Errata File (November 2014)
Cryptography and Network Security: Principles and Practice, Sixth Edition
William Stallings

SYMBOLS USED

| ti = ith line from top; bi = ith line from bottom; Fi = Figure i
| X -> Y = replace X with Y; Ti = Table i; Pi = Problem i

The documents and papers referenced in the book as being at the Premium Web site have been moved to https://www.box.com/Crypto6e

---

November LIST

PAGE CORRECTION

248 b2: extra right parenthesis at end of equation

451 b17: use authentication -> user authentication

APRIL LIST

68 b18: depicts the structure -> depicts the encryption structure
   b16: L_0 -> LE_0 R_0 -> RE_0
   b16: L_{i-1} -> LE_{i-1} R_{i-1} -> RE_{i-1}

82 b2: encryption -> decryption

97 t9: not only calculate -> not only calculates

103 F4.2: The order of the categories should be reversed, starting with groups from top to get to fields at bottom. A clearer illustration is provided at https://www.box.com/shared/static/3g06ez9qqmyr7wh46ngl.pdf

145 Equation 5.4: missing an end parenthesis in second line of equation

153 T5.4: Because 10th round of AES does not contain mix column, 4th column of the 2nd last row should be kept blank.

221-222: the indentation for the code snippets for initialization, initial permutation, and stream generation for RC4 need to be adjusted so that all of the code executes within the loop.

243 t8: $0 \leq A < M$
   Eq 8.9: i = 1 not i – 1 under Sigma

244 b14, last word in line: modulo -> and

292 t11: Y^A -> Y_A

320 t2: Chapter 21 -> Chapter 22

325 t13: Appendix 11A -> Appendix U
Equation 11.1 -> Equation 1

335 $SHR^n(x)$ = right shift of the 64-bit argument x by n bits with padding by zeros on the left

346 F11.18a: underneath third column: Lt[2,3] -> L[2,3]

400 t15: $p - 1 \equiv 0 \pmod{q}$

527 b18: secret encryption key -> symmetric encryption key
(Note: the meaning is the same but this is consistent with the following bullet item)

579 t22: to the AS -> to the STA

636 t6: IP address 1.2.3.10 -> IP address 1.2.3.101

637 t12: entry made in the SA -> entry made in the SAD

A current version of this file, named Errata-Crypto6e-mmyy, is available at https://www.box.com/Crypto-Errata

---