AN INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY (HOFFSTEIN, PIPHER, SILVERMAN) TYPOS

Compiled by the Math/CS 295 class at the University of Vermont in Fall 2012, led by John Voight. Thanks to Craig Agricola, Ethan Eldridge, Jonathan Godbout, Michael Musty, Susan Ojala, Rebecca Norton, Sam Schiavone, Jennifer Swasey, Isabella Torin, and Jameson Voll.

(1) Theorem 1.31 (Primitive Root Theorem) is confusing. It mixes a theorem statement with the definition of *primitive root*, which is confusing.
(2) 1.7.1, item 4: This is a very strange formulation of a "chosen plaintext" attack. What is "chosen" here? This looks to me like Eve knows a bunch of plaintext/ciphertext pairs, not that she has chosen them. In the chosen plaintext attack, Eve has the capability to choose arbitrary plaintexts to be encrypted by Alice.
(3) Exercise 1.24: The notation $\lfloor x \rfloor$ is usually called the *floor* of x; it is always confusing that the "greatest integer function" means to round down, whereas there is no such confusion by saying "take the floor". It is potentially confusing, without indent, to know if Step 4 is always suppose to be executed or only if the "if" clause in Step 3 holds. Step 5 of the algorithm is superfluous: you do not need to remind us to continue looping!
(4) Exercise 1.33: You must assume p does not divide g.
(5) Section 2.5, page 73, Example 2.12(f): The example of the matrices not commuting is one where they commute!
(6) Section 2.6: The use of $\mathcal{O}$ for order is confusing. For many, it means local ring (Dummit and Foote is a favorite around here); it is preferred to use an italicized O, as in many other computer science textbooks.
(7) Exercise 2.3(b)(c): It is probably more helpful for the students to write
$$\log_g(h_1 h_2) \equiv \log_g(h_1) + \log_g(h_2) \pmod{p-1}$$
since this is a common point of confusion. (In some contexts, the discrete logarithm is taken to be the least nonnegative integer representing the class modulo $p-1$.)
(8) Exercise 2.6: Yes, we can figure out the exponent! Wait, did you mean for us to do so?
(9) Exercise 2.11: Use either e or 1 for the identity, but not both.
(10) Exercise 2.17: 156 is not a primitive root modulo 593: it has order $(593-1)/4 = 148$. This doesn't affect the statement of the problem, but it is potentially confusing given that the discrete logarithm problem has been primarily developed in the context of powers of a primitive root.
(11) Exercise 3.10: $c_1 =\equiv m g_1^{s_1}$ should be $\equiv$ and "Alice use the Chinese remainder theorem" should be "uses".
(12) Exercise 3.14: 3.14(b) and 3.14(c) are identical, which is probably not the intent.

Date: November 13, 2012.

(13) Table 4.3: After the third line, the “Difference” column is shifted up and the values are incorrect.