# Courrier Électronique Sécurisé

## OpenPGP
## Certificats PGP

-

Master II ISRAD

-

Faculté de Mathématiques et
d'Informatique d'Amiens


**Samuel MONTEIRO**

**Ludovic DUPENT**

**Julien DURIEUX**

# ..:: Sommaire ::..

1. OpenPGP
2. Chiffrement / Déchiffrement d’un mail
3. Certificats Numériques
4. Mise en pratique : logiciels & plugins
5. Législation
6. Conclusion

# 1.a] Qu'est-ce que PGP ?

- **OpenPGP** : standard de chiffrement de courrier électronique.
- **PGP** (modestement appelé *Pretty Good Privacy)* : version payante
- **GnuPG** (*GNU Privacy Guard*) : version gratuite *open source*

- Auteur de PGP : **Philip Zimmermann**
- Première version : **décembre 1991**
- Problèmes judiciaires : **1993 – 1996**
  - NSA
  - RSA Data Security
  - Conséquence : PGP devient payant

- Un **crypto-système hybride** :
  - Cryptage symétrique : **clef de session**
  - Cryptage asymétrique : **clef publique \ privée**

# 1.b] Pourquoi utiliser PGP ?

- De **solides préjugés** empêchent l'utilisation de PGP :
  - Difficile à utiliser/installer
  - Inutile pour moi au quotidien
  - Je n'ai rien à cacher
  - Inefficace à cause de *backdoors* pour la N.S.A.

- Et pourtant, tout ceci est faux, **PGP** :
  - A un niveau de sécurité suffisant (mais pas inviolable)
  - Est gratuit (pour GnuPG)
  - S'utilise de façon transparente
  - Est autorisé en France

*Ne pas utiliser PGP revient à envoyer*
*une carte postale sans enveloppe.*
*Tout le monde peut la lire !*

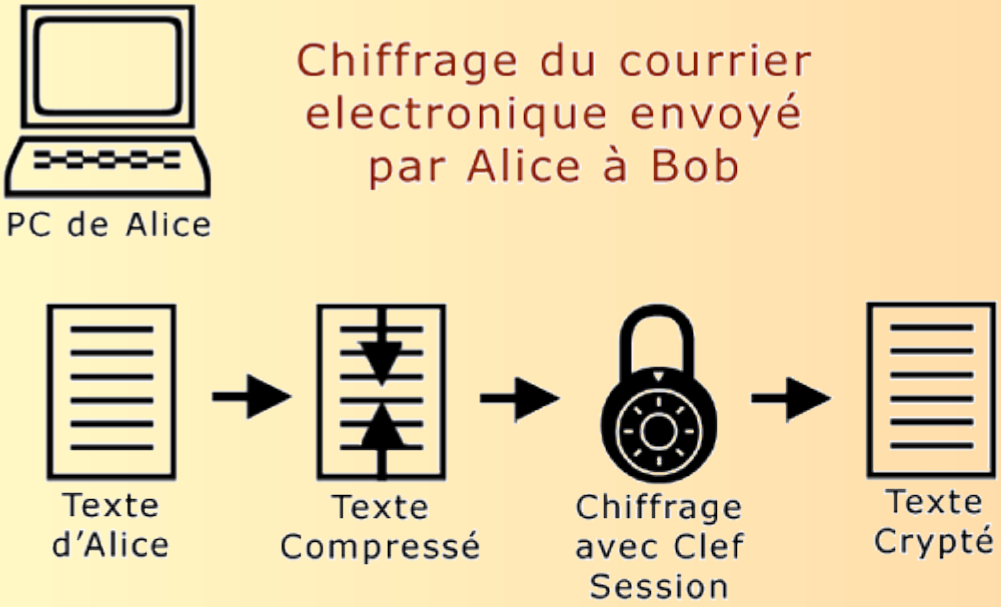
# 2.a] Chiffrement d'un mail PGP

- **Chiffrement hybride**
  - chiffrement symétrique avec la clef de **session**
  - chiffrement asymétrique avec la clef **publique/privée**

- **Clef de session**
  - générée aléatoirement pour chaque mail (sur 128 bits)
  - sert à chiffrer le mail
  - algorithmes utilisés : AES, Twofish , CAST5

- **Clef publique / privée**
  - générée une fois pour toute (sur 1024 bits à 4096 bits)
  - sert à chiffrer / déchiffrer la clef de session
  - algorithmes utilisés : RSA, DSA & EL Gamal pour GnuPG, et également IDEA pour PGP.

