CENTRE NATIONAL D'ÉTUDES SPATIALES

Aristote
Groupe PIN

Utilisations pratiques de la cryptographie

Frédéric Pailler (CNES)

13 janvier 2009

Objectifs

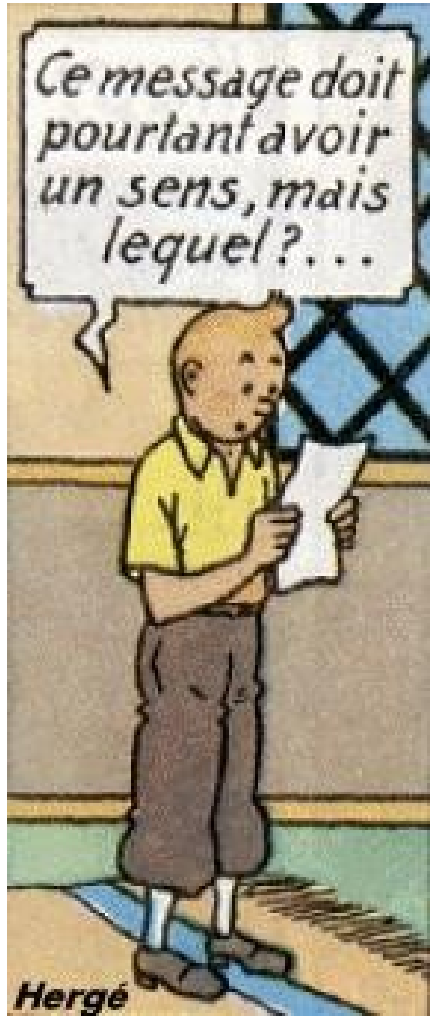
- Décrire les techniques de cryptographie les plus courantes
- Et les applications qui les utilisent
- Peu de détails sur les algorithmes, en particulier les aspects mathématiques

Histoire

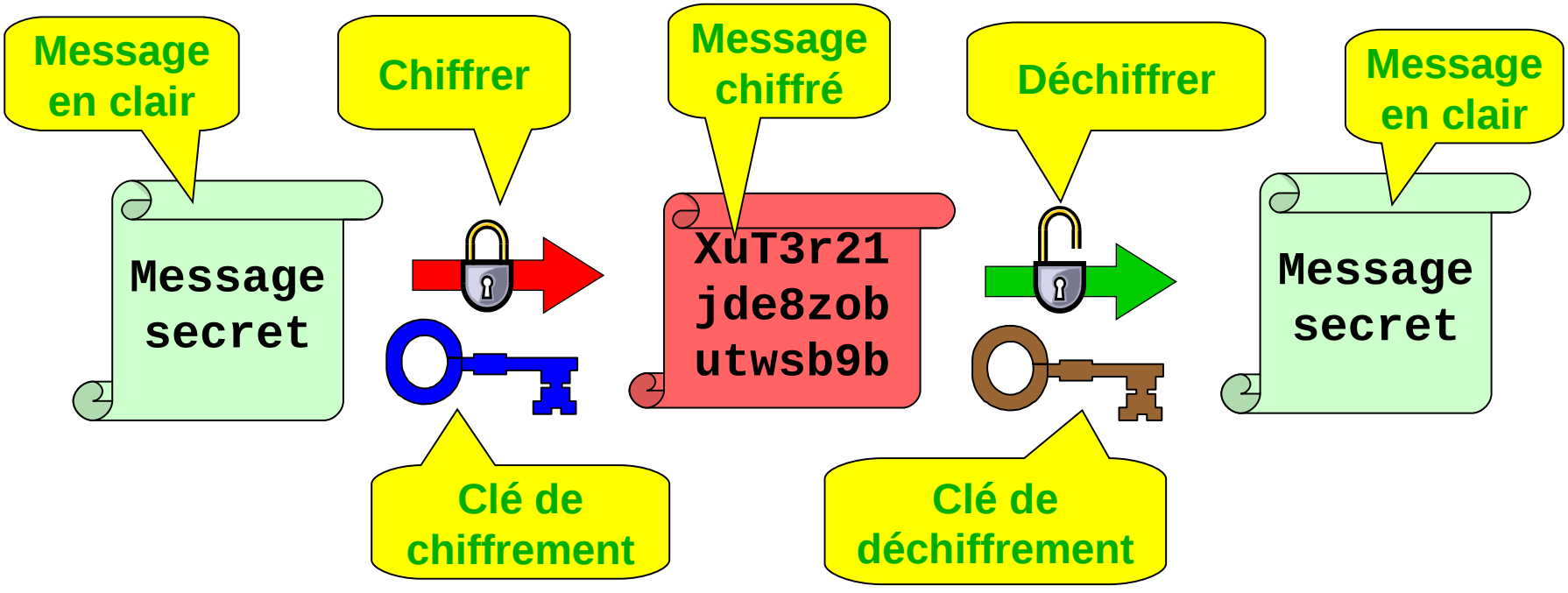
- Technologie très ancienne (depuis Jules César)
  - Développée pour des raisons militaires
  - Fondée sur les mathématiques
- Permet de répondre à des besoins de :
  - Confidentialité
  - Intégrité
  - Authentification
- Principe : algorithme + secret (clé)
  - Exemple

Terminologie

- **Cryptographie** (du grec kruptos : caché, secret et graphein : écrire, dessiner) : ensemble des techniques et applications permettant de mettre en œuvre des écritures secrètes
- **Cryptanalyse** : étude de l'art de compromettre (ou mettre en défaut) des mécanismes cryptographiques
- **Cryptologie** : l'ensemble des deux disciplines précédentes
- **Stéganographie** (du grec steganos : couvert) : ensemble des procédés visant à dissimuler l'existence même de l'information



Terminologie



A quoi sert la cryptographie ?

