

An introduction to Cryptography, OpenPGP and the Free Software implementation : GnuPG.

""I have even had 13 days in prison for not revealing our PGP pass phrases, but it was a very small price to pay for protecting our clients."" a NGO in the Balkans.



Alexandre Dulaunoy - <http://www.foo.be/>
adulau@foo.be

Agenda

- ☐ Cryptography
- ☐ Misconception around cryptography
- ☐ Symmetric cryptography
- ☐ Asymmetric cryptography
- ☐ Hybrid cryptosystem
- ☐ PGP/OpenPGP History
- ☐ GnuPG initial setup
- ☐ GnuPG signing key
- ☐ GnuPG encrypt/decrypt
- ☐ GnuPG signature
- ☐ GnuPG web-of-trust
- ☐ Bibliography/ref/link
- ☐ Q&A and key signing ?

Cryptography

- Cryptography provides these functions :
 - Confidentiality (or privacy)
 - characteristic of a communication which prevents eaves-dropping
 - Authentication
 - process of identifying the user accessing the system, server, or data
 - from shared secret to digital signature
 - Message Integrity
 - characteristic of a communication which ensures the data received is the same as the data transmitted
 - digital signatures assure both that the signer actually originated the message and also that the transmitted message has not been altered
 - Non-repudiation
 - difficult/impossible to deny a correct message

Misconception about cryptography

- ❑ Security is a process not a product
- ❑ Obscurity is not security
- ❑ "Snake oil"
 - <http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>
- ❑ We can't use it
 - <http://rechten.kub.nl/koops/cryptolaw/cls2.htm#be>
 - Free usage in Benelux but a licence is required for exporting
 - Criminality law : decryption order
- ❑ Cryptography is a complex matter

Symmetric cryptography (Private-key cryptography)

