Information Security: Principles and Practice, 2nd edition

Errata

December 16, 2016

1. Page 22, ciphertext displayed near the bottom of the page: Change from

   `IRXUVFRUHDAGVHYHABHDUVDIR`

   to

   `IRXUVFRUHDQGVHYHQBHDUVDJR`.

2. Page 43, problem 3: Change the final letter in the ciphertext from `U` to `V`.

3. Page 44, problem 8: Insert a period after "This problem deals with the concepts of confusion and diffusion".

4. Page 45, problem 13: Delete the parenthetical phrase "(with respect to frequency counts)". Instead, simply swap adjacent elements of the key (i.e., elements of the permutation that represents the key) without regard to frequency counts.

5. Page 67, second paragraph: Change "...and an algorithm known a Rijndael" to "...and an algorithm known as Rijndael".

6. Page 68, third line: `MixColumn` is part of the linear mixing layer, *not* part of the nonlinear layer.

7. Page 69, second paragraph: Change the last sentence of this paragraph to "The overall operation is an invertible linear transformation, and, as with `ShiftRow`, it serves a similar purpose as the DES permutations."

8. Page 89, second line: Change "know" to "known".

9. Page 104, equation (4.5): The discriminant of this curve is 0 which implies that the curve does not match that in Figure 4.3 and hence is not a valid for use in ECC. For more details, see, for example, "elliptic discriminant" at Wolfram MathWorld
   `http://mathworld.wolfram.com/EllipticDiscriminant.html`
   A valid curve is

   $$y^2 = x^3 + 2x + 1 \pmod 5$$

   which yields

   $$\begin{aligned}
   x = 0 &\Longrightarrow y^2 = 1 \Longrightarrow y = 1, 4 \bmod 5 \\
   x = 1 &\Longrightarrow y^2 = 4 \Longrightarrow y = 2, 3 \bmod 5 \\
   x = 2 &\Longrightarrow y^2 = 13 = 3 \Longrightarrow \text{ no solution mod } 5 \\
   x = 3 &\Longrightarrow y^2 = 34 = 4 \Longrightarrow y = 2, 3 \bmod 5 \\
   x = 4 &\Longrightarrow y^2 = 73 = 3 \Longrightarrow \text{ no solution mod } 5
   \end{aligned}$$

   giving us the points

   $$(0,1)\ (0,4)\ (1,2)\ (1,3)\ (3,2)\ (3,3) \text{ and } \infty.$$

10. Page 116, problem 8, part b: Change "not not" to "not".

11. Page 117, problem 15: Change the last "provides" to "provide".

12. Page 120, problem 29, part b: This problem should ask for a non-trivial solution, since $M = 0$ and $M = 1$ always work.

13. Pages 120–121, problem 32: It should also be noted that the letter encoding uses base 95. For example, "To b" is encoded as

$$52 \cdot 95^0 + 79 \cdot 95^1 + 0 \cdot 95^2 + 66 \cdot 95^3 = 56594307.$$

    Also, an excellent source on using the CRT to solve such a problem (including a worked example) can be found here: `www.di-mgt.com.au/crt.html`

14. Page 137, Table 5.1, 3rd line: Change x_2 to w_2.

15. Page 138: Change the uppercase H in the HMAC formula to a lowercase h. That is, the HMAC formula should read

$$\text{HMAC}(M, K) = h(K \oplus \text{opad}, h(K \oplus \text{ipad}, M)).$$

16. Page 180, second-to-last sentence of first paragraph of Section 6.3.1: Change "the the" to "the".

17. Page 191, Table 6.7: The first row of this table represents the constant 0. So, this row of the table shows that each of the three functions, y_0, y_1, and $y_0 + y_1$, is "balanced," that is, they each produce an equal number of 0s and 1s over the set of all eight possible choices for (x_0, x_1, x_2). In general, a constant (0 or 1) might serve as a good approximation, but that's not the case for this particular S-box.

18. Page 191, fourth full paragraph, 2nd sentence: Change "Each DES S-boxes..." to "Each DES S-box...".

19. Page 200, third paragraph: Change "the the" to "the".

20. Page 204, top: Change "the the" to "the".

21. Page 205: Replace the matrix with the following

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ u_7 \\ u_8 \\ u_9 \\ u_{10} \\ u_{11} \\ u_{12} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

22. Page 215: It should be noted that on this page, "E" is used to denote expected value (i.e., the statistical mean), not symmetric key encryption.

