

Re: Stream cipher against block cipher

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/1543.html>

From: David Hopwood (david.hopwood_at_zetnet.co.uk)

Date: 06/29/03

Date: Sun, 29 Jun 2003 08:07:54 +0000

-----BEGIN PGP SIGNED MESSAGE-----

"John E. Hadstate" wrote:

> "aditya" <truman@rediffmail.com> wrote:

> > You guys seem to be having an interesting conversation out here. Whats

> > a block cipher? At times it helps to get back to the basics.....so can

> > I add?

>

> > A block cipher encrypts plaintext in blocks. While a stream

> > cipher encrypts plaintext 1-bit or 1-byte at a time.

>

> The distinction is not so black and white. Some have suggested that a

> better characteristic is to look for the preservation of state across blocks

> or "encryption units". Even this is very slippery ground. How big is an

> "encryption unit"? It could be the size of the whole message. That

> point-of-view sees every "stream cipher" as a very-large-block cipher in ECB

> mode.

A block cipher is any symmetrically-keyed *permutation* (or a family of symmetrically-keyed permutations on blocks of different lengths, in which case it is called a "variable-length block cipher"). A stream cipher is any symmetrically-keyed *encryption scheme*.

Thus modes, including ECB, construct stream ciphers from block ciphers.

Equivalently, they construct encryption schemes from keyed permutations.

The problem occurs when people assume that because these terms have the form "<foo> cipher" and "<bar> cipher", they must be subclassifications of a class of "ciphers" such that "cipher" has a consistent meaning for both cases. "stream cipher" and "block cipher" should each be treated as indivisible phrases, not as applications of an adjective to "cipher".

(A similar problem occurs with "dynamic typing" and "static typing", incidentally, but that's off-topic.)

David Hopwood <david.hopwood@zetnet.co.uk>

sci.crypt: Re: Stream cipher against block cipher

Home page & PGP public key: <http://www.users.zetnet.co.uk/hopwood/>

RSA 2048-bit; fingerprint 71 8E A6 23 0E D3 4C E5 0F 69 8C D4 FA 66 15 01

Nothing in this message is intended to be legally binding. If I revoke a public key but refuse to specify why, it is because the private key has been seized under the Regulation of Investigatory Powers Act; see www.fipr.org/rip

-----BEGIN PGP SIGNATURE-----

Version: 2.6.3i

Charset: noconv

iQEVAwUBPv6RQzkCAxeYt5gVAQG/Ngf+KmnmkXHpHWBFUwXg5fNCeA/0a9ErH8bU
M7UUrG+g2o2T8WBWB7vV28i6yOl+GpbVyvy1RoiL3/yP/igMmghaSSh6CZJsBaY/
qTzcGTyvoTgFu/CCd+7owHfQ19JBY7cxNtBXwI7crxIsnaj3Xj3dH13afqQM2p6p
Pd9l+KYqRnj5g4xESomIpd7aw6J06x5I/xrFzpsQMGolSGRsGut/mCk0n6gOBiKb
aYianntv8NzGahGKOq4iYHwrDHmfMiS7eph67/dHWhqz+t967J/u4c/+75n4xg
gE9srvENgGaOzdviwroUWYwlA28OEM8thqd91jDu0czFOMTCeJnpKA==
=m5XX

-----END PGP SIGNATURE-----