Obtaining and Using PGP

Recipes from the RXTE Cook Book

- Introduction
- Obtaining and installing PGP
- Decrypting your RXTE realtime data

Introduction

PGP, or Pretty Good (TM) Privacy, is a high-security cryptographic software application that allows people to exchange information with both privacy and authentication. It was written by Philip Zimmermann, and is available free for non-commercial use to U.S. citizens and permanent residents of the United States via MIT. We encourage you to study the information at the MIT Distribution Site for PGP to find out more about PGP. Overseas users should visit the International PGP Home Page for further information.

The RXTE SOF uses PGP to encrypt realtime data, to allow its use by authorized GO teams and prevent use by all other parties. The following recipe, written by the RXTE GOF, tells you how to obtain and apply PGP to RXTE data.

Note that using the recipe below does not absolve you from the responsibility of reading and understanding the documentation provided by MIT and PGP. Also, bear in mind that for various legal and practical reasons the XTE SOC cannot provide the same complete support for PGP as for our own in-house software like Ftools, Xanadu etc.

Obtaining and Installing PGP

1. Connect to the MIT Distribution Site for PGP.

2. Read the page, then click on the "here" at the end of the sentence: "To obtain the current version of PGP from MIT via the WWW click here."

3. Read the files `rsalicen.txt` and `mitlicen.txt`. Please pay particular attention to the export limitations and conditions of use of this software.

4. Answer the four simple questions on the form on the same page, to confirm your status and agreement to the terms of use. Submit the form.

5. If approved, a new page will appear with various flavors of PGP. Click on the version of PGP relevant to your machine (here we assume DOS/Unix, gzipped). The gzipped tarfile will be transferred to your machine, where you should make a new directory for it.

6. Unpack the data:

```
gunzip pgp262s.tar.gz
tar xvf pgp262s.tar   (will create pgp262si.tar, rsaref.tar)
tar xvf pgp262si.tar  (creates PGP source directory)
tar xvf rsaref.tar    (creates the RSA cryptographic toolkit)
```

7. Compile the code:

```
cd rsaref/install/unix
make
```

[If you don't have GCC, type `make CC=cc`. If you have other problems, go back up to the directory level containing the tar files and look again at the `setup.doc` file to find which make options to apply in your specific case.]

```
cd ../../../src
make
```

[This "make" will give you a list of system names. Choose the appropriate system from the list]

```
make {system}
```

8. Move the resulting executable `pgp` to an appropriate bin directory.

Decrypting your RXTE Realtime Data

1. Look in your schedule notification for the access key, which will be a many-digit number.

2. Connect to the anonymous FTP server for the RXTE SOF public access site and save your data to a file on your computer. (In Netscape this is done by holding the right mouse button while pointing to the dataset, and selecting "save link as".)

   Alternatively, FTP to xgo2.nascom.nasa.gov, login as 'anonymous', give your email address as your password, then:

```
cd pub/FITS/
binary
get obsid.tar.pgp
quit
```

3. To decrypt your data, type:

```
pgp obsid.tar.pgp
```

   and when prompted for the pass phrase, use the access key from (1).

4. Untar the data and proceed with analysis, being sure to refer to the RXTE GOF recipe *Working with Realtime Data*.

If you have a question about RXTE, please send email to one of our help desks. This page is maintained by the RXTE GOF and was last modified on Friday, 19-Jun-1998 17:59:58 EDT.

Part of the NASA OSS *Structure and Evolution of the Universe* theme.

A service of the Laboratory for High Energy Astrophysics (LHEA) at NASA/ GSFC

XTE Project Scientist Jean Swank, swank@pcasun1.gsfc.nasa.gov
Technical Rep: Sherri Calvo, sherri.calvo@gsfc.nasa.gov
Questions/Comments/Feedback
NASA's Privacy Statement
Tell me about black holes, astronomy, and more!