ERRATA for Cryptography Book—Complete List for 3rd Printing (2013)

Note: The following list of errata has been incorporated in the third printing of the book. They should be penciled in (at least before reading the affected chapters) if you have either the 1st or 2nd printings (both are identical).

~~~~~~

NOTATION INDEX (inside front cover):
□ (symbol page 1; Line 2) Delete last "□" at end of Line
$\mathscr{C}$(symbol page 2; Line –11) Delete "$\mathscr{K}$" at end of Line
$|A|$ (second page, line 6) Change "cordinality" to "cardinality"

~~~~~~

TABLE OF CONTENTS: page xii
Change third to last item from
"Index of Corollaries, Lemmas, Propositions, and Theories"
To "Index of Corollaries, Lemmas, Propositions, and Theorems"
Same change is needed on pages 623 and 624 (heading appears once on each page)

~~~~~~

CHAPTER 1:
Page 2: FIGURE 1.1, under the text "Bob, intended" insert "recipient"; also change the upper right instance of "Encryption Key" to "Decryption Key"
Page 7: Second paragraph, last symbol "σ_2" should be "σ_1"
Page 8: FIGURE 1.4, change "f^1" to "f^{-1}"
Page 20: Change "1973" to "1977"
Page 21: Para 3, line 2 Change "if one knows how a message gets encrypted," to "if one knows the encryption scheme,"

~~~~~~

CHAPTER 2:
Page 49: Algorithm 2.1, displayed equations. The indices on the some of the q's in the displayed equations are off; change as follows:

$$\begin{array}{llll}
b & = q_2 r_1 + r_2, & 0 \le r_2 < r_1 & \\
r_1 & = q_2 r_2 + r_3, & 0 \le r_3 < r_2 & \to r_1 = q_3 r_2 + r_3 \\
 & \cdots & & \\
r_{n-2} & = q_{n-1} r_{n-1} + r_n, & 0 \le r_n < r_{n-1} & \to r_{n-2} = q_n r_{n-1} + r_n \\
r_{n-1} & = q_n r_n + 0 & & \to r_{n-1} = q_{n+1} r_n + 0
\end{array}$$

The corresponding changes in the proof of Theorem 2.6 on pages 50-51 should be made: Basically, each instance of the form $r_{i-1} = q_i r_i + r_{i+1}$ should be changed to $r_{i-1} = q_{i+1} r_i + r_{i+1}$
Page 51: Exercise for the Reader 2.5, part (a), last Line, change "1165" to "1665"
Page 54: (Shaded) Propostion 2.8, part (c) (transitivity), change "$b \equiv a(\bmod m)$" to "$b \equiv c(\bmod m)$"
Page 55: Statement of Propostion 2.9 (shaded), line 2: change "$\cdots, n-1\}$" to "$\cdots, m-1\}$"
Page 56: (Shaded) Propostion 2.10,
part (a), change "$a + a' \equiv b + b'(\bmod m)$" to "$a + b \equiv a' + b'(\bmod m)$"
part (d), change "$a - a' \equiv b - b'(\bmod m)$" to "$a - b \equiv a' - b'(\bmod m)$"

Page 57: Proof of Proposition 2.10
part (a), change "$a + a' - (b + b') = (a - b) + (a' - b')$" to $a + b - (a' + b') = (a - a') + (b - b')$
and "$a + a' \equiv b + b'(\bmod m)$" to "$a + b \equiv a' + b'(\bmod m)$"
ALSO Part(c), line 2: change "$(a - a')b = a(\ell m) + (km)b = [a\ell + kb]m$" to "$(a - a')b' = a(\ell m) + (km)b' = [a\ell + kb']m$"
Page 61: line 3, change "relative" to "relatively"

Page 63: line 11, raise the decimal to a multiplication, i.e., change “$36.[2,-1,2]$” to “$36\cdot[2,-1,2]$”

ALSO line 12, 14, 15: change all three instances of “ [2, -1, 1]” to “ [2, -1, 2]”

