

Re: Looking for Suggestions on Hash Key Creation

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2008-03/msg00033.html>

- *From:* Unruh <unruh-spam@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 26 Mar 2008 21:02:49 GMT
-

John Mason Jr <notvalid@xxxxxxxxxxxxxxxx> writes:

jwwest wrote:

I'm building a CGI eCommerce store and I'm looking for ways to create a decent 2 way encryption. Of course in a scripted language, I don't want my key in the script itself, but would rather store it somewhere obfuscated such as in a compiled C++ binary. (I know it doesn't help – much–, but defense in layers)

A .NET programmer friend of mine uses a method that involves generating a hash from the Volume ID of the hard drive to use as a key. I like this approach, but am wary of hardware/software changes that will break my key.

Am I going about this the correct way? Is there a better method for creating a decently secure 2 way encryption using a scripted language?

Any help is very much appreciated. Thanks.

Why are you trying to reinvent the wheel. Use ssh.
or ssl.

.