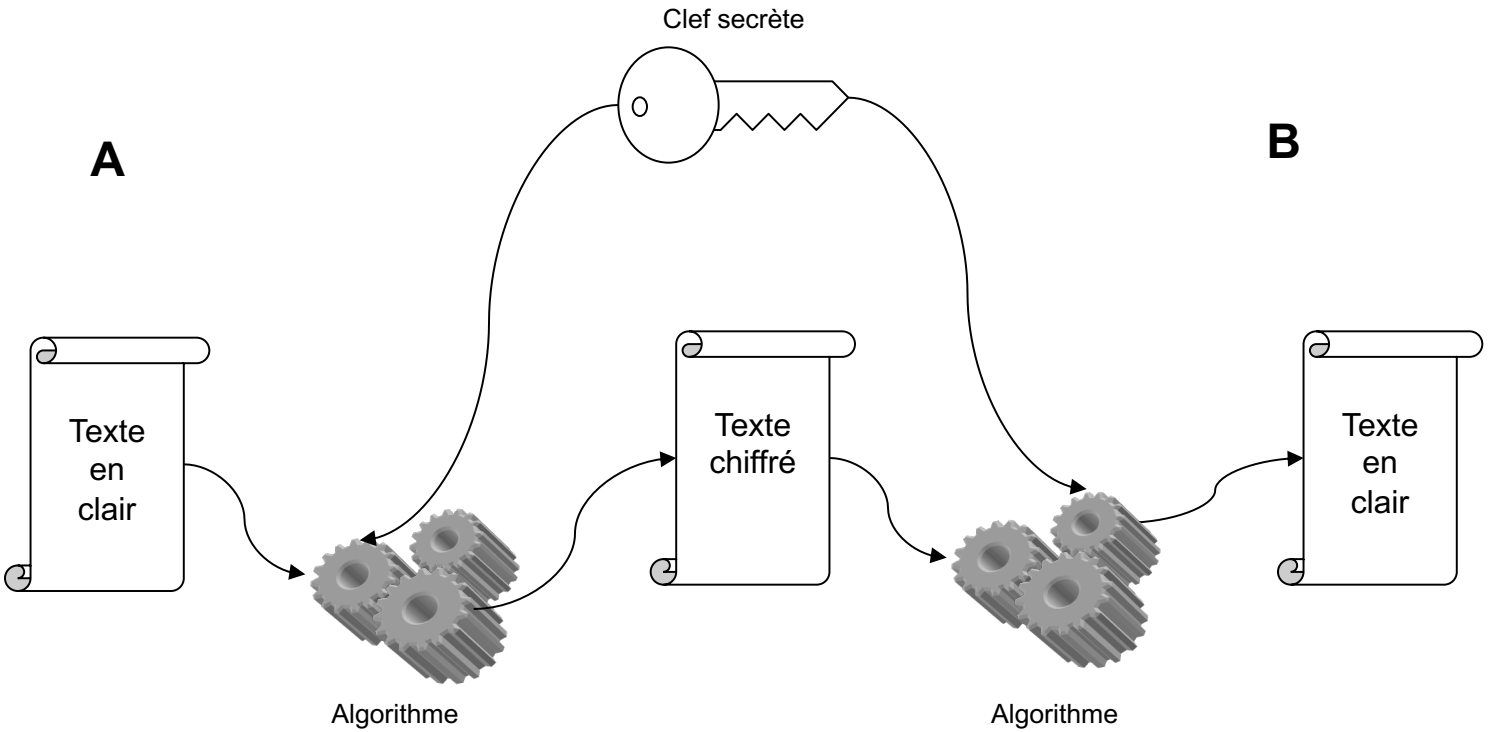
RAPPEL : Cryptographie : Méthodologies

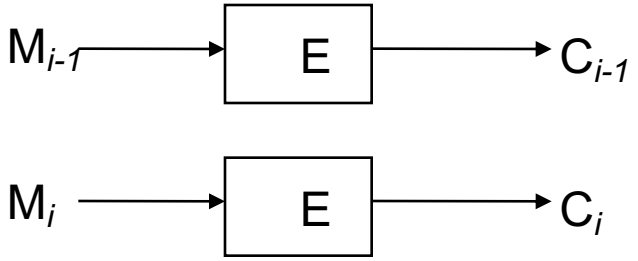
- **La cryptographie vise à encoder les messages pour qu'ils ne puissent pas être décodés sans connaissances spécifiques**
  - Ces méthodes utilisent des clés connues seulement par les personnes autorisées
- **Les mécanismes de cryptage reposent sur**
  - La transposition de caractères
  - La substitution de caractères
- **On distingue deux méthodes**
  - Utilisation de clés secrètes (par exemple, DES)
  - Utilisation de clés publiques (par exemple, RSA)
- **La majorité des systèmes de cryptographie exploitent des nombres aléatoires**
  - Il faut donc s'assurer que ces nombres sont effectivement de nature aléatoire

