Errata for *Introduction to Number Theory with Cryptography, 2nd edition*

page 29, line -9: The proof of the relation $\gcd(a_1, a_2, \ldots, a_{k+1}) = \gcd(\gcd(a_1, a_2, \ldots, a_k), a_{k+1})$ is missing and is left as an exercise for the reader.

page 39, line 6: change the second (c) to (d)

page 40, Exercise 29: part (b): remove 15

page 40, Exercise 31: change "greater than equal to" to "greater than or equal to"

page 54, line -1: change "the previous section" to "Section 2.7.1"

page 61, Exercise 8: It should say that 880 is the largest, not the smallest, and $10x + 11y$ should be $10x + 11y = n$

page 71, problem 7(a): The rightmost term "$a + b$" should be "$a + c$".

page 152, line 10: $1 \leq i \leq n$ should be $1 \leq i \leq r$

page 193, line -1: number "10" should be "1"

page 199, line -10: 2.14 should be 2.15

page 200, line 18: number "11" should be "2"

page 205, line -8: 900 should be 1100

page 246, line 8: "mod p" should be "mod n"

page 214, Exercise 26: Part (a): Change the first sentence to "Let p be an odd prime and let $p \equiv 2 \pmod 3$.
Part (b): Change last line to "Let $N = (2p_1p_2 \cdots p_n)^2 + 3$.)"

page 244: Throughout Section 11.2, p denotes a prime.

page 266, line 9: Lemma 11.5 should be Lemma 11.16

page 315, line 2: Insert "$\equiv 0$"

page 318, section "Answers to Check Your Understanding," problem #2: change $5^{(p+1)/2}$ to $5^{(p+1)/4}$

page 320, line 9: It should be "$43771 = 7 \times 13^2 \times 37$"

page 561, line 7: change x_i to $x + i$.

page 564, Problem 27: Change "Exercise 12" to "Exercise 14"

We thank Manjit Bhatia, Jonathan Saewitz, Tom Barber, Jeff Adams, Giovanni Forni, Nathan Manning, and Debraj Chakrabarti for pointing out some of the above errors.