

# SSI : Chiffrement

*LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*

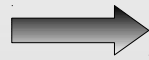
*« Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.*

[...]

Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre.”



# Plan



- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

# Principe du chiffrement

Principe de Kerkhoffs :

Les algorithmes de chiffrement  $E$  et déchiffrement  $D$  sont connus. Seules les clefs sont secrètes et nécessitent un échange préalable.

# Principe du chiffrement

## ■ Définitions

- Chiffrer / chiffrement : (to crypt, to cypher)

En cryptographie, le chiffrement est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

- Crypter / cryptage :

Abus de langage, faux amis (mais néanmoins existent).

- Déchiffrer : (to decypher)

Obtenir le document en clair à partir du document chiffré et de la clef de déchiffrement.

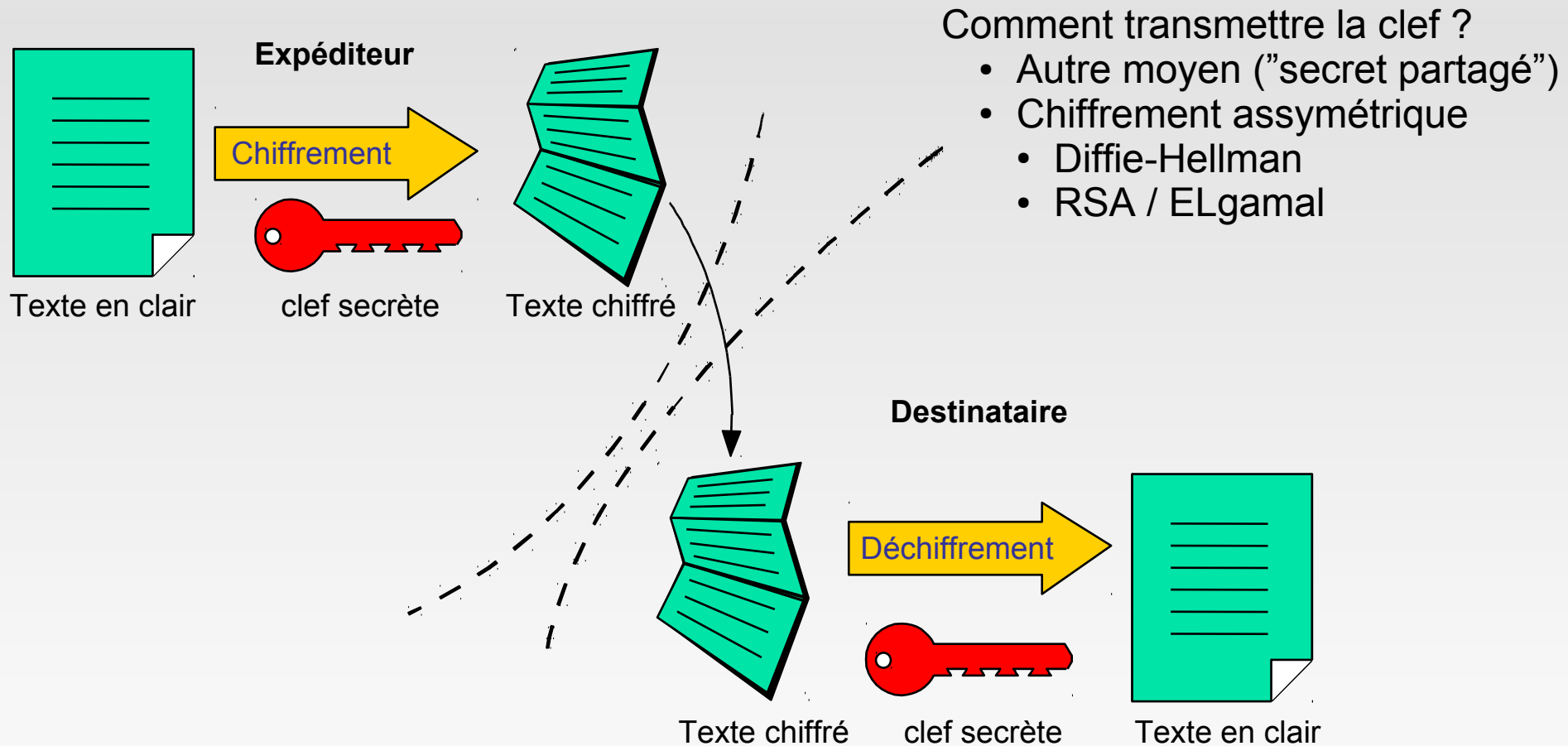
- Décrypter / cryptanalyse : (to crack)

La cryptanalyse est la recherche de la clé permettant de déchiffrer, de la manière la plus simple possible, un message codé. On dit qu'un algorithme est cassé uniquement si l'attaque permet de trouver la clef en moins d'opérations qu'une attaque par force brute.

# Plan

- Principe / définitions
- ➔ ■ Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

# Chiffrement à clef secrète



# Chiffrement à clef secrete

## ■ La clef

- La cle est un secret partage par l'expéditeur et le destinataire, qui leur permet de chiffrer des messages (documents, paquets IP, flux SSL, ...).
- Constitution d'une clef :
  - Chaîne d'octets.
- Condition nécessaire de sécurite :
  - le nombre de clefs doit être sufisamment grand pour échapper à la recherche exhaustive.
    - Dépends de la durée de vie de l'information véhiculée.
    - Mini 128bits.
- Le choix de la clef doit être parfaitement aléatoire (chaque bit de la clef doit avoir une chance sur deux d'être un 1).
- Attention à l'entropie des langues → attaques possible sur l'aléa.

