

## Re: SRP protocol plaintext equivalence query

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-02/3156.html>

---

**From:** Panu Hämäläinen ([panu.hamalainen@NOSPAM.tut.fi.invalid](mailto:panu.hamalainen@NOSPAM.tut.fi.invalid))

**Date:** 02/21/03

From: "Panu Hämäläinen" <[panu.hamalainen@NOSPAM.tut.fi.invalid](mailto:panu.hamalainen@NOSPAM.tut.fi.invalid)>

Date: Fri, 21 Feb 2003 09:53:57 +0200

"Paul Crowley" <[paul@JUNGCATCHER.ciphergoth.org](mailto:paul@JUNGCATCHER.ciphergoth.org)> wrote  
> [\*] Nitpick: *ISTR an attack was found that allowed you to test two*  
> *instead of one.*

Recently, the protocol has been improved (SRP-6) so that only one test is possible. The description can be found at <http://srp.stanford.edu/doc.html>.

-- Panu