
Subject: bug: in Crypto/Sha1

Posted by [cyrille](#) on Mon, 20 Aug 2007 21:58:42 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello,

I found a bug in Crypto/Sha1::Put() function.

You don't have the same hash if you put all your buffer in one call or if you put the last 1 to 63 bytes in another call.

The line code while(length >= 64) should be while((pos+length) >= 64), and the last lines
memcpy(buffer, s, length);
pos = length; should be memcpy(buffer+pos, s, length);
pos += length;.

Regards.

Subject: Re: bug: in Crypto/Sha1

Posted by [mirek](#) on Tue, 21 Aug 2007 11:45:24 GMT

[View Forum Message](#) <> [Reply to Message](#)

Thank you, patch applied.

Mirek
