Re: brute−force estimation

Source: http://www.derkeiler.com/Newsgroups/sci.crypt/2006−02/msg00504.html

- *From*: "Richard Revis" <richard.revis@xxxxxxxxxxxxxxxxxxx>
- *Date*: Wed, 22 Feb 2006 10:12:12 −0000

"Elenhil" <elenhil@xxxxxxxxx> wrote in message
news:1140599172.853058.63330@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

> Say, I have a 20 character long password consisting of latin characters (capital and lower−case), numbers and basic punctuation. That is roughly 80 symbols to play with.
>
> How many combinations one must look through from 1 to 20 (the exact length is unknown) with unoptimized brute force?

I'm ashamed to admit that I haven't done any mathematics more complicated than adding up my shopping bill since the second year of University, but I don't think the problem is as complicated as you are making it.

Assuming 80 valid symbols in the password field and a length of exactly 20 with no limitation on the number of repeats of symbols the number of combinations is 20^80.

If the password can be of any length up to 20 characters then the number of combinations is 20^80+19^80+...+1^80.

As for your second point − yes the maximum time for decryption of a message* is (number of keys)/(time to test each key). This time can be significantly shortened if the method used to secure the data is weak because it is not necessary to test every key.

*at least where there is only one key in the domain which produces a valid output − otherwise you can't be sure that you have the correct message.

.