

sci.crypt.research FAQ

Source: <http://sci.tech-archive.net/Archive/sci.answers/2004-12/0032.html>

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

Date: 12/24/04

Date: 24 Dec 2004 05:19:13 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, computer source code. By "completely document" we mean that the description is sufficient for anyone skilled in the art to implement or simulate your algorithm. If you have doubts about export restrictions on the source code for the algorithm, you may choose to provide a pointer to a place where the source code can be obtained by qualified people, rather than posting it. If you have a complete application using encryption, and you are posting from the USA or Canada, then providing a pointer to the program rather than just posting it is recommended, but the text description should still be posted.

D. DO describe the advantages of your algorithm compared to others in existence, including comparison of efficiency and other relevant design parameters. Make sure that you provide evidence to support your claims.

E. DO try to break your own scheme before you post it. This could save some embarrassment.

F. DO take a look at similar postings from other people on sci.crypt and sci.crypt.research and try to analyze them. This will give you some insight into how others will look at your posting and perhaps allow you to make yours more clear. It also gives you a chance to try to break some other cryptosystems.

G. DO read the sci.crypt FAQ, posted monthly and archived at [rtfm.mit.edu](http://rtfm.mit.edu/pub/usenet/sci.crypt) under /pub/usenet/sci.crypt.

H. DO describe which quantities in your scheme are public and which are private. Explicitly mention what the key is and what the message is.

I. DO include the design principles you used and mention any assumptions you made which you think may be relevant. Explain why you think your system is secure.

J. DON'T expect a response from a ciphertext only ("Try and break this") challenge. Although there are techniques for attacking ciphertext only, most of them require lots of examples, some of which correspond to known plain text. They are also rather time consuming. If you do feel the urge to issue a challenge, you should make sure your posting complies with all of the above guidelines. Offering a cash reward if someone breaks your cryptosystem may help someone to be more motivated to try (and is also a good test of how much you believe in your own system).

K. DO include the information covered in the points above in your posting, or at least include enough to allow people to evaluate your scheme. DON'T post a message containing ONLY a URL and little more.

L. Be ready to carefully evaluate and learn from any feedback you get.

4. "What effect do export regulations have on this group?"

You are advised to familiarize yourself with the current export regulations pertaining to your country. In the USA, a good starting place is at <http://www.bxa.doc.gov/Encryption/Default.htm>. Most postings to this group are international academic discussions pertaining to cryptography and cryptanalysis that are protected as free speech and free publication by the U. S. Constitution (in the USA), and are not restricted from export. In the USA, cryptographic source code relevant to a discussion in this news group may be required to be reported as discussed in <http://www.bxa.doc.gov/Encryption/PubAvailEncSourceCodeNotify.html>.

Discussions of export controls are considered "off topic" for this group, and are better posted in talk.politics.crypto.

Comments, questions, or suggested additions to this FAQ should be directed to the sci.crypt.research moderators at <crypt-request@cs.auckland.ac.nz>.

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

Version: GnuPG v1.0.7 (Cygwin32)

iD8DBQE9WaI5RI/gxxfXR7sRAjM4AJ9UT8u+nwhFJjH/GyZVbmtX9YltACfSTXD
PTPPsv4rKhH+nIU4Vburlc=
=YOa8

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