# Chiffrement à clef secrete

- Chiffrement à clef secrete : comment partager la clef ?
  - Transmission par un autre moyen ("secret partagé")
  - Chiffrement asymétrique (RSA, Diffie-Hellman)
- Algorithmes :
  - DES(56) & 3DES (128-192)
  - AES (128), Twofish (128, 192, 256),
  - Blowfish (32 → 448), ...
- Ordre de grandeur :
  - Clef de 128 bits :  $2^{128} \sim 3,4 \times 10^{38}$
  - A 1000 milliards de clefs / secondes, il faut 1 milliard de fois l'age de l'univers pour les essayer toutes.




# Chiffrement à clef secrete

## ■ Cryptanalyse

- Comment trouver la clef ?
  - Mot probable (enigma),
  - Quadratique (XSL), modulo  $n$ , rencontre au milieu
- Attaque par force brute
  - Moyens de réduire la surface
    - Attaques par canaux auxiliaires (temps CPU, rayonnement, bruit, fuites mémoire ...)
    - Biais statistiques
    - Caractère non aléatoire de la clef (générateur à entropie faible)
    - Attaque par dictionnaires, rainbow tables
    - ASICs dédiés, grilles de calcul, ...



# Plan

- Principe / définitions
- Chiffrement à clef secrète
-  ■ Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

# Chiffrement asymétrique

## ■ Diffie-Hellman

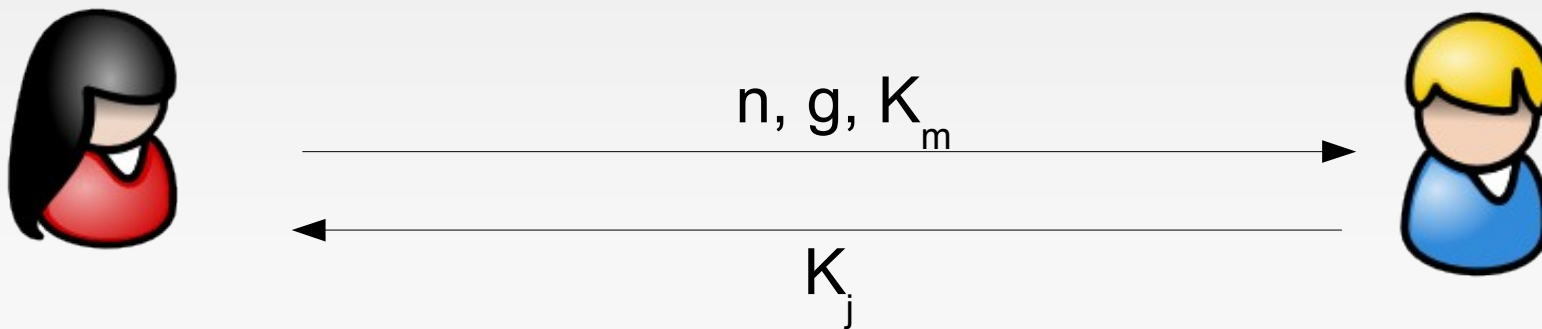
*Permet à deux personnes de partager un secret, sans transmission de ce secret sur le réseau.*

- 2 entiers sont publics  $n$  et  $g$  tels que  $g < n$
- Alice choisi  $X_m$  au hasard, et calcule  $K_m = g^{X_m} \pmod n$
- Bob choisi  $X_j$  au hasard, et calcule  $K_j = g^{X_j} \pmod n$
- Ils s'envoient les valeurs  $K_m$  et  $K_j$ .

# Chiffrement asymétrique

- Diffie-Hellman

- Alice calcule  $(K_j)^{x_m} = (g^{x_j})^{x_m} \pmod n$
- Bob calcule  $(K_m)^{x_j} = (g^{x_m})^{x_j} \pmod n$
- Ces deux chiffres sont identiques, c'est le secret partagé.



# Chiffrement asymétrique

## ■ RSA (en un slide)

- Choisir  $p$  et  $q$  deux nombre premiers distincts.
- Calculer  $n=pq$  (produit de chiffrement)
- Choisir  $e$  (exposant de chiffrement) aléatoire tel que :  $e$  et  $(p-1)(q-1)$  (*indicatrice d'Euler*) non premier entre eux et  $e > p, q$
- Choisir  $d$  tel que  $d$  inversible  $e \bmod ((p-1)(q-1)) = e * d \bmod ((p-1)(q-1)) = 1$
- $(n, e)$  est la clef publique
- $(n, d)$  est la clef privée

Chiffrer :

$$X^e \pmod n = K$$



Déchiffrer :

