Status: Verified (2)

RFC 2202, "Test Cases for HMAC-MD5 and HMAC-SHA-1", September 1997

Source of RFC: Legacy
Area Assignment: sec

Errata ID: 480

Status: Verified
Type: Technical

Reported By: Deron Meranda
Date Reported: 2004-05-05

In the Appendix, it says:

```
          /**** Outter Digest ****/

          SHAInit(&octx) ;

          /* Pad the key for outter digest */
```

It should say:

```
          /**** Outer Digest ****/

          SHAInit(&octx) ;

          /* Pad the key for outer digest */
```

Notes:

Errata ID: 481

Status: Verified
Type: Technical

Reported By: Kevin Springle
Date Reported: 2002-09-17

Section 3 says:

```
  test_case =     7
  key =           0xaa repeated 80 times
  key_len =       80
  data =          "Test Using Larger Than Block-Size Key and Larger
```

```
                Than One Block-Size Data"
   data_len =   73
   digest =     0xe8e99d0f45237d786d6bbaa7965c7808bbff1a91
   data_len =   20
   digest =     0x4c1a03424b55e07fe7f27be1d58bb9324a9a5a04
   digest-96 =  0x4c1a03424b55e07fe7f27be1

   test_case =  6
   key =        0xaa repeated 80 times
   key_len =    80
   data =       "Test Using Larger Than Block-Size Key - Hash Key
   First"
   data_len =   54
   digest =     0xaa4ae5e15272d00e95705637ce8a3b55ed402112

   test_case =  7
   key =        0xaa repeated 80 times
   key_len =    80
   data =       "Test Using Larger Than Block-Size Key and Larger
                Than One Block-Size Data"
   data_len =   73
   digest =     0xe8e99d0f45237d786d6bbaa7965c7808bbff1a91
```

It should say:

```
   test_case =  7
   key =        0xaa repeated 80 times
   key_len =    80
   data =       "Test Using Larger Than Block-Size Key and Larger
                Than One Block-Size Data"
   data_len =   73
   digest =     0xe8e99d0f45237d786d6bbaa7965c7808bbff1a91
```

Status: Held for Document Update (1)

RFC 2202, "Test Cases for HMAC-MD5 and HMAC-SHA-1", September 1997

Source of RFC: Legacy
Area Assignment: sec

Errata ID: 3851

Status: Held for Document Update
Type: Editorial

Reported By: Antonio Bueno
Date Reported: 2013-12-28
Held for Document Update by: Sean Turner
Date Held: 2014-01-12

Section 2 says:

```
test_case =     3
key =           0xaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
key_len         16
data =          0xdd repeated 50 times
data_len =      50
digest =        0x56be34521d144c88dbb8c733f0e8b3f6

test_case =     4
key =           0x0102030405060708090a0b0c0d0e0f10111213141516171819
key_len         25
data =          0xcd repeated 50 times
data_len =      50
digest =        0x697eaf0aca3a3aea3a75164746ffaa79
```

It should say:

```
test_case =     3
key =           0xaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
key_len =       16
data =          0xdd repeated 50 times
data_len =      50
digest =        0x56be34521d144c88dbb8c733f0e8b3f6

test_case =     4
key =           0x0102030405060708090a0b0c0d0e0f10111213141516171819
key_len =       25
data =          0xcd repeated 50 times
data_len =      50
digest =        0x697eaf0aca3a3aea3a75164746ffaa79
```

Notes:

Notice the equal signs missing after "key_len"

spt: I changed the classification to editorial and made it hold for document update because I don't believe implementers will be confused by the missing "=".