

Emails Ciphering

Usage of cryptography in emails – October 2009

Julien Thomas



Overview

- **Quick Overview of cryptography principles and ciphering techniques**
- **Usage of cryptography in email software**

Quick Overview of cryptography principles and ciphering techniques

■ Symmetric ciphering

- A single key, K
 - Ciphering: $[M]K$
 - Deciphering: $[[M]K]K$

- Services
 - Confidentiality

- Advantage: fast algorithms (XOR based)
- Inconvenient
 - Shared secret $\Rightarrow N * (N-1) / 2$ keys are required for each couple (among N entities) to communicate

Quick Overview of cryptography principles and ciphering techniques

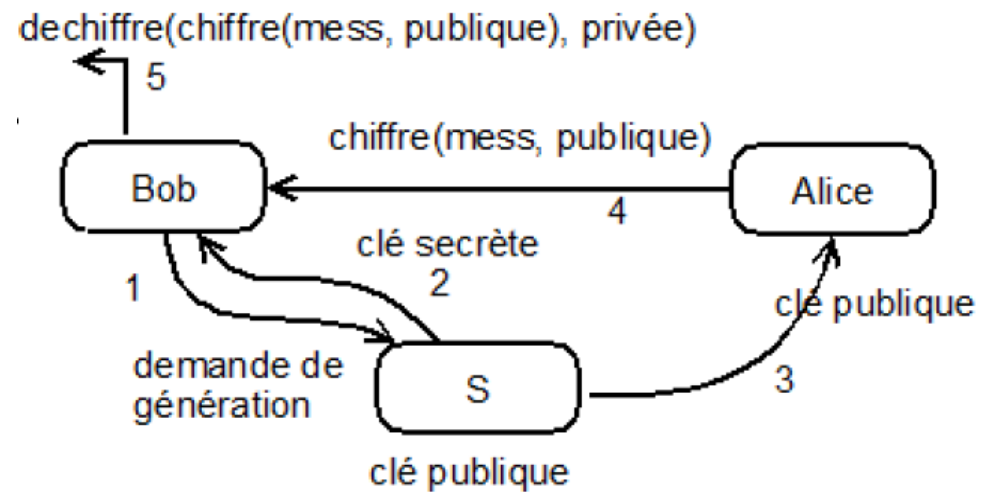
■ Asymmetric ciphering

- Two keys
 - One is secret, the private key, priv
 - One is public, the public key, pub
 - $2N$ keys are required (N couples (priv, pub))
 - Two cryptographic functions are used
- Services
 - Confidentiality: $[M]_{pub}$
 - Integrity and Authentication: $[M]_{priv}$
- Cryptanalysis: problems considered as hard
 - RSA: Big number factorisation problem

Quick Overview of cryptography principles and ciphering techniques

■ Ciphering

- Alice wants to send a message to Bob



■ Signature

- Bob wants to prove its identity to Alice



Quick Overview of cryptography principles and ciphering techniques

■ Common Cryptographic Algorithms

- Standard: PGP – OpenPGP (PGP 5.x as a basis)
 - RFC 4880 - OpenPGP Message Format
 - Algorithms
 - RSA (Encrypt or Sign)
 - RSA Encrypt-Only
 - RSA Sign-Only
 - Elgamal (Encrypt-Only)
 - DSA (Digital Signature Algorithm)
 - Recommendations
 - An implementation SHOULD NOT implement X keys of size less than 1024 bits.
- Implementation: GnuPGP (see second part of the presentation)

Quick Overview of cryptography principles and ciphering techniques

■ Common Cryptographic Algorithms

- Standard: PGP – OpenPGP (PGP 5.x as a basis)
 - RFC 4880 - OpenPGP Message Format
 - Algorithms
 - RSA (Encrypt or Sign)
 - RSA Encrypt-Only
 - RSA Sign-Only
 - Elgamal (Encrypt-Only)
 - DSA (Digital Signature Algorithm)
 - Recommendations
 - An implementation SHOULD NOT implement X keys of size less than 1024 bits.
- Implementation: GnuPGP (see second part of the presentation)

Quick Overview of cryptography principles and ciphering techniques

■ Common Cryptographic Algorithms

- RSA http://fr.wikipedia.org/wiki/Rivest_Shamir_Adlema

- Keys:

- Choose p&q (prime numbers) $\varphi(n) = (p - 1)(q - 1)$
- $\text{pgcd}(e, \varphi(n)) = 1$
- $ed = 1 + k\varphi(n)$

- Encryption: $C \equiv M^e \pmod{n}$

- Decryption

- $C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$
- Fermat-Euler theorem (*Petit théorème de Fermat*)
 - » $M^{p-1} \equiv 1 \pmod{p}$ donc $M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$
 - » $M^{1+k(p-1)(q-1)} - M$ est donc un multiple de p et de q .
- Gauss Lemma
 - » $M^{1+k(p-1)(q-1)} - M$ est un multiple de pq , c'est-à-dire de n

Pour calculer d à l'aide de e et n , il faut trouver l'inverse de e modulo $(p - 1)(q - 1)$ ce qui nécessite de connaître les entiers p et q , c'est-à-dire la décomposition de n en **facteurs premiers**.

