

『暗号技術入門 第3版 秘密の国のアリス』正誤表

結城浩

© Hiroshi Yuki

http://www.hyuki.com/cr/pdf/errata_cr3.pdf

2016年4月20日更新

目次

1	第1刷	2
1.1	2015-08-29: 第1刷: p.v: 下から11行目: 不要な句点	2
1.2	2015-09-03: 第1刷: p.83: 9-10行目	2
1.3	2015-09-03: 第1刷: p.391: 12-13行目	2
1.4	2015-09-06: 第1刷: p.202: 4行目: 文字のヨゴレ	2
2	第2刷	2
2.1	2015-10-14: 第2刷: p.445: 索引項目の漏れ	2
2.2	2015-10-14: 第2刷: p.198: 19行目: 不正確な記述	2
3	第3刷	3
3.1	2015-11-24: 第3刷: p.95: 下から11行目: 誤植	3
3.2	2015-11-24: 第3刷: p.106: 下から3行目: 参考文献の参照漏れ	3
3.3	2015-11-24: 第3刷: p.259: Table 10-1の7行目: 補足	3
3.4	2015-11-24: 第3刷: p.259: Table 10-1の8行目: 補足	3
3.5	2015-11-24: 第3刷: p.397: 18行目: 誤植	3
3.6	2015-11-24: 第3刷: p.397: 20行目: 誤植	3
3.7	2015-12-09: 第3刷: p.402: 3行目: 誤解を招く表現	3
3.8	2015-12-09: 第3刷: p.7: 下から2行目: スペルミス	4
3.9	2016-02-23: 第3刷: p.142: 11行目以降: RSAと素因数分解の等価性	4
3.10	2016-02-23: 第3刷: p.149: 15行目以降: RSAと素因数分解の等価性	4
3.11	2016-02-23: 第3刷: p.153: 下から3行目以降: RSAと素因数分解の等価性	4
4	第4刷	5
4.1	2016-04-20: 第4刷: p.71: 7-9行目: Rijndaelのブロック長	5
4.2	2016-04-20: 第4刷: p.187: 1行目: 誤植	5

1 第1刷

1.1 2015-08-29: 第1刷: p.v: 下から11行目: 不要な句点

誤: 注目されている認証付き暗号も紹介します。。

正: 注目されている認証付き暗号も紹介します。

1.2 2015-09-03: 第1刷: p.83: 9-10行目

誤: AESのブロック長は128ビット、192ビット、256ビットのいずれかから選べます。128ビットのブロック長を選んだ場合、AESは128ビットの平文をまとめて暗号化して、128ビットの暗号文を作ります。

正: AESのブロック長は128ビットです。したがって、AESは128ビットの平文をまとめて暗号化して、128ビットの暗号文を作ります。

1.3 2015-09-03: 第1刷: p.391: 12-13行目

誤: デジタル署名のアルゴリズムとして、鍵や初期化ベクトルやノンスなどを作るために用いられています。

正: デジタル署名のアルゴリズムとして、RSAやElGamal, DSA, 楕円曲線DSA (ECDSA), エドワーズ曲線DSA (EDDSA)などが用いられています。

1.4 2015-09-06: 第1刷: p.202: 4行目: 文字のヨゴレ

誤: ハッシュ値を

正: ハッシュ値を

2 第2刷

2.1 2015-10-14: 第2刷: p.445: 索引項目の漏れ

誤: (なし)

正: 復号オラクル …… 145

2.2 2015-10-14: 第2刷: p.198: 19行目: 不正確な記述

誤: SHA3-512の場合、ハッシュ値は512ビットですから、 2^{512} 回の試行回数を行えば目的のメッセージが確実に見つかります。これは現実的には不可能な回数です。

正: SHA3-512の場合、ハッシュ値は512ビットです。 n 個のメッセージを用意すれば、目的のハッシュ値を持つメッセージは平均して $\frac{n}{2^{512}}$ 個含まれています(期待値)。期待値を1にするためには 2^{512} 個のメッセージが必要になりますが、これは現実的には不可能な個数です。

