

# brute forcing – numbers of passwords possible?

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-01/msg00045.html>

---

- *From:* bealoid <signup@xxxxxxxxxxxxxx>
  - *Date:* Fri, 04 Jan 2008 12:31:13 GMT
- 

A software allows a user password of up to 62 characters, selected from a set of 95 characters.

Is the total number of different passwords given by:

$$62^{95}$$

or by:

$$62^{95} + 61^{95} + 60^{95} \dots + 3^{95} + 2^{95} + 1^{92}$$

And if it's the latter, is there an easier way to do it than the way I've shown?

When talking about brute forcing such a password is it best to say "there are X number of passwords possible", or "there are X possible passwords, but you'd expect to break a password with brute force after Y tests"?

And what would Y be, about X/2?

Thanks in advance for help.

.