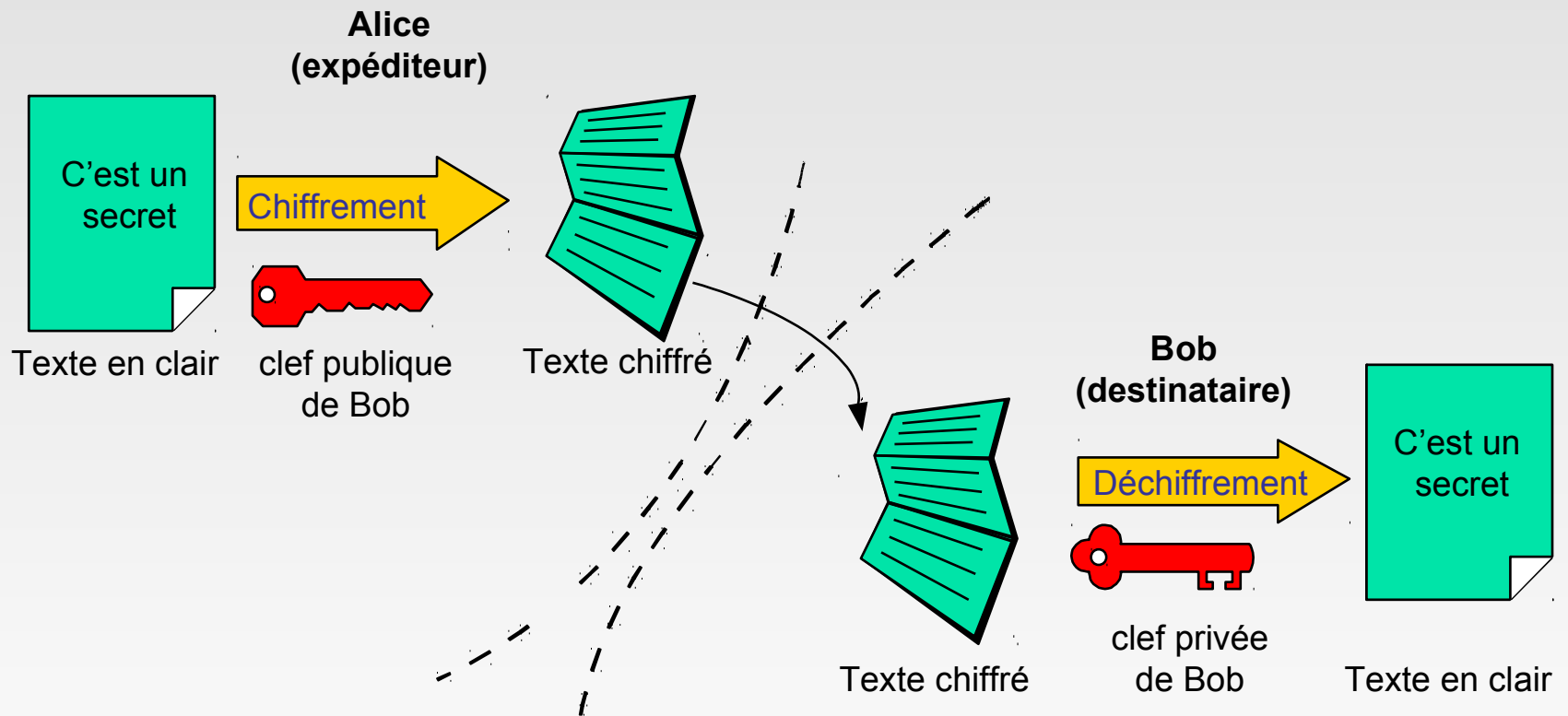
$$K^d \pmod n = X$$

# Chiffrement asymétrique

- El Gamal (en un slide)
  - Utilisé dans GPG,
  - Alice choisi  $p$  (le groupe donc grand),  $g$  (générateur),  $s$  (la clef privée).
  - Alice calcule  $h=g^s \bmod p \rightarrow (p,g,h)$  est la clef publique.
  - Bob choisi  $k$  et chiffre  $m$  (message en clair) en calculant  $c_1=g^k, c_2=m.h^k$
  - Alice déchiffre en calculant :  $c_2/c_1^s = m.h^k/g^{ks} = m.h^k/h^k = m$