ALSO line 15, 16: change all two instances of “ [0, -75, 147]” to “ [0, -75, 148]”

Page 69: line above displayed equation (2.8), add the following sentence right before “We claim that…”: “e_i is just the inverse of N/n_i (mod n_i)”

Page 82: item 55(a), line 3, change “11|930391” to “11|193039”

ALSO item 55(b), line 3, change “7|4001006002” to “7|2006001004”

~~~~~~

CHAPTER 3:

Page 94: Definition 3.1, line 7, change “$d_\kappa : \mathscr{P} \to \mathscr{C}.$” to “$d_\kappa : \mathscr{C} \to \mathscr{P}.$”

Page 95: Example 3.1(a), Line 3, change “sequence” to “sequences”

Page 96: Exercise for the Reader 3.1 (a), Line 1, change “$\phi_{\alpha,\beta}^{-1}$” to “$\phi_{\alpha,\beta}^{-1}(y)$”

Lines 2-3, bring “$\phi_{\alpha,\beta}$” and “(x)” together into “$\phi_{\alpha,\beta}(x)$”

Page 96: footnote, change two occurrences of “$\phi_{\alpha,\kappa}$” to “$\phi_{\alpha,\beta}$”

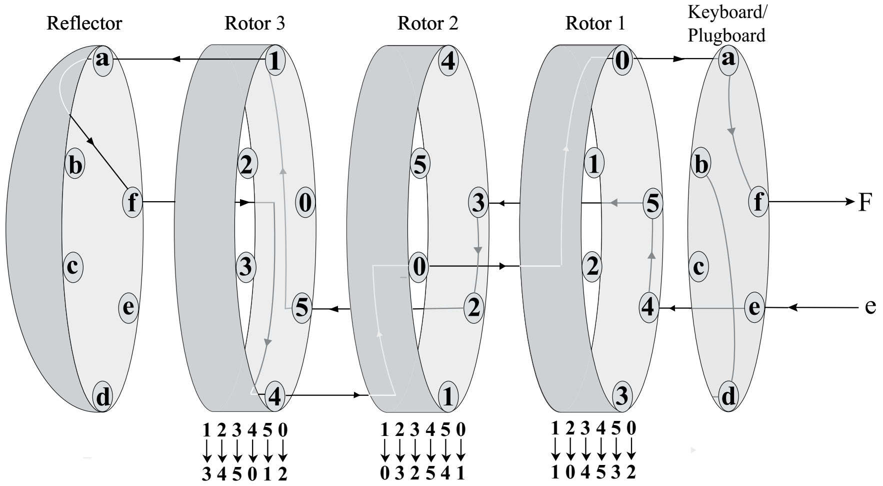
Page 98: Example 3.3, part (b) (i) Line 2 change “$\mathrm{e} \mapsto \mathrm{X}$” to “$\mathrm{e} \mapsto \mathrm{Y}$”

and Line 5, change “$\phi_{\alpha,\beta}(4) = 23$” to “$\phi_{\alpha,\beta}(4) = 24$”

Page 113: Line -11, change “mod 20” to “mod 10”

Page 120: Longest paragraph, Line 9, change “ciphertext letter” to “ciphertext encryption”

Page 121: Modify Figure 3.12 to what is shown on the next page:


Reflector
Rotor 3
Rotor 2
Rotor 1
Keyboard/
Plugboard
a
b
f
c
e
d
1
2
0
3
5
4
4
5
3
0
2
1
0
1
5
2
4
3
a
b
f
c
e
d
F
e
1 2 3 4 5 0
3 4 5 0 1 2
1 2 3 4 5 0
0 3 2 5 4 1
1 2 3 4 5 0
1 0 4 5 3 2

Page 121: Paragraph (b), Line 1, delete “counter-”

Page 121: Paragraph (b), Line 3, change “turns advances one” to “turns/advances another”

Page 121: Paragraph (b), Line 4, change “number 5” to “number 1”

Page 122: Line 1 below caption, change “it may be Rotor 2 that is” to “suppose that $\rho(2)=1$ and the rotor is”

Page 122: Lines 3-4 below caption, delete “resulting”

Page 122: Line 11 below caption, change “and this” to “and the”

Page 128: Exercise 7 parts (a) and (b), plaintexts, remove space between two asterisks

Page 128: Exercise 5(a): Change “three-row, eight-column” to “four-row, seven-column”

Page 129: Exercise 8 parts (a) and (c), plaintexts, remove space between two asterisks

