Errata (Handbook of Applied Cryptography)

The Handbook was reprinted (5th printing) with corrections and various minor changes in August 2001. The 4th printing is identical to the 3rd printing. Errors that were not corrected in the 3rd and 4th printings are listed here. Additional Errors that were corrected in the 3rd and 4th printing, but which remain in the 1st and 2nd printings are listed below.

Notation:

- An asterisk * denotes additions made in the most recent updates.
- Subscripts are denoted by "_". Thus, a_{i} denotes "a sub i".
- Exponents are denoted by "^". Thus, a^{i} denotes "a to the power i".

Errata (5th printing) *Last updated: September 28, 2011*

Page 83, Iteration 1: In the assignment for h(x), change "+1" to "+x". Also, in Iteration 2, change "+1" to "+x" in the assignment for g(x).
(Reported on Aug 28, 2001 by Linda Maas and on July 10, 2006 by Joshua Nekl)

Page 215, Example 6.70: "R[511]" should be "T[511]".
(Reported on Feb 6, 2002 by Sebastian Mrowiec)

---

* Page 236, Note 7.37: delete "(fixing s bits eliminates 2^s entries)".
(Reported on Jul 24, 2011 by Robert Spielmann)

Page 241, 3rd line of paragraph following Definition 7.53: "i, i+s, i+2s,..." should be "i, i+t, i+2t,...".
(Reported on Nov 22, 2001 by Nelson Uto)

---

* Page 299, Algorithm 8.30, step 1(c): The error vector z should have *exactly* t 1's.
(Reported on Jul 7, 2011 by Michael Noisternig)

Page 451, Note 11.50: We don't know of a square-root algorithm to find the pair (l,t). To correct, delete "based on the birthday paradox (see S2.1.5)" and replace "O(sqrt(e))" by "O(e)".
(Reported on Aug 27, 1999 by Francois Grieu)

Page 468, Example 11.99: "p = 3 (mod 4)" should be "p = 3 (mod 8)".
(Reported on Feb 18, 2002 by Lars Knudsen)

---

* Page 478, Step 1(a) of Algorithm 11.128: Delete " and the discrete logarithm problem in Z^*_q is intractable".
(Reported on Jul 8, 2011)

---

* Page 481, Algorithm 11.134: Delete step 2.
(Reported on Jul 7, 2011 by Michael Noisternig)

Page 708, reference [118]: "Algebric" should be "Algebraic".
Page 485, line 2 of Section 11.6 Notes: "Diffie and Hellman [347]" should be "Diffie and Hellman [345]".
(Reported on Oct 4, 2001 by Chris Mitchell)

Page 601, Algorithm 14.32, Step 1: A should have $2n+1$ words instead of $2n$.
(Reported on Sep 6, 2011 by Marco Macchetti)

Page 610, Note 14.64: When Algorithm 14.61 terminates, it may not be the case that |D| < m, so it is not guaranteed that z lies in the interval [0,m-1]. The following changes guarantee that z lies in [0,m-1].
(1) At the end of the first line of step 6 of Algorithm 14.61, add "If B>0 then A <-- A+y and B <-- B-x.
(2) At the end of the second line of step 6 of Algorithm 14.61, add " If D>0 then C <-- C+y and D <-- D-x.
(3) When Algorithm 14.61 terminates, set z=D+m if D<0, and z=D otherwise.
(Reported on Sep 6, 2009 by James Muir)

---

* Page 624, third line of Section 14.6.3(ii): e_N, e_i, should be x_N, x_i.
(Reported on Jul 7, 2011 by Michael Noisternig)

Page 708, reference [118]: "Algebric" should be "Algebraic".
(Reported on January 10, 2008 by Eric Fung)

Errata (3rd and 4th printing) *Last updated: January 13, 2001*

Page 58, Example 2.51(ii): Change "of degree k" to "of degree at most k".
(Reported on May 26, 1998 by Huaxiong Wang)