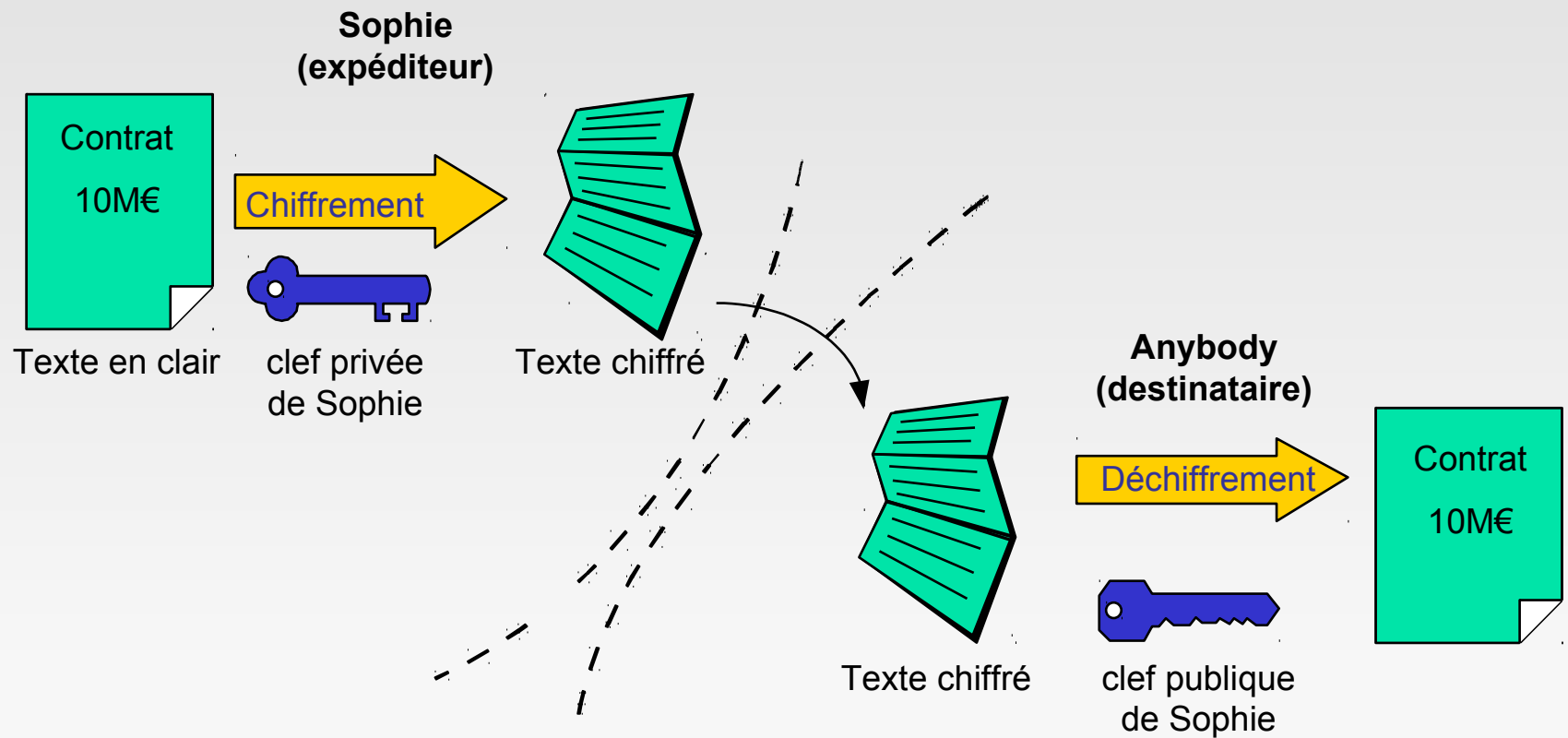
# Chiffrement asymétrique

- Chiffrer un document



# Signature

- Signer un document





# Signature

- Signature numérique : Loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
  - Art. 1316-1 du Code civil français "L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité."
  - Art. 1316-3 du Code civil français "L'écrit sur support électronique a la même force probante que l'écrit sur support papier."
  - L'article 1317 du Code civil français évoque quant à lui la possibilité offerte pour la première fois à l'officier ministériel de conserver l'acte authentique au format électronique.

# Robustesse

- Sécurité de RSA tiens sur le caractère premier de  $p$  et  $q$ .
- RSA 2048 bits min conseillé.

08/01/2010

Quatre ans après le dernier record qui a permis de casser une clé RSA de 663 bits, l'Inria et ses partenaires démontrent la vulnérabilité d'une clé RSA de 768 bits. En conjuguant différentes capacités de calcul mises à leur disposition pendant 2 ans et demi, ils sont parvenus à casser cette clé de 232 chiffres en retrouvant les facteurs premiers qui la composent. Ce nouveau record est une belle illustration de l'efficacité des systèmes de calcul distribué. Il confirme les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en démontrant la vulnérabilité d'une clé RSA de 768 bits.

- Grande longueur de clefs par rapport au chiffrement symétrique  
→ Performance "catastrophiques" → nécessiter de combiner les systèmes de chiffrement.

# Plan

- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- ➔ ■ Condensat
- Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

# Condensat

*Une fonction de hachage est une fonction qui convertit un grand ensemble en un plus petit ensemble, l'empreinte.*

- `> cat contrat.odt | md5sum -`  
`693f40a4d6a497d422372ce4bfd2bbc2 -`
- `> echo "coucou" | md5sum -`  
`4c2383f5c88e9110642953b5dd7c88a1 -`
- Unicité "statistique" de l'empreinte
- Algorithmes :
  - MD4 (obsolète)
  - MD5 (peu sûr)
  - SHA-1 , SHA-256 (recommandé), SHA-512

# Application aux mots de passe

- Application du hashage à la gestion des mots de passe : ne pas stocker les mdp en clair

passwordHash = SHA( salt + motdepasse )

- Utilisation d'un salt (grain de sel) pour ne pas se faire craquer par les rainbow-tables
- Ajout éventuel du login pour éviter (en cas de salt unique) d'avoir le même password haché.

root:\$6\$FXV4/nhQ\$VgENrxUI...gzYbqpGrm/:14855:0:99999:7:::

