

Re: PGP 6.5.8ckt 08 setup question please

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2126.html>

From: Thomas J. Boschloo (*nospam_at_hccnet.nl.invalid*)

Date: 04/30/05

Date: Sat, 30 Apr 2005 15:13:17 +0200

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

[X-Posted to sci.crypt and alt.security.pgp]

Zax wrote:

> On Fri, 29 Apr 2005 19:20:55 +0200, Thomas J. Boschloo wrote in
> Message-Id: <42726d22\$0\$148\$3a628fcd@reader2.nntp.hccnet.nl>:

>
>

>>>Zax wrote:

>>>

>>>>["Followup-To:" header set to alt.privacy.anon-server.]

>>>>

>>>>Fair, I just wanted some professional opinions from sci.crypt (and ASP

>>>>because this issue applies more to PGP than it does to Mixmaster).

>>>>That's all.. Hope nobody got upset by not setting up a line on top of

>>>>the message that I had in fact X-Posted.. I know it is being misused by

>>>>trolls.. I also know that this group just hasn't got the expertise to

>>>>address this specific question correctly.. ASP might, SC sure does (but

>>>>APAS seems to be loathed by most (some) sci.crypt posters..)

>

>

> Hi Thomas,

>

> I wasn't criticising you for x-posting your message, nothing wrong with

> widening the audience when it's on-topic. :) My newsreader prepends

> that to a posting when I've set a Followup-To header. Good netiquette

> dictates that a Followup-To header should always be applied when

> responding to x-posted articles. If responders wish to keep other

> groups in the thread, they can reinsert them.

That's good :-) I also remember the right and wrong formula for the
Birthday attack problem:

Good: $1 - (365/365)(364/365)(363/365) \dots (336/365)$ for 30 pupils

Bad: $30 * (1/365)$

sci.crypt: Re: PGP 6.5.8ckt 08 setup question please

Good ~= 71%

Bad ~= 8% (not completely sure about the formula)

The case with SHA-1 is that with a collision attack that requires 2^{69} operations is that all ($\sim 2^{68}$) previous results are stored just like in a class with pupils. So while the second collision is only being compared to the first, the third collision is also being compared to the second and so on. So each evaluation becomes slower than the previous one, still it is only considered to be one operation. With a vector computer it might be possible to make these massively parallel operations pretty fast. Still, the (SHA-1) result is highly academic and doesn't apply to real life DSS signatures AFAIK.

OTOH, Bruce Schneier says in his Cryptogram that cryptographic attacks only become better in the future and not worse!

Hope I got this right. I am cross-posting again,
Thomas

"Nothing is true. Everything is permitted" – W.S. Burroughs, Naked Lunch

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

Version: GnuPG v1.4.1 (MingW32)

Comment: Using GnuPG with Thunderbird – <http://enigmail.mozdev.org>

iQB5AwUBQnOEbQEP2l8iXKAJAQHbYgMfXo8GAhBmcWRTOwfNOEZwV+CcVtkEyNTK
pou1bbjgKgRezb38LE7AZ0gQVEn1/apRnyntwd6od8rvv7thX1lp9MWYEj2rVfHD
9AcF2bFYVAyl6COaJiCGkFBEEmQK7biQq75WScA==
=YPZD

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