note that one wants security against chosen plaintext attacks, i.e., an attacker should not be able to determine whether a guessed plaintext corresponds to the given ciphertext. A solution is to add randomness to the plaintext. Naively, one might simply concatenate a random string to the plaintext, but there are various reasons why this is not a good idea. In practice some sort of encoding method is applied to the plaintext and a random string. This encoding method (at least) has the properties that it is easy to invert and that changing any bit of either the plaintext or the random string has an unpredictable effect on every bit of the output. Then this "randomized" plaintext is encrypted using an ephemeral key.

Page 393, Line -14
The text says that the coefficients of $\mathbf{m}(x)$ are "between $-\frac{1}{2}p$ and $\frac{1}{2}p$." This is ambiguous if p is even, since in that case we want to include exactly one of the endpoints. The correct statement is that if p is even, then the coefficients should satisfy $-\frac{1}{2}p < m_i \le \frac{1}{2}p$.

Page 393, Line -14
"the plaintext $\mathbf{m}(x)$ is is a polynomial" has a repeated "is".

Page 393, Equations (6.34)**,** (6.35)**,** (6.36)
It might be worth noting that when we say that the congruence holds modulo q, the computation is being done in R_q.

Page 394, Table 6.4
There is actually no need to require that p be prime. However, if p is even, then one doesn't get a set of coset representative modulo p that is symmetric around 0, so some choice needs to be made. Thus it's probably easiest for expositional purposes to at least assume that p is odd. In real-world applications, there may be situations where one would take $p = 2$ and q odd.

Page 395, Remark 6.50
There are potential problems with choosing the ephemeral key deterministically as suggested in this remark. See the correction to Remark 6.37 on page 387. The same comments apply to this remark.

Page 395, Line 6
"possible coefficient fo $\mathbf{f} \star \mathbf{m}$" should be "possible coefficient of $\mathbf{f} \star \mathbf{m}$".

Page 395, Third displayed formula
The first line reads

$$\mathbf{b}(x) = \mathbf{F}_p(x) \star \mathbf{a} \qquad \text{from (6.36).}$$

But (6.36) is really just a congruence modulo p, so replace this line with a congruence

$$\mathbf{b}(x) \equiv \mathbf{F}_p(x) \star \mathbf{a} \pmod{p} \qquad \text{from (6.36).}$$

Then should make the next line a congruence, too.

Page 401, Proposition 6.61
This proposition assumes that $q \approx 6d$, but the NTRU decryption condition is $q > (6d+1)p$, so we should really assume that $q \approx 6dp$. In practice, one might take $p = 3$, so $q \approx 18d \approx 6N$, which changes the numbers in the statement and proof of Proposition 6.61. However, the conclusion that $(\mathbf{f}, \mathbf{g})$ is a factor of $\mathcal{O}(1/\sqrt{N})$ smaller than predicted by the Gaussian heuristic is still valid.

Page 407, Line 11 (line after (6.51))
It reads "where $\mathcal{F}$ is the volume... ." It should read "where $\mathrm{Vol}(\mathcal{F})$ is the volume... ."

Page 408, top
The next-to-last entry in the last line of the matrix M displayed at the top of the page should read $\mu_{n,n-1}$, not $\mu_{n-1,n}$.

Page 409, Equation (6.56)
There are two terms in this formula that should have squares on them. It currently reads

$$\|\mathbf{v}_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{v}_{i-1}^*\| \geq \frac{1}{2}\|\mathbf{v}_{i-1}^*\|.$$

It should read

$$\|\mathbf{v}_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{v}_{i-1}^*\|^2 \geq \frac{1}{2}\|\mathbf{v}_{i-1}^*\|^2.$$

Page 410, Line 13
This displayed formula starts

$$\|\mathbf{v}_i\|^n \leq \cdots,$$

but it should be

$$\|\mathbf{v}_1\|^n \leq \cdots.$$

Page 411, Table 6.7
There are two mistakes in this description of the LLL algorithm. First, the loop in Steps [5]–[7] should count down, not up. This is necessary becaue the span of $\{\mathbf{v}_1, \ldots, \mathbf{v}_j\}$ is the same as the span of $\{\mathbf{v}_1^*, \ldots, \mathbf{v}_j^*\}$, while the span of $\{\mathbf{v}_j, \ldots, \mathbf{v}_{k-1}\}$ is not necessarily the same as the span of $\{\mathbf{v}_j^*, \ldots, \mathbf{v}_{k-1}^*\}$ Second, there is a typo in the formula in Step [6], it should be $\mathbf{v}_j$, not $\mathbf{v}_j^*$. (Otherwise the new value of $\mathbf{v}_k$ won't necessarily be in the lattice!). So Steps [5]–[7] should read as follows:

```
[5]   Loop $j = k-1, k-2, \ldots, 3, 2, 1$
[6]       Set $\mathbf{v}_k = \mathbf{v}_k - \lfloor \mu_{k,j} \rceil \mathbf{v}_j$        [Size Reduction]
[7]   End $j$ Loop
```