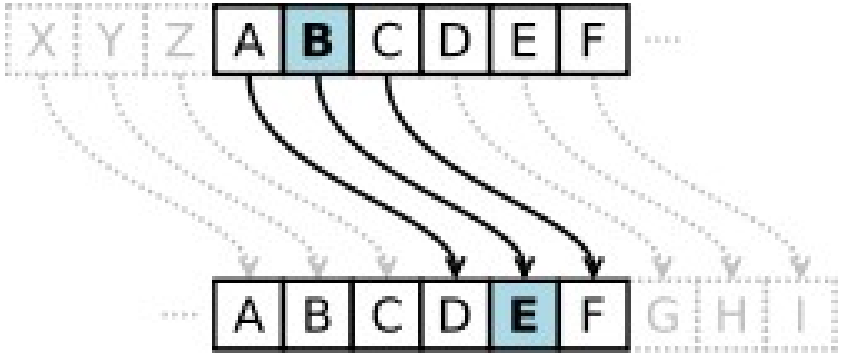
- Offre des services pour répondre à des besoins de sécurité de l'information :
  - Empêcher un tiers d'intercepter et lire les messages (Confidentialité)
  - Empêcher un tiers d'intercepter et modifier les messages (Intégrité)
  - Empêcher un tiers de créer de faux messages que le destinataire pourrait considérer comme valides (Authentification)
- Exemples :
  - Transmission de l'information sur un medium de communication non sûr
  - Stockage sur un medium non sûr
- Non sûr = qui n'offre pas intrinsèquement les services attendus

Limites

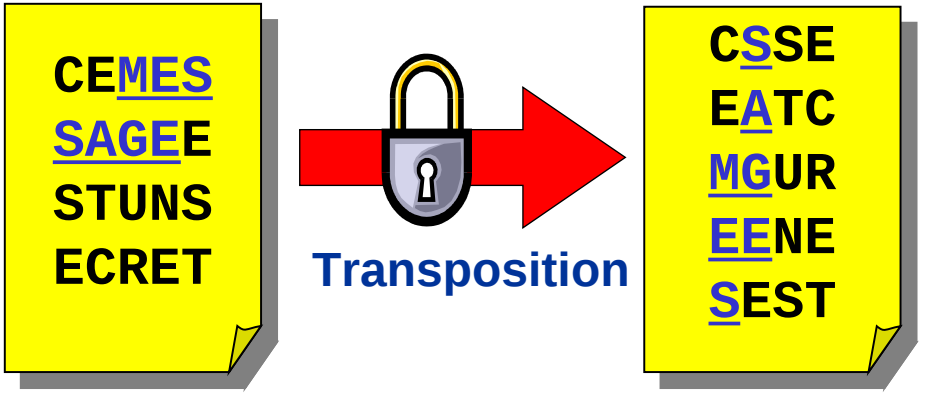
- Toutes les techniques de chiffrement sont **vulnérables**
  - Avec suffisamment de ressources (temps, puissance de calcul...)
  - L'ensemble de ces ressources est appelé l'**effort**.
- L'information est protégée si l'effort nécessaire pour l'obtenir dépasse sa propre valeur
  - Objectif : Faible rapport valeur/effort.
- Attention aux erreurs courantes :
  - Protéger les clés !
  - Protéger l'information lorsqu'elle est déchiffrée !
- La sécurité à 100 % n'existe pas...

Histoire

- **Utilisée depuis plus de 4000 ans pour garantir la confidentialité des transmissions de données**
- **Jusqu'à très récemment, essentiellement utilisée à des fins militaires**
- **Avant l'informatique les algorithmes étaient fondés sur des opérations des base :**
  - **Substitution : substituer un caractère ou un groupe de caractères par un autre**
    - Exemple : code de César
  - **Transposition : mélanger les positions des caractères dans le message**

