

sci.crypt: Re: Key length for ARC4 and RC5 key length contradiction (Please, help me)

## Re: Key length for ARC4 and RC5 key length contradiction (Please, help me)

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/1510.html>

---

**From:** David Hopwood ([david.hopwood\\_at\\_zetnet.co.uk](mailto:david.hopwood_at_zetnet.co.uk))

**Date:** 06/28/03

Date: Sat, 28 Jun 2003 13:37:31 +0000

-----BEGIN PGP SIGNED MESSAGE-----

Gustavo Rios wrote:

> *I am implementing ARC4 and RC5 and found some misguiding  
> documentation, at least to my eyes! The problem is the key length for  
> both algorithms. The IETF Draft for Arcfour, i.e.,  
> <draft-kaukonen-cipher-arcfour-03.txt> states for following:  
[...]  
> My doubt is: The code prevents keylength of 0 bytes to be used, right  
> ? In other words, ARC4 do REQUIRES for key length bigger than 0, this  
> is a MUST be!  
[...]  
> The RC5 Algorithm is the same. The paper "The RC5 Encryption  
> Algorithm", by Ronald L. Rivest states one contradiction:  
[...]  
> c in this case the the length to bytes expanded, if b was 0, than so  
> is c. My question is where is the error, the allowable sizes for b or  
> the computation itself?*

In the case of RC4, the minimum key size is one byte/octet. The Internet Draft (which is expired anyway) does not contradict this, although if the draft were revived it should probably be specified more clearly.

In the case of RC5, the minimum key size is zero bytes/octets, and the key scheduling algorithm in RFC 2040 handles that case correctly – not that anyone should want to use zero-length keys.

The paper "The RC5 Encryption Algorithm" has a revised version that corrects this as well as another error in the reference code (see <http://theory.lcs.mit.edu/~rivest/publications.html>) and search in page for "RC5").

<plug> The SCAN site at <http://www.users.zetnet.co.uk/hopwood/crypto/scan/> would have given you the answers to these questions. </plug>

Re: Key length for ARC4 and RC5 key length contradiction (Please, help me)

sci.crypt: Re: Key length for ARC4 and RC5 key length contradiction (Please, help me)

-- --

David Hopwood <david.hopwood@zetnet.co.uk>

Home page & PGP public key: <http://www.users.zetnet.co.uk/hopwood/>

RSA 2048-bit; fingerprint 71 8E A6 23 0E D3 4C E5 0F 69 8C D4 FA 66 15 01

Nothing in this message is intended to be legally binding. If I revoke a public key but refuse to specify why, it is because the private key has been seized under the Regulation of Investigatory Powers Act; see [www.fipr.org/rip](http://www.fipr.org/rip)

-----BEGIN PGP SIGNATURE-----

Version: 2.6.3i

Charset: noconv

iQEVAwUBPv2Z6DkCAxeYt5gVAQFhmAf+IWliOoIKNajPOoA39f89NjuYUTWHMXwn  
aIHrITY1czyJAKxEceh0RuEzhywFlizhmhJfF2grg8bFjxKBCo3mb8PBRDSZseoz  
KXArrRlmhbnVPOVeHEzc6orB2ZUFKfoNffZmErPDZP11rZsbd9qNpoVKQzUDG260  
l1+BgUD2fMOjO0xvZv3ufVPx6SKmpVJQS1rQyoDFi525Ov06y1IbjN1U/4KGGGIL  
Yadx2PTPgDFx6Rp8hjEwn+ziQa9VphCQAxL91jeqFUqeaIAe8FSB7fq6Z3oOOMJg  
9q+2ixySyBuPRjW18bTmpSD/f71RAeX1rwzCOu46bR0bN8rIf2vr3Q==  
=19Gr

-----END PGP SIGNATURE-----