

# Re: Interesting Discussion with US Government Computer Expert

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/2414.html>

---

**From:** Mark Wooding ([mdw\\_at\\_nsict.org](mailto:mdw_at_nsict.org))

**Date:** 08/30/03

Date: 30 Aug 2003 01:02:30 GMT

No One <[no-one-no-spam@home.com](mailto:no-one-no-spam@home.com)> wrote:

> *He implied that RSA-type keys were inherently unsecure because of  
> known plaintext attacks. That is if I have your public key and use it  
> to encrypt one or more text messages (or I guess any other data), by  
> knowing the algorithm I can calculate the private key by comparing the  
> ciphertext and the know plaintext.*

He doesn't understand how public-key encryption is done in practice.

If we just took a message and applied the plain ol' RSA encryption function to it, then yes you'd be able to do the same on some test messages and then, if your ciphertext matches mine then you'd know which message I sent.

To pick a trivial example, suppose that you know that my message says either `yes' or `no'. By encrypting those two strings yourself, you could tell which I'd sent.

But that's such an obvious crapness that we fixed it ages ago. The basic idea is that, instead of sending just `yes' or `no', I pad my message out with random rubbish first. Then, in order to test a guess of what you think my message was, you have to guess the random rubbish correctly.

The best padding schemes provide[1] a security property called `indistinguishability of plaintexts'. That is: if you give me /any/ two messages of your choice[2], and I encrypt one of them at random and give you the resulting ciphertext, guess then there's no efficient way for you to guess which of your messages I encrypted that's much better than just tossing a coin.

[1] Strictly, `are conjectured to provide'. There are schemes which provably provide indistinguishability of plaintexts, under the /assumption/ that a `trapdoor one-way permutation' exists. The RSA function is conjectured to be one of these, but we don't know of a

proof.

[2] Subject to some restriction on message lengths. For example, some schemes might require that both messages be the same length; others might only work on messages shorter than some given size.

-- [mdw]