# 2.a] Chiffrement d’un mail PGP



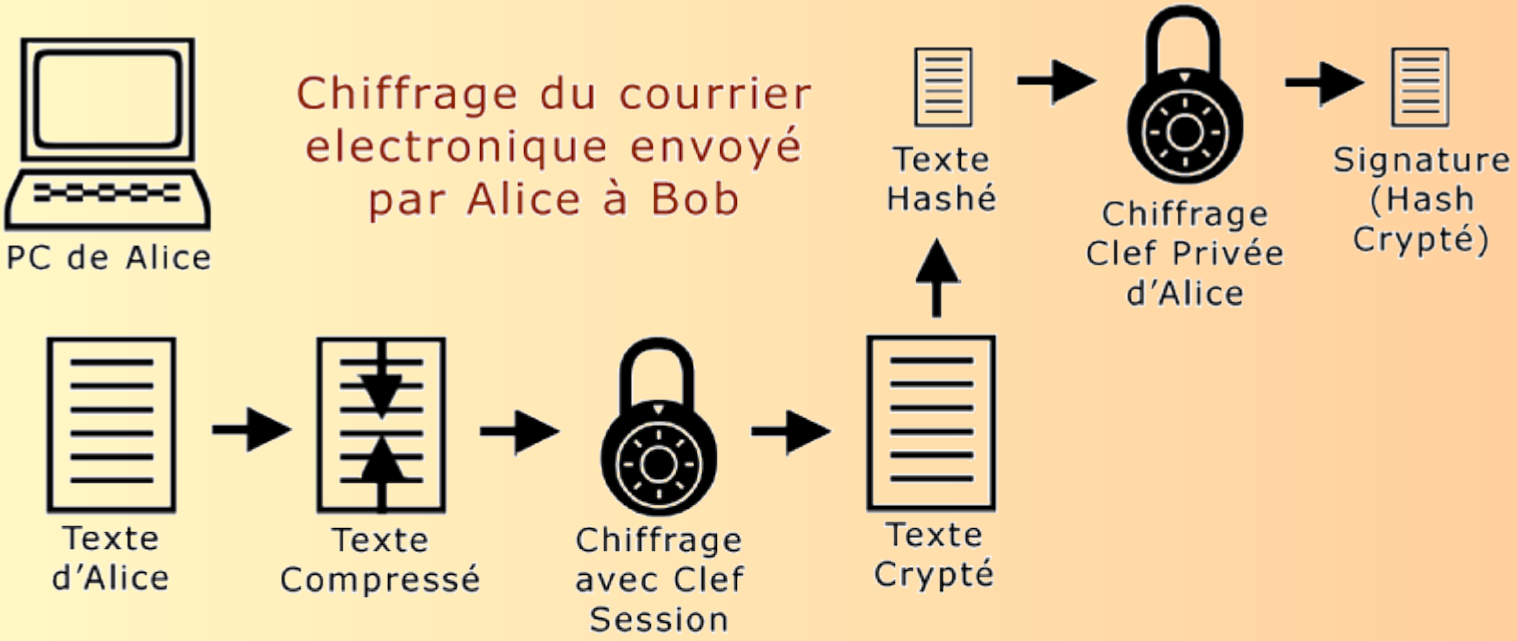

- compression des données
- création d'une clef de session générée aléatoirement
- chiffrement des données à l'aide de cette clef secrète

