

Re: What's the Toughest Branch in Electronics?

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2007-09/msg01368.html>

- *From:* Bob <bob9@xxxxxxxxxxxxxxxx>
 - *Date:* Sat, 08 Sep 2007 04:31:08 -0700
-

On Sep 8, 4:53 am, ChairmanOfTheBored <RUBo...@xxxxxxxxxxxxxxxx> wrote:

On Sat, 08 Sep 2007 03:02:45 GMT, D from BC <myrealaddr...@xxxxxxxx> wrote:

What's the Toughest Branch in Electronics?

Secure communications. Wired or RF, digital or analog.

Nothing fundamentally difficult about secure comms these days. Review the literature, choose an algorithm that has been in widespread use for a few years without significant vulnerabilities be found and use plenty of key bits.

The problems of things like WEP have arisen due to system designers
a) ignoring the principles that the cryptographers have spent years working out
such as keeping the algorithm secret only helps short term and algorithms created by people who haven't spent twenty years learning cryptoanalysis usually turn out to be insecure.
and b) cutting down the crypto to fit the amount of processing and battery power available. Technology has moved on to the point that should not be a problem anymore.

Bob

.