

## Re: Johnny Mnemonic

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3092.html>

---

**From:** Rob Warnock (rpw3\_at\_rpw3.org)

**Date:** 10/31/03

Date: Fri, 31 Oct 2003 09:56:33 -0600

G. Orme <newsgroups@harmakhiss.org> wrote:

+-----

| I just read the story and screenplay, that was made into the well known  
| movie with Keanu Reeves. In the story Johnny takes 3 snapshots of a TV  
| signal each from 3 different channels and uses that as a key to encode the  
| data he carries, 320 gig of it.

| The same 3 snapshots are sent to the receiver separately for decryption  
| later. Is this a sensible idea, I assume it is something the author William  
| Gibson thought up.

+-----

Maybe, but he's hardly the only one to use the idea. Vernor Vinge's excellent SF novel "A Fire Upon The Deep" contains the same concept as an oft-mentioned plot element, namely, that a simple way to improve the security of physically distributing OTP material is to generate \*lots\* more pad material than you really need, break it up, and send it via several \*different\* transportation paths [different ships, routes, couriers, etc.]. Alice & Bob then communicate by XOR'ing sections of pads sent by different routes, and using \*that\* as the actual pad for their OTP communications. Even if Eve intercepts & copies one or more of the different versions, as long as she doesn't get \*all\* of them the communication between Alice & Bob will still be secure.

Vinge suggests that "3" is a good number of different couriers/routes to use. That seems like a minimally-adequate number. More would be better, of course, but the costs go up proportionately, and some pairs of sources and destinations may not \*have\* a plethora of alternate routes available between them for the couriers/cargo to take.

[Another poster replied that Gibson had his character take all three TV signals \*himself\*, which is of course a flagrant violation of the "independent couriers & routes" principle Vinge espouses. I'll go with Vinge's method, myself...]

-Rob

-----  
Rob Warnock <rpw3@rpw3.org>

Re: Johnny Mnemonic

sci.crypt: Re: Johnny Mnemonic

627 26th Avenue <URL:<http://rpw3.org/>>  
San Mateo, CA 94403 (650)572-2607