# 2.a] Chiffrement d'un mail PGP


Chiffrage du courrier electronique envoyé par Alice à Bob

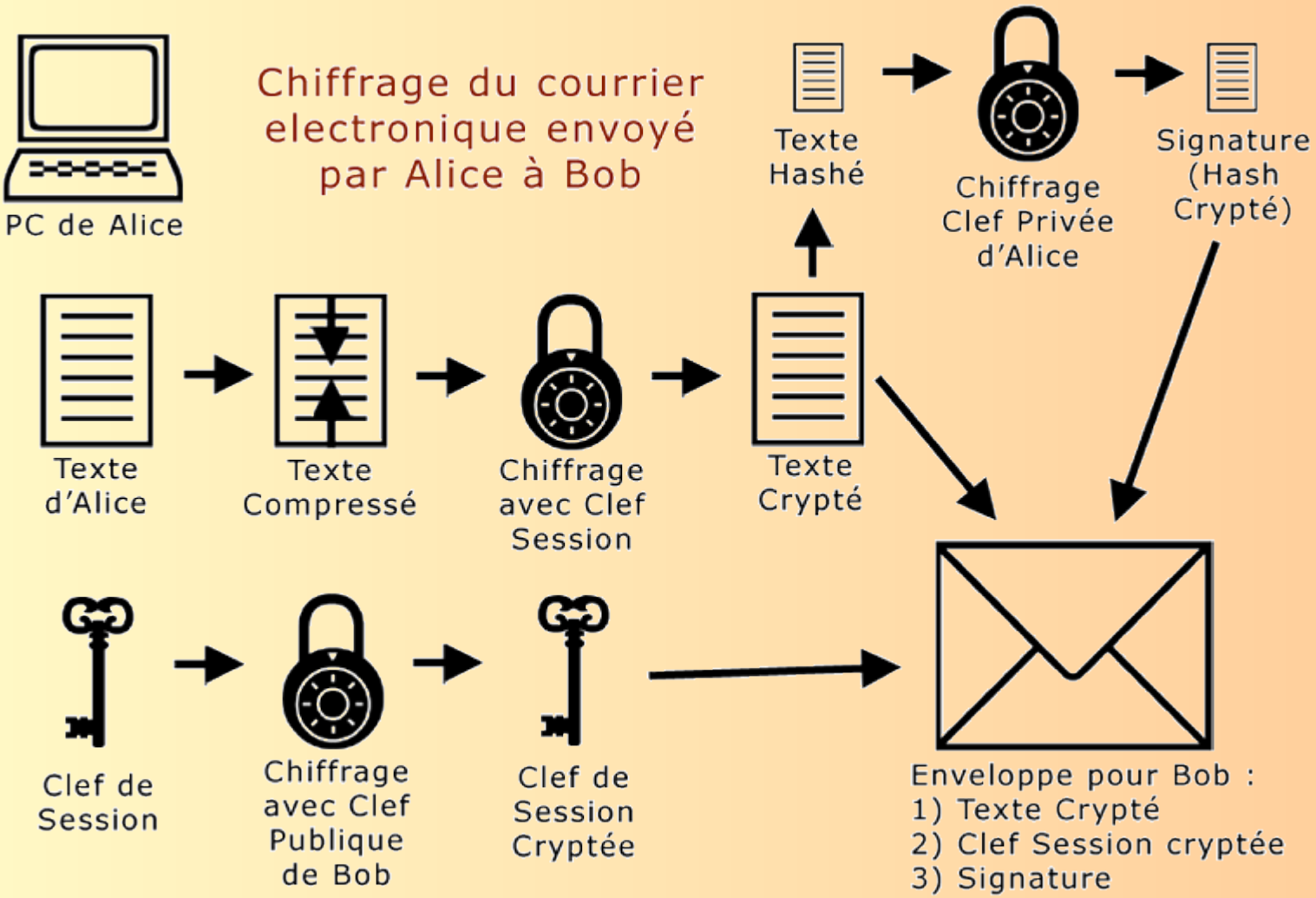
- La clef de session est envoyée avec le mail. Il faut la chiffrer.
- Comme on envoie le mail à Bob, Bob est le seul à être autorisé à utiliser cette clef.
- On va donc la chiffrer avec la clef publique de Bob.

