

Re: What is a "perfect secret" ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1099.html>

From: Guy Macon (<http://www.guymacon.com>)

Date: 09/30/04

Date: Wed, 29 Sep 2004 21:06:21 -0700

Gustavo L. Fabro <gustavo_fabro%removethis%@hotmail.com> says...

>I saw one giving an example of a 'perfect secret' being a simple XOR on
>a plain text, using a key with the same size of the plain text. Something
>like this would be impossible to break since the same possibility would
>occur for,
>
>say, 'cat', 'rat', 'tap', 'dog' and so on.
>
>But one could not (that's the question), on such a case, with infinite
>system resources, scan the possibilities of a whole text (say, 2 pages
>of text) "matching" something in some language? Like, in English, if
>20 characters XORed with a brute force trying key matched "the dog is
>beautiful", and no else key did that, wouldn't the cipher be, in that
>case, successfully hacked?

The attacker would indeed find a key that returns "the dog is beautiful."
He would also find keys that return:

the cat is beautiful
the dog is very ugly
your bases belong to
abcdefghijklmnopqrst
We eschew obfuscation
Aaaaaaaaaaaaaagghh!!
<http://guymacon.com/>
)t3cTp(c=^~lL|gyyK!v

...and EVERY other possible 20 character message.

So the attacker with infinite system resources, can't do any
matching with a known language because he will just get a
list of every possible match.