~~~~~~

CHAPTER 4:

Page 148: Example 4.2, Solution: Part (a), in last matrix, change “17” to “18”

Page 149: (shaded) Proposition 4.1, part(c), line 2, change “*AB* + *AC*” to “*AC* + *BC*”

Page 154: Exercise for the Reader 4.5, change the row 1, col 2 entry from “6” to “ –6”

Page 154: footnote, line -2, change “$\det(d_{ij})$” to “$\det(A_{ij})$”

Page 155: very last line: change (last) matrix: “$\begin{bmatrix} 1 & -3/2 \\ -1 & 1 \end{bmatrix}$” to “$\begin{bmatrix} -1 & 3/2 \\ 1 & -1 \end{bmatrix}$”

Page 162: Para 2, line 4 Change “All of the contemporary ciphers of the computer age are block ciphers” to “All contemporary ciphers are block ciphers or stream ciphers”

~~~~~~

CHAPTER 6:

Page 223: Last Line of Shaded Box, change “$\text{floor}(c_k / b^k) = \lfloor c_k / b^k \rfloor.$” to “$\text{floor}(R/b^k) = \lfloor R/b^k \rfloor.$”

Page 223: 2nd line after “Solution:” paragraph. Change “128 + 32 + 16 + 8 + 2 + 1 = 187” to “128 + 16 + 8 + 2 + 1 = 155”

Page 228: last 2 paragraphs (starting with line –10), change all six instances of “$c_s - d_s$” to “$d_s - c_s$”

Page 233: line 5, displayed math item, the row of numbers on the top need to be shifted one letter to the right:

change “$\begin{array}{ccccc} -1 & -1 & -1 & & \\ & 6 & F & A & A \\ & 4 & F & E & D \\ \hline & 1 & F & B & D \end{array}$” to “$\begin{array}{ccccc} & -1 & -1 & -1 & \\ & 6 & F & A & A \\ & 4 & F & E & D \\ \hline & 1 & F & B & D \end{array}$”

Page 239: Algorithm 6.5, Step 3 should be the last Line that is shaded (i.e., remove shading from the proof).

~~~~~~

CHAPTER 7:

Page 263: Example 7.2, Line 3 change “ = 2A8” to “=2D9”
Make the same change on Line 4 of Step 2

~~~~~~

CHAPTER 8:

Page 294: line 9 after (shaded) theorem, change “304-digit” to “305-digit”
ALSO, line 10 after (shaded) theorem, change all three instances of “n_{364}” to “n_{305}”

Page 294: Paragraph after Theorem, Line 11, change “$\pi(10^{52})10^{52}$” to “$\pi(10^{52}) \sim 10^{52}$”

Page 295: Line 3, change “$\pi(10^{49})$” to “10^{49}”

Page 295: end of Line 5, change “$/10^{50} \approx 1/128.$” to “$/9 \cdot 10^{49} \approx 1/115.$”

Page 295: end of Line 8, change “$1/64.$” to “$1/58.$”

Page 298: para. 3, line 4, change “these to” to “these two”

Page 299: Change the final subscript “n” to “k”, i.e., change each of the four instances of “p_n” to “p_k” and each of the three instances of “α_n” to “α_k”

Also, on Line 3 after Prop. 8.3, change “$3^3 \cdot 7^2$” to “$2 \cdot 3^3 \cdot 7$” and on the next Line, change “$\phi(3^3 \cdot 7^2) = (3-1) \cdot 3^2 \cdot (7-1) \cdot 7^1$” to “$\phi(2 \cdot 3^3 \cdot 7) = (2-1) \cdot 2^0 \cdot (3-1) \cdot 3^2 \cdot (7-1) \cdot 7^0$”

Also, in Exercise for the Reader 8.3, add “$, \phi(6624)$” before the period.

Page 304: Line 4 in shaded Theorem, change “and *t* is” to “and *s* is”

Page 306: Example 8.6, line -5change "58(mod 29)" to "58(mod59)"

Page 307: Very first displayed equation, after first “=” sign, replace the two occurrences of “$\text{ord}_2(59)$” with “$\text{ord}_{59}(2)$”

Page 322: Line 8 (part (f)), change “*n* = 29,791” to “*n* = 961”

