

CRYPTOGRAPHIE

1. Introduction :

1.1 Pourquoi chiffrer le courrier électronique ?

Il faut savoir que lorsque vous envoyez un message électronique depuis votre poste, celui-ci transite par plusieurs ordinateurs avant d'arriver sur l'ordinateur du destinataire. Ce voyage n'est pas sans péril, en effet, derrière ces ordinateurs se cachent, des entreprises, des administrations ou des personnes peu scrupuleuses qui pourront lire votre courriel qui circulent à découvert, c'est-à-dire non chiffré sur Internet « comme une carte postale sans enveloppe ».

L'intérêt du chiffrement est là, il vous permet de cacher des informations portant sur vos secrets professionnels ou tout simplement sur votre intimité.

1.2 Présentation de l'outil :

GnuPG est un logiciel gratuit destiné à remplacer PGP. Il peut être utilisé sans aucune restriction parce qu'il n'emploie pas l'algorithme breveté IDEA . GnuPG est une application se référant au RFC2440 (d'OpenPGP)..

2. Installation :



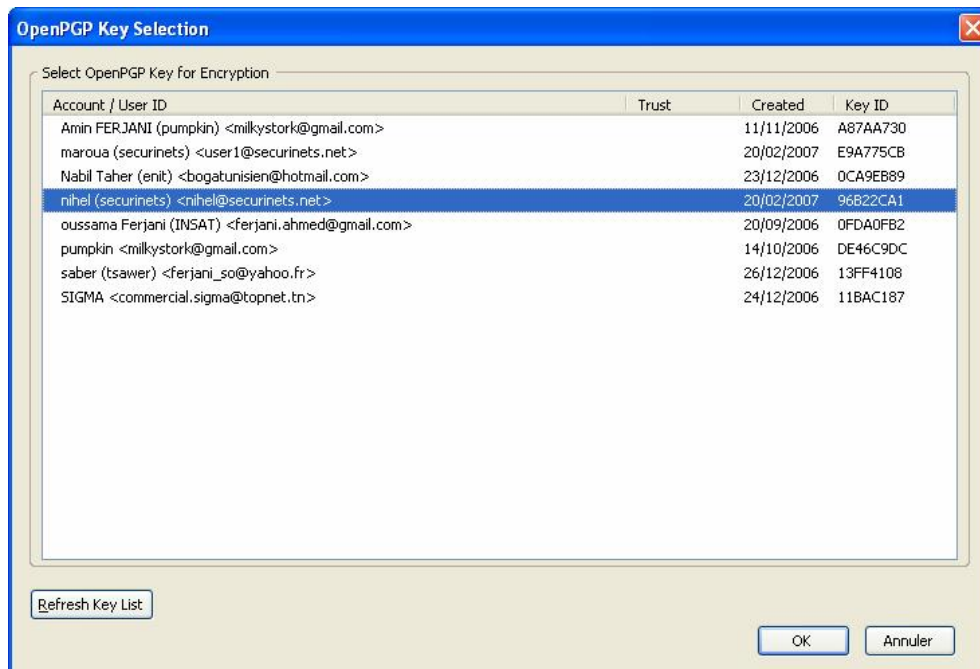
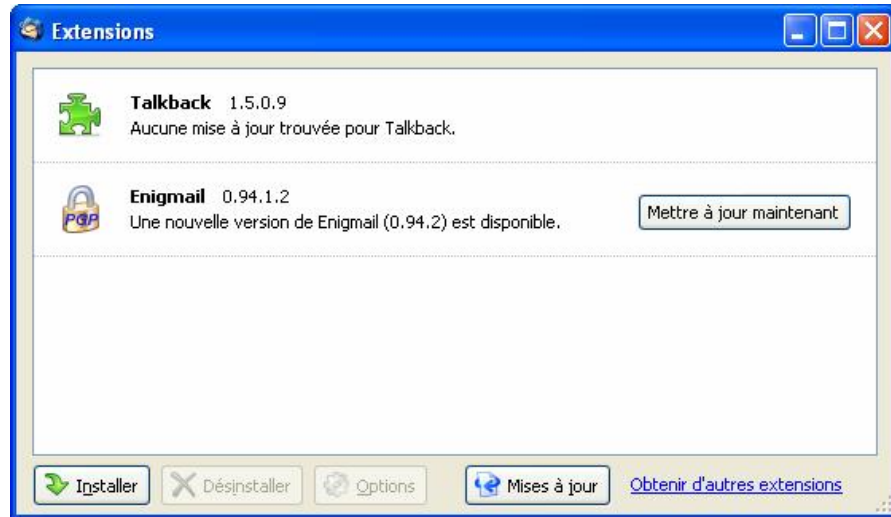
- installer *gpg4win-1.0.8.exe*
- Ajouter une extension à votre client de messagerie pour qu'il puisse gérer les opérations de cryptage