# 2.a] Chiffrement d’un mail PGP

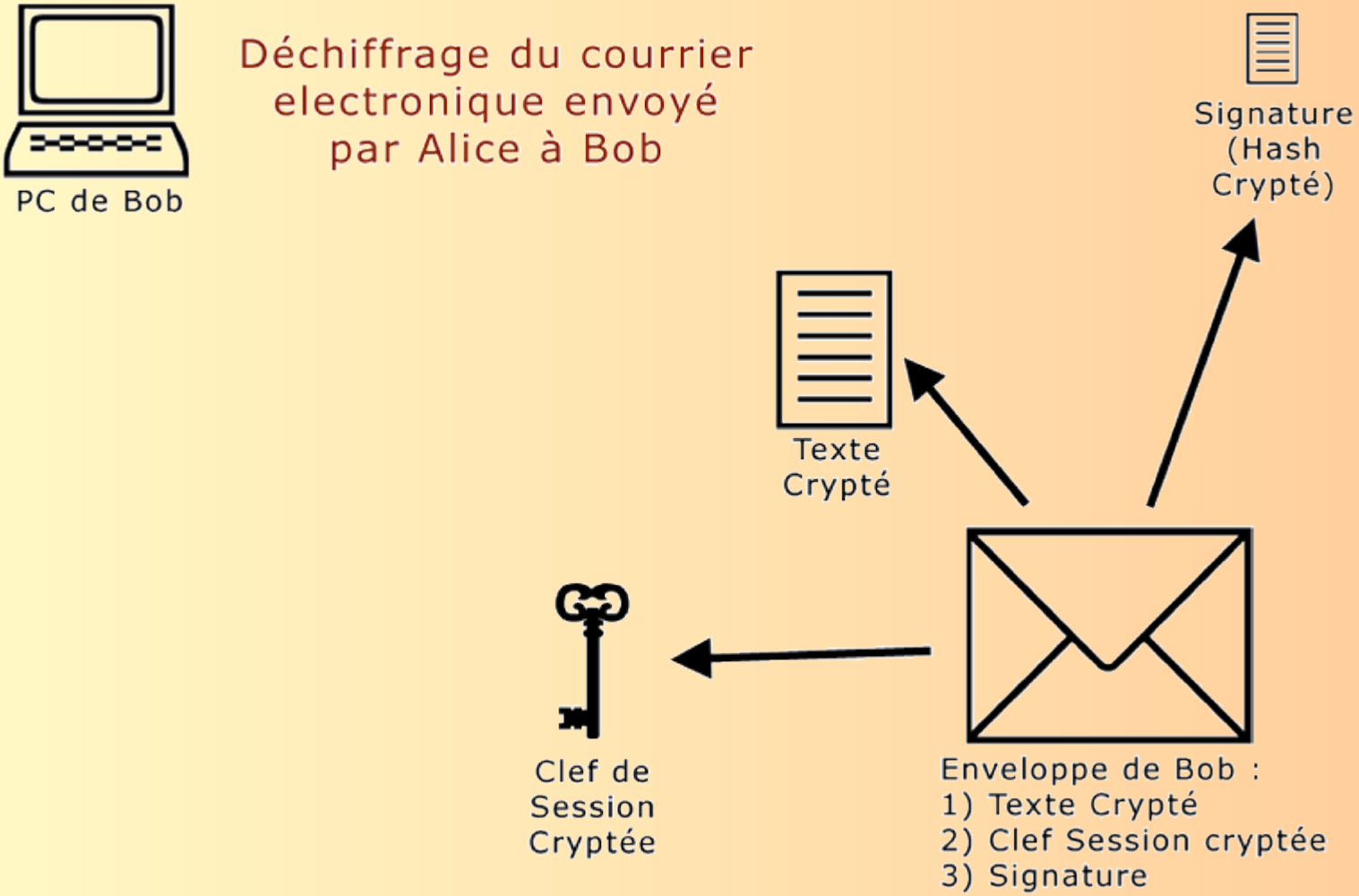



- Pour améliorer la sécurité, Alice **doit** signer le mail.
- Pour cela, on récupère notre mail chiffré, et on applique un algorithme de *hash* (MD5, SHA-1, RIPE-MD-160 et TIGER).
- Ce *hash* est ensuite chiffré avec la **clef privée d'Alice**.
- On obtient alors la **signature** (authentification d’Alice)

