

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/2004-09/0995.html>

---

**From:** Roger Schlafly ([rogerscl\\_at\\_mindspring.com](mailto:rogerscl_at_mindspring.com))

**Date:** 09/28/04

Date: Mon, 27 Sep 2004 23:09:02 -0700

"George Ou" <[533george\\_ou234@netzero234.com](mailto:533george_ou234@netzero234.com)> wrote  
> *According to Bruce, the NSA may have been 20 years ahead of the*  
> *academic community in 1970.*

He says:

It took the academic community two decades to figure out that the NSA "tweaks" actually improved the security of DES. This means that back in the '70s, the National Security Agency was two decades ahead of the state of the art.

But I don't think that's true. I believe that the advantages of DES over Lucifer were known much earlier.

I also don't agree with his statement that weaknesses in SHA-1 have been demonstrated.