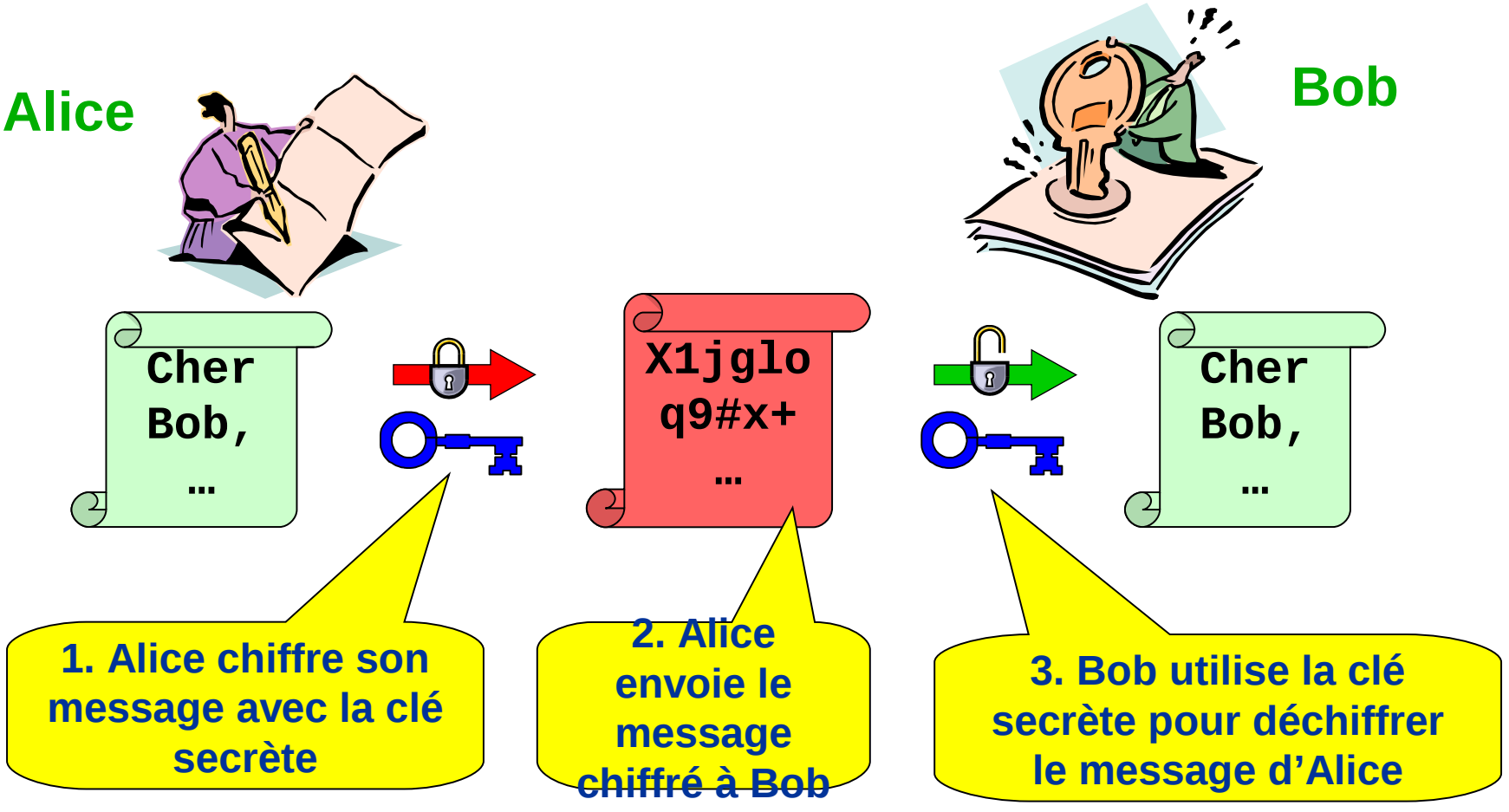


Source : Wikipedia



Cryptographie à clé secrète

- La même clé pour chiffrer et déchiffrer

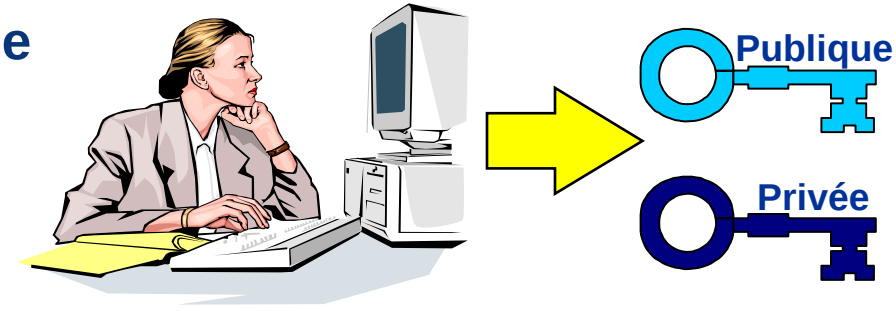


Cryptographie à clé secrète

- **Algorithmes les plus connus :**
  - **DES (clé de 56 bits), ancien standard gouvernement US**
  - **3DES (triple DES) (clé de 112 ou 168 bits)**
  - **AES (clé de 128, 192 ou 256 bits), nouveau standard US**
  - **IDEA (clé de 128 bits), utilisé par PGP**
  - **RC4 (longueur de clé variable)**
- **Avantage : très rapides (même en logiciel)**
- **Problèmes :**
  - **Se communiquer la clé secrète de manière sûre**
  - **Nombre de clés très élevé si correspondants nombreux**
    - Augmente selon le carré du nombre de correspondants