ThunderBird ► Outils>extensions>installer *enigmail-0.94.1.2.xpi*

Outlook ► installer *GDATA_plugin_091-eng.exe*



S E C U R I N E T S
Club de la sécurité informatique
I N S A T

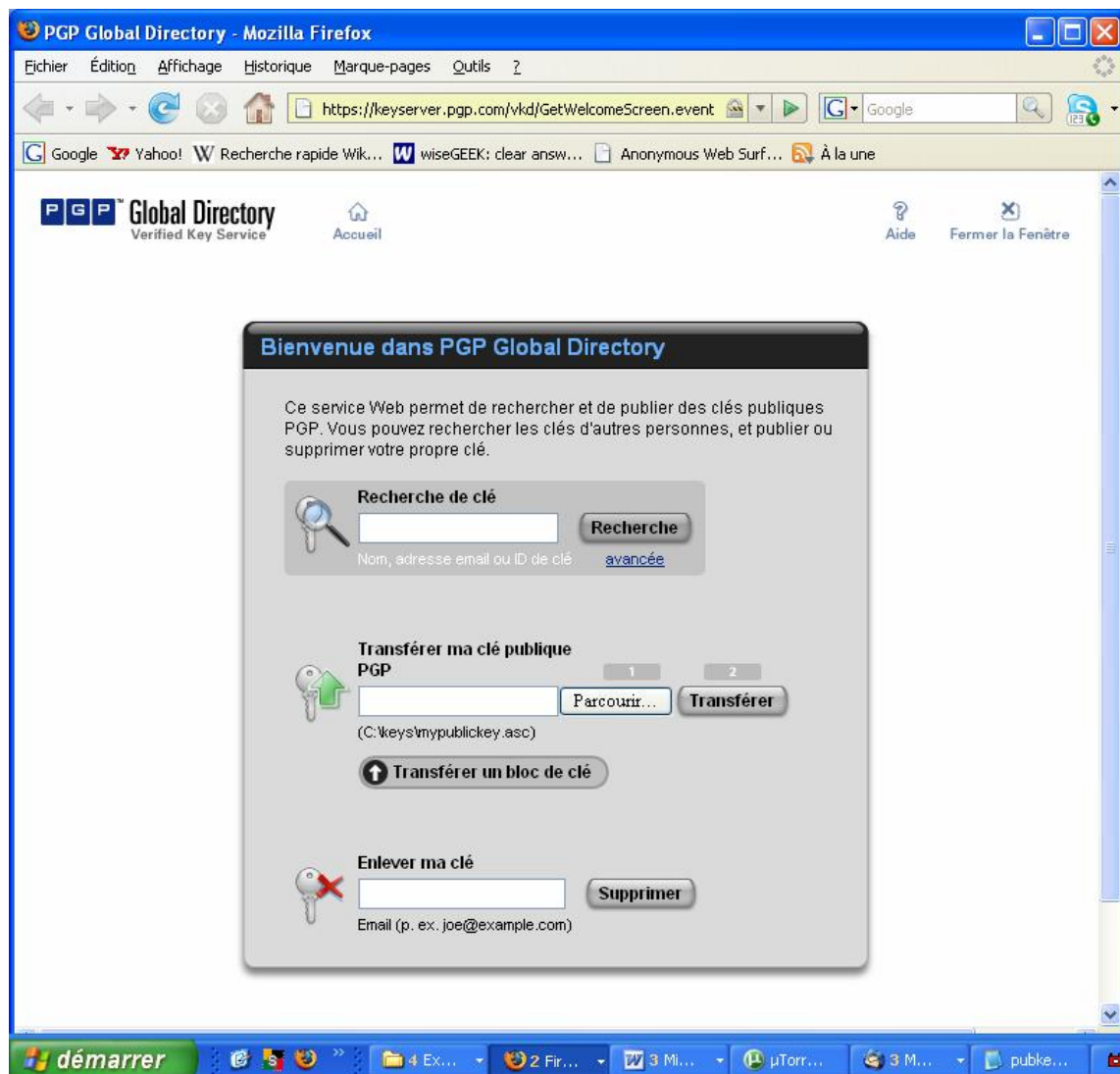




S E C U R I N E T S
Club de la sécurité informatique
I N S A T

3. Préparation de l'utilisation :

- Créer une paire de clé
- Publier votre clé publique sur l'un des serveurs de clé les plus connus
 - random.sks.keyserver.penguin.de,
 - subkeys.pgp.net, pgp.mit.edu,
 - ldap://certserver.pgp.com
 - https://keyserver.pgp.com