Quick Overview of cryptography principles and ciphering techniques

■ Common Cryptographic Algorithms

- ElGamal

- Keys generation

- Alice chooses a random x from $\{0, \dots, q-1\}$.
- Alice computes $h = g^x$.
- Public Key: (G, q, g, h) .
- Private Key: x

- Encryption

- Initial calcul: $c_1 = g^y$.
- $s = h^y$, and $c_2 = m' \cdot s$.

- Decryption

- $s = c_1^x$
- $c_2 \cdot s^{-1} = m' \cdot h^y \cdot (g^{xy})^{-1} = m' \cdot g^{xy} \cdot g^{-xy} = m'$.

Un attaquant éventuel, pour retrouver m' , doit pouvoir calculer g^{xy} , connaissant g^x , g et g^y . Il doit donc découvrir y , et est confronté au problème du **logarithme discret**.

Quick Overview of cryptography principles and ciphering techniques

- **End of the Theory ... lets get practical**

Usage of cryptography in email software

■ Public / private keys

- Public key ... public so unprotected
- Private Key ... private
 - Shared passphrase
 - Expiration:5 years
 - Cryptographic algorithm ... to be found
- Repository: public and protected private keys
 - Repository not passphrase protected
 - Key: common shared passphrase
 - The passphrase must be kept secret
 - Mnemonic, as usual

Usage of cryptography in email software

■ Software overview

- http://www.gnupg.org/related_software/frontends.fr.html
- Linux
 - Enigmail: Thunderbird
 - KMail
 - Evolution
- Windows
 - Enigmail: Thunderbird
 - OL/OLExpress : Gpg4Win

Usage of cryptography in email software

■ Software overview

- http://www.gnupg.org/related_software/frontends.fr.html
- MAC :
 - Enigmail: Thunderbird
 - Mutt
 - GPGMail: Mail
 - Macgpg2
 - GPGMailb - <http://macgpg.sourceforge.net/>
 - GPGPreference - <http://macgpg.sourceforge.net/>
 - GPGKeychainAccess - <http://macgpg.sourceforge.net/>

Usage of cryptography in email software

■ Software example: Thunderbird and Enigmail

- Available in Linux, Windows and MAC
 - Note: OL/OLExpress : Gpg4Win
 - GPGol, GPAssistant and WinProtectionToolkit
 - (+ GPGexplorerextension, GPG Manual)
- Step 1: getting enigmail
 - <http://enigmail.mozdev.org/home/index.php>
 - Choose system settings
 - Download addon file (.xpi)
- Step 2: installing enigmail
 - Tools > additional Modules > Install – choose .xpi file
 - Restart thunderbird



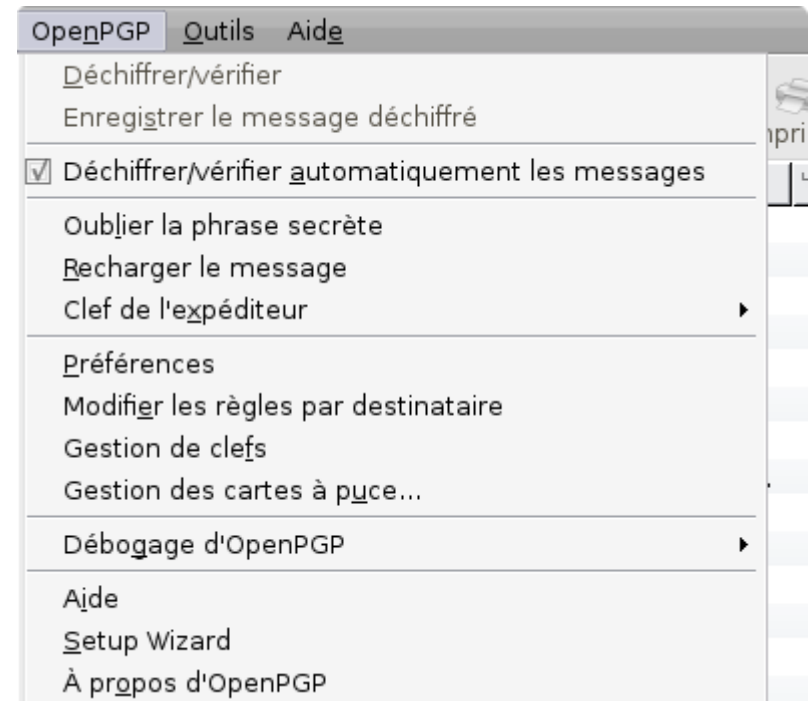
Usage of cryptography in email software

- Step 3: Installing GnuPG
 - <http://www.gnupg.org/download/index.en.html>
 - (<ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.10b.exe>)
 - Why GnuPG ?
 - Enigmail: interface between Thunderbird and GnuPG
 - Enigmail: internal preferences management
 - Enigmail: not an OpenPGP implementation