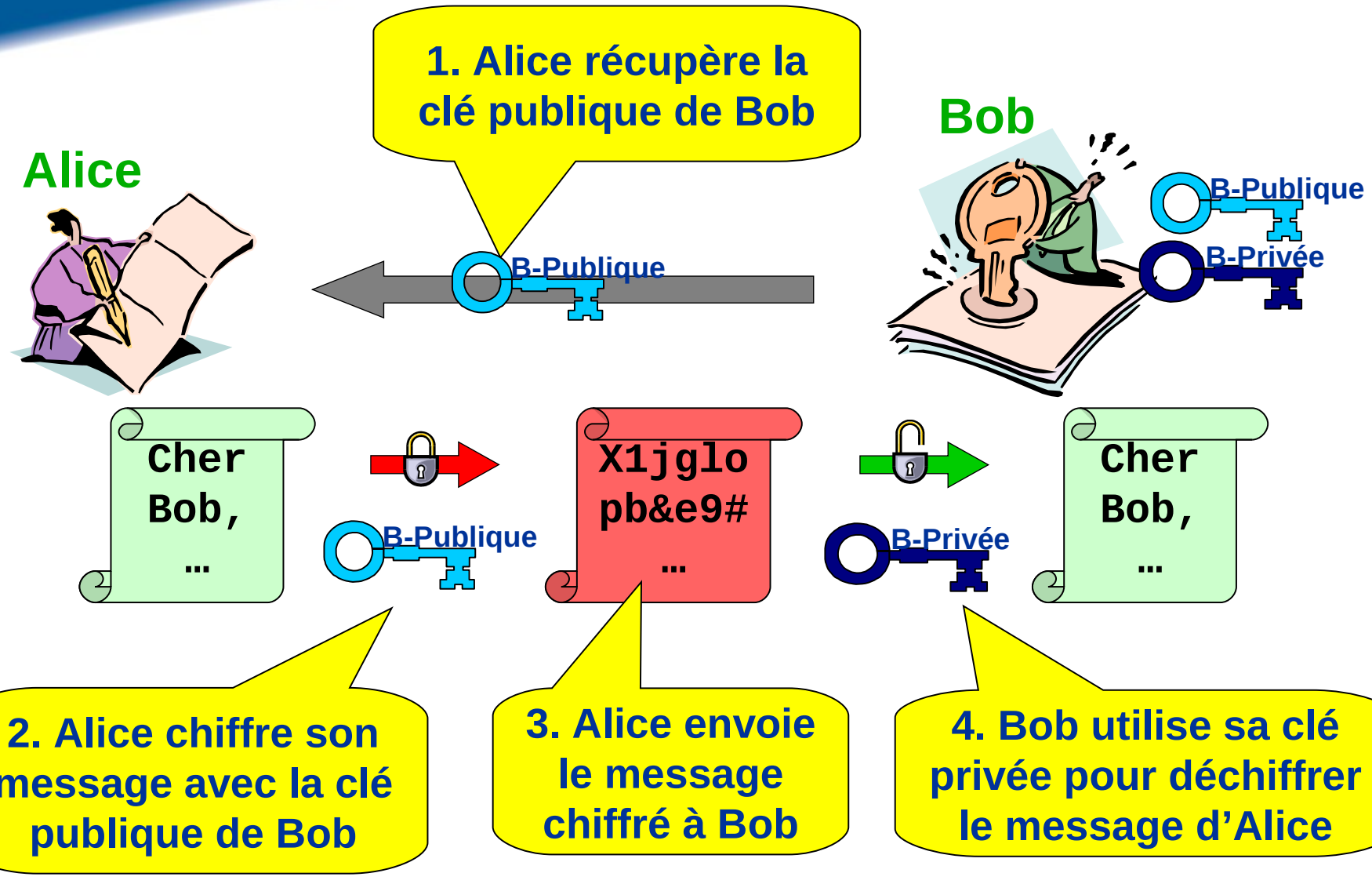
Cryptographie à clé publique

- Paire de clés liées : 1 publique et 1 privée
- Ce qui est chiffré par l'une est déchiffré par l'autre
- La clé publique peut être communiquée à tout le monde



- Avantages : pas de problème d'échange de clés
  - L'échange peut se faire sur un canal non sécurisé
- Algorithme le plus connu :
  - RSA (www.rsa.com/rsalabs/node.asp?id=2213)
  - Utilise la décomposition des très grands nombres en facteurs premiers
- Inconvénient : algorithmes très lents
  - 100 à 1000 fois plus lents que les algorithmes à clé secrète

Chiffrer avec un algorithme à clé publique

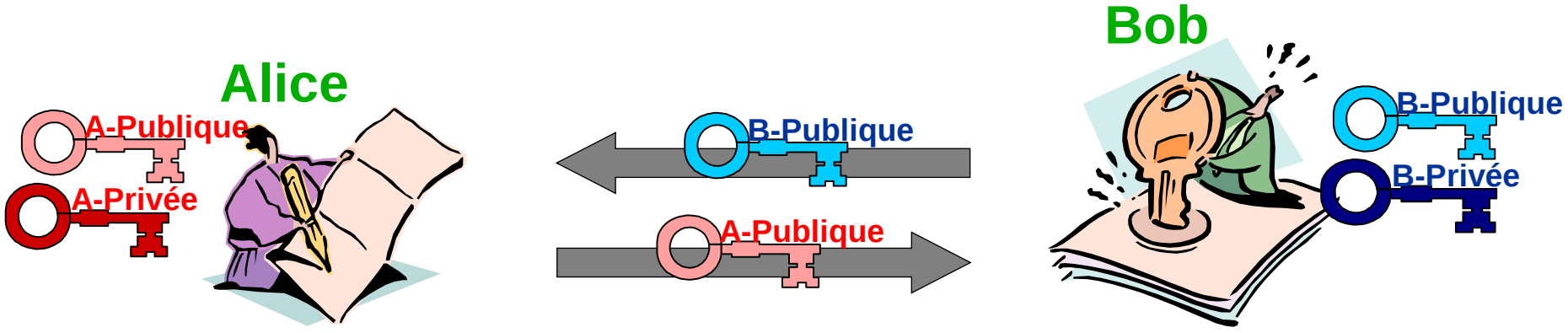


Cryptographie hybride

- En pratique, on combine les 2 types d'algorithmes : cryptographie hybride
  - Cryptographie à clé secrète = rapidité
  - Cryptographie à clé publique = gestion facile des clés
- Principe :
  - Utiliser la cryptographie à clé publique comme canal sécurisé pour transmettre une clé secrète
  - Une nouvelle clé secrète est créée à chaque session entre les deux correspondants (on l'appelle la clé de session)
  - Lorsque la session se termine, chaque correspondant détruit la clé de session

Algorithme de Diffie-Hellman

- Permet de créer une clé secrète sans la faire circuler
- Catégorie des algorithmes à clé publique