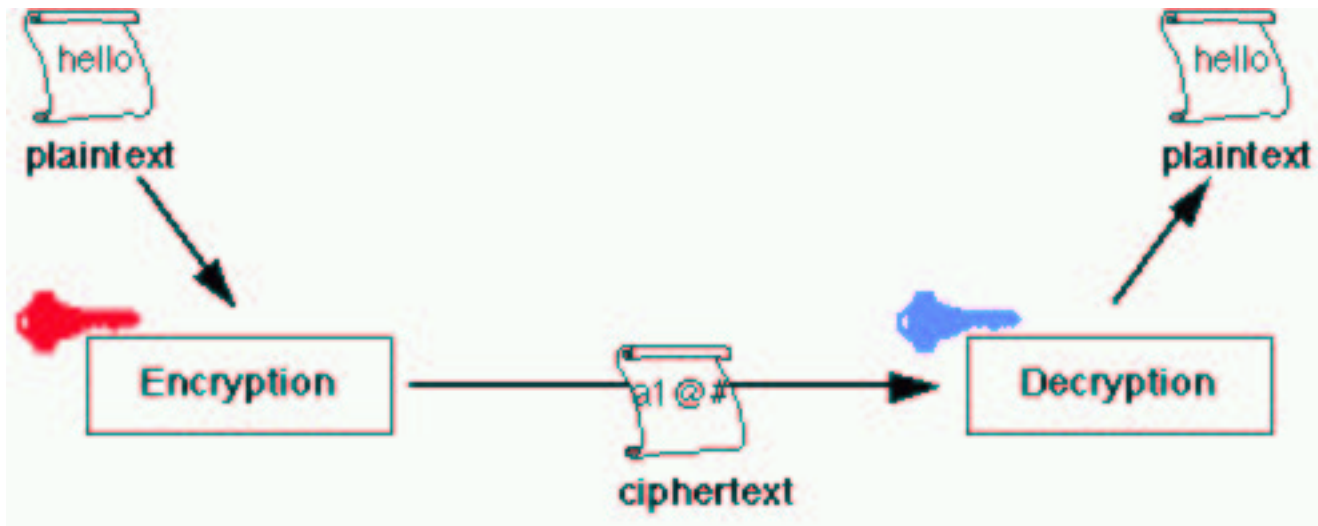


- Security is in the key

- Issue

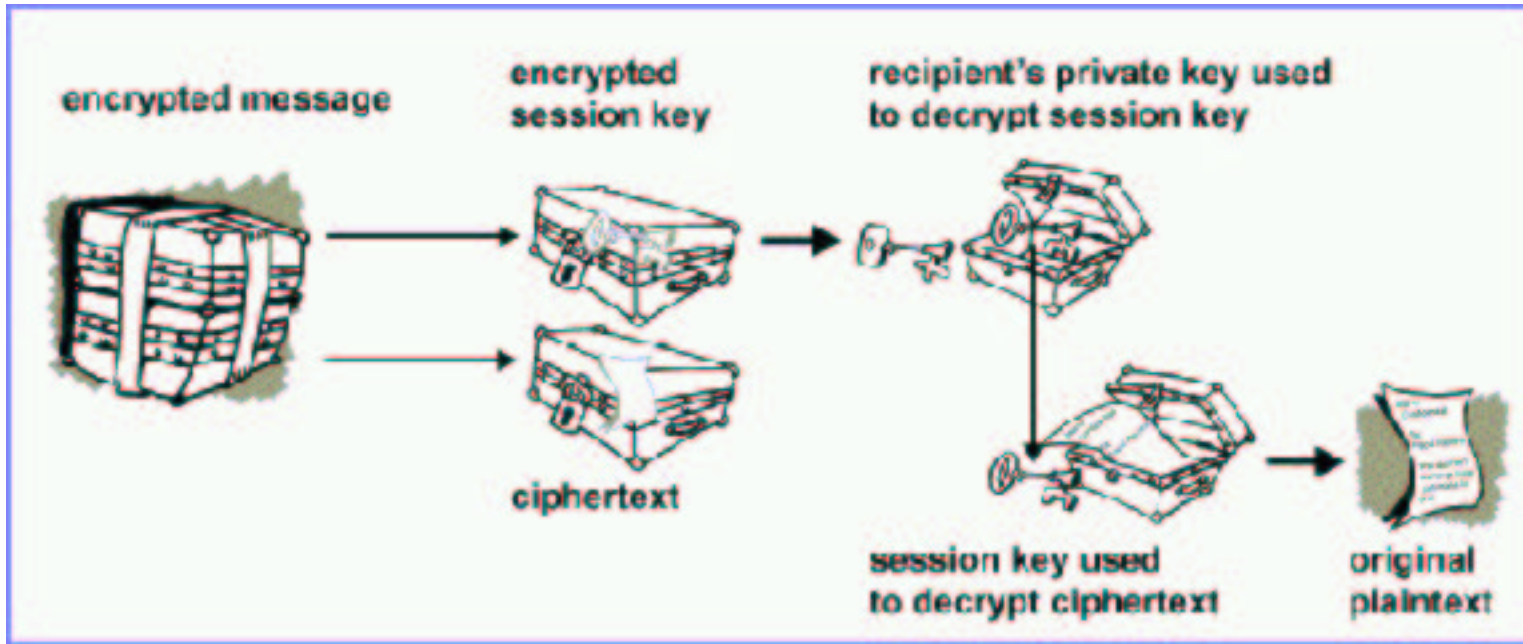
 - Secret channel to transmit the key

Asymmetric cryptography (Public-key cryptography)



- ☐ Concept by Whitfield Diffie and Martin Hellman (1976 IEEE)
 - A public-key cipher uses a pair of keys
 - The two keys are for the same persons (one public, one private)
- ☐ Security is also in the keys like symmetric cryptography
- ☐ Issue
 - Slow
 - Key size (>1024 bits)
- ☐ -> Elgamal RSA (reversibility)

Hybrid cryptosystem



- ❑ Combined usage of symmetric cryptography and asymmetric cryptography
- ❑ A hybrid cryptosystem is no stronger than the weakest cipher (Asymmetric)
- ❑ -> OpenPGP, SSL/TLS are hybrid cryptosystems
- ❑ In OpenPGP, session key is variable for each messages

PGP/OpenPGP History

- Phil Zimmermann in 1991 introduced the first version of PGP
 - > Legal issue
 - > Usable tools
- PGP Inc in 1996 -> NAI
 - > John Callas (and others) -> OpenPGP / RFC
- GnuPG (Werner Koch)
 - full OpenPGP implementation
 - released under GNU GPL and part of the GNU project
 - backward compatibility with old proprietary PGP NAI

GnuPG initial setup

- Install GnuPG (<http://www.gnupg.org/>)
- Generating a new keypair
 - `gpg --gen-key`
- Generating revocation certificate for all cases
 - `gpg -output revokeX.asc --gen-revoke myname`
- Make a copy of the `.gnupg` directory and all the revocation certificates and put that in a secure place
- Export your public key to keyserver (pgp.mit.edu) and website
 - `gpg --armor --export myname` (if not armored, binary format)
- and now, there is nothing secure ;-)

GnuPG signing key

- ❑ Importing the key

- `gpg --import friend.gpg`

- ❑ Check the fingerprint with your friend (PHYSICALLY !! with identity card)

- `gpg --fingerprint yourfriend`

- ❑ If it's ok, sign the key

- `gpg --sign-key yourfriend`

- ❑ Send the signed key to him and to the keyserver

- `gpg --armor --export yourfriend`

- ❑ Too complex ? : <http://aplit.org/damien/gpgsig/>

GnuPG encrypt/decrypt

- Sending a crypted document to your friend
 - `gpg --output document.gpg --encrypt --recipient yourfriend document`
- Your friend (with private key) will do that to decrypt
 - `gpg -output document -decrypt document.gpg`

GnuPG signature

- Sending a signature of the document to your friend
 - `gpg --output document.sig --sign doc`
- Sending a detached signature of the document to your friend
 - `gpg --output document.sig --detach-sig document`
- Sending a clearsign of a ascii file
 - `gpg --clearsign document.txt`
- GnuPG web-of-trust
 - (unknown, none, marginal, full)
- [img]

Bibliography/ref/link

□ Introduction to cryptography

- The Code Book, Simon Singh (ISBN 1-85702-889-9)
- Applied Cryptography, Bruce Schneier (ISBN (fr) 2-84180-036-9)
- <http://www.foo.be/docs-free/applied-cryptography/>
- Introduction to Cryptography with Coding Theory (0-13-061814-4)

□ Cryptography and network security protocol

- Network Security Essentials, William Stallings (ISBN 0-13-016093)
- OpenPGP Message Format, RFC-2440
<ftp://ftp.isi.edu/in-notes/rfc2440.txt>
- GNU privacy Guard <http://www.gnupg.org/gph/en/manual.html>

□ Advanced cryptography and cryptosystem

- Modelling and analysis of security protocols, Peter Ryan (ISBN 0-201-67471-8)
- Making, Breaking Codes: Introduction to Cryptology, Paul Garrett (0-13-030369-0)

Q&A

- 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
(adulau@foo.be)