

## Re: PuTTY: Server key initialization problem.

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-01/0290.html>

---

**From:** Simon Tatham ([anakin\\_at\\_pobox.com](mailto:anakin_at_pobox.com))

**Date:** 01/31/04

Date: 31 Jan 2004 09:40:12 +0000 (GMT)

Charles Wilcox <[willo@wpi.edu](mailto:willo@wpi.edu)> wrote:

```
> -----  
> PuTTY Fatal Error  
> -----  
> Server's host key did not match the signature supplied  
> -----
```

I'm afraid this error is an indication of an actual bug in either the server or the client; it's reasonably commonplace for the provided host key not to match the one you have stored in the registry, but for the provided host key and the provided `_signature_` not to match is pretty bad.

I don't suppose (out of sheer desperate hope) you were using the Unix port of PuTTY? I fixed a bignum bug in that the other day which might reasonably have caused this symptom.

If not, I'm afraid you probably do need to mail the PuTTY team. Please supply an SSH packet log of a failing connection. (This can't risk giving away vital information if it fails before you authenticate.)

--

Simon Tatham                   "Imagine what the world would be like if  
<[anakin@pobox.com](mailto:anakin@pobox.com)>           there were no hypothetical situations..."