User's Guide to Cryptography and Standards: Errata

Alexander W. Dent and Chris J. Mitchell

1st March 2009 (version 0.37)

Introduction

The purpose of this document is to provide a list of all known errors in the *User's Guide to Cryptography and Standards*. The first discoverer of the error and the date it was notified to us are listed in each case.

Errata

Chapter 1

- **Page 5, Section 1.3, definition of $\mathcal{S}$, line 5**. Change 'where the public key' to 'where the private key'. [Kevin Eagles, 14/3/05].

Chapter 2

- **Page 11, penultimate line**. Change 'the the ISO' to 'the ISO'. [Kevin Eagles, 20/3/05].

Chapter 4

- **Page 50, paragraph starting 'These attacks', line 1**. Change the text to 'The differential and linear cryptanalysis attacks were first published in the early 1990s, and caused ...'. [Soichi Furuya, 17/12/04].
- **Page 50, Equation (4.3)**. Change to

$$X := d_{K_1}(e_{K_2}(d_{K_3}(Y)))$$

  [Soichi Furuya, 17/12/04].

- **Page 53, Section 4.2.5, last line**. Change 'ciphers' to 'cipher'. [Mark Milton, 23/2/09].

- **Page 65, Notes on Section 4.4.1, line 5**. 'Addleman' should be 'Adleman'. [CJM, 6/11/04].

- **Page 65, Notes on Section 4.4.2, line 6**. Delete 'the' before 'both'. [CJM, 6/11/04].

Chapter 5

- **Page 75, Figures 5.3 and 5.4**. A down arrow is missing from both figures (connecting the central $\oplus$ to the e_K box below in Figure 5.3, and connecting the rightmost d_K box to the $\oplus$ beneath in Figure 5.4). [Soichi Furuya, 6/1/05].

- **Page 78, Equation (5.12)**. X_q should be X_i, i.e. the equation should read $P_i = C_i \oplus (e_K(X_i)|_j)$. [Soichi Furuya, 6/1/05].

- **Page 78, Equation (5.14)**. X_i should be X_q, i.e. the equation should read $P_q = C_q \oplus (e_K(X_q)|_t)$. [CJM, 9/1/05].

Chapter 6

- **Page 93, paragraph 3, line 6**. Change 'then' to 'than'. [Soichi Furuya, 6/1/05].

- **Page 97, Section 6.2, paragraph 2, line 2**. Change 'FIBS' to 'FIPS'. [Soichi Furuya, 6/1/05].

- **Page 100, Figure 6.2**. Change the left input to the dotted box from H_i to H_{i-1}. [Soichi Furuya, 6/1/05].

- **Page 103, Figure 6.3**. The outputs of the leftmost 'Split' box (near the top of the figure) should be H_{i-1}^L and H_{i-1}^R instead of H_i^L and H_i^R respectively. [Soichi Furuya, 6/1/05].

- **Page 104, line 7**. Change 'Pub' to 'Pub.'. [Soichi Furuya, 6/1/05].

- **Page 104, lines 14/15**. The name 'Rijmen' should not be hyphenated 'Ri-jmen'. [Vincent Rijmen, 8/2/05].

- **Page 106, Notes on Section 6.1, line 7**. Change 'was first' to 'were first'. [CJM, 6/11/04].

- **Page 106, Notes on Section 6.1, para. 3, line 1**. Change 'significantly' to 'significant'. [CJM, 6/11/04].

Chapter 7

- **Page 123, Equation 7.6**. Change '$e_{K''}[e_K[(D_1)]$' to '$e_{K''}(e_K(D_1))$', i.e. the equation should read $H_1 = e_{K''}(e_K(D_1))$. [Soichi Furuya, 6/1/05].
- **Page 128, line -18**. Change 'algorithms 1 and 3 should be used' to 'algorithms 1 and 3 are in most cases to be preferred to algorithm 2'. [Vincent Rijmen, 8/2/05].
- **Page 130, line -9**. Change 'Rackhoff' to 'Rackoff'. [AWD, 10/7/05].

Chapter 8

- **Page 146, paragraph starting 'The idea', line 7**. Change 'signing key e' to 'signing key d'. [Anonymous, 16/3/05].
- **Page 150, Section 8.6, line 8**. Change 'use' to 'used'. [Vincent Rijmen, 8/2/05].

Chapter 10

- **Page 206, last paragraph, line 5**. Change 'the previous issue' to 'one of the previous issues'. [Vincent Rijmen, 8/2/05].

Chapter 11

- **Page 226, line 14**. Change 'TSRM' to 'TRSM'. [Soichi Furuya, 25/2/05].
- **Page 229, Ref. [6]**. Change 'Withdrawl' to 'Withdrawal'. [CJM, 6/11/04].
- **Page 230, Ref. [11]**. Change 'Techniques for' to 'Techniques using'. [CJM, 8/11/04].

Chapter 16

- **Page 342, line 4**. Change 'be be' to 'be'. [Renato Menicocci, 25/9/06].
- **Page 348, Notes on Section 16.2, paragraph starting 'It was thought', lines 2–4**. Change 'This advice ... other properties' to 'This advice has now largely been superseded, as it seems that suitably large randomly generated prime numbers will satisfy these conditions with overwhelming probability'. [AWD, 16/12/04].

Appendix A

- **Page 365, Table A.7, 11568-4 title**. Change 'Techniques for' to 'Techniques using'. [CJM, 11/11/04].