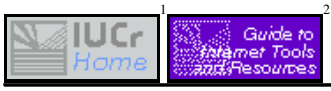

PGP – Public Key Cryptography

There is little security in basic Internet services such as e–mail. One can not be sure that a message:

- really comes from the address in the `From:` field,
- has not been intercepted and read by a third person and
- has not be tampered with or altered.

PGP – Public Key Cryptography is designed to make e–mail secure by pre–processing the message body prior to transmission. In this system each user owns two related keys:

Public key
: This is used for encryption and should be made public. It may be distributed freely and openly. People very often include it in the signature file of their e–mails or make it available on their WWW home page. One should always take steps to verify that a public key really comes from the person who claims to have sent it.

Private key
: This is used for decryption and should be kept strictly private.

A person who has a copy of your public key will be able to encrypt a message that subsequently only you will be able to read by using the private key.

PGP Functionality

Key management:
: PGP generates the personal key pair, extracting and adding public keys from and to your public key ring, supports key verification and digital signatures on documents.

Digital signatures – creation:
: For the person with access to the private key, a digital signature can be added to message. PGP adds starting and ending marks to the message and right at the end a digital signature in the form of line of characters.

Digital signature – verification:
: On receipt of a digitally signed message, PGP removes the starting and ending marks and checks that the signature matches the contents. This operation requires knowledge of the public key of the originator. The check proves that the person signing the message had access to the private key corresponding to the public one.

Encryption:
: Using the public key, PGP transforms the message into an apparent jumble of characters.

Decryption:
: Using the private key, PGP transforms the message back into clear form. This ensures that the message can only be read by someone having access to the corresponding private key.

PGP – Usage

On first use of PGP, a pair of related keys (one public and one private) are created and stored in separate files, called key rings. The private key resides in encrypted form on the private key ring, the public key being on the public key ring. To send a secure e–mail one must undertake the following operations:

1. The public key must be extracted from the public key ring and be communicated to all people with whom one wishes to have secure communication. A fine way to do this is to put the public key on a public key server[3]
2. Collect the public keys from your partners and put those keys on your public key ring.

[1] http://www.iucr.ac.uk/iucr–top/welcome.html
[2] int.index.html
[3] http://www.ifi.uio.no/pgp/

3. Verify and electronically sign the public keys you have received. PGP can display a so–called fingerprint of a public key and suggests that you verify the correctness of the key by comparing the fingerprints over the phone or during a meeting with the owner of the key.

The use of PGP is illegal in some countries. The issuing of the keys does not depend on the presence of any external authority or regulatory body. The safeness of the system depends on the distribution of the private keys which is left entirely in the hands of the user. Some other systems of encryption, such as PEM (Privacy Enhanced Mail), depend a certificate hierachy in the hands of a certification authority.

Further information on PGP

1. PGP Workshop[4] from *Electronic Frontiers Houston*
2. International PGP Home Page[5]
3. List of PGP Tools[6]
4. Binaries of PGP Software[7]
5. Public Key Cryptography[8]

[Index[9]] – 21st June 1996 – © Howard Flack[10] – **Not to be copied or reproduced without permission**

[4] http://www.efh.org/pgp/pgpwork.html
[5] http://www.ifi.uio.no/pgp/
[6] http://www.ifi.uio.no/pgp/utils.shtml
[7] http://www.ifi.uio.no/pgp/download.shtml
[8] http://stasi.bradley.edu/privacy/public_key_krypto.html
[9] int.index.html
[10] ../ahdf/Howard.Flack.html