Errata for
Elliptic Curves: Number Theory and Cryptography, 2nd ed.

by Lawrence C. Washington

page vi, line 17: Insert a period at the end of the sentence.

page xviii, line -2: the references start on page 499 (not 501)

page 92, Exercise 3.1(b): the gcd equals $x(x-1)$

page 109, lines 17-22: change n to m (13 times) and change m to n (once)

page 125, line 6: change page 47 to page 51

page 150, line -2, to page 151, line 4: this paragraph and the preceding description of the lambda method do not match Pollard's explanation of kangaroos, which are assumed to have bounded jump length. See Pollard's paper [87] and his more recent paper in J. of Cryptology 13 (2000), 437-447.

page 163, line 17: m_2 should equal 579383/300

page 340, line 18: change $u(P) = 0$ to $u_P(P) = 0$

page 479, line -8: the first G_2 should be G_3

(last updated 4/15/2009)

Many thanks to Andreas Peter, Ten H Lai, John M. Pollard, Loren Olson, John McColgan, and Yu Tsumura for pointing out some of the above errors.