Applied Cryptanalysis: Breaking Ciphers in the Real World

Errata

February 21, 2023

Most of the items listed here are minor typos and a few are simply clarifications of possible points of confusion. For the most significant errors, the page number is preceded by "*".

1. Page xiv: In the table, chapter 5 topics, change "Nostrasamus attack" to "Nostradamus attack".
2. Page 13: Last paragraph, second sentence, change "If the keyword is known" to "If the keyword length is known".
3. Page 18: In the second sentence after Table 1.8, change the key K from 110 100 001 to 110 100 101.
4. Page 23: Problems 9 and 10 are essentially the same.
5. Page 44: The displayed equation where the number of possible keys is computed should read: $(6!)^{25} \cdot (20!)^{75} \approx 2^{237} \cdot 2^{4581} = 2^{4818}$.
6. Page 52: First paragraph of Section 2.4, 3rd line, change "every" to "ever".
7. Page 52: The following paper expands on the Sigaba section (and provides more careful analysis of work factors, etc.): M. Stamp and W. O. Chan, SIGABA: Cryptanalysis of the full keyspace, *Cryptologia*, July 2007.
8. Page 62: Last paragraph, 5th line, change 0.000427 to 0.00427.
9. Page 71–72: Problem 15. The threshold of 0.1 refers to the numbers in Table 1.3, which are percentages. That is, the threshold is 0.1%, or, in decimal, 0.001.
10. Page 74: Problem 25, part b, remove the phrase "the index rotors are inserted in a fixed order," (under the assumptions of Section 2.4.3, the index rotors can be inserted in any order).
11. Page 76: Problem 29 begins "For each letter encrypted by the Sigaba cipher machine ...", but it would be more accurate to replace this with, simply, "For the Sigaba cipher machine ...".
12. Page 85: In Table 3.2 (the Berlekamp-Massey algorithm for binary sequences), the coefficients of the connection polynomial $C(x)$ can be taken mod 2.
13. Page 98: The shifted register fills that are displayed are simply the initial fills shifted as indicated, without the feedback bits computed using the polynomials, not the fills after one iteration of the algorithm, as implied by the preceding paragraph. To be consistent with the description, the fills should be

$$\begin{aligned}(X \gg 1) &= \texttt{0xef56df77}\\(A \gg 1) &= \texttt{0x8091a2b3}\\(B \gg 1) &= \texttt{0xbb2a1908}\\(B \gg 2) &= \texttt{0xdd950c84}.\end{aligned}$$

Note that when the attack is conducted, the actual fills after one iteration are recovered, which will include the feedback bits.

14. Page 108: In the second full paragraph, last line, change $j = 0 + S_0 + K_0 = 3$ to $j = 0 + S_0 + K_0 = 4$.

15. Page 127: In the sentence that reads, "Provided that the same key is used, the same plaintext block will always be encrypted to the same plaintext block, and vice versa", the second "plaintext" should be "ciphertext".

16. Page 152: In the 6th line from the bottom, replace "essential" with "essentially."

17. Page 152: In the 5th line from the bottom, replace "but it is can be" with "but it can be".

18. Page 175: In the second paragraph below Figure 4.19, change "and $\tilde{Z}_1$, (a putative value for Z_0)" to "and $\tilde{Z}_1$ (a putative value for Z_1)".

19. Page 175: Three lines above the displayed equation involving $M(A)$, change "for the string of bit" to "for the string of bits".

20. Page 204: Second-to-last line, change "Trudy can has" to "Trudy has".

21. Page 207: Second sentence below the second displayed equation, change "consists of $k + 1$ messages" to "consists of $k + 1$ blocks".

22. Page 209: In the second to last paragraph, change "Table 5.10" to "Table 5.4".

23. Page 210: MD4 algorithm, change Round0(Q, X), Round1(Q, X) and Round2(Q, X) to Round0(Q, W), Round1(Q, W) and Round2(Q, W), respectively.

24. Page 212, Table 5.4: The value of $\sigma(15)$ is 15, not 14.

25. * Pages 214, 217, and 221: To be consistent with the definition of Δ_j, we should have written $\Delta_{19} = (2^{25}, -2^5, 0, 0)$, not $\Delta_{19} = (0, 2^{25}, -2^5, 0)$. This error occurs on p. 214, equation (5.9), p. 217 in the second line after Table 5.6, and on p. 221 in the second line from the bottom.

26. * Page 217: Equation (5.13) should read $Q'_{12} = (Q'_8 + F(Q'_{11}, Q'_{10}, Q'_9) + X'_{12}) \lll 3$. Then the equation at the top of p. 218 relies on the fact that $X'_{12} = X_{12} + 1$.