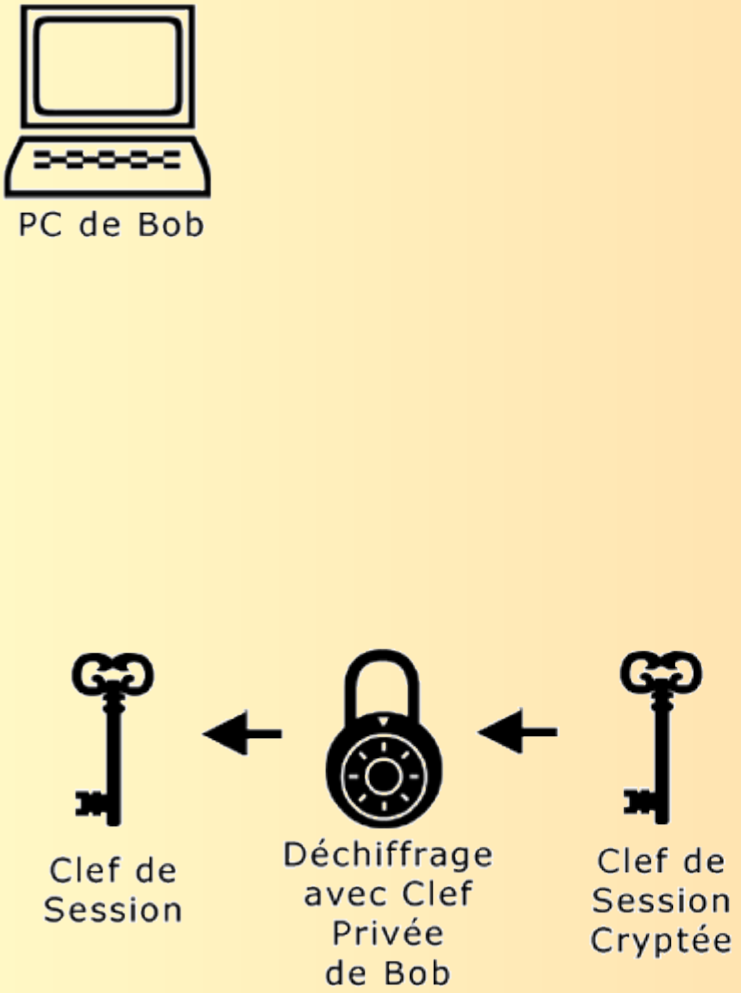
# 2.a] Chiffrement - Récapitulatif



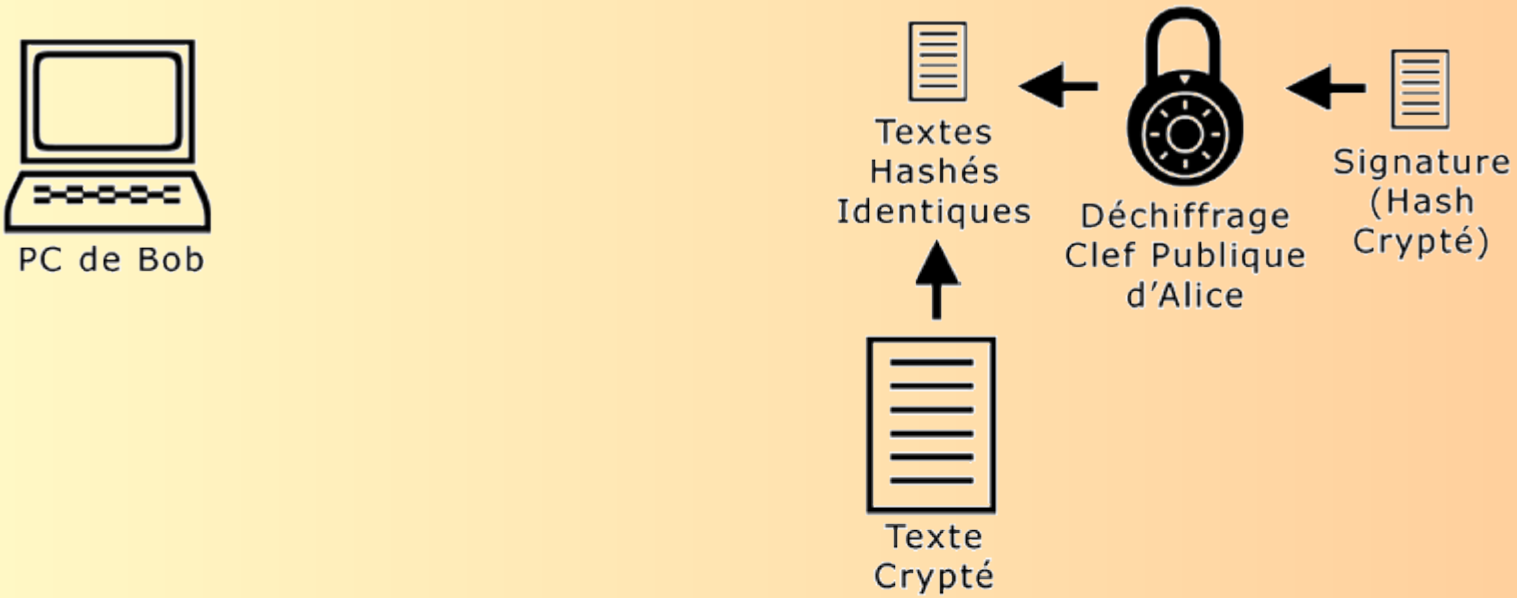
# 2.b] Déchiffrement d'un mail



# 2.b] Déchiffrement d’un mail

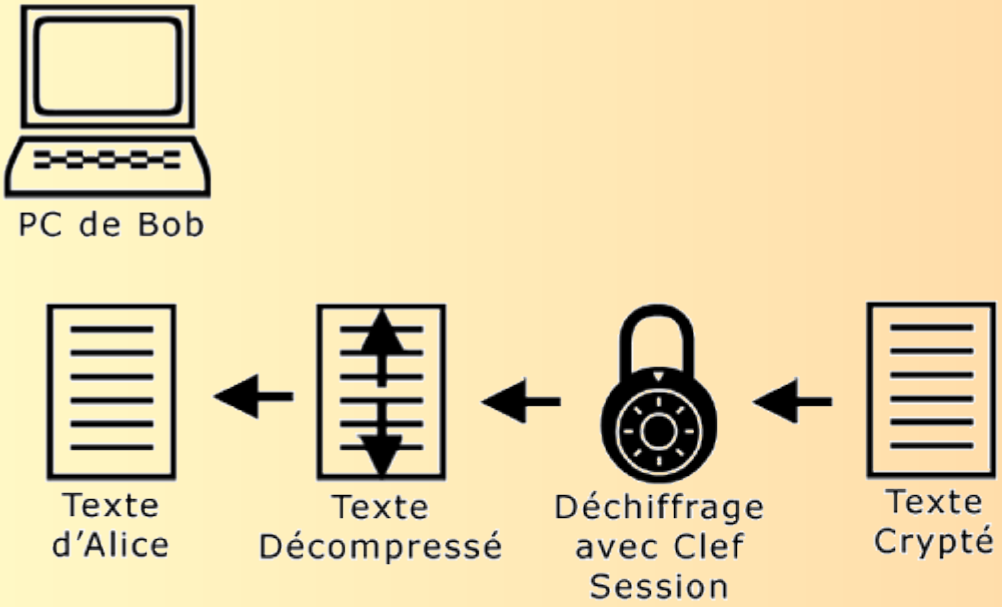


# 2.b] Déchiffrement d'un mail



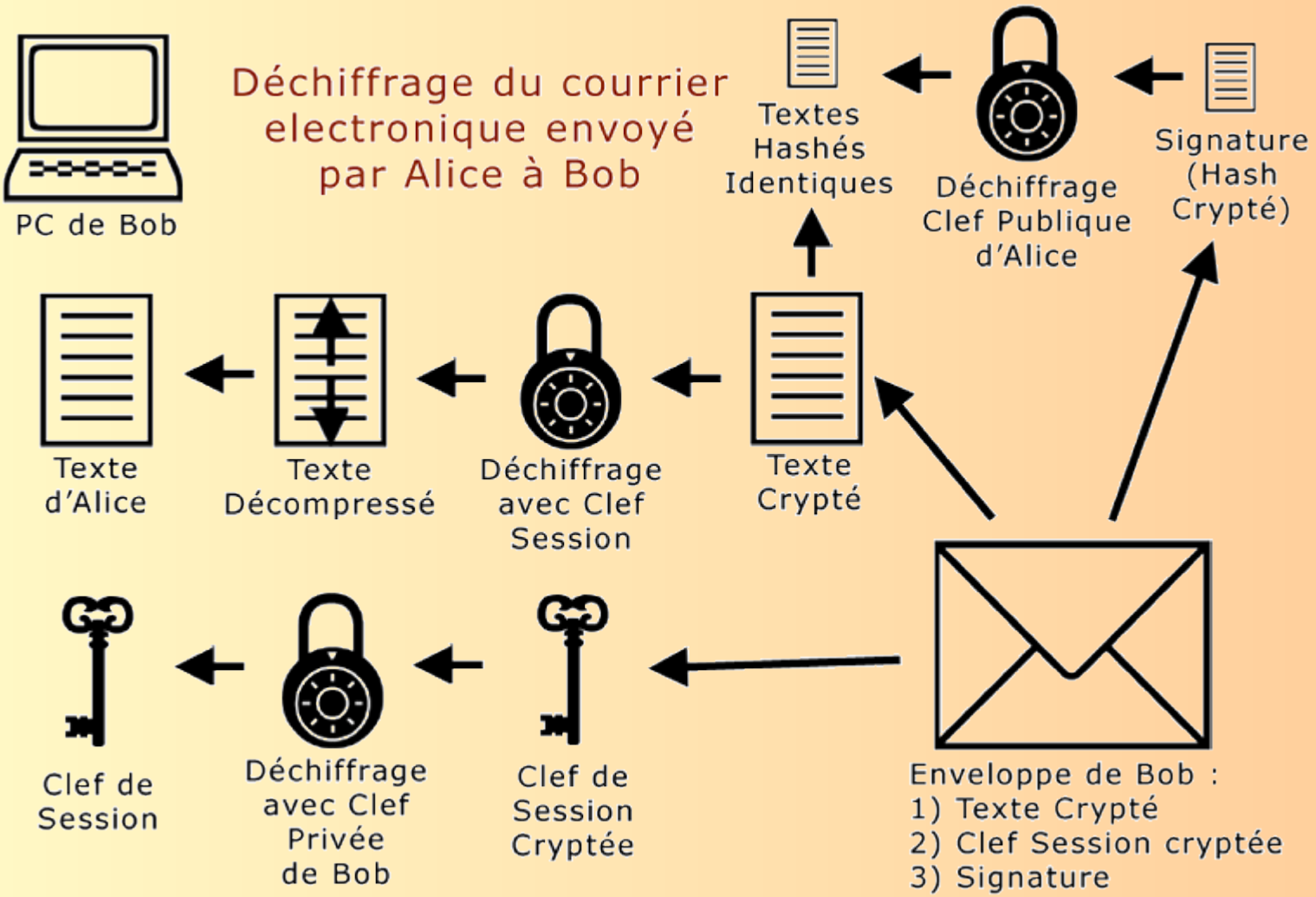

- Vérification de l'**authenticité** du message.
- Le *Hash* est déchiffré et est comparé au *Hash* du texte crypté.
- Si les deux concordent, **le message n'a pas été modifié et provient bien d'Alice**.

# 2.b] Déchiffrement d'un mail




- Si le message est authentifié, il peut être traité normalement :
  - Déchiffrage
  - Décompression

# 2.b] Déchiffrement - Récapitulatif



# 3.a] Certificats Numériques

- Talon d'Achille du système clefs publiques / privées :
  - Echange des clefs publiques
- Le certificat numérique permet d'échanger des clefs publiques de façon sécurisée
- Deux standards de certificats numériques :
  - X.509 : une signature (par une autorité de certification)
  - PGP : plusieurs signatures possibles (confiance mutuelle)
- Obtenir un certificat d'une source sûre (éviter *Man In The Middle*)
  - En main propre (clef USB, support numérique)
  - D'une personne de confiance (ayant signée le certificat)
  - Depuis un serveur de clefs PGP fiable