Cryptographie classique : Chiffrement Symétrique

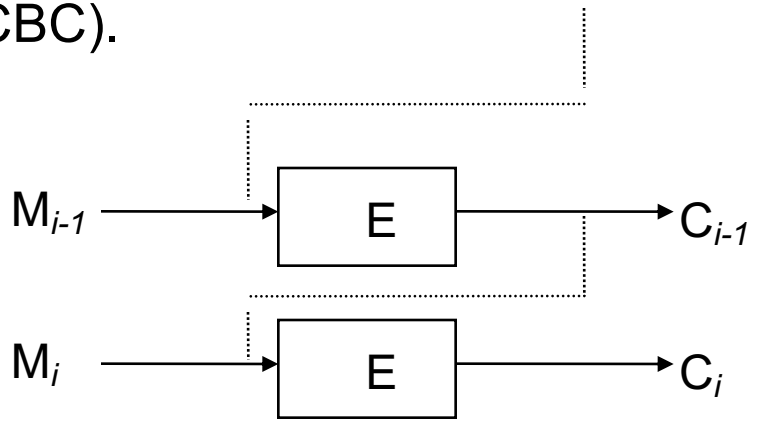


Méthodes modernes : Algorithmes Symétriques

- Deux modes:
  - Chiffrement symétrique en stream
  - Chiffrement symétrique en bloc
    - Electric Code Block (ECB).
    - Cipher Block Chaining (CBC).



ECB Mode



CBC Mode

Algorithmes Symétriques

Algorithme	Nom et commentaires	Type de chiffrement	Longueur de la clé	Normalisé
DES	*Data Encryption Standard*	en bloc de 64 bits	56 bits	FIPS Pub 81,1981 ANSI X3.92, X3.105, X3.106 ISO 8372 ISO/IEC 10116
IDEA	*International Data Encryption Algorithm,*	en bloc de 64 bits	128 bits	
RC2	dévelopé par Ronald Rivest	en bloc de 64 bits	variable, 40 b.export.	Non et propriétaire
RC4	dévelopé par R. Rivest	enfilé	variable 40/ 128 bits	Non, mais divulgé sur l'Internet en 1994
RC5	dévelopé par R. Rivest	en bloc de 32, 64 ou 128 bits	variable jusqu'à 2048 bits	Non et propriétaire
SKIPJACK	Confidentiel développé aux États Unis par la NSA (*National Security Agency* - Agence de sécurité nationale des États Unis) pour des applications sur la carte PCMCIA Fortezza.	en bloc de 64 bits	80 bits	Secret défence aux États-Unis
Triple DES		en bloc de 64 bits	112 bits	ANSI X9.52