S E C U R I N E T S
Club de la sécurité informatique
I N S A T

```
pubkey_pumpkin.txt - Bloc-notes
Fichier Edition Format Affichage ?
pub 1024D/DE04B051 30/07/2006 pumpkin <milkystork@gmail.com>
  Primary key fingerprint:  A012 EA89 F28E 7BD5 D40A EDC6 84A0 901E DE04 B051

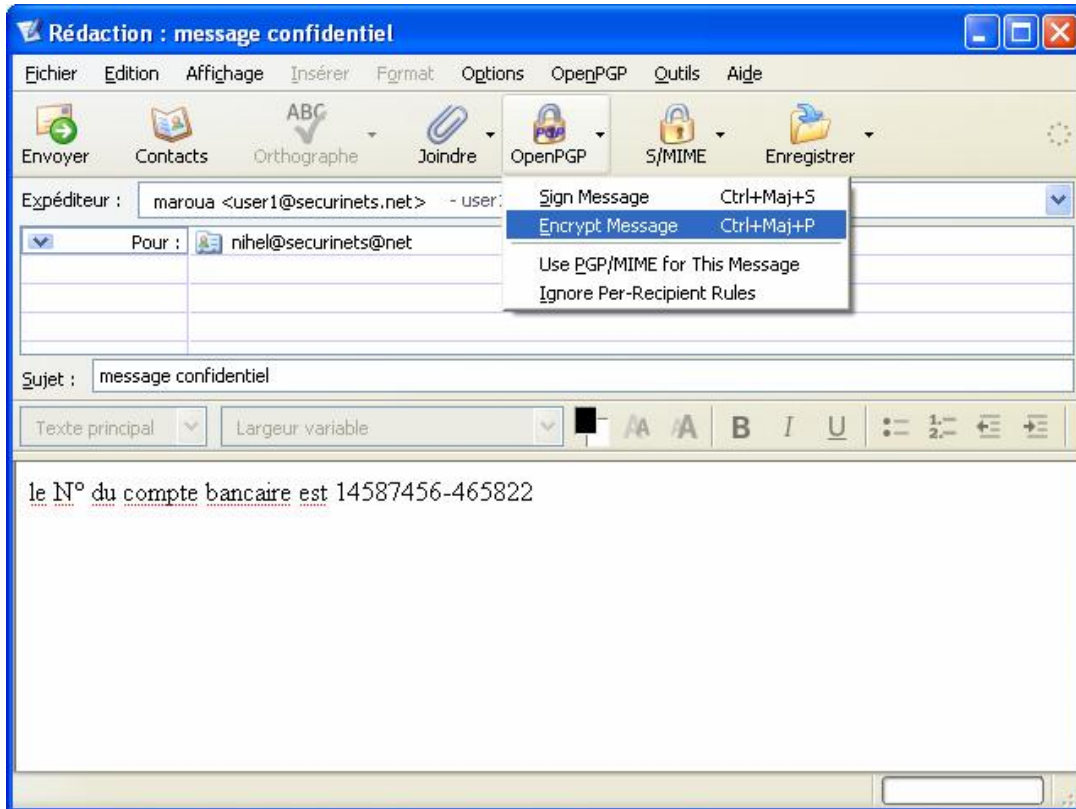
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.4 (Mingw32) - winPT 0.12.3

mQGfBETMRVIRBACFrFWUA4MXN8VVbnjt0ow1ImhCCyhcuu+x6j9/wGfs+BasdHWQ
szd1xufkqmg2iWA6uD788FFIh3LIzod6h4L1y6rpgiD091Tts1G4oG6m/zoh250U
paD+IsFdigyHqQxREYEs644aGUv0iXRr21yUF6MC65bnZRgk5F5qopQCzwcg8VPS
kOMRxcuA2YcuAqDSI+yzbkD/jdagkumWU2knjAjMG725pFHUNL7ZPo4ZyaC33Mi
x+iu+8WRwJFUHPaxxbEwOnwhTesiLS+mvarb+YjhxJUoq57Kxgm3aouoz65mXJ
at0IX2iN8EWTJAG+6+wauYTeew+eLeTCgmyjYLQFTLKU7OUETw6RU+dxvi/uawtN
f+RxA/0UhuKCLUBQ0T1YvTt+wTN7LwiZF+rCYTOPLUnssU/1Du0enk3gG0vXIotF
DvnHwRoqz1U2cMkP2jnIm+AYyvSZ+wsw+a8WNXNgeQk2huim3+oBfng2wELm1xpc
v1soo0uHnhv7i7cLhIgtmjslVF9q0gyyxNgALd3j6AJBFwstKLQechvtcGtpbiA8
bw1sa3lzdG9ya0BnbwFpbC5jb20+igAEEeXECACAFakTMRVICGyMGCwkIBwMCCBUC
CAMEFgIDAQIEAQIxAAGKCRCEoJAe3g5WUZokAJ91yC8S0p7G4bLAXR8bwcr/m41B
4qcFwf4Jph84Bd74QwwiUUUIqbtVG7m5AQ0ERMxFVBAEAOr6cFG4SXlo+6VEgOVI
o0l+CcmbQeTaPr0XUV2z0g3PzLXYg/N53w8GZF/01qbH0y+CBZlUX2GJMSm7pCQI
IXup2/FHjlyVpBPGgo0+oBBA+9h9IfgE+Yl09R9bsPJ0fmNLwy8KZxvrBalLmkKB
J7baBkdEab3F3uxrAlaboPnAAMFA/4oxvk1EUcep/ak/qj6bnznjjiEpx/TARHF