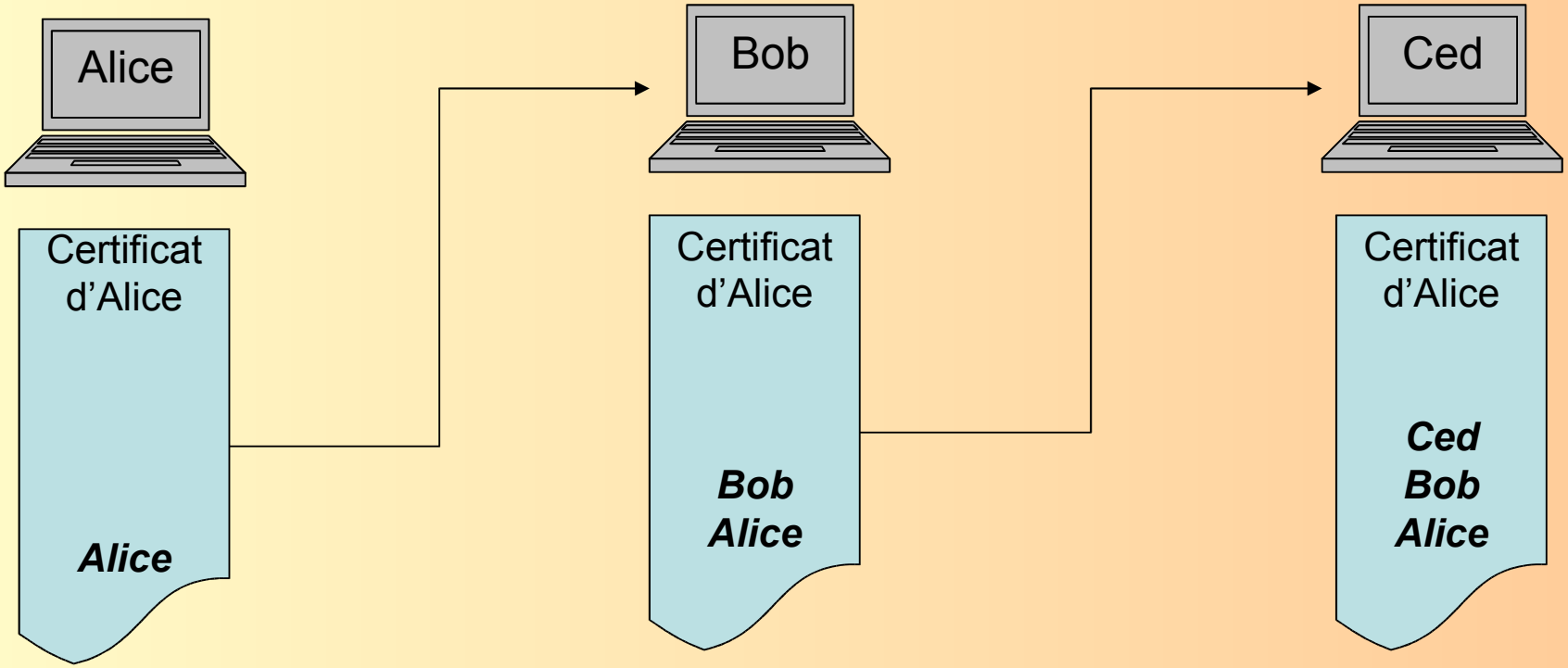
# 3.b] Certificats Numériques

- **Le certificat numérique (fichier *.asc) contient :**
  - Numéro de version de PGP
  - Clef publique
  - Informations (nom, mail, photo optionnelle, …)
  - Période de validité du certificat
  - Algorithmes de chiffrement symétrique préférés
  - Une ou plusieurs signatures

- **Signature d'un certificat (*Fingerprint*)**
  - *Hash* du certificat, chiffré avec la clef privée
  - Il y a au moins la signature du détenteur du certificat
  - D'autres signatures peuvent être ajoutées (pour renforcer la confiance accordée à l'authenticité du certificat)
  - Un niveau « moyen » de confiance est alors calculé (4 niveaux de confiance mutuelle)

# 3.c] Certificats Numériques

- Échange de certificats



# 3.d] Révocation d’un certificat

- **Qui ?**
  - Le détenteur du certificat
- **Dans quel circonstance ?**
  - Perte du mot de passe
  - Quelqu’un qui quitte une entreprise
- **Comment prévenir ?**
  - Serveur de certificats : Liste de révocation (CRL)

# 4.a] Installation des programmes

- **GnuPG** (compatible Windows et Linux)
  _ version 1.0.0 - 7 septembre 1999
  _ dernière version stable et gratuite : 1.4.2
  _ http://www.gnupg.org/(en)/download/index.html

- **Mozilla Thunderbird** (compatible Windows et Linux)
  _ version 1.0.0 - 2004
  _ dernière version stable et gratuite : 1.0.6
  _ http://www.mozilla-europe.org/fr/products/thunderbird/

- **Mode d'Emploi PGP**
  _ Récapitulatif d'installation
  _ Support de l'exposé
  _ Certificats (*.asc) avec nos clefs publiques
  _ http://belzel.free.fr/pgp/openpgp.html