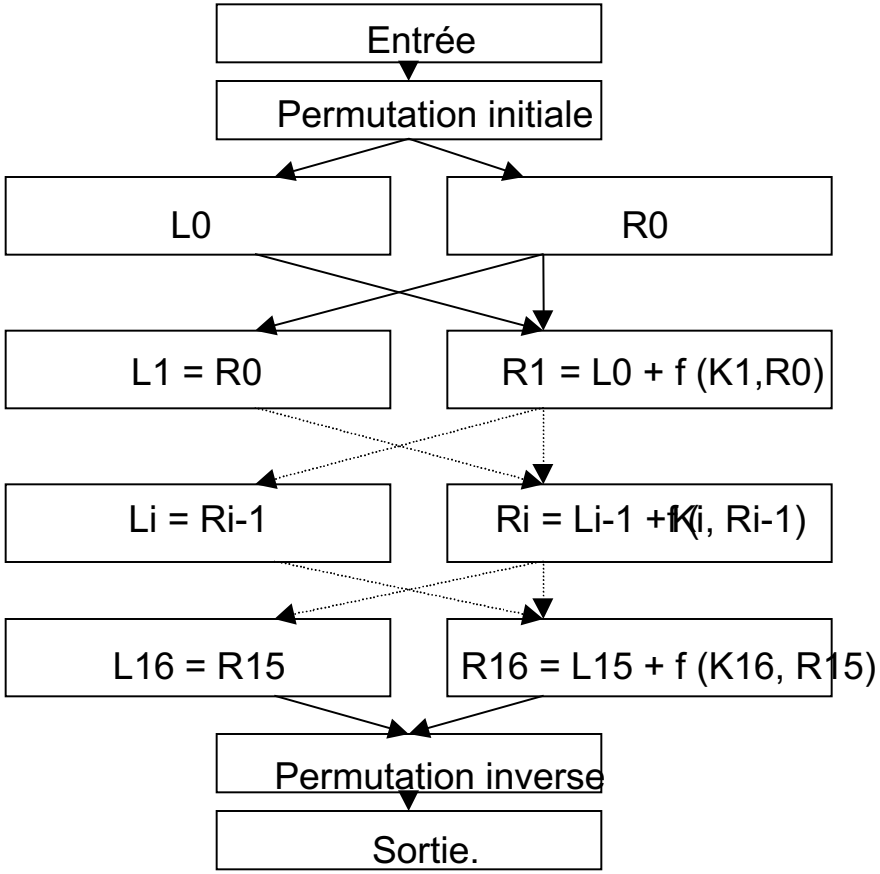
Exemple : Chiffrement symétrique – DES

- **DES (Data Encryption Standard) IBM 1977**
- Les étapes des cette élaboration sont restés secrets, (la conception des S Boxes).
    - Les S Boxes sont des tables qui définissent des permutations.
- Le message est découpé en blocs de 64 bits.
- Initialisation : permutation de tous les bits formant ce bloc.
- On le coupe en deux parties : L0 et R0.

Exemple : Chiffrement symétrique – DES

- La clé secrète est transformée en 16 parties Ki de 48 bits.
- Puis, on permute les deux parties en introduisant une fonction de la clé.
  - L1 = R0.
  - R1 = L0 + f (K1, R0).
  - Cette opération se répète 16 fois. A chaque étape i, on a :
  - Li = Ri-1.
  - Ri = Li-1 + f (Ki, Ri-1).

Exemple : Chiffrement symétrique – DES



Les étapes de DES.

Exemple : Chiffrement symétrique – DES

- Ki représente la sous clé numéro i obtenu à partir de la clé secrète.
- Le calcul de f se fait de la manière suivante :
  - les 32 bits de la partie R sont étendue à 48 bits grâce à une table appelée E (Expansion).
  - Ce nouveau R, E(R) pour être plus précis, est additionné à Ki.
  - Le résultat est découpé en huit suites Bi de six bits : Grâce à la table S-Box, les données de ces huit suites donne un résultat de 32bits.

Exemple : Chiffrement symétrique – DES

- Il y a 8 S-Box, une pour chacun Bi.
- Chaque S-Box à 16 colonnes et 4 lignes.
- Bi = b1b2b3b4b5b6. On calcule
  - r = b1b6
  - c = b2b3b4b5.
- On regarde le nombre qui figure à la ligne r et à la colonne c. Il est codé sur 4 bits est correspond à la sortie Si(Bi).
- Ensuite on effectue une permutation représentée par une table appelée P et le résultat de cette permutation est retourné par la fonction f.
- Pour le déchiffrement, il suffit de faire l'opération inverse.

DES : Attaque par force brute

Key Size	1995	2005	2015	2030
40 bit key	.2 seconds	2 milliseconds	.02 milliseconds	.02 microseconds
56 bit key	3.6 hours	2 minutes	1 second	1 millisecond
64 bit key	38 days	9 hours	5.5 minutes	.3 seconds
80 bit key	7000 years	70 years	251 days	6 hours
112 bit key	$10^{(13)}$ years	$10^{(11)}$ years	$10^{(9)}$ years	$10^{(6)}$ years
128 bit key	$10^{(18)}$ years	$10^{(16)}$ years	$10^{(14)}$ years	$10^{(11)}$ years

Pour en savoir plus sur les algorithmes de cryptographie

LaCryptogr@phie expliquée!