Id=6 → SHA512

salt

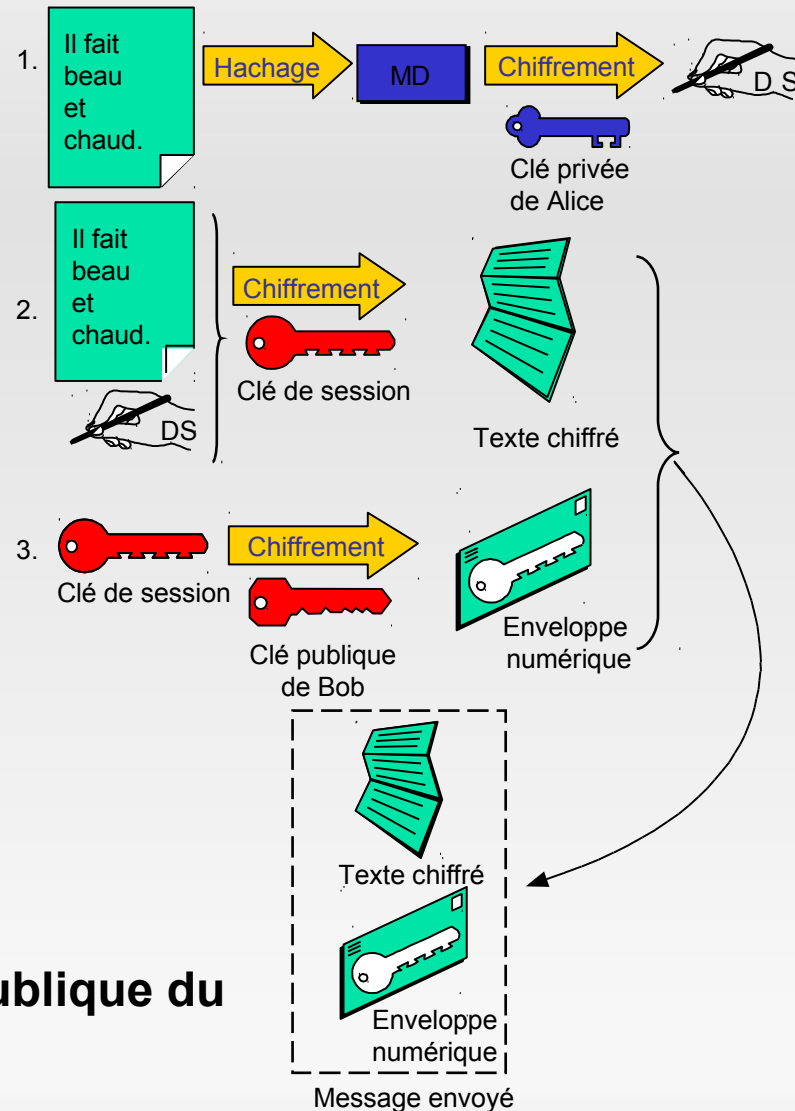
SHA512(salt+mdp)

# Plan

- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- ➔ ■ Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