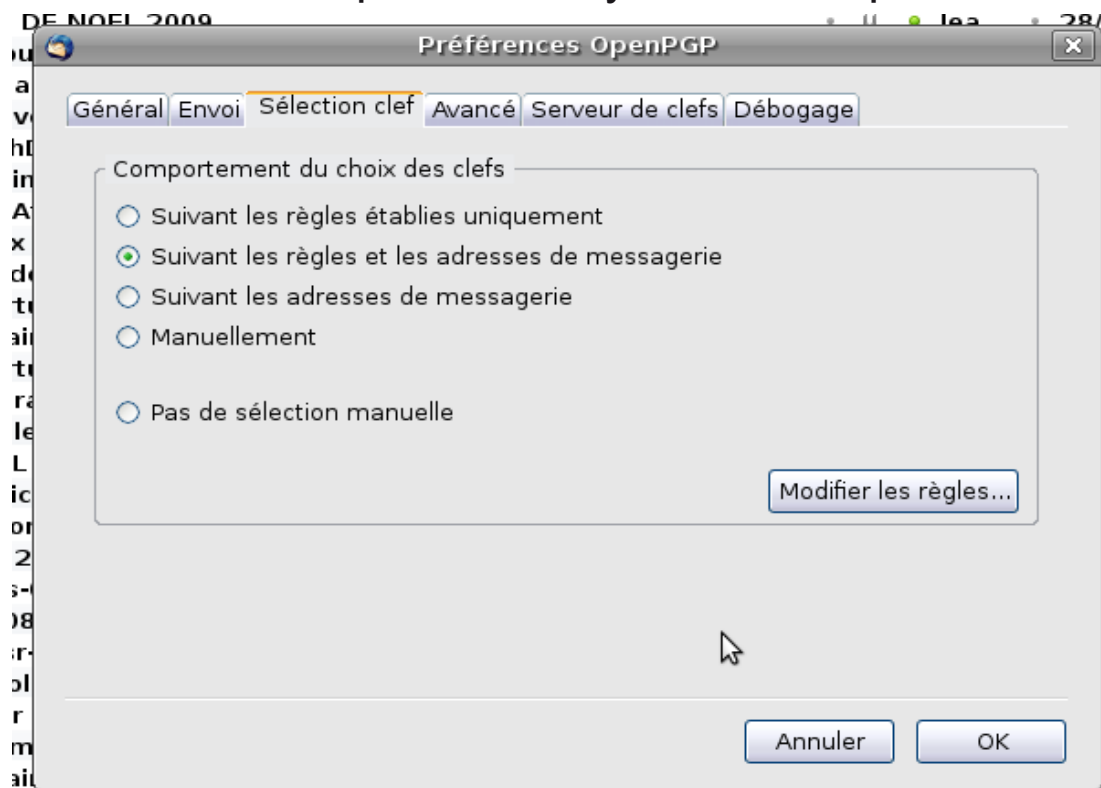
Usage of cryptography in email software

- Step 4: Using enigmail
 - Enigmail / GnuPG Preferences
 - Account Preferences
 - Rules per destination
 - Key management
- Others interesting
 - Forget the passphrase