~~~~~~

CHAPTER 9:

Page 333: line 4, change "first on, first off" to " first on, last off "

Page 333: Para After Boxed Def 9.1: Change “The trapdoor terminology stems from the fact that” to “An important special case is a **trapdoor function**, which”

Page 335: Example 9.1, line 2, change "$\phi(52) = 26$" to "$\phi(52) = 24$"and then on line 3, change “half” to “nearly half”.

Page 342: Para 3, line 7 Change “use primes that do not” to “use a prime p such that $p-1$ does not”

Page 343: Line 2, change “1999” to “2095”

Page 345: Exercise 9.3, (a) last line, change “2569” to “2659”

Page 346: Algorithm 9.4, Encryption Scheme, last line, change “ $e_\kappa(m)$ ” to “ $e_\kappa(P)$ ”

Page 346: Algorithm 9.4, Decryption Scheme, Line 2, change “the *c*” to “the *C*”

Page 347: Exercise for the Reader 9.5(b), after “a = 212” insert “, and Bob chooses his to be *b* = 954”

Page 348: Example 9.6, Line 1, change “Example 6.5” to “Example 9.5”

Page 361: Exercise 3, Line 3, change “smallest primitive” to “smallest odd primitive”

~~~~~~

CHAPTER 12:

Page 477: Example 12.12, line 2: Change “ = 345, 283” to “= 345,283” (i.e., remove the space)

~~~~~~

APPENDIX C:

Page 516: Soln to EFR 1.5(a), line 1, change: “letter b” to “letter a”

Page 518: Soln to EFR 2.4, change very last equation from “gcd(1665,755) = 5” to “gcd(1665,910) = 5”

Page 519: EFR 2.8 second-to-last Line, change “ $\{0,1,2,\cdots,m\}$ ” to “ $\{0,1,2,\cdots,m-1\}$ ”

Page 520: Soln to EFR 2.12(a), Step 1 lines 2/5, change: “(mod 4)”/”(mod 9)” both to “(mod 3)”

Page 522: Soln to EFR 2.15, line -4, change “ M/n_i ” to “ N/n_i ” in the displayed equation

Page 523: Line 1, change “ $5^{-1}=21$ ” to “ $21^{-1}\equiv 5$ ”
Line 2, change “ $\phi_{5,21}^{-1}(y)\equiv 21(y-11)\equiv 21y+3$ ” to “ $\phi_{21,4}^{-1}(y)\equiv 5(y-4)\equiv 5y+6$ ”

Page 527: EFR 4.4, Line 2, change “same number of rows” to “same number of columns”

Page 529: Answer to EFR 4.7(b), for A + B’s answer, change the row 2, column 2 entry from “1” to “9” (last two matrices)

Page 530: EFR 2.10 in matrix C, change row 3 column 1 entry from “7” to “17”
Make the same change in this matrix that reappears 3 Lines below (U = …)

Page 537: EFR 6.3, line 5, change "[101101] + [001111]" to "[101101] – [001111]"

