

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

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1006.html>

---

**From:** Douglas A. Gwyn (*DAGwyn\_at\_null.net*)

**Date:** 09/28/04

Date: Tue, 28 Sep 2004 06:08:42 -0400

George Ou wrote:

- > *According to Bruce, the NSA may have been 20 years ahead of the*
- > *academic community in 1970. Is it possible that the rumors that the*
- > *NSA already had Public Key Cryptography well before Diffie Hellman or*
- > *even the British spooks are true? Given the apparent superiority of*
- > *the NSA back in those days, it would seem possible.*

There were some asymmetric encryption schemes around, but nothing very general. The NSA's "customer base" for cryptosystems didn't see much need for PKCS; the closest requirement was for key management for the STU IIIs (secure telephones). GCHQ gets credit for the invention of PKCS.

In some areas NSA's technical abilities have been more than 60 years ahead of the public state of the art (and counting). And of course in some areas they are at the leading edge of the public state of the art. Just how much if any lead depends on the area.

- > *From what Bruce says about DES, it sounded like the NSA just wanted to*
- > *see what the public could come up with. Then IBM submits something*
- > *that was elementary to them, and they just decided to be generous and*
- > *throw in a minor improvement and give it back to the community in the*
- > *form of the current DES.*

No, that is not even close to the actual DES story. For one thing, the solicitation came from NBS, not NSA; also, it is absurd to think NSA would "decide to be generous" and "give back to the community" some minor improvement. NSA did work with the winning proponent of the DES solicitation, IBM, to ensure that the final system would be secure enough for its intended use in securing unclassified but sensitive government information; they would have been remiss not to have done so.