Subject: What if RSA is broken (conjecture inside)
Posted by cryptomaniac on Sun, 15 Oct 2006 20:17:06 GMT
View Forum Message <> Reply to Message

No really, what if? Despite the vast improbability of it occuring before quantum computers are perfected, I'm just kind of wondering what the RG team would do. Basically, this is settling something with a friend, he thinks that nothing would happen, and that you guys would continue using the (newly compromised) RSA. I think you'd at least try to find a new more suitable algorithim.

Its really a question of little consequence, but I just thought it would be neat to know.

Subject: Re: What if RSA is broken (conjecture inside)
Posted by scguy318 on Mon, 16 Oct 2006 02:24:30 GMT
View Forum Message <> Reply to Message

If RSA was broken in the future, then a newer version of the RenGuard client would switch to a stronger algorithm most likely.

Subject: Re: What if RSA is broken (conjecture inside)
Posted by Nightma12 on Mon, 16 Oct 2006 16:13:46 GMT
View Forum Message <> Reply to Message

if RG team gets the time, i think they should write there own algorithem

Subject: Re: What if RSA is broken (conjecture inside)
Posted by scguy318 on Tue, 17 Oct 2006 04:14:00 GMT
View Forum Message <> Reply to Message

The problem with that is, the RG team isn't composed of expert skilled cryptographers. They may write a pretty shoddy algorithm which a skilled cracker could break. Better to rely on proven and free algorithms.

Subject: Re: What if RSA is broken (conjecture inside)
Posted by xptek on Tue, 17 Oct 2006 04:47:24 GMT
View Forum Message <> Reply to Message

Nightma12 wrote on Mon, 16 October 2006 12:13if RG team gets the time, i think they should write there own algorithem

What would be the point of that?

Stick with something tried and tested.

Subject: Re: What if RSA is broken (conjecture inside)
Posted by light on Tue, 17 Oct 2006 09:29:12 GMT
View Forum Message <> Reply to Message

RSAs strength is that it's a public algorithm that relies on mathematics and the current state of PCs for its security. Everyone can find out how RSA works but it works so well it's incredibly secure.

The RG team would probably make an algorithm then hide it to prevent it being broken. Security by obscurity has always been flawed.

Also, if RSA became broken i'd be more worried about my bank account than RenGuard.

Subject: Re: What if RSA is broken (conjecture inside)
Posted by 0x90 on Tue, 17 Oct 2006 20:58:36 GMT
View Forum Message <> Reply to Message

and what has the security of RSA to do with renguard?! rg's security is broken anyways.. i didnt even know that theyre using rsa for something anywhere.
but since rgh catches the transferred data in RG right before it gets crypted and right after it gets decrypted it really doesnt matter what encryption you are using.
rsa like any other encryption only helps against people who try to sniff the traffic on the outside or something. (man in the middle for example and similar stuff).

0x90