3 第3刷

3.1 2015-11-24: 第3刷: p.95: 下から11行目: 誤植

誤: 暗号化ブロックをパディングの代わりに利用

正: 暗号文ブロックをパディングの代わりに利用

3.2 2015-11-24: 第3刷: p.106: 下から3行目: 参考文献の参照漏れ

誤: *Practical Cryptography* では

正: *Practical Cryptography*[Schneier, 2003] では

3.3 2015-11-24: 第3刷: p.259: Table 10-1 の7行目: 補足

誤: 有効期限

正: 有効期限 (開始日時)

3.4 2015-11-24: 第3刷: p.259: Table 10-1 の8行目: 補足

誤: 有効期限

正: 有効期限 (終了日時)

3.5 2015-11-24: 第3刷: p.397: 18行目: 誤植

誤: 2つを通してハッシュ値を

正: 2つに通してハッシュ値を

3.6 2015-11-24: 第3刷: p.397: 20行目: 誤植

誤: Base56Check 符号化

正: Base58Check 符号化

3.7 2015-12-09: 第3刷: p.402: 3行目: 誤解を招く表現

誤: 分岐が発生した場合、P2P ネットワークの各ノードは計算がたいへんなほうを選択し、ブロックチェーンの分岐を抑止するのです。

正: ノードは、最初に受信したブロックをブロックチェーンに暫定的に追加しますが、同時に受信した他のブロックも念のために保存します。そして、これ以降のブロック受信によって、どちらか長く伸びた方を「正しい」と判断するのです。

3.8 2015-12-09: 第3刷: p.7: 下から2行目: スペルミス

誤: cryptography

正: cryptography

3.9 2016-02-23: 第3刷: p.142: 11行目以降: RSAと素因数分解の等価性

誤: N を素因数分解して p と q を求めることができれば、 D を求めることができます。

しかし「 D を求めること」が「 N を素因数分解すること」と等価であるかどうかは、数学的に証明されているわけではありません。もしかしたら、 N を素因数分解せずとも (p と q を知らなくても)、 E と N から D を求める方法が発見されるかもしれません。

このような方法はまだ見つけられていませんし、そもそも存在するののかもわかっていません。

正: N を素因数分解して p と q を求めることができれば、 D を求めることができます。

しかし「 D を求めること」と「 N を素因数分解すること」とが等価であるかどうかは、数学的に証明しなければならないことです。「 D を求めること」と「 N を素因数分解すること」が決定的多項式時間で等価であることは、2004年に Alexander May が証明しています。

(脚注追加)

Alexander May, Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring, *Advances in Cryptography, CRYPTO '04*, Springer-Verlag, 2004.

<https://www.iacr.org/archive/crypto2004/31520213/det.pdf>

3.10 2016-02-23: 第3刷: p.149: 15行目以降: RSAと素因数分解の等価性

誤:

等価かどうか、まだわかっていません。

確かに、素因数分解が高速にできれば、RSA は解読されます。しかし、RSA を解読するのに素因数分解を行わなければならない、ということが証明されているわけではありません。もしかしたら、素因数分解を行わなくても解読できる方法が見つかるかもしれません。

正:

RSA のプライベート鍵を求めることが N の素因数分解と等価であることは、2004年に Alexander May が証明しました。

3.11 2016-02-23: 第3刷: p.153: 下から3行目以降: RSAと素因数分解の等価性

誤:

ただし、素因数分解を解くことと、RSA 暗号を解くことが等価であることは証明されていません。すなわち、素因数分解ができなくても、RSA 暗号を高速に解くアルゴリズムが発見される可能性はゼロではありません。

正:

その通りです。

4 第4刷

4.1 2016-04-20: 第4刷: p.71: 7～9行目: Rijndaelのブロック長

誤: Rijndaelのブロック長は128ビットで、鍵のビット長は128ビットから256ビットまで32ビット単位で選択することができます(ただし、AESの規格上では、鍵長は128,192,256ビットの3種類だけです)。

正: Rijndaelのブロック長と鍵のビット長はそれぞれ独立に、128ビットから256ビットまでの32ビット単位で選択することができます。ただし、AESの規格では、ブロック長は128ビット固定で、鍵のビット長は128,192,256ビットの3種類だけです。

4.2 2016-04-20: 第4刷: p.187: 1行目: 誤植

誤: Keccakでは、

正: KECCAKでは、