23. Page 243, first line: Change "authorization" to "authentication".

24. Page 244, second paragraph: Change "the the" to "the".

25. Page 263, problem 37, first sentence: Change "systems" to "system".

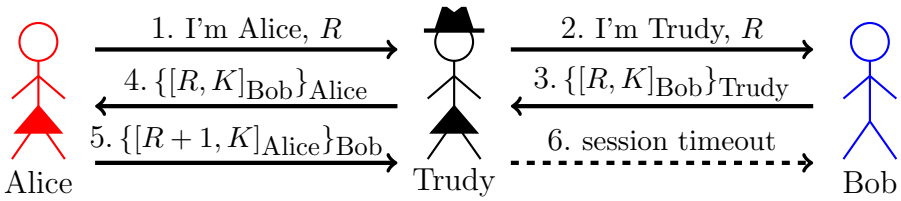
26. Page 263, problem 38, second sentence: Change "SecureID" to "SecurID".

27. Page 271, last sentence before Section 8.3: Change "IDS" to "IDSs".

28. Page 288, C2: Change the dash from "—-" to "—" (I know it probably doesn't really matter much, but this one bugs the heck out of me).

29. Page 302, problem 3, part a: Change "advantaged" to "advantages".

30. Page 326, Figure 9.17: This protocol is insecure. The following attack (thanks to David Furcy and Max Beauchemin) shows that Trudy can convince Alice that she is Bob, and in the process establish a valid session key K that Alice and Trudy will share.



31. Page 329, Figure 9.22: Encryption is not necessary in message 2 or 3. Signing the Diffie-Hellman values is sufficient to prevent the MiM attack, while signing the nonces prevents a replay.

32. Page 331, second paragraph: The protocol in Figure 9.17 is not secure—see number 30, above.

33. Page 337, second full paragraph: Change "that that" to "that".

34. Page 356, first sentence of first full paragraph: Change "The attentive reader may wonder why $h(\text{msgs}, \text{CLNT}, K)$ is encrypted in messages three and four" to "The attentive reader may wonder why $h(\text{msgs}, \text{CLNT}, K)$ is encrypted in message three".

35. Pages 374–376: There are several places on these pages where a semicolon is used instead of a comma in a symmetric key encryption. There is no significance to the semicolons, and to be consistent with the usage elsewhere in the text, these semicolons should all be commas. For example, on p. 374, you should change

$$\text{TGT} = E(\text{"Alice"}, S_A; K_{\text{KDC}})$$

to

$$\text{TGT} = E(\text{"Alice"}, S_A, K_{\text{KDC}}).$$

Similar changes apply to the REPLY and "ticket to Bob" encryption formulas.

36. Page 382, first paragraph after Figure 10.24, last sentence: Change "know" to "known".

37. Page 388, first paragraph: Change "the the" to "the".

38. Page 391, Problem 2, part b: Change "Based on Problem 1, part b" to "Based on Problem 1, part c".

39. Page 404, first sentence: Change "Mars Lander" to "Mars Climate Orbiter". The Climate Orbiter was never intended to land on the planet. It disintegrated due to "atmospheric stresses" when it got too close to the planet, and an error in the units (metric vs English) was the cause of the failure. Also, the cost of the spacecraft is said to have been slightly over $193 million, not $165 million, as stated in the book.

40. Page 405, first full paragraph: Change "4.5 million" to "45 million".

41. Page 420, first full paragraph: Change "the the" to "the".

42. page 423, footnote: Change "the the" to "the".

43. Page 439, Problem 15. The given code has a minor bug. If the memory immediately following `buf2` is not zero, then some extraneous characters will be printed. This could be fixed by, for example, initializing `size` to 9 (instead of 8), and inserting `buf2[8] = '\0';` after the first memset.

44. Page 445, problem 40, part a: Change "eight-digit" to "seven-digit".

45. Page 450, first paragraph: Change "the the" to "the".

46. Page 481, problem 3, part a: Instead of using CafeBabe, it is easier to use an online Java decompiler, such as the one found at
`http://java.decompiler.free.fr/?q=preview`

47. Page 484, problem 8, part a: Insert a comma after "In Visual C++".

48. Page 484, Problem 10: Change "the the" to "the".