# 4.b] Configuration Thunderbird

- Téléchargez le plugin **Enigmail** pour Thunderbird :
  - page officielle : http://enigmail.mozdev.org/
  - mirroir avec patch FR : http://belzel.free.fr/pgp/thunderbird/

- Allez dans **Outils > Extensions**
  - Installez le plugin et son patch FR
  - Redémarrez Thunderbird

- Si Thunderbird est en français, mais pas Enigmail :
  - Installez le plugin **switch-locales-1.0.xpi** pour changer de langue.
  - Choisissez **Outils > Codages de caractères > fr-FR**
  - Redémarrez Thunderbird

# 4.c] Créez clefs publiques/privées

- Dans Thunderbird, menu **OpenPGP > Gestion de clefs**.
  - Dans la fenêtre **Gestion de clefs OpenPGP**
  - Choisissez **Générer > Nouvelle paire de clefs**.
  - Choisissez votre mail.
  - Indiquez une **phrase de passe** (très recommandée et la plus complexe possible).
  - Indiquez un commentaire si nécessaire (il sera visible de tous).
  - Une fois toutes les informations remplies, générez la clef !
- Créez ensuite un certificat de révocation
  - clef privée perdue
  - clef privée compromise
- Partagez votre clef
  - Créez un nouveau mail
  - Depuis le menu **OpenPGP**, ajoutez votre clef en fichier joint.

# 4.d] Commandes GnuPG

**Aide** : gpg --help | more

**Génération d'une paire de clef** : gpg --gen-key

**Extraction d'une clef publique** : gpg --export -a nom_de_la_clef > nom_du_fichier_a_creer

**Importation d'une clef publique** : gpg --import nom_du_fichier_contenant_la_clef

**Liste des clefs** : gpg --list-keys

**Signature d'un fichier** : gpg -sa fichier_a_signer

**Chiffrement d'un fichier** : gpg -e -r clef_du_destinataire fichier_a_chiffrer

**Chiffrement et signature d'un fichier** : gpg -se -a -r clef_du_destinataire fichier_a_signer

**Signature en clair d'un texte** : gpg --clearsign texte_a_signer

**Signature détachée d'un fichier** : gpg --detach-sign fichier_a_signer

**Déchiffrement/vérification** : gpg nom_du_fichier_a_dechiffrer/verifier

# 5] Législation

<table>
<tr><th></th><th>UTILISATION</th><th>Publication d’un Logiciel</th><th>IMPORTATION (extérieur à l’UE)</th></tr>
<tr><td>Authentification Signature</td><td colspan="3">LIBRE</td></tr>
<tr><td>Clé de chiffrement ≤ à 40 bits</td><td rowspan="3">LIBRE</td><td rowspan="2">Déclarer le logiciel</td><td>LIBRE</td></tr>
<tr><td>Clé de chiffrement > à 40 bits et ≤ à 128 bits</td><td>LIBRE *</td></tr>
<tr><td>Clé de chiffrement > à 128 bits</td><td colspan="2">Demander une autorisation</td></tr>
</table>

** soumise à DÉCLARATION seulement si le fournisseur ou l'importateur ne l'a pas déjà déclaré et si le moyen de cryptologie n'est pas exclusivement destiné à usage personnel.

# ..:: Conclusion ::..

- Un outil très pratique, bien écrit et qui répond à un besoin de plus en plus croissant de sécurité sur Internet.
- Gratuit et très diffusé,
- Les sources sont disponibles,
- Puissant et sûr,
- Interface peu évoluée mais puissante et rapide.

L'idéal serait que tout le monde utilise un système de ce genre de manière à rendre le courrier chiffré aussi commun que l'usage des enveloppes pour le courrier classique.

Pour finir, la phrase célèbre de Zimmermann :

***If privacy is outlawed, only outlaws will have privacy.***

# ..:: Sources ::..

- **Généralité PGP** :
  - http://openpgp.vie-privee.org
  - http://www.commentcamarche.net/crypto/pgp.htm
  - http://fr.wikipedia.org/wiki/Portail:Cryptologie
  - http://www.chez.com/winterminator/cryprisk.html
- **Logiciels** :
  - http://www.gnupg.org
  - http://www.mozilla-europe.org/fr/products/thunderbird/
  - http://enigmail.mozdev.org/
- **Législation** :
  - http://www.ssi.gouv.fr/fr/reglementation/
  - http://fsffrance.org/news/article2002-08-07.fr.html
- **Zimmermann** :
  - Pourquoi j'ai écrit PGP : http://biblioweb.samizdat.net/article4.html
  - Je ne regrette pas PGP (suites au 11/09/2001) : http://infos.samizdat.net/article.php3?id_article=96
  - Au sujet des portes dérobées pour la NSA : http://www.philzimmermann.com/FR/faq/index.html
- **Livres** :
  - La cryptographie décryptée (2001) H.X. Mel et Doris Baker
  - Hacker's Guide (2004) Eric Charton