Page 73, step 7 of Algorithm 2.149: Replace step 7 by "If a_{1}=1 then return(s); otherwise return (s * JACOBI(n_{1},a_{1}))."
(Reported on February 18, 1999 by Serge Mister)

Page 121, first line: Replace "y" by "y_{i}".
(Reported on October 3, 1997 by Lars Knudsen)

Page 126, 8th line of first paragraph: "99-digit" should be "179-digit".
(Reported on Mar 20, 2000 by Gabriel Belingueres)

Page 153, step 1.2. Change "less than" to "less than or equal to".
(Reported on Jan 9, 2001 by Benne de Weger)

Page 183, part (v) of Example 5.31. The example is wrong (A(3)=78).
Change "d=3" to "d=8", "A(3)=35" to "A(8)=100" and "-6.9434" to "3.8933".
(Reported on Feb 18, 1998 by Ching Yen Choon)

Page 231, Properties of the CFB mode of operation: In list items 2, 3 and 4, change "ceiling(n/k)" to "ceiling(n/r)" (3 occurrences in total).
(Reported on November 4, 1998 by Erkko Lehtonen)

Page 231, Note 7.24: Change "permutations on n elements" to "permutations on 2^n elements".
(Reported on March 13, 2006 by Nelson Uto)

Page 236, Fact 7.39 Justification, 5th last line: Change "P_{i}" to "P_{j}"; 3rd last line: Change "P_{i}=B_{j}" to "P_{j}=B_{i}".
(Reported on October 3, 1997 by Lars Knudsen)

Page 259, 3rd last line: Change "32 x 16" to "32 + 16".
(Reported on May 3, 2000 by Kouichi Sakurai)

Page 269, 4th last line: Change "bits of w suffice" to "bits of y suffice".
(Reported on May 19, 1998 by Renato Menicocci)

Page 270, OUTPUT line of Algorithm 7.115: Change "plaintext" to "ciphertext".
(Reported on Aug 19, 1998 by Lehtonen Erkko)

Page 273, lines 3 and 4: Change "an n-bit cipher" to "a cipher with N=2^m ciphertexts". Also change "O(n" to "O(N" (3 occurrences).
(Reported on Aug 27, 1997 by Vincent Rijmen)

Page 281, second line: Change "128" to "512".
(Reported on May 21, 1997 by Lars Knudsen)

Page 287, 7th last line: After "Then it can be shown that", add "there exists an i in [1,s] such that a^{{2^i}t} \equiv 1 (mod n) and". In 4th, 6th and 7th last lines, replace "s-1" by "i-1" (3 occurrences).
(Reported on Nov 27, 1997 by Niels Provos)

Page 311: Plaintext-aware encryption does not imply semantic security. The following changes should be made:
First line after Fact 8.61: Change "An even stronger" to "Another".
First line after Definition 8.62: Replace with "In the `random oracle model', the property of being plaintext-aware is a strong one - coupled with semantic security, it can be shown to imply that the encryption scheme is non-malleable and also secure against adaptive chosen-ciphertext attacks."

Fifth line after Definition 8.62: add "and semantically secure" at the end of the sentence.
Page 312, second line after Figure 8.1: Add "and semantically secure" after "plaintext-aware".
(Reported on Oct 22, 1997 by Yiannis Tsiounis)

Page 339, 5th line after Table 9.3: Change "block ciphers not do" to "block ciphers do".
(Reported on September 25, 1998 by Rolf Oppliger)

Page 346, Algorithm 9.49: For round 2 and round 3, change "s[j])" to "s[j]".
(Reported on December 6, 1999 by Andreas Curiger)

Page 455, Note 11.66(ii): Replace "s1 - s2 \not\equiv 0 mod (p-1)" by the condition "gcd(s1-s2,p-1) = 1".
(Reported on September 27, 1999 by Anton Stiglic)

