

## Re: XOR without repeated key

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/1890.html>

---

**From:** Joe Peschel ([jpeschel\\_at\\_no.spam.org](mailto:jpeschel_at_no.spam.org))

**Date:** 08/28/04

Date: Sat, 28 Aug 2004 02:37:53 -0000

Guy Macon <<http://www.guymacon.com>> wrote in  
news:10ivaacskv81m6b@news.supernews.com:

>

> Joe Peschel <[jpeschel@no.spam.org](mailto:jpeschel@no.spam.org)> says...

>>

>> Guy Macon <<http://www.guymacon.com>> wrote in

>> news:10iusur26685025@news.supernews.com:

>>

>>> Unless you are correcting Tim Smith's minor omission (the key has to be

>>> random, secret, and used once, not just random)

>>

>> Minor omission?

>

> By "minor" I mean "likely to be assumed by the reader."

Ha! That's quite a definition for "minor."

> for example,

> most sci.crypt posts omit the fact that you should keep your key secret.

>

Yes, I think most sci.crypt readers would grant, in this case, that the key is secret. What puzzles me is this: why do some of the readers here assume that the cipher Robert mentions is a one-time pad? All he has said is that the key is as long as the ciphertext, and the key is XORed against the plaintext. He hasn't said how that key was generated. He hasn't said that the key is used only once. Robert's cipher sounds like a stream cipher akin to RC-4 to me. It could be a classical cipher, too.

J

--

---

When will Bush be tried for war crimes?

"Our enemies are innovative and resourceful, and so are we. They never stop thinking about new ways to harm our country and our people, and neither do we." --G. W. B.

Joe Peschel

D.O.E. SysWorks

sci.crypt: Re: XOR without repeated key

<http://members.aol.com/jpeschel/index.htm>

---