ERRATA FOR INTRODUCTION TO
CRYPTOGRAPHY WITH CODING THEORY

Wade Trappe and Lawrence C. Washington

The following lists corrections for the First printing (September 2001). There was a Second Printing in January 2002 that presumably corrected some of these errors. These are marked with *.

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 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 Vigen¶ere to Vigenµere

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

*page 92, line -18: change “such” to “such that”

*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 248, line -2: change $c_1$ 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”
page 289, line -6: change Alice to Bob
page 292, line 4: remove comma
*page 292, lines 17, 18: change $m$ to $n'$
*page 293, line 19: change $m$ to $n$
*page 320, line -12: remove one of the right parentheses
*page 320, line -8: change the vector to $(0,0,0,0,1,0,0,0,0,0,0)$
*page 320, line -6: change the vector to $(0,0,0,0,1,0,0,0,0,0,0,0)$
*page 341, line 13: change “In following” to “In the following”
*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 $a v + c$, 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 $g(X)$
*page 374, line 17: choose $[\text{txt, m, n}]$ lists the characters in txt in positions congruent to $n \pmod{m}$. ($m$ and $n$ were reversed)
*page 419, lines 6; 8: change $]$ to $)$
*page 428: in the three displayed Maple commands, change $\text{mult}$ to $\text{mul}$

(last updated 7/8/2002)