Page 545: EFR 8.1(a), Line 4, change “ 2^{300-1} ” to “ $2^{300}-1$ ”
Line 5, change “ $2^{299-1}\approx 5.093\times 10^{89}$ ” to “ $2^{299}-1\approx 1.019\times 10^{90}$ ”
Line 6, change “ $\pi(2^{299})-\pi(2^{298})$ ” to “ $\pi(2^{300})-\pi(2^{299})$ ”
Line 8, change “ $2^{299}/\ln(2^{299})-2^{298}/\ln(2^{298})\approx 2.449\times 10^{87}$ ”
to “ $2^{300}/\ln(2^{300})-2^{299}/\ln(2^{299})\approx 4.882\times 10^{87}$ ”

Page 545: EFR 8.1(b), Line 4, change “ $2.449\cdots 1/2080$ ” to “ $4.882\cdots 1/104$ ”

Page 546: line right above EFR 8.3, change “ 1^{80} ” to “ 1^{28} ”

Page 546: EFR 8.3, $\phi(208)$ Line, change “ $\cdot 5^0=96$ ” to “ $\cdot 13^0=96$ ”

Page 547: line 6, change “(mod n)” to “(mod m)” ALSO on line 7 and 8, change “ a^{K-1} ” to “ a^K ”

Page 547: EFR 8.5, Line –3, change “ $5\cdot 4+17$ ” to “ $5\cdot 400+17$ ”
Line –2, change “ $1\cdot 13\equiv 933$ ” to “ $1\cdot 13^{17}\equiv 933$ ”

Page 547: EFR 8.6 part b, the table entry for a=4, k=5, change “1” to “7”.

Page 548: EFR 8.7(a), Line 2, change “ $\phi(334)=166$ ” to “ $\phi(\phi(334))=\phi(166)=82$ ”

Page 550: EFR 9.1(a), Line 5, change “ $2^{13}\equiv 23$ ” to “ $2^{13}\equiv 55$ ”

Page 551: EFR 9.3(b), Line 4, change “ 1903^{2569} ” to “ 1903^{2659} ”

~~~~~~

APPENDIX D:

Page 570: item 11., (b) At the end of the paragraph add the following:
“Alternatively, the fact that f is onto follows from the result of Exercise 6(a) and the fact that f is one-to-one (which was proved in Part (a)).”

Page 572: item 25., third-from-bottom Line, change “cba” to “cab”

Page 573: item 9., (a), change “q = 22” to “q = 33”

Page 574: Answer to 15(b): line 4, change “ $4=12-1\cdot 8=12-1\cdot 44$ “ to “ $4=12-1\cdot 8=12-1\cdot(44-3\cdot 12)$ “
~~~~~~

Page 575: item 21, in rightmost (fourth) table, change "+" to "$\times$"
Also, in the Line 3 of that table, change the last "3" entry to "2"
Item 27, (b), change "$3-2\equiv 7 \Rightarrow\ x\equiv(7^{-1}\cdot 7\equiv 7\cdot 7\equiv 49\equiv)\ 1$" to
"$3-2\equiv 1 \Rightarrow\ x\equiv(7^{-1}\cdot 1\equiv 7\cdot 1\equiv)7$"

Page 576: Soln to Exercise 33(c), change: "$\equiv 677\cdot 225\equiv 789(\mathrm{mod}1353)$" to "$\equiv 677\cdot 1225\equiv 1289(\mathrm{mod}1353)$"

Page 576: item 35(b) Delete whole sentence, and replace with:
"Since *d* = gcd(15,51) = 3|21, the congruence has 3 solutions. To find them, Algorithm 2.3 first has us solve the congruence $(15/3)y\equiv(21/3)(\mathrm{mod}\,51/3)$, or $5y\equiv 7\,(\mathrm{mod}17)$, which, when multiplied by $5^{-1}\equiv 7\,(\mathrm{mod}17)$, yields the (unique) solution $y\equiv 15(\mathrm{mod}17)$. The solutions of the original congruence are now {7, 7 + 51/3, 7 + 2(51/3)} = {15, 32, 49} (mod 51)."