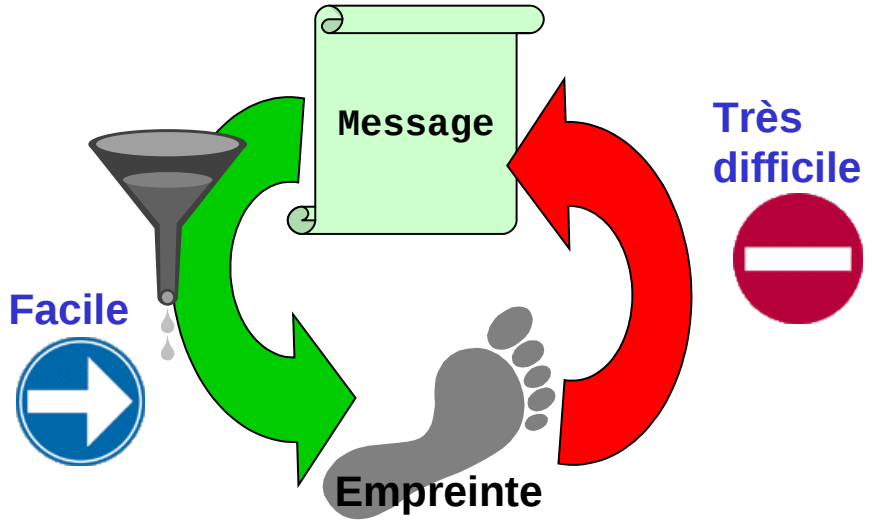
Alice calcule :
f_1*(B-Pub,A-Pri)* **= secret**

Bob calcule :
f_2*(A-Pub,B-Pri)* **= secret**

IDENTIQUES : c'est la clé de session

Fonctions de hachage

- y=f(x) très facile à calculer
  - Mais connaissant y, il est très difficile de calculer x
- Quel que soit x, y est de longueur fixe
  - y est appelé l'empreinte de x (en anglais : *hash* ou *digest*)



- Assure l'intégrité du message x :
  - L'émetteur calcule l'empreinte et la transmet avec le message
  - Le destinataire recalcule l'empreinte à partir du message reçu et la compare à celle reçue avec le message
- Mais sensibilité aux attaques « *man in the middle* »
  - Le pirate modifie le message en route, et aussi l'empreinte
  - Elle sera considérée comme valable par le destinataire
- Algorithmes les plus connus : MD5 (128b), SHA-1 (160b)

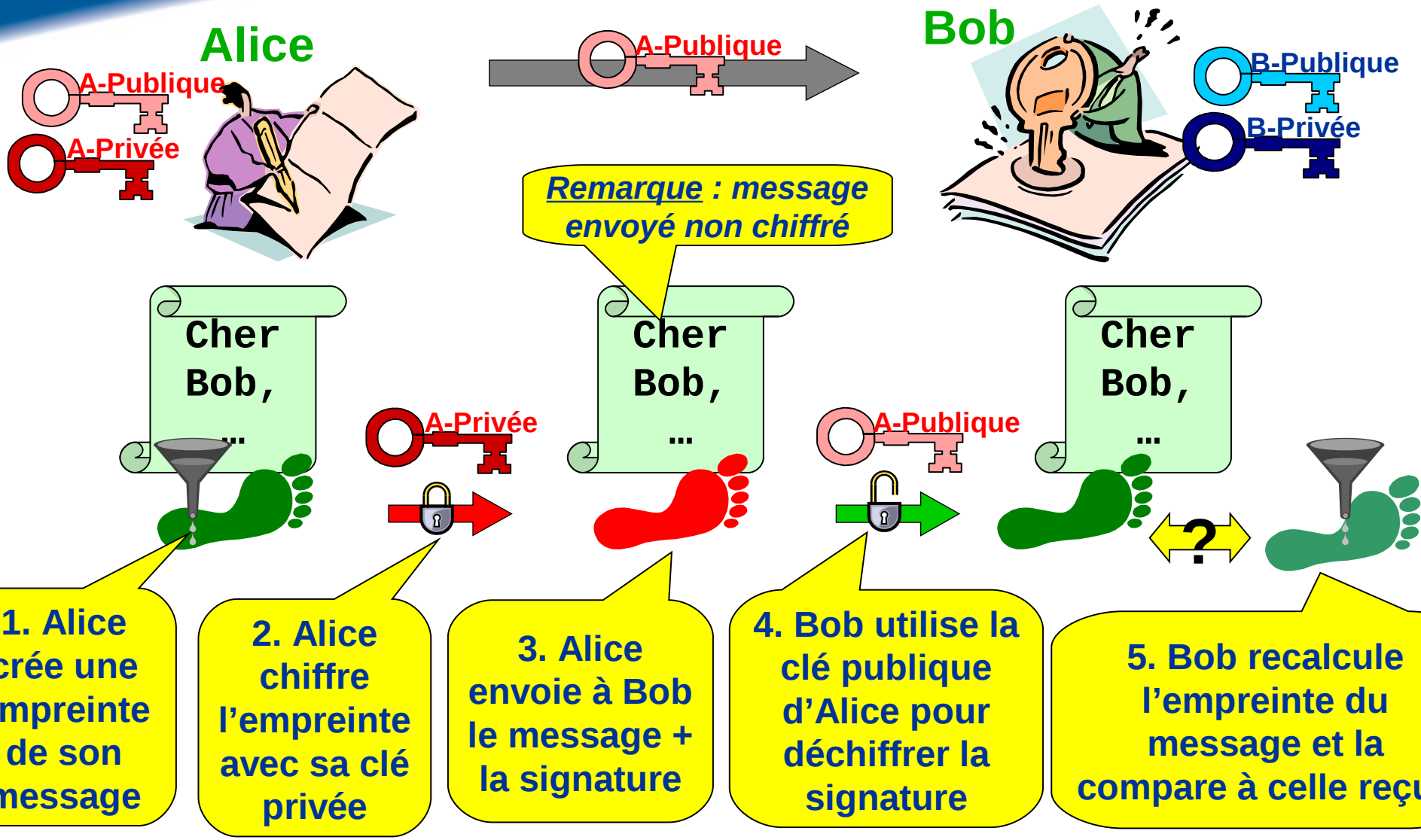
Signatures numériques

- **Propriétés attendues d'une signature :**
  - **Infalsifiable**
  - **Authentifie son auteur**
  - **Liée au document :**
    - Non réutilisable pour un autre document
    - Rendue invalide par une modification du document
  - **Ne peut pas être reniée par son auteur**

