rootCON®

PGP Key Signing Party Introduction

Key-ID: F108E41A

Fingerprint: E6E9EB7811C0B BE0196091E91B5 08441F108E41A

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

--Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C.

What is PGP?

- PGP - ("Pretty Good Privacy") **- Privacy software developed by Phil Zimmermann, which includes public key cryptography, a standard packet and key format, and symmetric encryption as well.**

- PGP is a ***cryptography***

- Cryptography **is the science of using mathematics to encrypt and decrypt data and it enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient**

rootCON

Why do we need PGP?

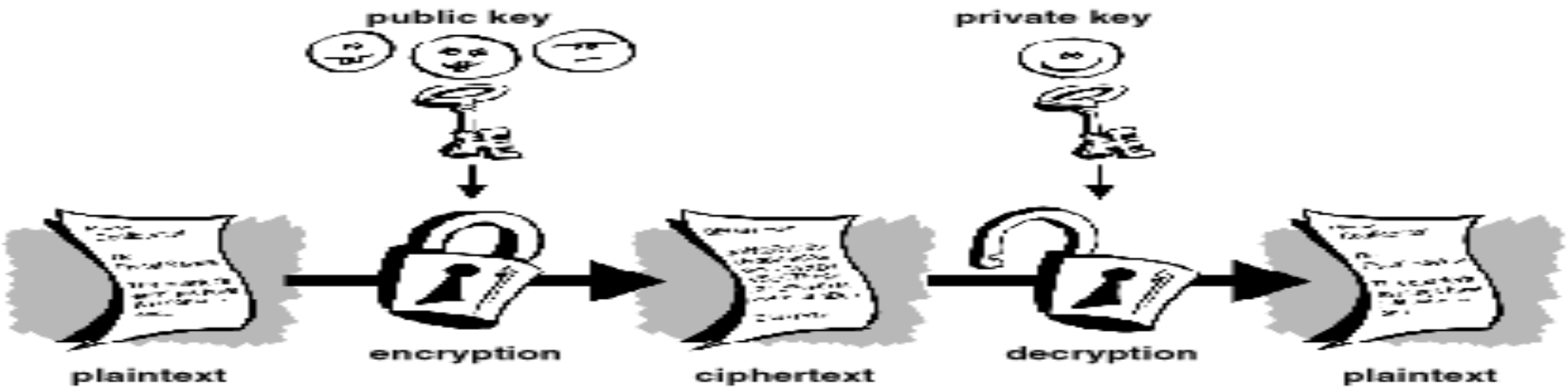
** for security*
** for personal*
** for private*

How PGP works?

The basic concept :
You generate a pair of matched keys. One of these is referred to as your "Public" key, and the other as "Private/Passphrase". You give the Public key to anyone who asks for it or you can even publish it on your web site.

The public key is always the one that you make public, and the private key is always the one that you keep private.

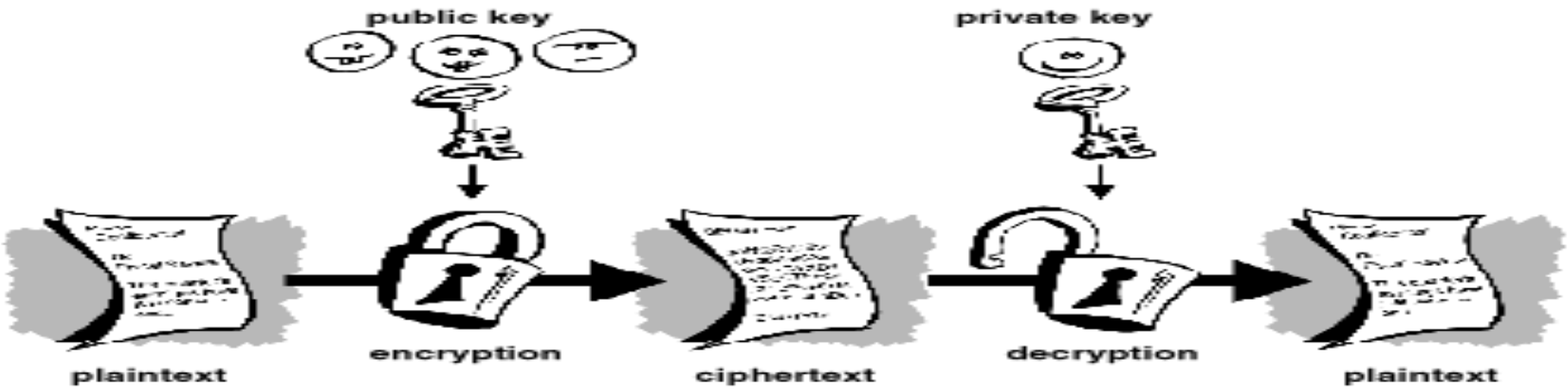
In fact, if you don't get the public key for the person receiving the email, then you cannot encrypt an email to them. This is also true for the person sending email to you - if they don't have your public key, then they can't send you encrypted email.



