Errata File (June 2012)
Cryptography and Network Security: Principles and Practice, Fifth Edition
William Stallings
(Prentice-Hall, ISBN 978-0-13-609704-4)

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

JUNE LIST

PAGE CORRECTION

53 key for second example should begin with *pft*

369 equation for MAC: MAC = C(K, M)

487 b15: Part Four -> Part Six

566 P17.5: should be x ⊕ x = 1; x ⊕ 0 = x

MAY LIST

47: The set of three equations should be

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$

$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$

$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

The plaintext row vector should start with p_1

99 P3.10: TDi(R||L) refers to the decryption algorithm

111 T4.3: second expression under commutative law, right-hand side should have a x instead of a +
T4.3, last row: *a a z* -> *a z*

113 concise Euclidean algorithm: assumes integer a, b, with $a \geq b > 0$

114 1st word, 2nd paragraph: Observer -> Observe

115 upper table, row n: r_{n-3} -> r_{n-1} row n+1: r_{n-2} -> r_n

131 T4.6b: The “1” in the last column should also be shaded

145 t2: nonzero integer -> positive integer

160 2nd line, last paragraph: **X** and **B** -> **X** and **Y**

167 F5.9: the bottom labels w44 w45 w46 w47
should be w40 w41 w42 w43

169 T5.3: the Key Word w2 is missing the last element, d6

172 T5.4: the last Round Key matrix is transposed

201 F6.4 caption: CFB -> CBC

205 t4: shift register -> encryption function
the OFB encryption formula: C_{j-i} should be changed to C_{j-1}

206 decryption definition for I_j (right column of the table, second line)
should read: $I_j = O_{j-1}$

235 t11: T is tranferred to T -> K is transferred to T
in the first block of code, indent the two lines below the "for i" line
in the second block of code, indent the last line ("Swap...")

252 first condition under "second property":
$a^q = 1 \pmod p$ -> $a^q \equiv 1 \pmod p$

281 F9.7b: In boxes 5 and 7: 2006 -> 2066

299 t18: 1012 -> 10^{12}

313 line following Equation 10.5: delete definition of alpha

317: $(\lambda + 1x)_R$ -> $(\lambda + 1)x_R$

325 P10.5: Section 10.2 -> Section 10.1

335, b14,b15: $2^{b/n}$ should read 2^{b-n} on both lines

336 b4: collision -> preimage

347 b11: 512-bit -> 1024-bit

351 Number 4. Instead of all a's, it should a, b, c, d, e, f, g, h

373 t12: tab is 32 bits -> tag is 32 bits

381-383: The main key is labeled K and is of length k
keys K1 and K2 are b bits in length, not n bits

383 b13: E(K_2,(M || T). -> E(K_2,(M || T)).

384 t3: there security -> there are security

387 F12.10b: =Yn* should be changed to =Y1||Y2||…||Yn*

388 8. Let X= X1||X2||… ||Xn-1||Yn* -> 8. Let Y= Y1||Y2||… ||Yn-1||Yn*

408 P13.6, Algorithm 2: exponent should be (p – 1)/q

427 b7: initial four -> initial five

437, b19: 2822 -> 4949

441, F14.17, Step 1: A -> ID_A

466 T15.3(c): Seq ≠ -> Seq #

471: step 6 should be:
$E(PU_a, [N_b \,||\, E(PR_{auth}, [N_a \,||\, K_s \,||\, ID_A \,||\, ID_B])])$

497 b2: include AES in the list

506 b6: search engines -> some search engines.
b7: Add: Google provides HTTPS as an option:
https://google.com redirects to https://encrypted.google.com

512 T16.3: hmac-md5 and hmac-md5-96 use MD5, not SHA-1

539 t21: STA and SP -> STA and AP

663 b1: should be: return [(o & 2)>>1, o & 1]

702, DENN81: the co-author is Sacco, G.

710, WOO92b: April -> March

A current version of this file, named Errata-Crypto5e-mmyy,
is available at http://www.box.net/shared/7978zk32dk
