

Re: Newbie question on encryption keys

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-07/msg00038.html>

- *From:* Ertugrul Soeylemez <do-not-spam-me@xxxxxxx>
 - *Date:* Wed, 11 Jul 2007 16:22:47 +0200
-

Mark Shroyer <usenet-mail@xxxxxxxxxxxxxxxx> (07-07-11 05:56:32):

This is imprecise. 32 characters will by far not be enough for the password to have 256 bits of entropy. Remember that users only use a subset of all possible characters (and they shouldn't use them all, because of localization issues).

In most cases one character of the password will have slightly less than seven bits of entropy, because you don't type eight bit characters, and you also don't type control characters.

Yes, you're right of course; by "32 random ASCII characters" I actually meant 32 characters from all possible ASCII values 0-127, printable or not. Just thought I'd leave out the discussion of practical specifics in the interest of brevity.

The set of printable ASCII characters is a less-than-seven bit character set, as you see directly from the fact that it contains only 95 characters (32..126). You need 39 completely random characters of this kind to get (slightly more than) 256 bits of entropy.

You cannot include the non-printable subset, because there is no easy and portable way to type them, especially in GUIs. Though, even including the non-printables, you will still need 37 random characters for 256 bits of entropy.

Regards,
Ertugrul Söylemez.

—

Security is the one concept, which makes things in your life stay as they are. Otto is a man, who is afraid of changes in his life; so naturally he does not employ security.

.