

## Re: When rsa vs dsa

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-01/0211.html>

---

**From:** Anne & Lynn Wheeler ([lynn\\_at\\_garlic.com](mailto:lynn_at_garlic.com))

**Date:** 01/24/04

Date: Sat, 24 Jan 2004 17:10:43 GMT

Simon Tatham <[anakin@pobox.com](mailto:anakin@pobox.com)> writes:

> *On the contrary. An RSA signature is about the same size as the*  
> *modulus of the RSA key. So for a 1024-bit key, that's \_128\_ bytes.*

yep, severe brain check there ...

minor additional information as to key strengths ... following  
from internet-draft on key lengths:

<http://www.ietf.org/internet-drafts/draft-orman-public-key-lengths-07.txt>

System

requirement Symmetric RSA or DH DSA subgroup

for attack key size modulus size size

resistance (bits) (bits) (bits)

(bits)

70	70	947	129
80	80	1228	148
90	90	1553	167
100	100	1926	186
150	150	4575	284
200	200	8719	383
250	250	14596	482

--

Anne & Lynn Wheeler | <http://www.garlic.com/~lynn/>

Internet trivia 20th anv <http://www.garlic.com/~lynn/rfcietff.htm>