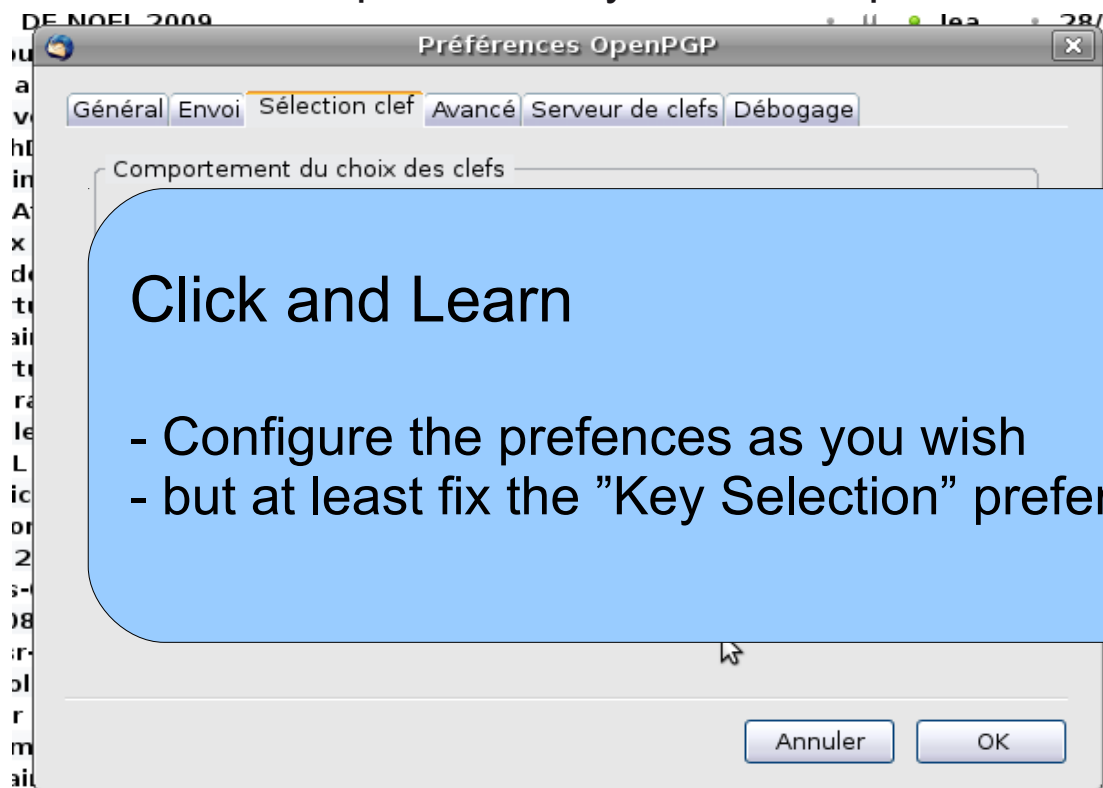
Usage of cryptography in email software

- Step 4: Using enigmail
 - Enigmail Preferences
 - Everything with defaults values
 - Excepted “Key Selection” preferences



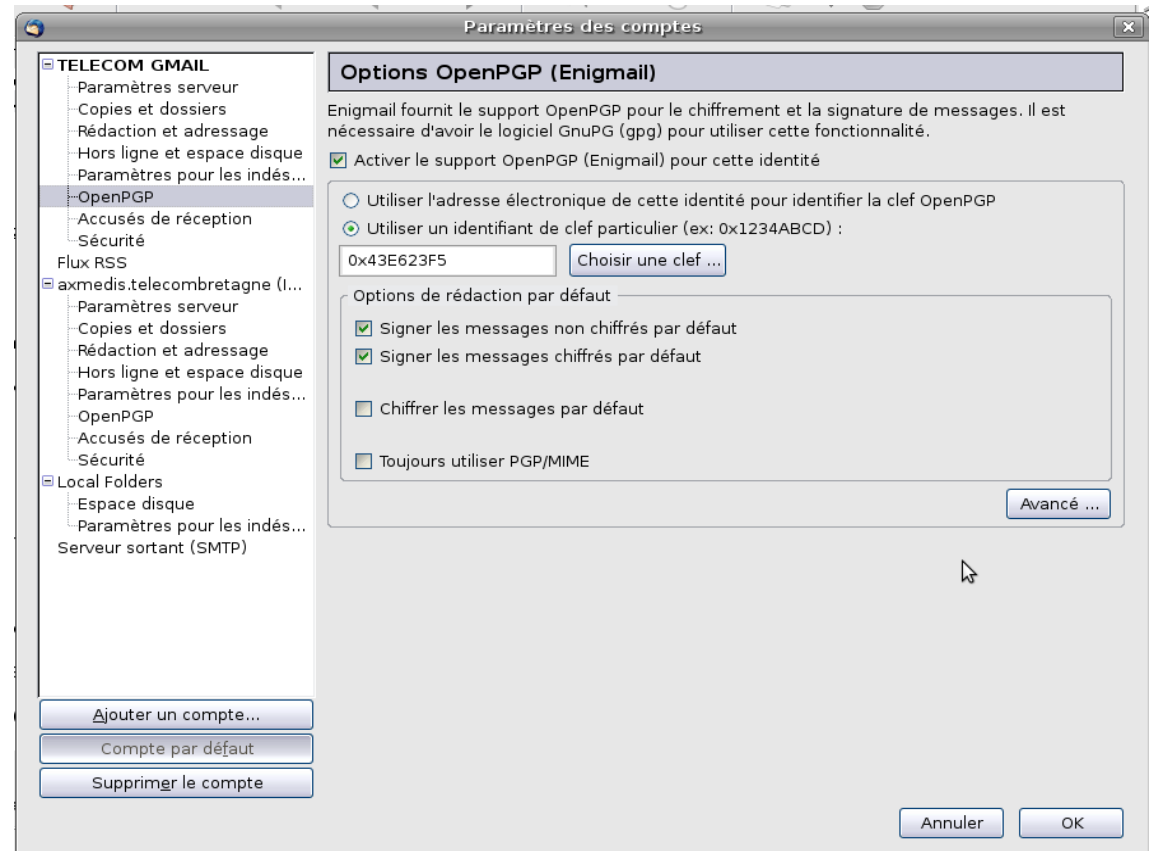
Usage of cryptography in email software

- Step 4: Using enigmail
 - Enigmail Preferences
 - Everything with defaults values
 - Excepted “Key Selection” preferences