# Vue globale

- Signer & chiffrer

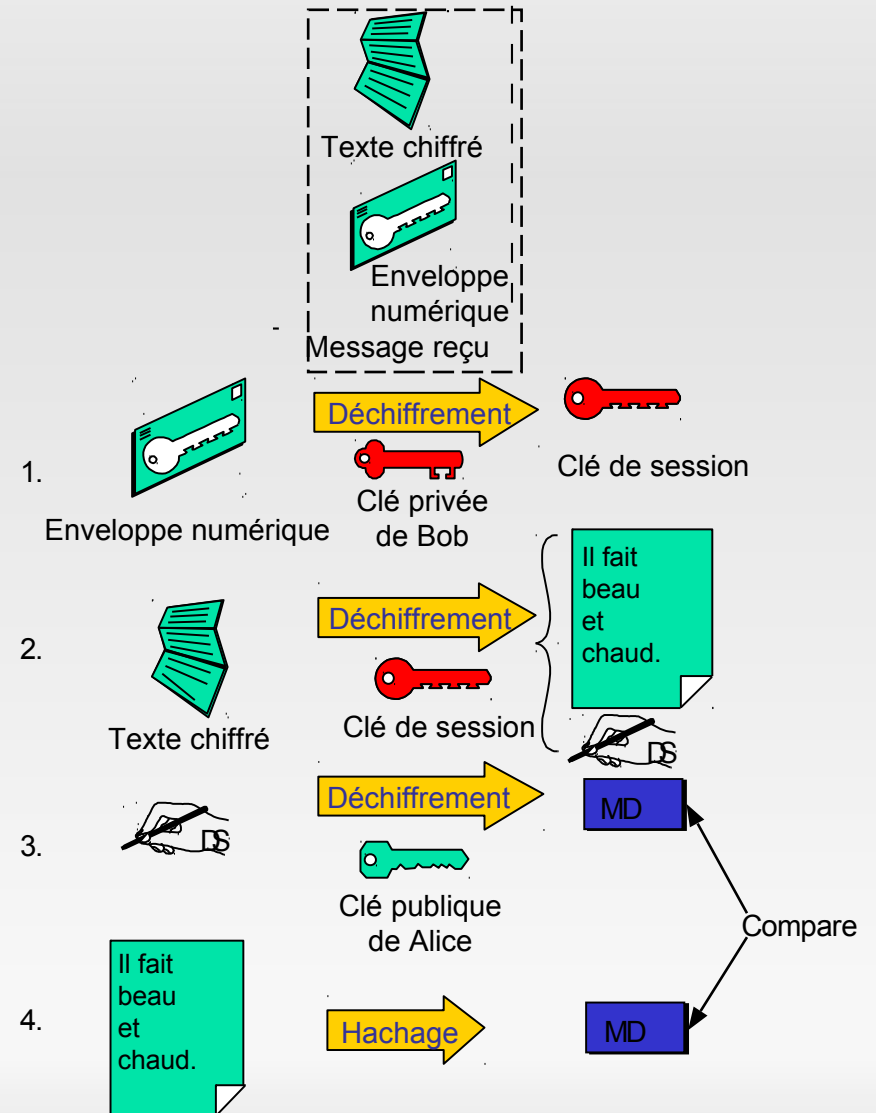


**Connaissance préalable : la clef publique du destinataire.**

# Vue globale

- Déchiffrer  
& vérifier la signature

**Connaissance préalable : la clef publique de L'émetteur.**



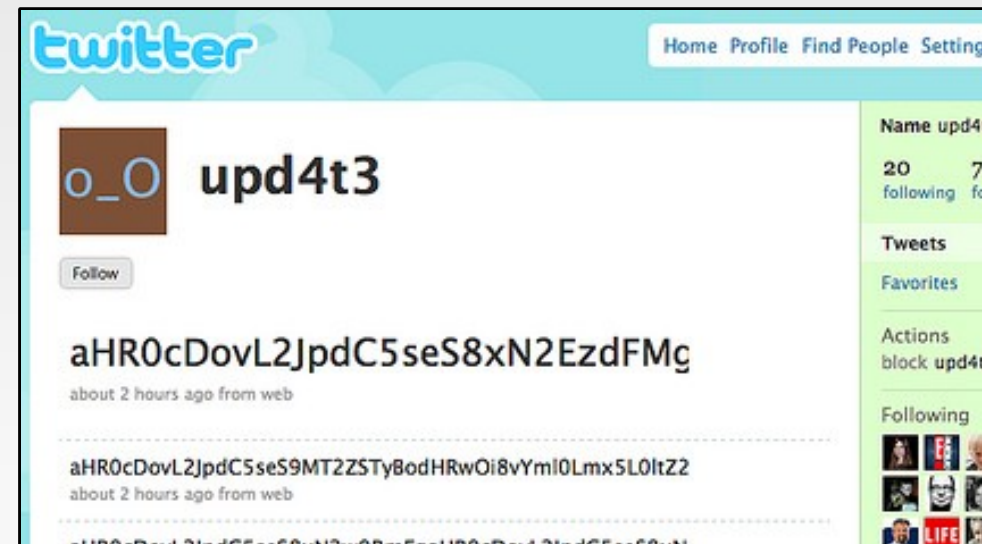


# Plan

- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- ➔ ■ Steganographie et canaux cachés
- Pièges du chiffrement

# Steganographie

- Steganographie = Dissimuler un message dans un autre message
  - Utilisation de bits de poids faible dans une image (LSB Lest Significant Bits), ou sur les teintes (TSL),
  - Utilisation des algorithmes de compression (format jpeg souvent utilisé : steg, JPhide, OutGuess, DissidentX ...),
  - Utilisation dans du Texte, html (SecureEngine, ...)
  - Utilisation via des spams (spammimic)
  - ...Canaux C&C via Twitter...



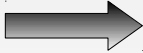
```
echo "aHR0cDovL2JpdC5seS9SN1NUViAgaHR0cDovL2JpdC5seS8yS29Ibw==" | openssl base64 -d
```

```
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoHo
```

# Steganographie

- Tatouage numérique (filigrane numérique)
  - Utilisation de la steganographie pour insérer des éléments de copyright "prouvant" l'auteur (=le seul à connaître ces éléments).
  - Visible et invisible
- Canaux cachés (dit de stockages ou temporels)
  - Insertions de données dans un événement 0 ou 1
    - Lock sur une ressource,
    - bit non utilisé dans une trame,
    - Numéros de séquences (SIP)
    - Commentaire html, ...
    - Utilisation de padding (cas ICMP)
    - Requetes DNS (RR TXT pour franchir les hotspots)

# Plan

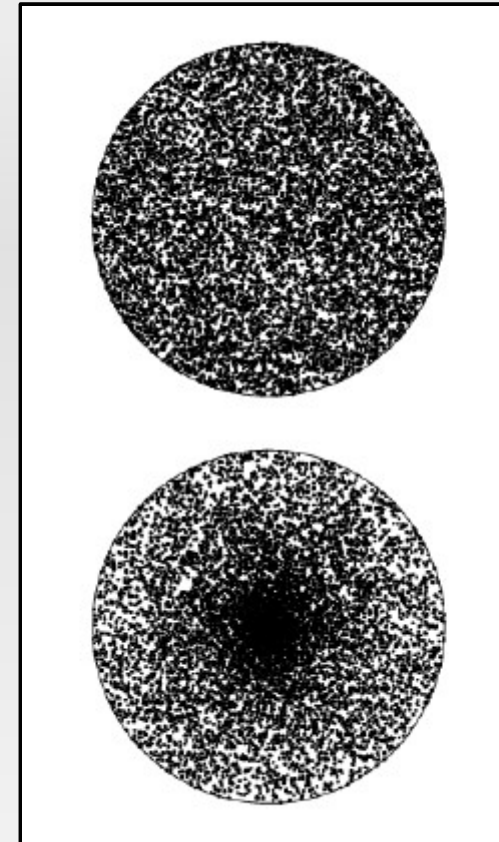
- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- Steganographie et canaux cachés
-  ■ Pièges du chiffrement

# Sécurité du chiffrement

- Sécurité des algorithmes plutôt bon.
- Sécurité des implémentations :
  - Repose sur le caractère "secret" de la clef privée.
  - Comment protéger cette clef ?
    - Droit sur les fichiers
    - Mot de passe
    - Puces TPM (Trusted Platform Module). Qui a accès au module ?
    - Token (physique + mot de passe)
    - Quid des applications (clef privé serveur WEB apache) ? Qui vient saisir le mot de passe au démarrage ?
- Où trouver les clefs publiques ?
  - Annuaire (pgp.mit.edu, ...) ? Partage bi-latéral ?

