Errata for *Introduction to Number Theory with Cryptography*

page 4, line -4: 1850 should be 1855

page 6, line 15: Valleé-Poussin should be Vallée-Poussin

page 14: Euclid's statement was that a finite set cannot contain all of the primes. Therefore, A, B, C represent the elements of a finite set of primes (Euclid didn't actually do this as a proof by contradiction, so this is not necessarily the set of all primes). The prime G that is constructed is an element not in the original set.

page 22, last line: remove one "the"

page 44, line 2: change x to 2 (four times)

page 56, line -3: remove one "a guess"

page 63, line 11: $p_2q_3\cdots q_s$ should be $q_2q_3\cdots q_s$

page 68, Project 1 (c): The number 1 is not a Hilbert prime.

page 78, last line of proof of Theorem 3.4: replace a_n with a_0 (twice)

page 85, line -3: it should read $c = n^2 + m^2$

page 78, line 2: $P(x)$ should be $P(X)$

page 94, line 1: $\gcd(m, nn)$ should be $\gcd(m, n)$

page 96, Chapter Highlights 3 should have $a = n^2-m^2$ in place of $a = n^2-n^2$. Also, change $m \not\equiv n \pmod 2$ to "one even and one odd"

page 97, Exercise 3: Add the assumption that $\gcd(a, b) = 1$.

page 98, problem 21: Change the hint to "If n is odd, $n = (k + 1)^2 - k^2$ for some k. If n is even, write $n = 2^r m$ with m odd and separately consider the cases $m = 1$ and $m \geq 3$."

page 108, Proposition 4.2: change "of" to "if"

page 108, first sentence of last paragraph, should be "gives" in place of "give"

page 108, line -2: change "lemma" to "proposition"

page 109, line 7: change "lemma" to "proposition"

page 109, line 3: change "positive" to "non-negative"

page 110, line 2: change "next section" to "Section 4.4"

page 113, lines 4, 9, 11: change x to c (4 times)

page 123, line -13: change "if try" to "if we try"

page 125, line -8: $\gcd(13, 101)$ should be $\gcd(13, 100)$

page 140, line 12: add subscript i to p in the first product (twice)

page 141, line -11: Change $p = 12$ to $n = 12$

page 145, line -8: $3m - 2$ should be $3m - 1$

page 183, line 12: 21666077416496^{233} should not have the exponent 233.

page 240, Answers to "CHECK YOUR UNDERSTANDING" 3: One primitive root is missing from the list: $2^{13} \equiv 3 \pmod{19}$

page 246, line -13: remove one "decides to"

page 268, line 2: replace $\left(\frac{4}{257}\right)$ with $\left(\frac{4}{11}\right)$ and change 257 to 11 on line 3.

page 284, middle: replace "As in the case $p \equiv q \pmod 4$" with "As in the case $p \equiv q \pmod{4a}$"

page 289, Problem 31: Include "$\equiv 0$"

page 291, line -7: change "in" to "is" and change "tell" to "tells"

page 297, line 6: Change "per seconds" to "per second"

page 300, line 7: remove "with"

page 339, line -4: This should be $B(r) = \{(x_1, x_2, \ldots, x_n) \in B \mid x_1^2 + x_2^2 + \cdots + x_n^2 < r^2\}$.

page 350, lines 6, 21, 23: Change $3/\sqrt{d}$ to $3\sqrt{d}$

page 375, line 4: the sum should be $\sum_{d|n}$

page 375, line 7: $g(n) = \sum_{d|n} \phi(d)$

page 376, line 13: $g(n) = \sum_{d|n} \phi(d)$

page 406, line -9: Change "proposition" to "lemma"

page 476: Project 15.7.2.1, part (b): Add "(This exercise requires Theorem 9.4(c).)"

page 527, lines -7 and -4: The indices on F_0 and F_1 are incorrect. These should be F_1 and F_2. Even better, the verification should use $n = 0$ and $n = 1$ instead of $n = 1$ and $n = 2$.

page 542, Problem 9(d): The displayed formula should read

$$-1 \equiv 3^{2^{2^m - 1}} \pmod{p}$$

page 550: the entry for "Euler ϕ-function" should include page 139

We thank Paul Baginski, Manjul Bhatia, Bruce Bromberg, Jon-Patrick Cook, Daniel Drucker, Tom Haines, Michael Hardy, Vince Lucarelli, Nathan Manning, Jared Ronning, Jonathan Rosenberg, Luke Rothman, and Sandy Zabell for pointing out some of the above errors.