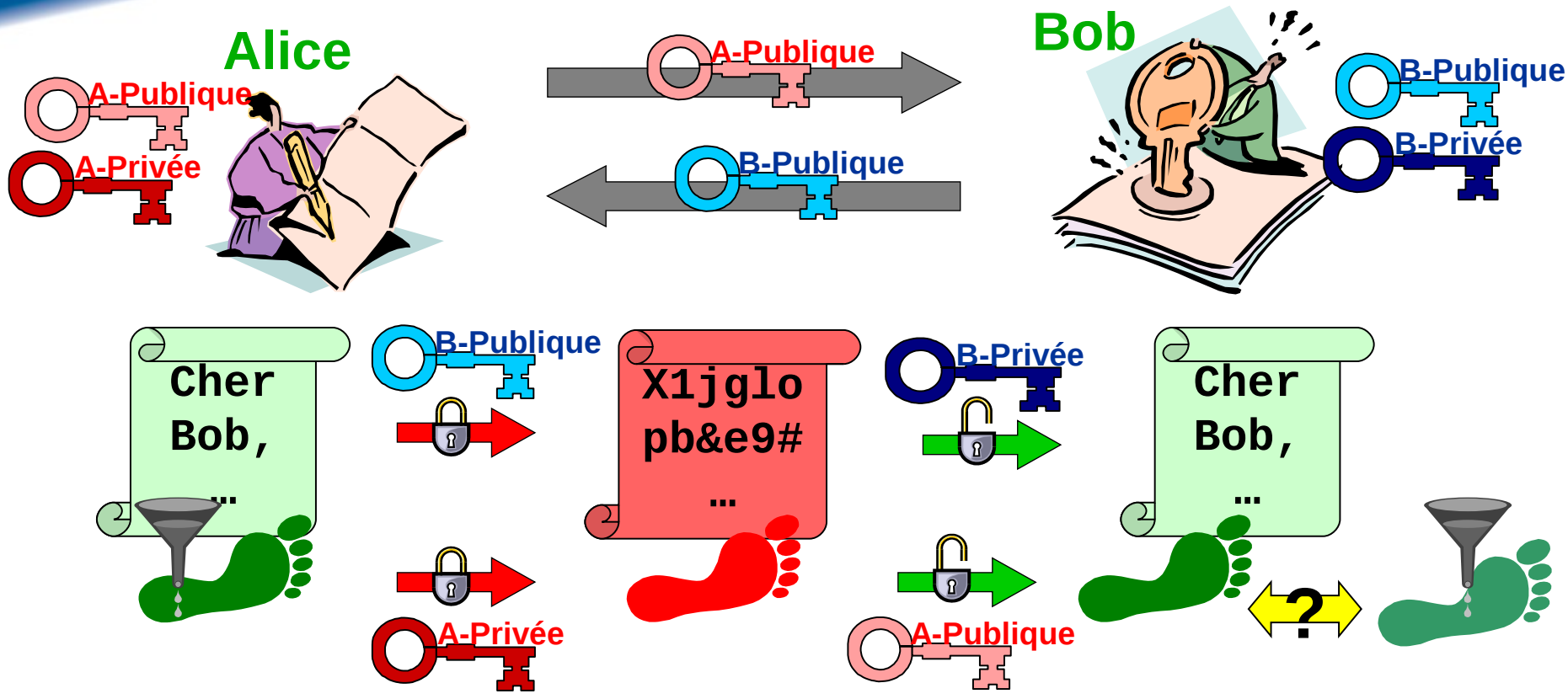
Les signatures manuscrites possèdent-elles ces propriétés ?

- **Signature numérique = cryptographie à clé publique + fonction de hachage**
- **Cryptographie à clé publique, mais utilisée à l'envers**
  - **Celui qui signe utilise sa clé privée**
  - **Celui qui vérifie la signature utilise la clé publique du signataire**