# Sécurité du chiffrement

- Les nombres aléatoires :
  - Comment obtenir des bits VRAIMENT aléatoires.
  - El gamal, clefs de sessions, ... reposent sur eux.
- Entropie des suites de bits
  - Bits statistiquement prédictibles => cryptanalyse
- Sources d'aléas externes
  - Les mouvements de l'utilisateur,
  - Les processus, activité du disque dur, réseau
  - La charge du processeur
  - Certains paramètres du noyau (/dev/random)
  - Bruits sur carte son/video
  - Hardwares dédiées (TRNG) ou cartes (Intel/AMD,...)
  - Générateurs pseudo-aléatoires (PRNG)



# Pieges du chiffrement

## ■ Difficultés :

- Comment être sûr que  $K_{pub}(\text{Bob})$  est bien celle de Bob ?
  - Infrastructure à clef publique.
  - PGP (Pretty Good Privacy)

”une key signing party est un événement pendant lequel des personnes s'échangent entre elles leurs clefs compatibles PGP. L'échange se fait de visu, de la main à la main. En partant du principe qu'on a confiance en le fait que la clef appartient bien à la personne qui le prétend, les participants signent numériquement le certificat contenant cette clef publique, le nom de la personne, et ainsi de suite.”
- Si Bob a perdu sa clef privée (ie son mot de passe) ?
  - Tous ses documents chiffrés lui sont désormais perdus !
    - Sauvegarde en clair ...
    - Un ”pass partout” = clef de recouvrement
    - Sequestre de ses clefs privés (tier de confiance)
  - Il ne peut plus signer de document

# Pieges du chiffrement

- Difficultés :
  - Si Bob refait une nouvelle paire de clefs ?
    - Une nouvelle signature... L'ancienne est toujours valide.
    - Comment invalider l'ancienne ?
    - Si on veut chiffrer vers Bob, quelle clef publique choisir ?
    - Révocation de l'ancienne paire de clefs ? Il faut maintenir des listes.
  - Si Bob s'est fait voler sa clef privée ?
    - A partir de quand peut-on affirmer que c'est son usurpateur qui signe à sa place ?
  - Comment avertir les autres (ceux qui ont gardé la clef publique) ?

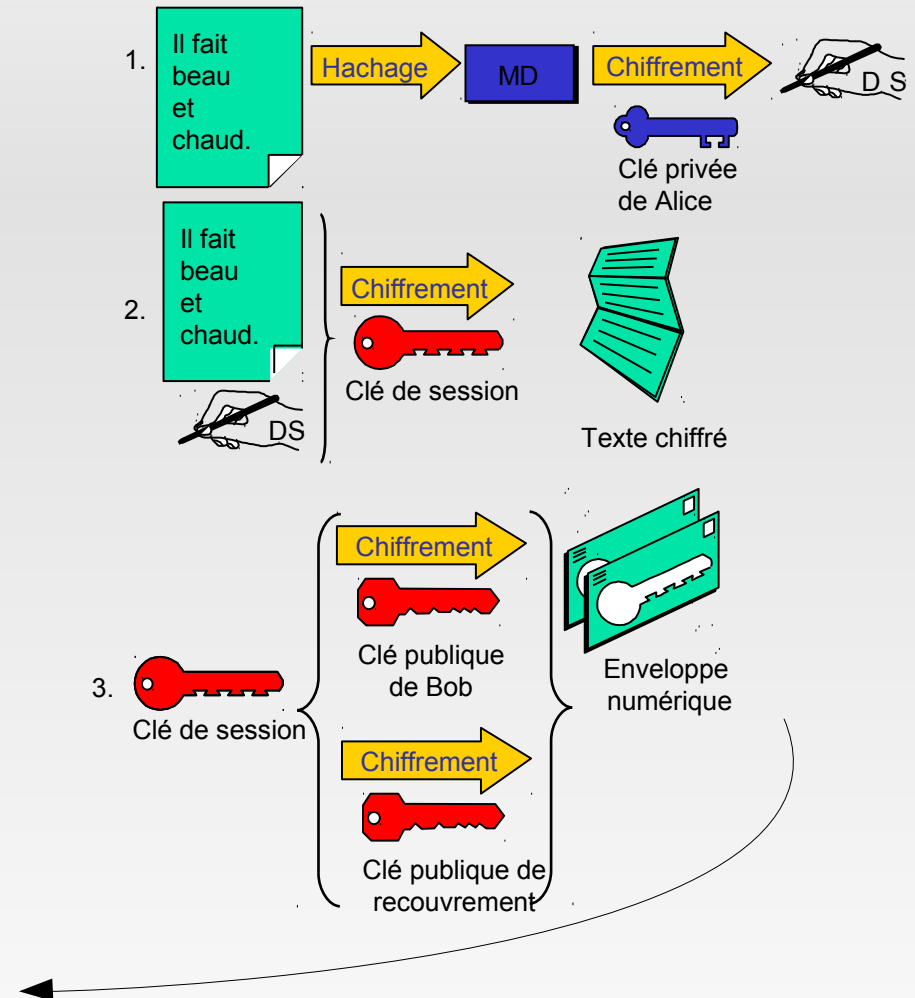
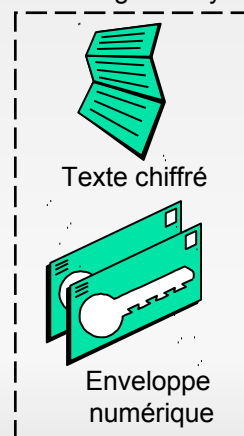