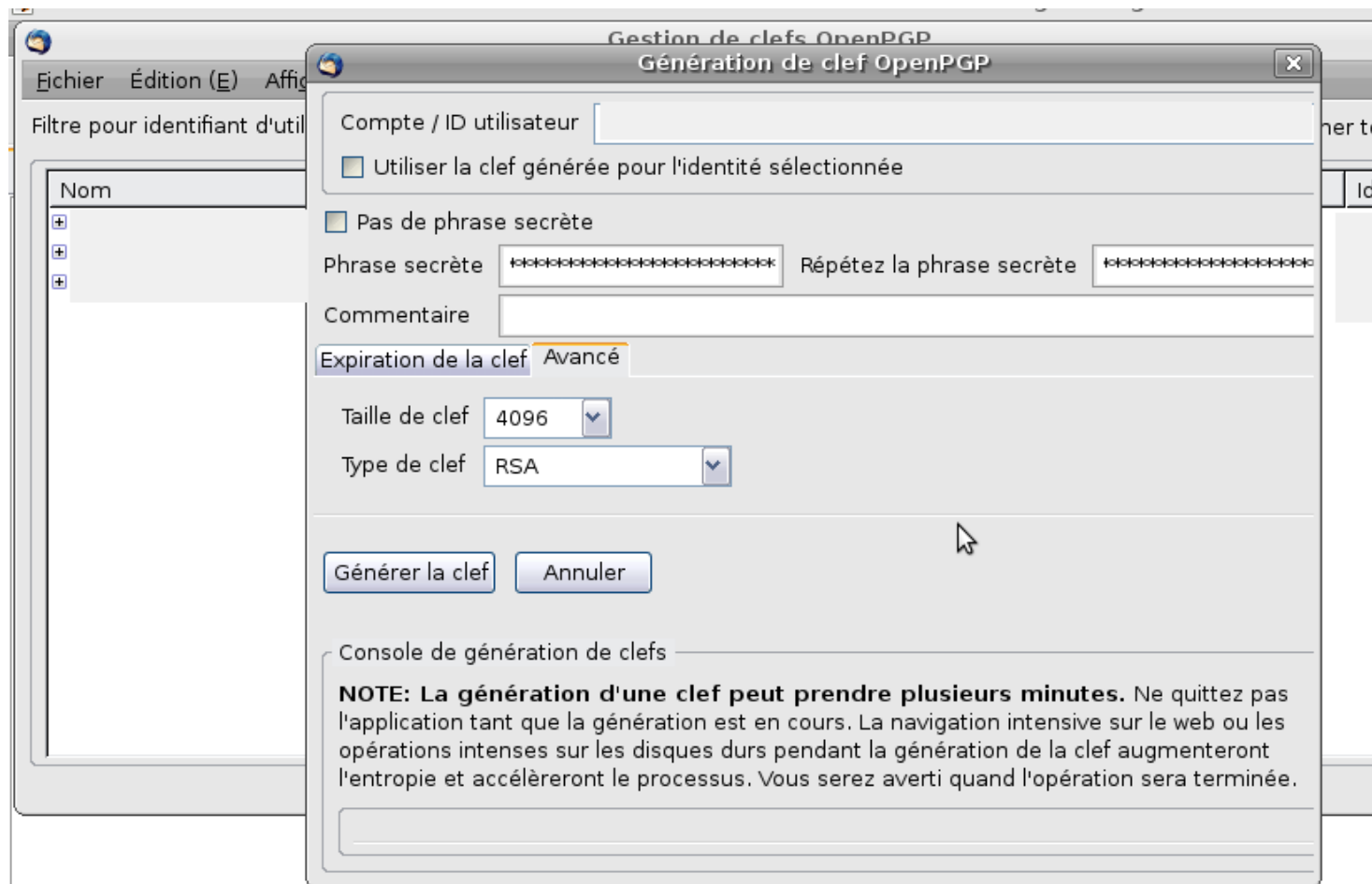
Usage of cryptography in email software

- Step 4: Using enigmail
 - Account Preferences
 - Policy : “**sign everything** per default with **my personal** private key”



