

RFC-2104, HMAC algo. with SHA256

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/2310.html>

From: mklooptbd (mklooptbd@yahoo.com)

Date: 03/31/03

From: mklooptbd@yahoo.com (mklooptbd)

Date: 31 Mar 2003 01:48:10 -0800

Hello, I've read the RFC-2104 specs and there is one thing I couldn't find (maybe missed it), I've put my question prepended with ---?>: after the key initialization process (padding etc.).

Thanks a bunch.

---!> this comes directly from the RFC paper, example with MD5

```
MD5Init(&context); /* init context for 1st
                    * pass */
MD5Update(&context, k_ipad, 64) /* start with inner pad */
---?>Does the next line mean I do it every pass in the loop
---?>(for every 512 bytes for sha256),
---?>because data isn't short, or only once?
MD5Update(&context, text, text_len); /* then text of datagram */
MD5Final(digest, &context); /* finish up 1st pass */
/*
* perform outer MD5
*/
MD5Init(&context); /* init context for 2nd
                    * pass */
---?>The following 2 lines are probably done once?
MD5Update(&context, k_opad, 64); /* start with outer pad */
MD5Update(&context, digest, 16); /* then results of 1st
                                 * hash */
MD5Final(digest, &context); /* finish up 2nd pass */
```