# Clefs de recouvrement

## ■ Objectif

- Intégrer un second chiffrement de la clef de session afin de pouvoir avoir deux moyens de déchiffrement.
- Sécurité = sécurité de la plus faible des deux clefs.
- Clef de recouvrement chiffre plus de données que les clefs de chacun => plus sensible

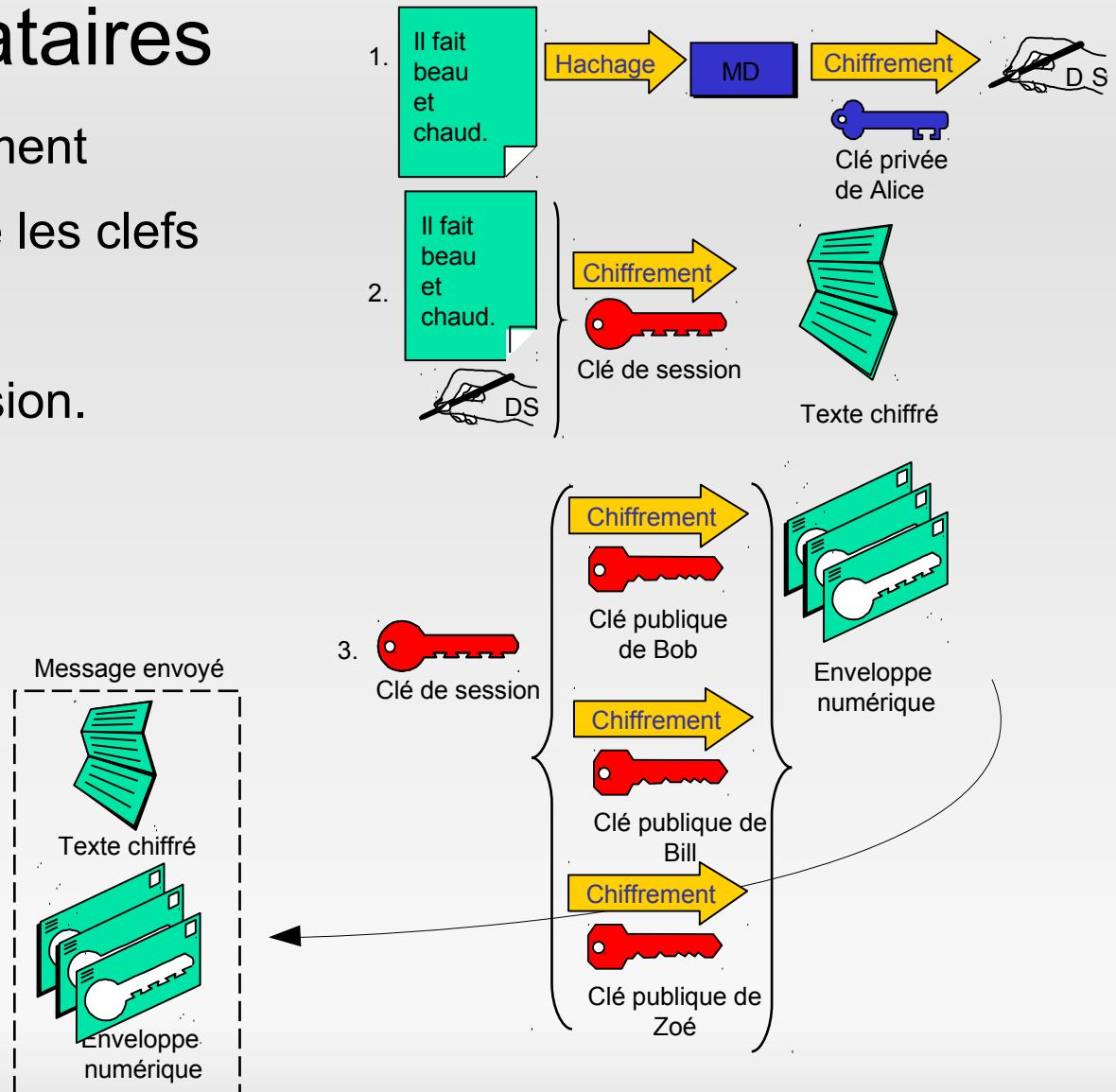
Message envoyé



# Chiffrer pour un groupe

## ■ Plusieurs destinataires

- Voir clefs de recouvrement
- Nécessite de connaître les clefs de chacun.
- Cas des listes de diffusion.



# Plan

- Principe / définitions
- Chiffrement à clef secrète
- Chiffrement asymétrique
  - Chiffrement
  - Signature
- Condensat
- Vue globale
- Steganographie et canaux cachés
- Pièges du chiffrement

*Il y a longtemps dans un pays lointain...*

# Classified as a weapon