How PGP works?

How do you exchange public keys?
Either directly, sending them to each other... or by putting your public key on a "keyserver".

For example:
If you want to send me something, you'd encrypt it using my public key. No one else can decrypt it; only my private key will work. On the other hand, I might be concerned that it really is you sending me a message. In that case, you'd encrypt your message using your private key (this is called "signing"). If I can decrypt it with your public key (presumably I somehow obtained that key and trust that it really is yours), I know that the message really came from you.



Benefits of using PGP?

*The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely.

*The need for sender and receiver to share secret keys via some secure channel is eliminated;

*All communications involve only public keys, and no private key is ever transmitted or shared.

rootCON

PGP key signing party

A key signing party is a get-together of people who use the PGP encryption system with the purpose of allowing those people to sign each others keys. Key signing parties serve to extend the web of trust to a great degree. Key signing parties also serve as great opportunities to discuss the political and social issues surrounding strong cryptography, individual liberties, individual sovereignty, and even implementing encryption technologies or perhaps future work on free encryption software.

rootCON

Types of PGP key signing party

There are different possible structures for keysigning parties. These different formats were designed to accommodate the increasing levels of participation as PGP has become more popular. The sections below describe three of the most common methods and provide instructions for each one.

1. Informal Method Party
2. List Based Method Party
3. Hash Based Method Party

Informal Method Party

1. The most common type of keysigning party is the informal party. Ideally, you should bring small pieces of paper with your name and pgp key fingerprint on them to hand out to people. Many people now have their PGP key fingerprint printed on the back of their business card along with the address of a preferred keyserver where people can download an up to date key. They also often include a small "verified" checkbox that someone can mark if they choose to check identification.

List Based Method Party

For a list based party, more coordination is necessary. A list PGP key fingerprints of everyone who had planned to attend the party is created by the party coordinator. The Coordinator can post the list on the web so that recipients can print it out, or much better can bring copies to the party for everyone.

The Coordinator should check and verify the identification and verify fingerprint information for each person at the party on against your list.

Hash Based Method Party

The Hash Based Method Party Specifically for numerous participants, parties involving a few hundred people . The party must be pre-announced. Key information is collected by a coordinator who publishes the list along with a hash value.

At the party, the entire group of participants should be asked if they are present and if their key information is correct. If no objections are raised, no one is absent, identities are verified, and the hash value for the master list is verified by all participants all keys on the list can be digitally signed.

