Errata to Practical Cryptography

Niels Ferguson

Version 2004-01-25

Introduction

All books contain errors. *Practical Cryptography* is no exception. This document is a complete list of all the errors we know of. We will regularly update this document. You can always find the latest version at `http://www.macfergus.com/pc`.

To make this list easier to use we classify the errors into three categories:

Misleading errors Errors that mislead the reader even when taken in the context of all the other information in the book. This is obviously the most serious type of error.

Confusing errors Errors that confuse the reader, but that are identifiable as errors from the context of all the other information in the book.

Minor errors Errors that are obviously errors, and which do not confuse the reader as to the intended meaning.

The errors are presented in this order, so that you won't have to dig through a long list of minor things to find the important ones.

If you find any more errors in *Practical Cryptography* or in this list, please let me know at `practical-cryptography@macfergus.com`.

Identifying locations

Locations in the book are normally identified by page number, paragraph number, and line number. To avoid cluttering the page we use a shorthand notation. Page numbers are written as "p23", paragraph numbers as "¶3", and line numbers within the paragraph as "ℓ2". For example, the location of the first spelling mistake that was found is written as p16 ¶2 ℓ5.

For counting purposes we define a paragraph as a block of normal text lines. Headings are not counted as paragraphs, and we count a new paragraph after each displayed equation even though it might textually be part of a paragraph that started earlier.

In some situations we use negative numbers for the paragraph or line number. Negative numbers are counted backward from the end. For example, "¶-1" would be the last paragraph on the page, and "ℓ-2" the second-to-last line in the paragraph.

Occasionally section numbers are given prefixed by "sec."

Misleading errors

p145 ¶2: . The numbers in this paragraph are wrong. 128 MB of memory is 10^9 bits, not 10^{12} bits, and that error propagates through the rest of the paragraph. If we keep the failure rate of a bit at 10^{-15} per second, we get one failure every 11 days in 128 MB of memory, and one failure every 32 hours in 1 GB of memory. This is still unacceptable, but not nearly as bad as the book suggests.

Confusing errors

Confusing errors are errors that confuse, but do not mislead. In other words, they give the wrong information when taken in isolation, but the reader should be able to identify them as errors from the rest of the information in the book.

p120 ¶2 ℓ-1: "$k_{\ell(m_i)+15}$" $\mapsto$ "$k_{\ell(m_i)+31}$"

p209 ¶4 ℓ2: "generator" $\mapsto$ "primitive element"

p224 ¶-2 ℓ4: "x' mod $p = b$" $\mapsto$ "x' mod $q = b$"

p235 ¶-2 ℓ-10: “extendedGCD$(t, 3)$” ↦ “extendedGCD$(3, t)$”

p235 ¶-2 ℓ-4: “extendedGCD$(t, 5)$” ↦ “extendedGCD$(5, t)$”

p241 ℓ-10: “GenerateRandomData” ↦ “PseudoRandomData”

p274–275 sec. 15.9: The discussion of the computational complexity of the DH protocol is all about the workload for one of the two parties. Both Alice and Bob have to do three exponentiations in the DH subgroup, one authentication generation, one authentication verification, and various efficient operations.

p311 ¶3 ℓ2: . A “ticket” is the message that Alice sends to Bob. This is standard Kerberos terminology, but it was not properly introduced in the book.

Minor errors

Minor errors are errors that do not confuse the reader as to the intended meaning of the text. Typical minor errors are things like spelling, punctuation, and some grammatical errors.

p14 ¶3 ℓ-4: “to say be” ↦ “to be”

p16 ¶2 ℓ5: “securited” ↦ “secured”

p19 ¶-1 ℓ2: “is” ↦ “are”

p30 ¶-1 ℓ2: “type of attacks” ↦ “types of attack”

p59 ¶-1 ℓ4: “depends” ↦ “depend”

p74 ¶-2 ℓ-4: “happens” ↦ “happen”

p80 ¶1 ℓ-2: “been” ↦ “be”

p89 ¶1 ℓ3: “196” ↦ “192”

p90 ¶1 ℓ-3: “cipher” ↦ “hash function”

p94 Definition 7: “$h_d := h(h(m))$” ↦ “$h_d(m) := h(h(m))$”

p107 ¶2 ℓ3: “are” ↦ “is”

p120 ℓ1: “byte” ↦ “bytes”

p149 ¶-2 ℓ-2: “solves” ↦ “solve”

p150 ¶3 ℓ1: “are” ↦ “is”

p161 ¶-1 ℓ1: “the Fortuna” ↦ “Fortuna”

p167 ℓ4: “forget” ↦ “forgets”

p199 ¶2 ℓ11: “$\ln x / \ln 2$” ↦ “$\ln x / \ln 2)$”

p199 ¶-2 ℓ1: “randomly” ↦ “random”

p202 ¶-2 ℓ-1: “basis” ↦ “bases”

p202 footnote: “small” ↦ “big”

p209 ¶4 ℓ2: “g^6” ↦ “g^5”

p242 ¶1 ℓ2: “now how” ↦ “know how”

p242 ¶-2 ℓ1: “arguments” ↦ “argument”

p246 ℓ-3: “drugs” ↦ “drug”

p247 ℓ-2: “in” ↦ “is”

p253 ¶2 ℓ-1: “attacks” ↦ “attack”

p269 ℓ-5: “are” ↦ “is”

p275 ¶1 ℓ-2: “use” ↦ “uses”

p370 ¶3 ℓ5: “criterium” ↦ “criterion”

p389: [21] and [22] are the same paper, and should be a single entry.