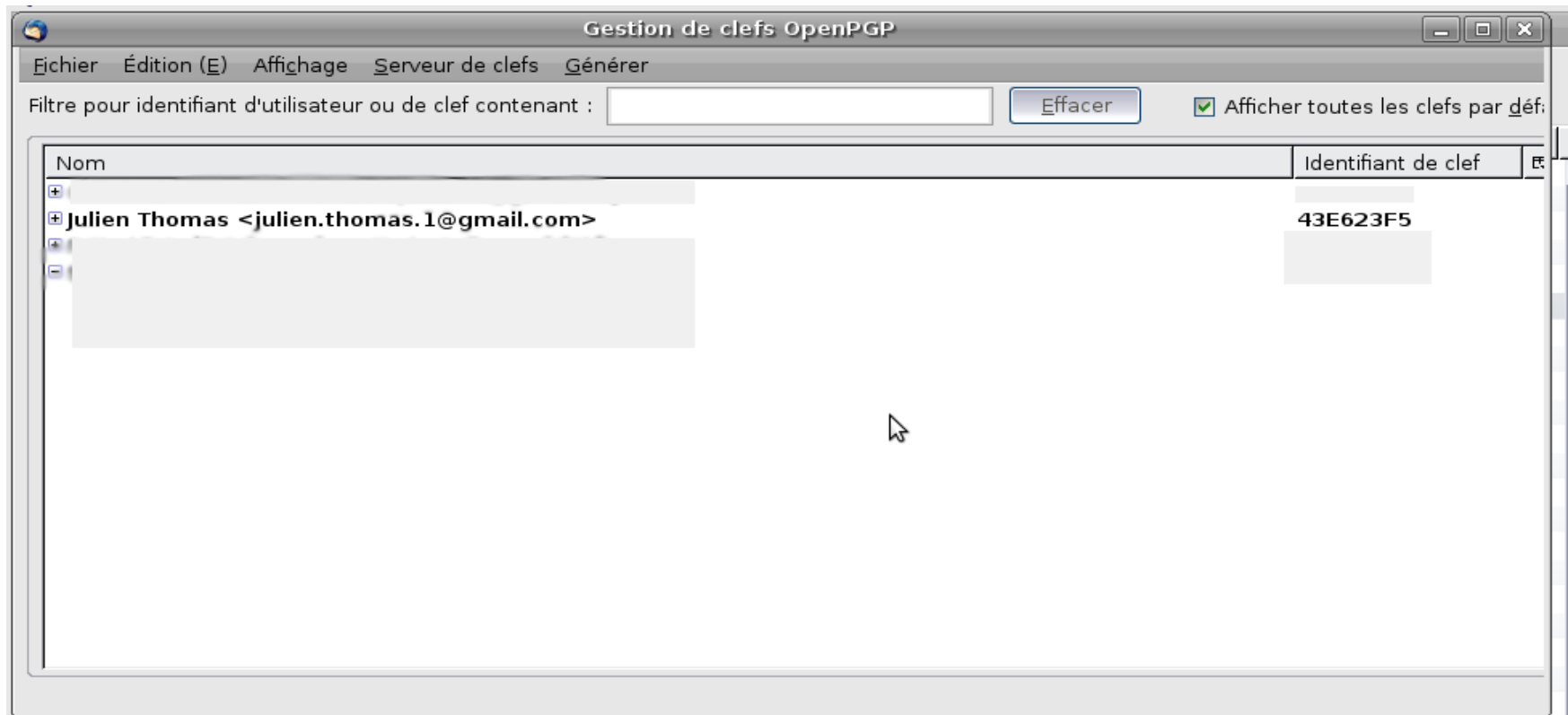
Usage of cryptography in email software

- Step 4: Using enigmail
 - Key generation



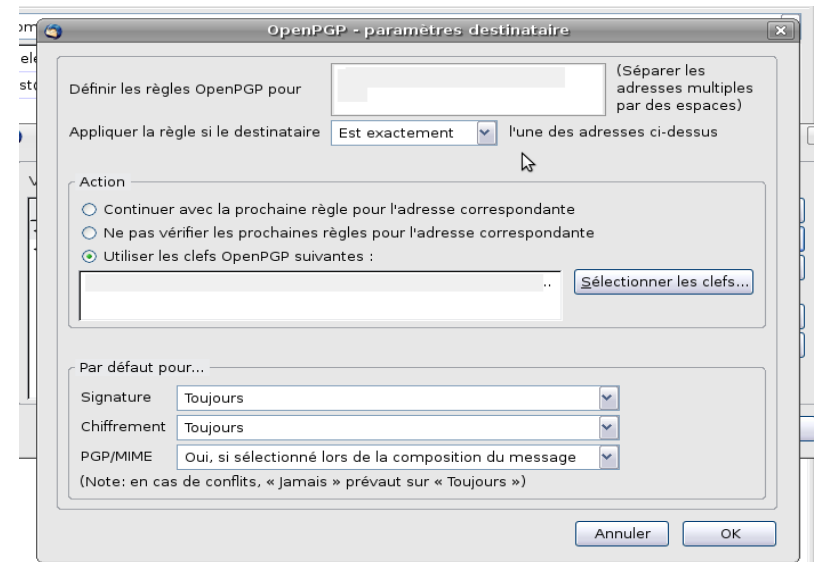
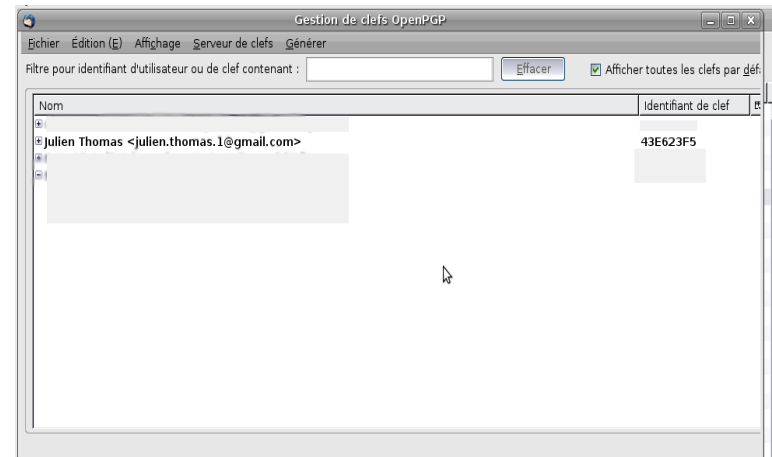
Usage of cryptography in email software

- Step 4: Using enigmail
 - Key management (importation, update, revocation, view ...)



