Subject: What if RSA is broken (conjecture inside)
Posted by cryptomaniac on Sun, 15 Oct 2006 20:17:06 GMT

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.