

sci.crypt: Re: Any truth to rumor that NSA had Public Key Crypto first?

Re: Any truth to rumor that NSA had Public Key Crypto first?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1011.html>

From: Roger Schlafly (rogerscl_at_mindspring.com)

Date: 09/28/04

Date: Tue, 28 Sep 2004 08:11:47 -0700

"Matt" <matt_crypto@yahoo.co.uk> wrote:

- > *It is quite possible, but there's no (or little) evidence. According*
- > *to one website, "Bobby Inman, when director of NSA, claimed (without*
- > *substantiation) that NSA had had public key crypto a decade earlier*
- > *than Diffie and Hellman."* --
- > <http://www.research.att.com/~smb/nsam-160/>

There is now some substantiation. "decade" is an exaggeration, but NSA did know of some similar ideas from British spooks a few years earlier. Eg, see:

http://www.wired.com/wired/archive/7.04/crypto_pr.html