Other useful PGP links

A few more links for PGP newbies, or those who wish to re acquaint themselves.

http://www.pgpi.org/ -- The International PGP Home Page
http://www.pgpi.org/download/ -- Download PGP
http://www.gnupg.org/ -- GNU PGP (Linux)
http://www.pgpi.org/products/tools/search/ -- PGP Tools, Shells, and Plugins
http://www.gpg4win.org/download.html
http://www.coresecure.com/v5/gnupg.html

Thanks for Listening…

Enjoy the booze and keep on hackin’

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.14 (MingW32)

mQENBEy/l3YBCADWzaMyqJu6fTA6/dZpZa+paAAHwcOwGKkV4sJ/q+i3Y5FqzW79
8t3GbCGmRYpNdsso0io9HBO1RoGrzdhkj5NstrtPW/TntfQmAxLFbkHnq91jyGNo
WVdJiT8+DlJKy2ZdKXsjF967N+BAZApR4wxxTuxLr811iEMBGjfqjCI1cuNzpmUa
t6IwmM72L8agIPbb/ifh9u/VHo8ptwlmJO1iO+mobpoqdjzv2+Igm5kxcoqe3PQR
iriBY24N+kwVsgJo8+LoZgoc32rcgMVGbohQ7ckHAKErw+Qpo4wgO5aoQyH2a5fk
qQICTWer8gVek/YN2gJJ+VWLFofFqfLg573lABEBAAG0IoRyZXggUmFraXNoYSA8
aGFrZXJyYWtlckB5YWhvby5jb20+iQE4BBMBAgAiBQJMv5d2AhsDBgsJCAcDAgYV
CAIJCgsEFgIDAQIeAQIXgAAKCRDpoFQETHIACV37CACZ3rvO16xUKpHijvrbTE2x
vTphlSb5YZ/ZTFiAImAQ3QXxNHjyjBzoTHVeC5gvHuI2Ip4Dk2Cq8Pg66rzy9FxA
Qs3d2inAaCPJTQnU1xbPyRPoJoewSMlOETs4dVSi8MTPnz1UhQlfebYmdHmqhORA
ZvoZAmM28RfQhqFCM3TlideTk10VtYtHJsi4QIBQzbePaF3GWzxVJjv1Z2KjXo3V
aboyAH67cjz+khR5SOdS95NysfzuobeHesDBaymnsbDCCwAuK7geYFak9BZsWOIp
cjaViOsR/cp7e4InCnJ2fnoZ8w4DVEAzuseLGktmPDExKT9kKMydJQAqLBRxJOUM
uQENBEy/l3YBCACeLrqpR+tqBSgG8uo9QihFNzNfvzs987WSigYgeYjVZ8ZipppF
Z9IPA4iAyo3lPsSrbEab/ESMNKearhIrlB8FRQ8lmmTQBpoBPW7x28Jb8CbNZvHE
UzXttyiiIoEwsB7mnjtrRdWQeib2wgQUz4nBaPrZ64SyKni8E+TGKfX1YETAGjIN
8Gwcp2D36sWCRoisqKMJHXoDXqJ4BW5VoOrLdB7wh+SaSjjjxwpmZjD1QXE+Gmmo
1yawnSkHF127a4ht7iiJJVtFX4KLCu401XWntlv+ioTo++gvlLhQH8aEq6kPga5d
++873374a7TES7bd2LKw0YaU8JEZ2QTOo56RnABEBAAGJAR8EGAECAAkFAky/l3YC
GwwACgkQ6dBUBExyAAn64wgAgTJfWY14kr7lrIEcvvS3lfB+mQAFDvfNjFi+rWs1
TlAZc8gqN1Hv1idwW9hU9EpY6/oe4MhQmocK4R5hrqZtp5phpEXmNte6AVyXCDH
7fZYg1QVEAEJD+pM5/YGQgrY2NSLg3uiiGJaXeEsZeoD5znhmJ/Fp6blsn5DgzFa
Nx+J6+HTTSx5mbJWyFrmOjMmFlBysc5c+chf6hLBDZgC+8u2GEgJbgujLddb10is
EzjsdMgFa8uhv32H29R629YlSktQ/+qowOEsF7/lixuJlreCCsPFvkntFLZvNVzn
IQTq42zmfJ7ucbUSNxNw4ouCq07OK+U5/d8pVpxImZWRRQ==
=N9Nr
-----END PGP PUBLIC KEY BLOCK-----

Key-ID: F108E41A

Fingerprint: E6E9EB7811C0BBE0196091E91B508441F108E41A