

Re: RC4 encrypt/decrypt keys

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/2305.html>

From: TC (a_at_b.c.d)

Date: 09/28/03

Date: Sun, 28 Sep 2003 16:01:45 +0930

Gregory G Rose <ggr@qualcomm.com> wrote in message
news:bl5u3f\$aq2@qualcomm.com...

> *In article <1064729114.153400@teuthos>, TC <a@b.c.d> wrote:*
> > *This is probably a reeeeeeeely stoooooopid question, but I can't quite*
> *get*
> > *my mind around it.*
> >
> > *Say I encrypt some data with n-bit RC4.*
> >
> > *Is there any possibility – even in principle – that the data could be*
> > *successfully decrypted with a key of bit length *less than* n?*
> >
> > *It's both theoretically and practically possible.*
> >
> > *Theoretically: All the key does is establish the*
> > *initial permutation. It's possible (though*
> > *unlikely) that two apparently different keys will*
> > *result in the same initial permutation.*
> >
> > *Practically: Any key that can be split into two or*
> > *more identical pieces is equivalent to any other*
> > *key built out of the same pieces. For example, the*
> > *key "abcabc" is equivalent to the key "abc".*

Ok! Thanks Greg for the informative & very speedy response.

So, let me ask this. Say I encrypt something three times: once with 56-bit RC4, once with 64-bit, and once with 72-bit (or whatever). If it is theoretically possible that each of those ciphertext could be decrypted with (say) a 16-bit key, then, does it make any sense to say that the 72-bit encryption is "stronger than" the 64-bit one, & the 64-bit encryption is "stronger than" the 56-bit one?

Previously I thought that longer RC4 keys were "more secure" than shorter ones, for the simple reason that longer keys take very much longer to 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

sci.crypt: Re: RC4 encrypt/decrypt keys

affect the whole "brute-force" idea?

Hope I'm being clear here...

TIA,
TC