Wo finde ich PGP

Grundsätzlich ist PGP auf einigen Fido Mailboxen zu finden.

Kommandozeilenbeispiele

generieren eines Schlüsselpaars: `pgp -kg`

Key in den Bund aufnehmen: `pgp -ka Key.txt`

Durchsucht die Datei `Key.txt` nach einem oder mehreren Keys und nimmt diese in den Pubring auf.

Verschlüsseln: `pgp -ea Msg.txt "Franz Fiala"`

Verschlüsselt die Datei `Msg.txt` mit dem Public Key von Franz Fiala.

Umgang mit PGP-Servern

Der Umgang ist recht einfach. Man schickt eine E-Mail an den Server. Im Subject steht das Kommando und eventuell im Mailbody der betreffende PGP Public Key.

Die Kommandos:

Command	Message body contains
`ADD`	Your PGP public key (key to add is body of msg) (-ka). Mit diesem Befehl hängt man einen Key in den Ring des Servers.
`INDEX`	List all PGP keys the server knows about (-kv). Liefert eine Liste der verfügbaren Public Keys.
`VERBOSE INDEX`	List all PGP keys, verbose format (-kvv). Auch eine Liste der Keys, aber mit mehr Infos.
`GET`	Get the whole public key ring (-kxa *). Damit bekommt man alle Schlüssel (Vorsicht! Riesendatei)
`GET <userid>`	Get just that one key (-kxa <userid>). Schickt einen einzelnen Public Key.
`MGET <userid>`	Get all keys which match <userid>. Gleich wie GET aber mit Patternmatching (Wildcards).
`LAST <n>`	Get all keys uploaded during last <n> days. Wird verwendet, um die neuen Keys der letzten n Tage zu holen.

Also wenn man z.B. seinen Public Key an den Server schicken will, dann schreibt man den Befehl 'ADD' ins Subject, der Key ist im Msgbody.

Liste der Server

pgp-public-keys@uit.no
pgp-public-keys@informatik.uni-hamburg.de
pgp-public-keys@kub.nl
pgp-public-keys@pgp.ox.ac.uk
pgp-public-keys@pgp.pipex.net
pgp-public-keys@dsi.unimi.it
pgp-public-keys@goliat.upc.es
pgp-public-keys@srce.hr
pgp-public-keys@kiae.su
pgp-public-keys@ext221.sra.co.jp
pgp-public-keys@sw.oz.au
pgp-public-keys@pgp.mit.edu (*)
public-key-server@martigny.ai.mit.edu (*)
pgp-public-keys@pgp.iastate.edu (*)
pgp-public-keys@burn.ucsd.edu (*)
pgp-public-keys@pgp.dhp.com (*)
pgp-public-keys@jpunix.com (*)
pgp-public-keys@gondolin.org (*)

(*) Key servers in the USA only accept keys labelled "Version: 2.4" or later.

Sites accessible via WWW:

http://www.service.uit.no/pgp/servruit.eng.html
http://www.cl.cam.ac.uk/PGP/pks-toplev.html
http://www.nic.surfnet.nl/pgp/pks-toplev.html
http://goliat.upc.es/~alvar/pks/pks-toplev.html
http://martigny.ai.mit.edu/~bal/pks-toplev.html

Key server keyrings accessible via FTP:

ftp://ftp.uit.no/pub/crypto/pgp/keys/pubring.pgp
ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/pubkring.pgp
ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP/public-keys.pgp
ftp://ftp.ox.ac.uk/pub/crypto/pgp/keys/pubring.pgp
ftp://ftp.sunet.se/pub/security/tools/crypt/pgp/keys/pubring.pgp
ftp://ftp.funet.fi/pub/crypt/cryptography/pgp/keys/pubring.pgp
ftp://pgp.mit.edu/pub/keys/public-keys.pgp
ftp://pgp.iastate.edu/pub/pgp/public-keys.pgp
ftp://burn.ucsd.edu/Crypto/public-keys.pgp
ftp://jpunix.com/pub/PGP/

Schnellste Zusammenstellung über PGP

ftp://ftp.tuwien.ac.at/pub/auxc/privacy/crypto/pgp

Weitere Info auch auf

http://www.pgp.net□

The Evolution of a Programmer

High School/Jr.High

```
10 PRINT "HELLO WORLD"
20 END
```

First year in College

```
program Hello(input, output)
begin
  writeln('Hello World')
end.
```

Senior year in College

```
(defun hello
(print
(cons 'Hello (list 'World))))
```

New professional

```
#include <stdio.h>

void main(void)
{
  char *message[ ] = {"Hello ", "World"};
  int i;

  for(i = 0; i < 2; ++i)
    printf("%s", message[i]);
  printf("\/n");
}
```