Signer numériquement un message



Signer et chiffrer un message

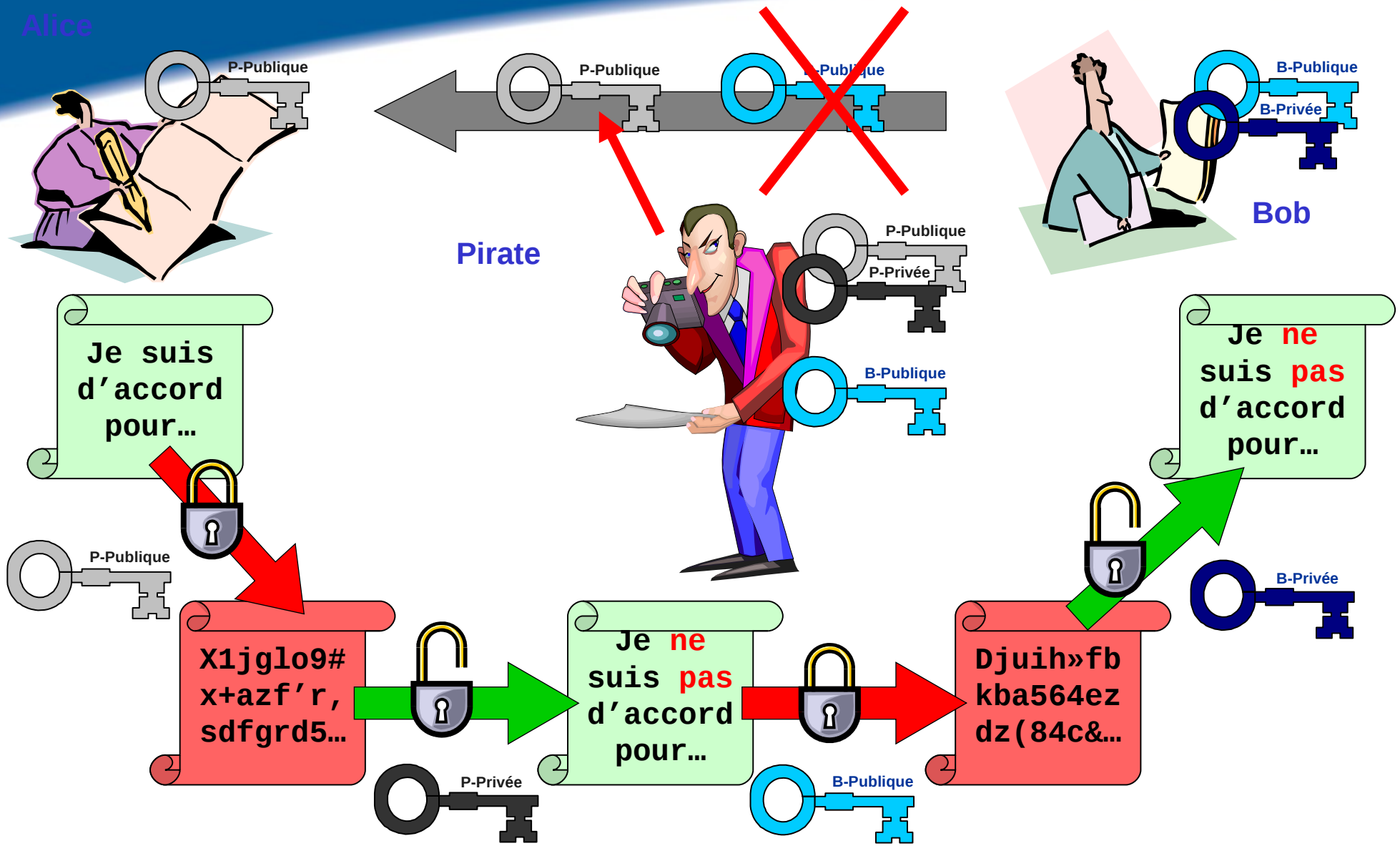


- Chiffrement = Confidentialité
- Signature = Intégrité + authentification

Limites de la cryptographie à clé publique

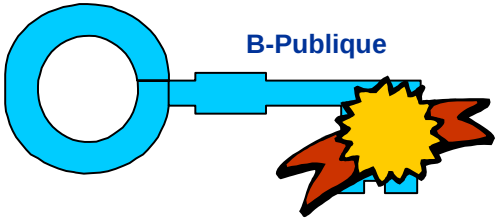
- **Clés publiques vulnérables aux attaques « *Man in the middle* »**
  - **Bob n'est pas sûr que la clé publique reçue est celle d'Alice**
  - **Un pirate peut se faire passer pour Alice auprès de Bob et inversement (interception des communications)**
  - **Ni Alice ni Bob ne se doutent de rien**

Man in the middle



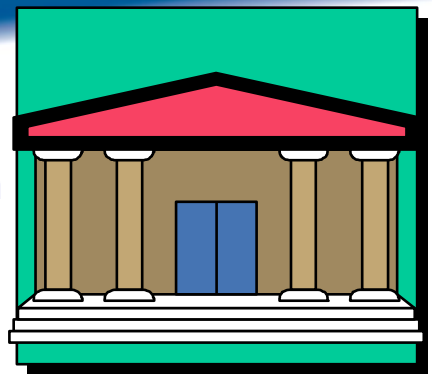
Les certificats

- Il faut un moyen de lier une clé publique à son propriétaire :
  - Nom d'une personne
  - Nom d'une entreprise
  - Adresse Mail (dupond@cnes.fr)
  - Nom de domaine (www.cnes.fr)
  - Adresse IP...



- Certificat = clé publique certifiée par une autorité
  - Clé publique signée par une clé d'autorité
  - Fichier binaire au format normalisé : X.509
    - La clé publique
    - A qui appartient la clé (adresse mail, nom de personne...)
    - A quels usages elle est destinée (chiffrer, signer...)
    - Les dates de validité (début et fin)
    - Le nom de l'autorité
    - Un numéro de série
    - La signature associée (créée par l'autorité)

