

Re: What is a "perfect secret" ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1110.html>

From: Giorgio Tani (giorgio.tani_at_email.it)

Date: 09/30/04

Date: 30 Sep 2004 00:46:24 -0700

"Gustavo L. Fabro" <gustavo_fabro%removethis%@hotmail.com> wrote in message news:<2s189uF1etngkU1@uni-berlin.de>...

> *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?*

Hi, this is an example of OTP, one important condition for this cypher is that the key ("pad") to xor with the text is true random data, is exactly for this reason that each decryption in each possible message of the same size is equally probable: since all keys are equally probable, all messages are equally probable.

You can certainly reduce the number of possible keys if you know the nature of the message and also part of its content, but it cannot be considered this a successfull attack, in the sense that you not gain further advantages about cracking the cypher, you are simply using what you jet know to reduce 1:1 the effort, but gain no knowledge i.e. on bits of the message you doesn't know or conextually to the content (you know that part of the messge is "See you at "XX but with OTP you could not use it in any way to know if XX is 09, 12, 15, 23, 3!...)

If the key you use is not true random the cypher can be studied in many ways and, yes, doesn't give perfect security even if it is as long as the message.

Remember that perfect secrecy doesn't mean perfect (or even good) security, in example anyone can corrupt a message crypted with OTP and you will need some external check and autentication tools, or the pad can get reused for error leading to a trivial cracking of the messages using the same pad, or the attacker could comprmise the "system" intercepting the key or gaining access to clear message before or after the enryption/decryption, or to memory jet storing temporary parts of the message or of the pad...