27. Page 223: The first line of the large display in the middle of the page contains an extraneous closed parenthesis. To fix this, change $Q_6 = (Q_8 \lll 29) - Q_4 - X_8)$ to $Q_6 = (Q_8 \lll 29) - Q_4 - X_8$.

28. Page 235: In the fifth line above Section 5.4.4, change "ensures" to "ensure".

29. Pages 243 and 244: The last line on p. 244 is a repetition of the first sentence in the last paragraph on p. 243.

30. Page 257: In Problem 2, first line, change "and want to" to "and we want to".

31. Page 258: In Problem 4, the last sentence is not a question—change the "?" to ".".

32. Page 264: Problem 26, part b, does not work as stated, since the collision given in the problem uses the standard MD5 initialization vector, but to obtain colliding postscript files (as discussed in the text), a non-standard IV must be used.

33. Page 279: Delete $ab^{-1}a^2b$ from the displayed equation that appears four lines from the bottom of the page.

34. Page 281: Change "Bob computes the set $\{b^{-1}s_1b, \ldots, b^{-1}s_{n-1}b\}$" to "Bob computes the set $\{b^{-1}s_0b, \ldots, b^{-1}s_{n-1}b\}$". This appears near the middle of the page.

35. Page 293: Line 10, change "sets if polynomials" to "sets of polynomials".

36. Page 295: The first sentence of the first full paragraph, change "Bob sends Alice an encrypted as follows", to "Bob encrypts a message for Alice as follows".

37. * Pages 295–298: There are several equivalent ways to give the NTRU formulas, which is our excuse for an annoying inconsistency involving the constant p on these pages. To fix the problem, change $h(x) = f_q(x) \star g(x) \pmod q$ to $h(x) = pf_q(x) \star g(x) \pmod q$ in the following three places: The first line on p. 295, the first line following the displayed public key and private key on p. 295, and the displayed equation on p. 297. Also, replace g with pg in the following places (all on p. 298): The second displayed equation from the top of the page, equation (6.11), and both of the equations involving g that immediately follow (6.11).

38. Page 309: The last paragraph of Section 6.9 begins "We then consider". Change this to read "We then considered".

39. Page 309: Section 6.10 does not include any knapsack problems. A couple of problems can be found here: `cs.sjsu.edu/faculty/stamp/crypto/knapsackProblems.pdf`

40. Page 310: Problem 5, 4th line, contains a spurious space before the comma following $h(\text{"Bob"}, R_A, \text{PIN})$.

41. Page 313: Problem 29, first line, change "parameters are" to "parameters". Also in Problem 29, part c, change "such that $C_0(x)$ does not decrypt to $M_1(x)$" to "such that $C_1(x)$ does not decrypt to $M_1(x)$".

42. Page 319: The second full paragraph, second sentences says that we choose $B = 13$, but then we choose $B = 15$ later in the same paragraph. By our definition of B-smooth, $B = 15$ is correct.

43. Page 339: In equation (7.19), the $\pmod{R}$ is not necessary.

44. Page 339: The discussion of Montgomery multiplication might be clearer with the following modifications. Change the second paragraph to read:

    > Observe that
    > $$a'b' \pmod{N} = abR^2 \pmod{N}.$$
    > We would like this result to be in Montgomery form, that is, we want to have $abR \pmod{N}$, not $abR^2 \pmod{N}$. Since $RR' = 1 \pmod{N}$, multiplication by R' yields $abR^2R' = abR \pmod{N}$, that is, we can obtain the desired result by multiplying by R' and reducing the result modulo N. However, we want to avoid mod N operations, if possible. Therefore, what we chiefly need is an efficient method to convert $a'b'$ to $abR \pmod{N}$. The Montgomery algorithm provides just such a method.

    Also, change the first line in the third paragraph to read "Let $X = a'b'$ and compute".

45. Page 346: In Table 7.6, the line $s = (z + rN)/R \pmod{N}$ is incorrect. It can be fixed by deleting the $\pmod{N}$. Note that in equation (7.19), this offending $\pmod{N}$ is replaced by $\pmod{R}$, which will give the correct results, but the $\pmod{R}$ is not necessary (see the errata for page 339, above).

46. Page 350: In the 3rd paragraph, "(7.6)" appears twice. In both cases, it should instead read "Table 7.6".

47. Page 359: In problem 20, part b, the "modulus" $N = 12{,}423$ is not a product of two primes. Change the modulus to $N = 12{,}827$.

48. Page 359–360: In problem 21, change "private key bits d_1 through d_9" to "bits p_1 through p_9". The Brumley-Boneh attack recovers the bits of the factor p, not the bits of the private key d.