

Re: RC4 encrypt/decrypt keys

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/2316.html>

From: Roger Schlafly (*rogersc_at_mindspring.com*)

Date: 09/28/03

Date: Sun, 28 Sep 2003 08:10:37 GMT

"TC" <a@b.c.d> wrote

> *brute-force*. But if there is a theoretical possibility that the data could
> be decrypted with a different, possibly **very short** key, doesn't that
> affect the whole "brute-force" idea?

Whether that is possible or not, there is always the possibility that a brute-force attack will be unusually lucky, and find the key much more quickly than expected.

Eg, suppose the key has 64 bits. An exhaustive brute force key search would take 2^{64} key attempts. On average, the key will be found about half-way thru the search, or after $2^{64}/2 = 2^{63}$ keys. But if the search is extraordinarily lucky, it might find the key after only 2^{40} key attempts, in which case the key will have turned out to be no better than a 40 (or 41) bit key.