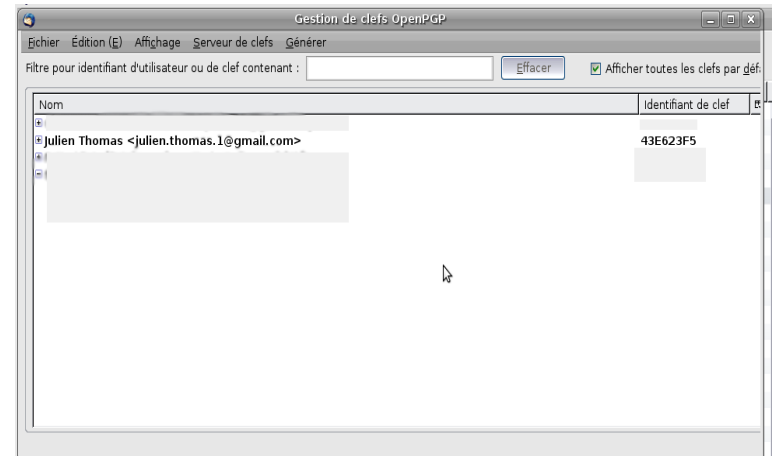
Usage of cryptography in email software

- Step 4: Using enigmail
 - Cryptographic rule management
 - Which key
 - » eg. key group
 - for who
 - » eg. group email
 - for what
 - » policy
 - According to the policy
 - Sign: never
 - Cipher: always
 - PGP/MIME: if precised



Usage of cryptography in email software

- Step 4: Using enigmail
 - Cryptographic rule management
 - Which key
 - for who
 - for what
 - Accepting GPG keys

