

# Re: Interesting Discussion with US Government Computer Expert

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/2502.html>

---

*From:* George Ou ([533george\\_ou234\\_at\\_netzero234.com](mailto:533george_ou234_at_netzero234.com))

*Date:* 08/31/03

Date: Sun, 31 Aug 2003 00:56:30 GMT

First of all, RSA or any other PKC system is never used to encrypt data. PKC is only used to initiate a symmetric crypto session. RSA is only used to encrypt a randomly generated session key used for symmetric encryption. You DON'T use RSA to encrypt plain text. You don't even use it to directly sign plain text. You only sign the hash.

The fact is, NO cryptographic implementation can withstand miss use. In WWII, the US had an easy time cracking Japanese encryption codes because the Japanese had a habit of always starting each message with something to the effect of "I am pleased to inform your excellency". A recent vulnerability with an implementation SSL in POP email applications was due to the fact that there was a precipitability in what was sent. Even then, it wasn't the private key that was compromised. It was grossly misrepresented by many as a crack in SSL itself.

This so called security "expert" is one of those people who know just enough to be dangerous.

George Ou

<http://www.LANArchitect.net>