Page 577: item 37(a), line 1, change "2|6" to "2|28"
Page 577: item 39(c), Change "$x=3446(\mathrm{mod}\,4290)$" to "$x=1886(\mathrm{mod}\,2730)$"
Page 579: line 2, change "a gcd(*a*,*c*)" to "*a*gcd(*b*,*c*)"
Page 582: item 5(a), change"TALHTPEIRAOOSNCSWEIIENLD" to: "TSORHSNOEIWCANIESALESTLDAIPX"
Page 582: item 7(a), third-to-last Line, change "$2\alpha+5\equiv 15\Rightarrow 2\alpha\equiv 10\Rightarrow\alpha\equiv 5$" to "$2\cdot 5+\beta\equiv 15\Rightarrow\beta\equiv 5$"
Item 7(c), Delete the last sentence "This …" and replace with the following:
"This yields $13\alpha\equiv 13(\mathrm{mod}\,26)$. Using Algorithm 2.3, the 13 solutions are $\alpha=1,3,\cdots,25$. We can rule out $\alpha=13$ since the key (α,β) must satisfy $\gcd(\alpha,26)=1$. We then test each of the remaining values for α to decrypt the ciphertext until we get something that makes sense. When we get to $\alpha=7$, the key $(\alpha,\beta)=(7,9)$ produces the meaningful decryption: grandcentralstation"

Page 588: item 7, change "$A^{-1}=\frac{1}{34}\begin{bmatrix}5 & -6\\ 4 & 2\end{bmatrix}$" to "$A^{-1}=\frac{1}{34}\begin{bmatrix}5 & 4\\ -6 & 2\end{bmatrix}$"

Page 588: Answer to 13(a): Change "$\begin{bmatrix}1 & 5\\ 3 & 0\end{bmatrix}$" to "$\begin{bmatrix}4 & 1\\ 3 & 4\end{bmatrix}$"

Page 591: item 27., line 5, change "$\sum_{k=1}^{m}(a_{ik}+b_{kj})c_{kj}$" to "$\sum_{k=1}^{m}(a_{ik}+b_{ik})c_{kj}$"

Page 596: item 3(b), line 2, insert "170," after "167,"
Page 596: item 9

(d) Change "12,587 = 12202101" to "12,587 = 122021012"
(e) Change "28,000 = 11021020" to "28,000 = 1102102001"
(f) Change "150,269 = 21122010" to "150,269 = 21122010112"

Page 596: item 11(a) At the ends of the answers to the three sub items append the following:
end of answer to sub item (i), append: "(bin); 00 06 04 OD (hex)"
end of answer to sub item (ii), append: "(bin); OC 04 13 (hex)"
end of answer to sub item (iii), append: "(bin); 0B 08 00 08 12 0E 0D (hex)"

Page 596: item 15(b) Change "56100010" to "56100013" and change "12,091,400" to "12,091,403"
Page 597: item 17(d) Add (right after "(d)") "[20 7 11 20]"
Page 601: items 1 and 3, change all instances of "$\to$" to "$\sim$" (5 changes)
Page 601: item 3(c), change "7216" to "7.7216"
Page 602: item 19(b)(ii) change "$\mathrm{ord}_{12}(2)$" to "$\mathrm{ord}_{13}(2)$"
Page 604: item 1(c), line 1, change "277^{333}" to "277^{603}"
Item 3(b), change "*B* = 300" to "*B* = 124"

~~~~~~

Acknowledgement: I sincerely thank the following individuals for their help detecting and correcting these oversights: Arash Aghazadeh, Jaime Aguilar, Jesus Arevalo, Matt Azer, Gerrardo Barajas, Brian Cabanas, John Cortese, Jason De Leon, Jarret Dixon, Edwin Espinosa, Carolyn Garcia, Aaron Hoffman, Isabel Leon, Amanda Lobello, Kevin Long, Frank Miles, Dien Nguyen, Chris Torres, Martha Zambrano, and Stacy Zeljak
~~~~~~