RFC Errata

Errata Search

RFC Number: 1319 **Errata ID:**

Source of RFC Status: All/Any

Area Acronym: All/Any Type: All/Any

WG Acronym: Submitter Name:

Other: All/Any Date Submitted:

Summary Table Full Records

Search Reset Fields

Found 4 records.

Status: Verified (4)

RFC 1319, "The MD2 Message-Digest Algorithm", April 1992

Note: This RFC has been obsoleted by RFC 6149

Source of RFC: pem (sec)

Errata ID: 554
Status: Verified
Type: Technical
Publication Format(s) : TEXT
Reported By: Jem Berkes
Date Reported: 2002-01-30

Section 3.1 says:

```
   Padding is performed as follows: "i" bytes of value "i" are appended
```

```
to the message so that the length in bytes of the padded message
becomes congruent to 0, modulo 16. At least one byte and at most 16
16 bytes are appended.
```

It should say:

```
Padding is performed as follows: "i" bytes of value "i" are appended
to the message so that the length in bytes of the padded message
becomes congruent to 0, modulo 16. At least one byte and at most
16 bytes are appended.
```

Errata ID: 555
Status: Verified
Type: Technical
Publication Format(s) : TEXT
Reported By: David Hopwood
Date Reported: 2002-02-11

Section 3.2 says:

```
   ...
   /* Process each 16-word block. */
   For i = 0 to N/16-1 do

      /* Checksum block i. */
      For j = 0 to 15 do
         Set c to M[i*16+j].
         Set C[j] to S[c xor L].
         Set L to C[j].
       end /* of loop on j */
    end /* of loop on i */

The 16-byte checksum C[0 ... 15] is appended to the message. Let
M[0
with checksum), where N' = N + 16.
```

It should say:

```
   ...
   /* Process each 16-word block. */
   For i = 0 to N/16-1 do
```

```
         /* Checksum block i. */
         For j = 0 to 15 do
            Set c to M[i*16+j].
            Set C[j] to C[j] xor S[c xor L].
            Set L to C[j].
          end /* of loop on j */
       end /* of loop on i */

   The 16-byte checksum C[0 ... 15] is appended to the (padded)
   message.
   Let M[0..N'-1] be the message with padding and checksum appended,
   where N' = N + 16.
```

Errata ID: 3575
Status: Verified
Type: Editorial
Publication Format(s) : TEXT
Reported By: Andrew Clark
Date Reported: 2013-03-29
Verifier Name: Sean Turner
Date Verified: 2013-08-14

Section 3.2 says:

```
      Set L to 0.

      /* Process each 16-word block. */
      For i = 0 to N/16-1 do

         /* Checksum block i. */
```

It should say:

```
      Set L to 0.

      /* Process each 16-byte block. */
      For i = 0 to N/16-1 do

         /* Checksum block i. */
```

Notes:

The comment should note that this section of the algorithm operates on a 16 byte -- rather than 16 word -- block.

Errata ID: 3576
Status: Verified
Type: Editorial
Publication Format(s) : TEXT
Reported By: Andrew Clark
Date Reported: 2013-03-29
Verifier Name: Sean Turner
Date Verified: 2013-08-14

Section 3.4 says:

```
   Do the following:

      /* Process each 16-word block. */
      For i = 0 to N'/16-1 do
```

It should say:

```
   Do the following:

      /* Process each 16-byte block. */
      For i = 0 to N'/16-1 do
```

Notes:

The comment should note that this section of the algorithm operates on a 16 byte -- rather than 16 word -- block.

Report New Errata