

# Re: Wikipedia "Cryptography" reaches Featured Article status

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00355.html>

---

- *From:* Juuso Hukkanen <[juuso\\_12\\_2003@xxxxxxxxxx](mailto:juuso_12_2003@xxxxxxxxxx)>
  - *Date:* Thu, 13 Jul 2006 13:08:07 +0300
- 

On Wed, 12 Jul 2006 19:53:43 GMT, "Douglas A. Gwyn" <[DAGwyn@xxxxxxxx](mailto:DAGwyn@xxxxxxxx)> wrote:

Roger Schlafly wrote:

ciphers. Bruce Schneier writes:

"Off the record, NSA has characterized DES as one of their biggest mistakes. If they knew the details would be released so that people could write software, they would never have agreed to it. DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure."

[http://en.wikipedia.org/wiki/Data\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard)

They worked with the winning entrant (IBM) to improve the original Lucifer-derived algorithm. How would any of that be a "mistake"?

I found interesting text from 1990 (written by DEG's Butler W. Lampson) which provides some flesh to the bones to said Bruce's statement. Sorry for long quotes

<SNIP>

[In contrast to DES] " Other private-key systems have been implemented and deployed by the NSA for the protection of classified government information. In contrast to the DES, the encryption/decryption algorithms within those crypto-systems have been kept private, to the extent that the computer chips on which they are implemented are coated in such a way as to prevent them from being examined.

</SNIP>

If NSA had always before used to force their algorithms into silicon chips with special "coating", that would clearly tell that NSA did not

## Re: Wikipedia "Cryptography" reaches Featured Article status

want algorithms to be examined. On the other hand such expertise in chip making, makes it obvious that NSA was able to build or carefully evaluate the chances of building the DES–Cracker at the 70's or 80's.

<SNIP>

The DES represents that first time that the U.S. government has developed a cryptographic algorithm in public. Historically, such algorithms have been developed by the NSA as highly classified projects. However, despite the openness of its design, many researchers believed that NSA's influence on the S–box design and the length of the key introduced a trap–door which allowed the NSA to read any message encrypted using the DES. In fact, one researcher described the design of a special–purpose parallel processing computer that was capable of breaking a DES system using 56–bit keys and that, according to the researcher, could be built by the NSA using conventional technology. Nonetheless, in over ten years of academic and industrial scrutiny, no flaw in the DES has been made public. Unfortunately, as with all cryptosystems, there is no way of knowing if the NSA or any other organization has succeeded in breaking the DES.

The controversy surrounding the DES was reborn when the NSA announced that it would not recertify the algorithm for use in unclassified government applications after 1987. (Note, DES has never been used to protect classified, government information, which is protected using methods controlled by the NSA.) An exception to this ruling was made for electronic funds transfer applications, most notably FedWire, which had invested substantially in the use of DES. NSA cited the widespread use of the DES as a disadvantage, stating that if it were used too much it would become the prime target of criminals and foreign adversaries. In its place, NSA has offered a range of private–key algorithms based on classified algorithms that make use of keys which are generated and managed by NSA.

<SNIP>

<http://research.microsoft.com/Lampson/43–ComputersAtRisk/WebPage.html>

HEY, could it be like this: NSA had build their algorithms on specially coated silicon chips and they didn't want anyone to snoop at those build in algorithms, AND they know that when somebody (else) builds a first hardware based DES–cracker, it will tell to every potential enemy that the way of breaking the algorithms (perhaps those in NSA's specially coated chips) is brute forcing the messages with special–purpose parallel processing hardware. Therefore the DES was a failure. And the central piece of evidence lies in NSA's ability to build parallel processing chips at the 70's and 80's. Does that make any sense?

Juuso Hukkanen

www.tele3d.com

(to reply by e–mail set addresses month and year to correct)

Re: Wikipedia "Cryptography" reaches Featured Article status