WEhdtx1+TJ7dsi0iNXSPHweCLlIwygtW0YZ5YK3cF/NZMaItYovB1w38FKdx06tI
74jkmPghSmABCwxtj7ds3cnfElavrFkHQwTruopHpmmeIVoibr1Hc5uQmX9xfagq
vY2dkf8mBYhJBBgRAgAJBQJEzEVUAhSMAAoJEISgkB7eBLBRcyAAoLGRi+h+xt1K
mzPHWUMLsfilfwxAJ47dsFF1wpeowuc1D7q0gzPu2RpLw==
=2pk7
-----END PGP PUBLIC KEY BLOCK-----
```

4. Exploitation :



S E C U R I N E T S
Club de la sécurité informatique
I N S A T



Les commandes courantes de *gpg* sous linux

Gpg reconnaît les options suivantes:

--gen-key

Generate a new key pair. This command is normally only used interactive.

-e, --encrypt

Encrypt data. This option may be combined with *--sign*.



-c, --symmetric

Encrypt with symmetric cipher only This command asks for a passphrase.

--edit-key name

Present a menu which enables you to do all key related tasks:

--list-keys [names], --list-public-keys [names]

List all keys from the public keyrings, or just the ones given on the command line.

--list-secret-keys [names]

List all keys from the secret keyrings, or just the ones given on the command line.

--export [names]

Either export all keys from all keyrings (default keyrings and those registered via option *--keyring*), or if at least one name is given, those of the given name. The new keyring is written to stdout or to the file given with option "output". Use together with *--armor* to mail those keys.