Page 466, 10th line of Note 11.95: Change "v_i = h(k_i)" to "v_i = h^{(2^k)-1} (k_i)".
(Reported on December 11, 1998 by Bryan Olson)

Page 466, 12th line of Note 11.95: Change "s_i = " to "s_{i+t} = ".
(Reported on December 9, 1999 by Ove Heigre)

Page 473, step 1(b) of Algorithm 11.113: Replace "p" by "pq". Phong Nguyen pointed out that the scheme as described is highly insecure. Also, in line 7 of Example 11.114 (page 474), replace "p=17389" by "pq".
(Reported on August 31, 1999 by Phong Nguyen)

Page 522, last line of step 4 of Mechanism 12.61: "mod p" should be "mod n".

Page 526, first line after Mechanism 12.71: Replace "at most t" by "less than t".
(Reported on October 12, 1998 by Rolf Oppliger)

Page 597, Algorithm 14.16: Delete step 3.
(Reported on Aug 27, 1997 by Danny De Cock)

Page 610, line 7 of Note 14.64: Change "m-D" to "m+D".
(Reported on Aug 14, 1997 by Andrew Waters)

Page 642, 13th line of (iv): Change the "1" in "This follows since x^{2^m} \equiv 1" to an "x".
(Reported on June 21, 1999 by Mats Naslund)

Errata (1st and 2nd printing) *Final update: November 4, 1998*

These changes have been incorporated into the 3rd and 4th printings.

Page 62, Definition 2.73: Change the definition to "A problem is NP-hard if there exists some NP-complete problem that polytime reduces to it".
(Reported on Mar 8, 1997 by Jeff Shallit)

Page 107, line 3 of Section 3.6.4: Change "1 <= i <= t" to "1 <= i <= r".

Page 126, 1st line of 4th paragraph: Change "Algorithm 3.2.6" to "Section 3.2.6".

Page 150, step 3 of Algorithm 4.53: Change "(2s" to "2(s".
(Reported on Jan 2, 1997 by Colin Boyd)

Page 150, fourth last line: Change "Section 9.53" to "Algorithm 9.53".

Page 166, seventh last line: Change "O((ln n)^8)" to ""O((ln n)^11)"

Page 169, line 3 of Section 5.1: Change "11.5.1" to "7.4.2".

Page 174, line 2 of Section 5.3.2: Change "Algorithm 11.5.1" to "Section 11.5.1".

Page 186, line 4 of Section 5.5.2: Change "Algorithm 8.55" to "Algorithm 8.56".

Page 270, Example 7.118: Change "M=B278C165 CC97D184" to "M=65C178B2 84D197CC" and "C=15E444EB 249831DA" to "C=EB44E415 DA319824".
(Reported by Ray Sidney)

Page 295, second last line: Change "Section 14.6.2" to "Section 14.6.3".

Page 314, 4th line of the 5th paragraph (on unbalanced RSA): Change "(say p)" to "(say q)".
(Reported on Feb 14, 1997 by Lewis McCarthy)

Page 336, last line of Section 9..3.4(ii): Change "t > n" to "t < n".
(Reported on March 20, 1997 by Rosario Gennaro)

Page 350, step 4(a), last lines of rounds 1, 2, 3 and 4: Change the "A_L" in the right side of the assignments to "E_L".
(Reported on March 4, 1997 by Frank Schaefers and on March 28, 1997 by Antoon Bosselaers)
For further information on RIPEMD-160, see the RIPEMD-160 Web page.

Page 456, Note 11.67(iii): Replace "Suppose" with "Suppose that p = 1 (mod 4) and"
(Reported on March 24, 1997 by Robert Zuccherato)
This error was carried over from an error in Corollary 2 of Bleichenbacher [153]. A corrected version of that paper is available at:
ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/ElGamal.ps

---

Page 526, displayed equation before Note 12.72: "cj" should be "ci".
(Reported on June 1, 1997 by Lewis McCarthy)

Page 702: Delete the paper by Syverson.
