

sci.crypt.research FAQ

Source: <http://sci.tech-archive.net/Archive/sci.answers/2004-07/0024.html>

From: Moderators (*crypt-request_at_cs.auckland.ac.nz*)

Date: 07/28/04

Date: 28 Jul 2004 04:15:57 GMT

Posting-Frequency: monthly

Archive-Name: cryptography-faq/research

Last-modified: 14 August 2002

URL: <ftp://cryptography.org/scrfaq.txt>

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

Hash: SHA1

Updated 14 August 2002

Last change: updated export regulation information

sci.crypt.research FAQ

1. "What is the charter of sci.crypt.research?"

The discussion of cryptography, cryptanalysis, and related issues in a more civilized environment than sci.crypt. In particular, we are more interested in the technical aspects of serious cryptology. This is a moderated news group. Before posting, you may want to consider if your post would be more appropriate in talk.politics.crypto (discussions of the relationship between cryptography and government), sci.crypt (technical discussions of cryptography, unmoderated), alt.security.pgp (discussion of Philip Zimmerman's Pretty Good Privacy program and related tools, programs, and issues), alt.security.ripem (Mark Riordan's Privacy Enhanced Mail program), alt.security (general computer security issues), or some other group.

2. "How do I submit an article to sci.crypt.research?"

Most news posting software will recognize sci.crypt.research as a moderated news group and redirect submissions to the submissions address. As an alternative, you can send your article directly to crypt-submission@cs.auckland.ac.nz for consideration.

3. "What do you think of my new cryptosystem?"

GUIDELINES FOR POSTING NEW ENCRYPTION SCHEMES TO SCI.CRYPT.RESEARCH

People frequently invent new encryption schemes and protocols and want to share the fruit of their creativity with other people sharing an interest in cryptography. Past experience on sci.crypt indicates that many of these postings tend to be just an annoyance, rather than serious research. In an attempt to cut down on the annoyances, while still encouraging serious research in this area, we have proposed the following guidelines for posting new algorithms.

A. DO research other encryption methods and understand how they work, including both historical and current work. There are lots of good books and journals devoted to this kind of work.

B. DO investigate methods of breaking encryption algorithms, or cryptanalysis. Knowing how a cryptanalyst might go about trying to break a cipher gives you much better insight into how to create a good one. Indeed, among professionals, experience attempting to break encryption methods is considered essential before designing new ciphers.

C. DO COMPLETELY DOCUMENT your algorithm with both a text description and, if applicable,