

Re: Newbie question on encryption keys

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-07/msg00027.html>

- *From:* Mark Shroyer <usenet-mail@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 10 Jul 2007 07:22:14 +0000 (UTC)
-

On 2007-07-10, rohanm79@xxxxxxxx <rohanm79@xxxxxxxx> wrote:

I am a little confused about creating encryption keys. How exactly does one create a 128, 512 or 1024 bit key? If I use an encryption software, does the encryption key mean the password? If so, is it enough if I create a $128/8=16$ char password or even $512/8=64$ char password?

How to specify key length depends on what kind of software you're talking about. Usually it's set as some sort of command-line argument or in a config file, or it may be prompted for interactively. Consult the man page for details.

Dealing with public key encryption systems, the actual encryption key generally has nothing to do with the password which you may or may not be asked to provide. When you create a keypair with, e.g., GPG or OpenSSL, the key parameters themselves are pseudorandomly (or randomly, depending on your hardware) generated in the program. The password is only used as the basis for a /symmetric/ key with which to protect the generated private encryption key; this is done to make it more difficult for an attacker to obtain your private key, should the file it is contained within fall into the wrong hands.

Let us know which particular software you're dealing with if that didn't completely answer your question.

Mark

--

Mark Shroyer
<http://markshroyer.com/>

.