Page 414, First paragraph and following

The given lower bound for D and its derivation are correct, but needlessly complicated. We have assumed that the lattice L is contained in $\mathbb{Z}^n$, so its basis vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ have integer entries. Thus the same is true of L_ℓ, which is spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_\ell$. Letting B_ℓ be the n-by-ℓ matrix of this matrix, we see that $d_\ell = (\det L_\ell)^2 = \det(B_\ell^t B_\ell)$ is a nonzero *integer*. Hence it trivially satisfies $d_\ell \geq 1$. It is then immediate that $D = \prod_{\ell=1}^{n} d_\ell \geq 1$, which is much stronger than (6.60). This lower bound completes the proof that the LLL algorithm terminates. Further, it simplifies the analysis of the running time of LLL on the rest of this page and gives the stronger result that the running time is $\mathcal{O}(n^2 \log B)$. The statement of Theorem 6.68 on page 4.11 should be adjusted accordingly.

Page 422, Exercise 6.3

There are two mistakes in this problem. First, the underlying sequence is not superincreasing, because the last two numbers in the list are 3253 and 6500. However, it is still true that each number in the list is larger than the sum of all of the previous numbers, which suffices to make the algorithm in Proposition 6.5 work. Second, the number $S = 26560$ cannot be written as a sum of elements from the list, because it is too large. Here is a revised version of Exercise 6.3.

Alice's public key for a knapsack cryptosystem is

$$\mathbf{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 637).$$

Eve intercepts the encrypted message $S = 4398$. She also breaks into Alice's computer and steals Alice's secret multiplier $A = 4392$ and secret modulus $B = 8387$. Use this information to find Alice's superincreasing private sequence $\mathbf{r}$ and then decrypt the message.

Page 425, Exercise 6.17(b)

The Hadamard ratio should have a square root. So it should read: "What is the value of the Hadamard ratio $\bigl(\det(L)/\|\mathbf{v}_1\|\|\mathbf{v}_2\|\bigr)^{1/2}$?"

Page 431, Exercise 6.43

(a) "Prove a more version of Theorem 6.66" should be "Prove a version of Theorem 6.66 assuming this alternative Lovász condition."

(b) "Prove a version of Theorem 6.68" should be "Prove a version of Theorem 6.68 assuming this alternative Lovász condition."

Page 433, Table 6.9, Step [5] of SWAP

In Step [5] of the SWAP subroutine, the value of B should be

$$B = B_k + \mu^2 B_{k-1}.$$

(The book has a minus sign.)

Page 437, Line 4

"It his thus" should be "It is thus".

Page 440, Section 7.2
In a future edition, possibly discuss RSA signing of private messages, i.e., Alice sends a signed encrypted message to Bob by using Alices private key and Bob's public key.

Page 442, top of page
The numerical values of v and s have been swapped. So line 4 should read

$$S \equiv D^s \pmod{N}, \quad S \equiv 1070777^{1051235} \equiv 153337 \pmod{2430101}.$$

line 6 should read

$$D = 1070777 \qquad \text{and} \qquad S = 153337.$$

and line 10 should read

$$S^v \bmod N, \qquad 153337^{948047} \equiv 1070777 \pmod{2430101}.$$

Page 442–447, Section 7.3
For ElGamal signatures, the random quantity e needs to satisfy $\gcd(e, p-1) = 1$, since the quantity $e^{-1} \bmod p - 1$ is used. For DSA the corresponding requirement is $\gcd(e, q) = 1$, or equivalently, $q \nmid e$, since q is prime.

Page 442, Line 3 of Table 7.2
"primtive" should be "primitive".

Page 444, Second line of fourth displayed equation
The congruence for S_2 should be modulo 21738, not 21736, since $p = 21739$ and the congruence is modulo $p - 1$.

Page 466, Second line of second paragraph of Remark 8.1
Remove the word "and" from the phrase "a bit string of length n and into another bit string of length n."

Page 490, Middle
In the definition of $H(X)$, "teh" should be "the".

Page 497, References [82]–[85]
These should refer to NIST (National Institute of Standards and Technology), not to NSB (National Bureau of Standards).

Page 499, Item [123]
This bibliography item should be updated to refer to the second edition, published in 2009.