Errata for Introduction to Cryptography with Coding Theory

by Wade Trappe and Lawrence C. Washington

The following lists corrections for the First printing (September 2001). There was a Third Printing in 2002 that corrected most of these errors. The remaining errors are marked with *

*page 16, line 9: change "it will always happen this way" to "it will always happen this way when the coefficients of α in the equations are even"

page 18, lines -19 to -15: the middle lines of the ciphertext are incorrect. The correct ciphertext is in the computer problems on pages 377, 408, 446.

page 38, Table 2.4: characters 60 and 62 should be < and >

*page 42, line -12: remove the second "is"

page 55, line 14: Change the first sentence to "A sequence generated by a length three recurrence starts 001110."

page 55, lines 17-18: change these lines to "the length three recurrence $k_{n+3} = k_n + k_{n+1} + k_{n+2}$. This sequence can also be given by a length two recurrence. Determine this length two recurrence"

page 57, line 20: change Vigenére to Vigenère

page 57, line -6: remove `a` at the end of the line

*page 62, line 12: this line should read

$$576 = 2^6 3^2, \quad 135 = 3^3 5, \quad \gcd(576, 135) = 3^2 = 9$$

*page 64, lines 13, 15: The second x_{j-2} on each line should be y_{j-2}

*pages 90-91: The explanation here for LFSR sequences is not correct. The transpose of the matrix associated to multiplication by X needs to be used. A corrected version of these pages is here:
`http://www.math.umd.edu/~lcw/ninety.pdf`

page 92, line -18: change "such" to "such that"

page 93, line 15: change "$2^{32} = 1 \pmod{65537}$" to "$2^{32} \equiv 1 \pmod{65537}$"

*page 93, line -8: it should be "$s_1 = 1$."

page 103, line 17: remove "that"

page 104, line -12: change "$K_1 = 010011010$" to "$K_2 = 01001101$"

page 116, line 2: remove "that"

page 122, line -10: change $K_1 \oplus E_{K_2}(K_3 \oplus m)$ to $K_3 \oplus E_{K_2}(K_1 \oplus m)$

*page 129, line -7: remove the period after "column"

page 132, line -4: change the second "is" to "in"

*page 133, lines 2-4: The sentence should read "Add 1 to each of these numbers (since the first row and column are numbered 0) and look in the 13th row and 12th column of the S-box."

page 140, line 14: change 1.2599 to 1.4422

*page 143, line -8: it should be "$s_1 = 1$."

page 148, line 21: it should be $b_0 \equiv 8 \pmod{17}$

page 148, line 22: it should be $b_1 \equiv -4 \pmod{17}$

page 152, line -11: $(6, 4, 6, 0, 2, 4, 0, 2)$ should be $(8, 4, 6, 0, 2, 4, 0, 2)$

page 174, line 15: change Alice to Bob

*page 189, line -12: change $D_k(m)$ to $E_k(m)$

page 192, lines 15 and 17: change α to a

page 194, lines -4, -5: the values of m_1 and s_1 are incorrect. They should be

$$m_1 = 418726553997094258577980055061305150940547956$$

$$s_1 = 749142649641548101520133634736865752883277237.$$

page 194, lines -2, -1: the last sentence should read "The numbers n_A, n_B, p_B, q_B are stored as *signa, signb, sigpb, sigqb*.)"

page 207, line 5: change r to b

page 207, line 6: change $A^r \equiv z^H r$ to $A^r \equiv z^H b$

*page 225, line -21: change "residues quadratic" to "quadratic residues"

page 234, line -2: change Alice to Peggy

page 248, line -2: change $c1$ to c

page 249, line 10: change $b_I = 13$ to $b_I = 23$

page 249, lines -3, -2: change K_3 to K_H

page 253, line 6: remove "is"

*pages 276-277: The polynomial $x^3 + 2x + 3$ has a double root mod 5 at $x = 4$, so the curve E is a degenerate curve in the sense of page 283. Therefore, the addition law for points behaves well only if we do not use the point (4,0). This is the same idea as in the example on page 283.

page 289, line -6: change Alice to Bob

*page 291, line -2: it should be "$S_1 = \infty$."

*page 292, line 3: change "Exercise 3.12(a)" to "Exercise 12(a) in Chapter 3"

*page 292, line 4: remove comma

*page 292, line 11: change "Exercise 3.12(b)" to "Exercise 12(b) in Chapter 3"

page 292, lines 17, 18: change m to n'

page 293, line 19: change m to n

*page 311, line 2: This sentence should read "The Singleton bound says that $16 = M \leq 2^5$, so it is not an MDS code."

page 320, line -12: remove one of the right parentheses

page 320, line -8: change the vector to (0,0,0,0,1,0,0,0,0,0,0,1,0,0,1)

page 320, line -6: change the vector to (0,0,0,0,1,0,0,0,0,0,0)

*page 330, line 13: change the last "((" on the line to "("

*page 333, line -11: change "by (4)" to "by (3)"

*page 334, line 8: change "part (5)" to "part (4)"

*page 334, line -5: change "part (5)" to "part (4)"

page 341, line 13: change "In following" to "In the following"

*page 344, lines 4-5: these should read: "is $n-\deg(g) = n+1-d$. Therefore a Reed-Solomon code is a cyclic $[n, n+1-d, d]$ code."

page 349, line -11: the code should be $\{(0,0,1),(1,1,1),(1,0,0),(0,1,0)\}$

page 351, line 14: add subscript $j-1$ to C

page 351, line 15: Replace the first sentence with "Let $av+c$, with $a \neq 0$, be an element of C_j, as in (c)."

page 351, line 16: change the last v to c

page 351, line -11: insert "of length 7" between "code" and "generated"

page 351, line -6: change the sentence to "Assume $0 \neq C \neq F^n$ and $p \nmid n$ (as in the Theorem on p. 336)."

page 351, line -3: change $h(X)$ to $g(X)$

*pages 368, 369: some statements about the approximation properties of continued fractions are inaccurate. Replacement pages are here:
`http://www.math.umd.edu/~lcw/three68.pdf`

page 370, line 11: change $= 2^{m-s}$ to $= 2^{m-s}e^{2\pi i x c_0/2^m}$

page 374, line 17: **choose[txt,m,n]** lists the characters in txt in positions congruent to $n \pmod m$. (m and n were reversed)

page 419, lines 6, 9: change]] to)

page 428: in the three displayed Maple commands, change `mult` to `mul`

(last updated 11/29/2004)