Création d'un certificat



Autorité de certification

Vérifie l'identité de Bob

Fait confiance à

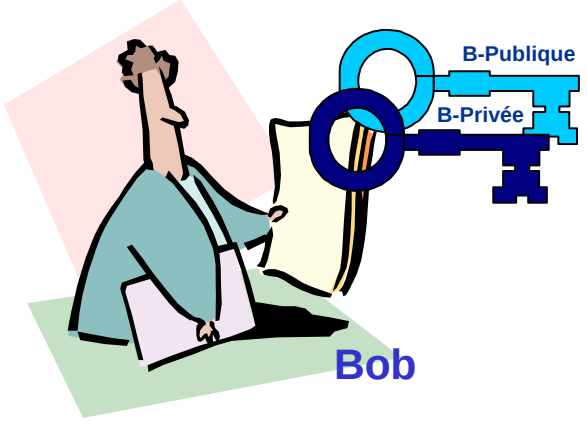
B-Publique

B-Publique

Certificat

Alice

B-Publique



B-Publique

B-Privée

Bob

Exemple de certificat X.509

- Certificate:
- Data:
- Version: 3 (0x2)
- Serial Number: 1 (0x1)
- Signature Algorithm: sha1WithRSAEncryption
- Issuer: C=FR, O=CNES, OU=0002 775665912, CN=AC RACINE
- Validity
- Not Before: Jun 30 12:33:07 2008 GMT
- Not After : Jun 30 12:33:07 2018 GMT
- Subject: C=FR, O=CNES, OU=0002 775665912, CN=AC CNES
- Subject Public Key Info:
- Public Key Algorithm: rsaEncryption
- RSA Public Key: (2048 bit)
- Modulus (2048 bit):
- 00:da:3a:d2:9b:8f:e5:ea:bc:3d:42:23:69:dc:68:
  .../...
- 14:37:92:6d:49:91:9d:d3:eb:47:6e:6e:b9:32:14:
- fc:67
- Exponent: 65537 (0x10001)
- X509v3 extensions:
- X509v3 Basic Constraints: critical
- CA:TRUE, pathlen:0
- X509v3 Subject Key Identifier:
- 4F:44:24:AD:A2:32:9B:14:2E:B8:F7:CD:32:FB:E3:7C:AD:25:E5:01

Exemple de certificat X.509 (suite)

- X509v3 Authority Key Identifier:
- keyid:AE:0C:07:3C:9B:42:0E:4E:C4:31:D1:C6:0D:56:40:07:79:32:BE:B5
- X509v3 Certificate Policies:
- Policy: 1.2.250.1.12.1.1.1.1.1
- CPS: http://www.cnes.fr/igc/PC_acracine.pdf
- X509v3 Key Usage: critical
- Certificate Sign, CRL Sign
- X509v3 CRL Distribution Points:
- URI:ldap:///CN=AC%20RACINE,CN=CDP,CN=Public%20Key %20Services,CN=Services,CN=Configuration,DC=ad,DC=cnes,DC=fr?certificateRevocationList?base? objectclass=cRLDistributionPoint
- URI:ldap://safir/cn=AC%20RACINE,ou=CDP,ou=IGC,ou=Applications,o=cnes,c=fr?certificateRevocationList?base? objectclass=crldistributionpoint
- URI:http://www.cnes.fr/igc/acracine.crl
- Authority Information Access:
- OCSP - URI:http://ocsp.cnes.fr/ocsp
- Signature Algorithm: sha1WithRSAEncryption
- 0f:3d:df:47:b2:33:e2:67:24:3d:0a:b5:c6:8f:fc:ed:80:53:
- 9b:db:db:e6:54:70:bd:cb:35:c4:70:86:d2:7b:7c:36:74:c5:

.../...

- d8:ee:dc:b2:65:7a:11:53:47:48:b0:f1:fe:54:b6:c0:93:8e:
- ec:62:13:2f

Portefeuille de clés

- **Bob possède une ou plusieurs clés privées**
  - **Elles restent en sa possession et ne transitent jamais sur le réseau**
  - **Il faut les protéger : carte à puce, mot de passe, etc.**
  - **C'est son portefeuille de clés : il y choisit la clé adéquate en fonction du service utilisé**
- **Comparaison : portefeuille classique**
  - **Carte d'identité, permis de conduire, badge d'entreprise, carte de transport, passeport...**
  - **Chaque papier est lié à une utilisation bien précise**
  - **L'utilisateur et le vérificateur font confiance en la même autorité qui a délivré le papier**
    - Aéroport : Préfecture
    - Entrée du CNES : service des badges

Infrastructures de Gestion de Clés

- **IGC ou PKI (*Public Key Infrastructure*) : délivre et gère les certificats**
- **Complexités techniques :**
  - **Expirations et renouvellements**
  - **Révocations**
    - Gestion des CRL (*Certificate Revocation Lists*) : listes de certificats ayant été compromis avant leur fin de validité
    - OCSP
  - **Transchiffrement : messages chiffrés avec un certificat expiré ou révoqué**
  - **Séquestre**
- **IGC = un peu de technique, mais surtout beaucoup d'organisation**
  - **Procédures d'identification**
  - **Procédures de gestion des portefeuilles de clés privées (y compris leur support de stockage) : un certificat (même émis par une autorité irréprochable) ne sert à rien si la clé privée associée est compromise !**
- **Complexités légales**

Implications pour la pérennité des informations

- **Pérennité du niveau de sécurité ? Non**
  - **Elle dépend de l'état de l'art des moyens techniques**
  - **DES était sûr dans les années 80, plus maintenant**
- **Pérennité des signatures ? Oui**
  - **A priori indépendante de l'information associée (empreinte signée)**
- **Pérennité des informations chiffrées ? A surveiller...**
  - **Problème du transchiffrement**
    - Faut-il conserver les anciennes clés ou tout transchiffrer ?
  - **Problème de la conservation de la clé**
    - Séquestre
    - Prise d'otage de données

Pour en savoir plus

- **Wikipedia :**
  - **http://fr.wikipedia.org/wiki/Cryptographie**
  - **Histoire : http://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie**
  - **Portail : http://fr.wikipedia.org/wiki/Portail:Cryptologie**
- **L'excellent site de Didier Müller : http://www.apprendre-en-ligne.net/crypto/**
- **Le site de Frédéric Bayart : http://www.bibmath.net/crypto/**
- **Au sujet de cette présentation : Frederic.Pailler@cnes.fr**

Merci de votre attention