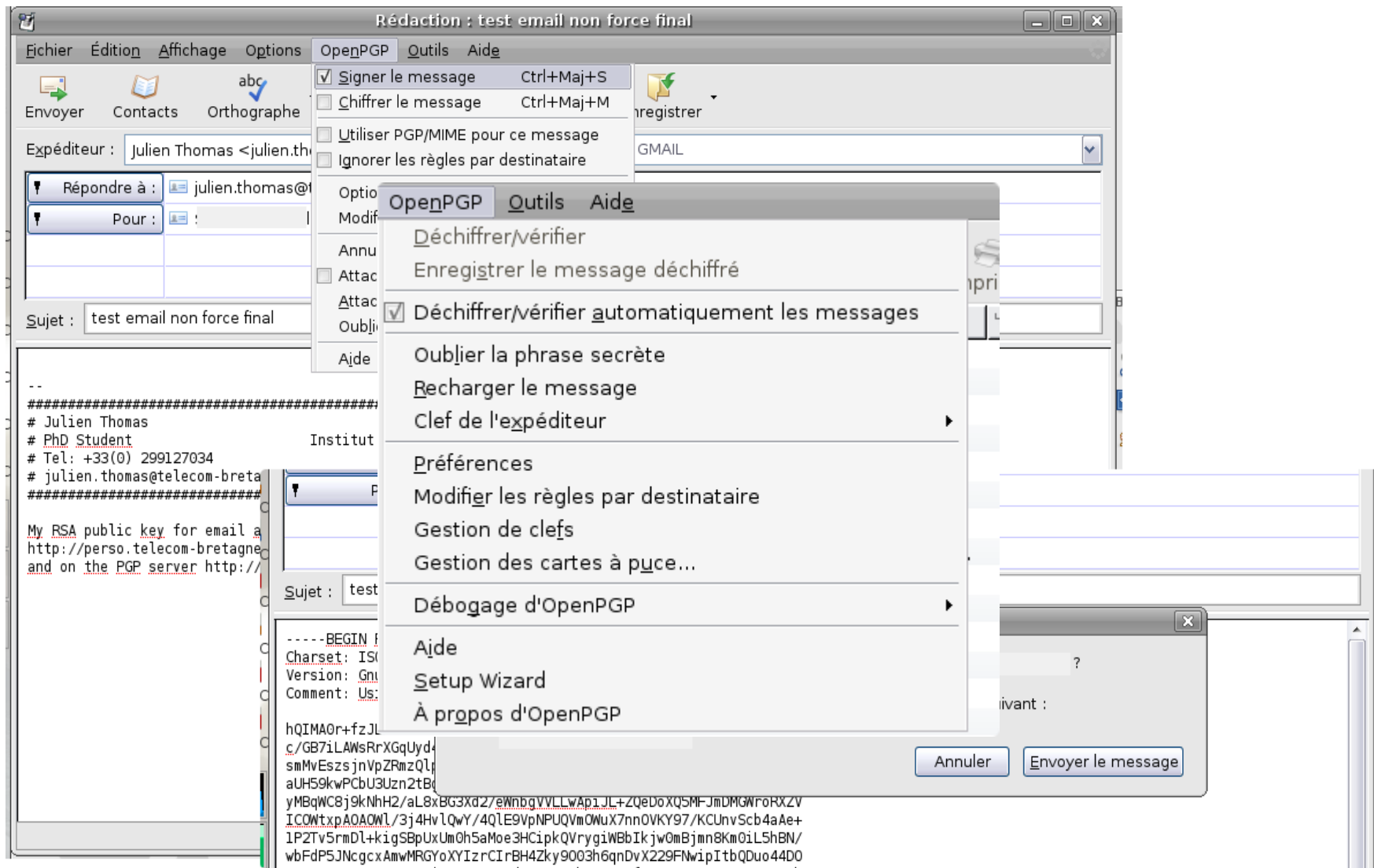


Click and Learn

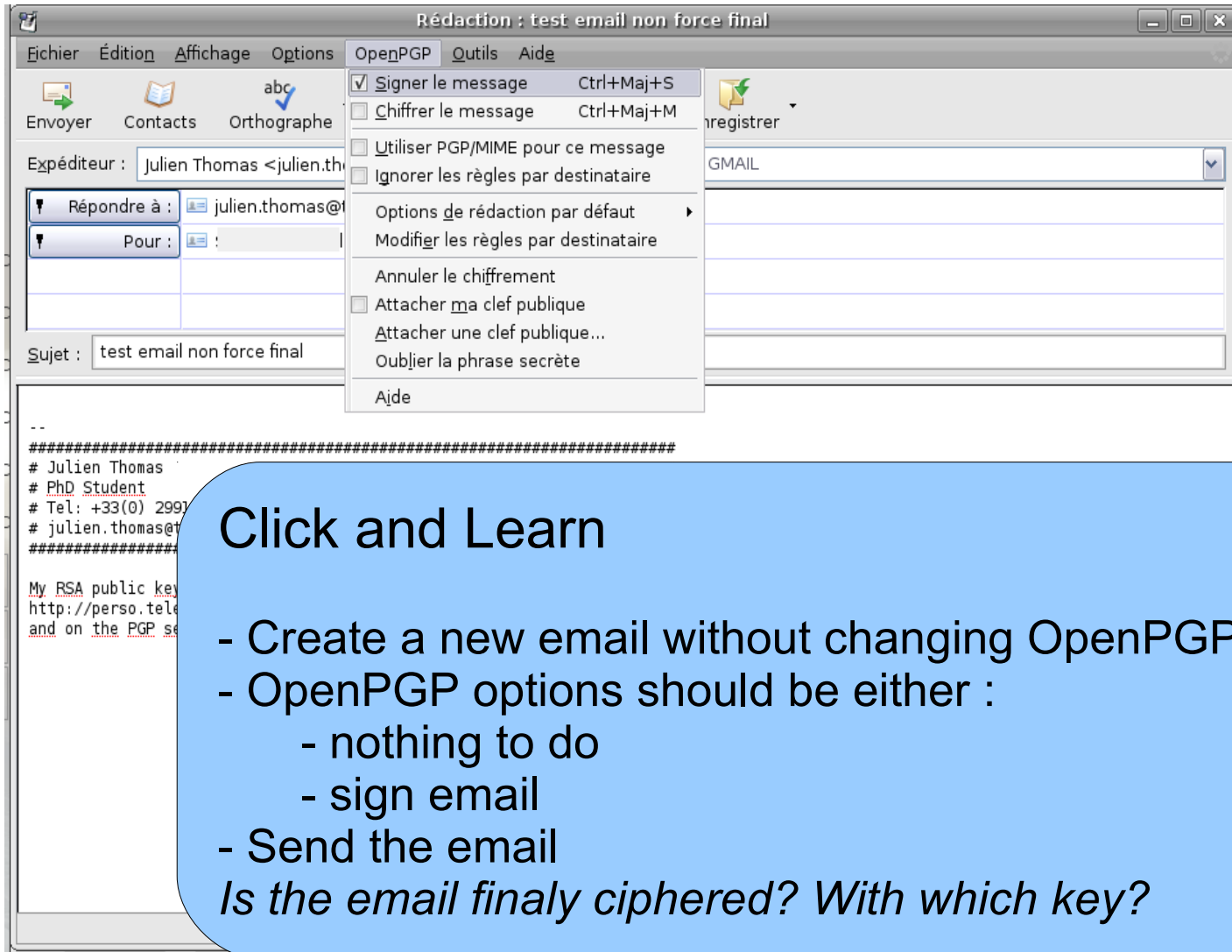
- Import Certificate
- View Certificate Information
 - What are the key generation algorithm and keysize?*
- Export Certificate
 - What is really exported?*



Usage of cryptography in email software



Usage of cryptography in email software



Click and Learn

- Create a new email without changing OpenPGP options
- OpenPGP options should be either :
 - nothing to do
 - sign email
- Send the email

Is the email finally ciphered? With which key?

