

Re: Chance of getting a sensible result with a bad key

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4632.html>

From: Peter Pearson (ppearson_at_nowhere.invalid)

Date: 02/26/05

Date: Fri, 25 Feb 2005 16:59:49 -0800

dominicsmith501@hotmail.com wrote:

...

- > *If you have just one block of ciphertext, assuming the keysize and*
- > *blocksize are identical, is it true to say that an exhaustive search*
- > *keys will yield every possible plaintext? Therefore brute force cannot*
- > *work (it is like a one-time pad in some sense).*

If the keysize and the blocksize are identical, the fraction of possible plaintexts that are not produced by any key will be $1/e$, on average.

...

- > *My thought is that if p is the proportion of all possible 16 bit*
- > *messages which "make sense", . . .*

- > *Can anybody make a (justified) estimate of p . I know it depends on what*
- > *"makes sense" means. But presumably when people are trying brute force*
- > *attacks, for research purposes, they do actually have a fixed criteria*
- > *for detecting a sensible message and therefore know what the value of p*
- > *is?*

I don't think people try brute-force attacks for research purposes, but they do them for demonstration purposes, as in the case of the RSA keysearch challenges. In those challenges, 24 bytes of the plaintext ("The unknown message is:") are given. See:

<http://www.rsasecurity.com/rsalabs/node.asp?id=2101>

English text is variously estimated to have between 1 and about 4 bits of information per character. If we use the 4-bit estimate, the number of sense-making 16-character messages is $(2^{**4})^{**16}$, so p is something like $(2^{**4})^{**16}/256^{**16}$.

In contrast, if the text was compressed before being encrypted, it might easily have 7 bits of information per character, which would bring p up to $(2^{**7})^{**16}/256^{**16} = 2^{**-16}$. (In practice, compressed files often begin with relatively predictable header

sci.crypt: Re: Chance of getting a sensible result with a bad key

bytes, though.)

--

Peter Pearson

To get my email address, substitute:

nowhere -> spamcop, invalid -> net