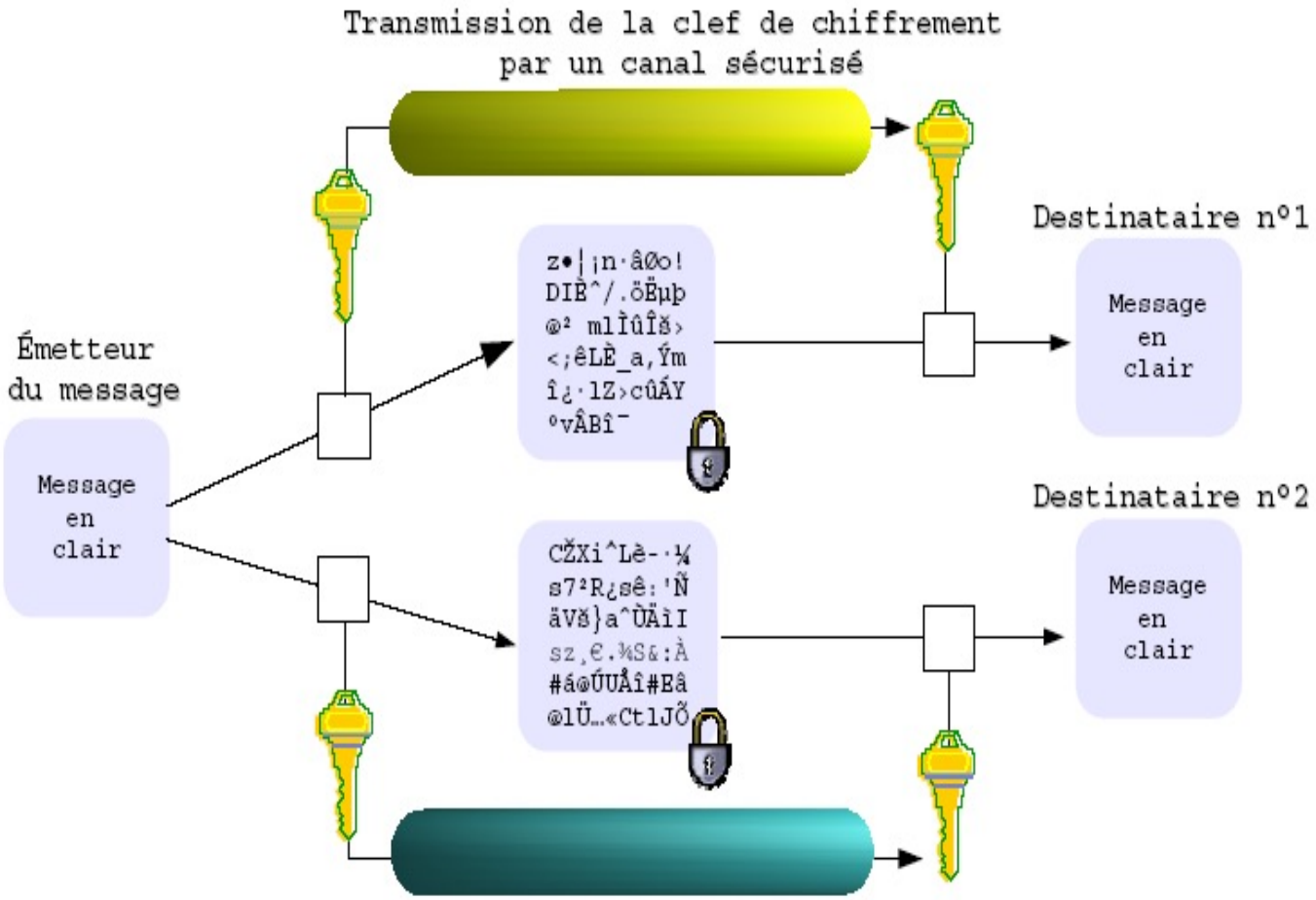
http://www.bibmath.net/crypto/

Cryptographie conventionnelle

- Le chiffrement conventionnel a des avantages. Il est très rapide. Il est particulièrement utile pour chiffrer des données qui ne vont *aller* nulle part.
- Cependant, le chiffrement conventionnel seul en tant que moyen de transmission de données sécurisées peut être assez onéreux simplement en raison de la difficulté de la distribution sécurisée de la clé.
- Pour qu'un expéditeur et un destinataire communiquent de façon sûre en utilisant un chiffrement conventionnel, ils doivent se mettre d'accord sur une clé et la garder secrète entre eux.

❖ le problème avec le chiffrement conventionnel est la *distribution de la clé*: comment donner la clé au destinataire sans que personne ne puisse l'intercepter?

Schéma de principe



Solution :
Protocole de Diffie et Hellman

- A et B se sont mis d'accord sur un algorithme à clé secrète à utiliser, ils veulent s'échanger une clé K, mais ils ne disposent pas de canal fiable pour cela.

Diffie et Hellman suggèrent l'échange suivant :

1. A et B choisissent, ensemble et publiquement, un nombre premier p, et un entier 1< a< p.
2. A choisit secrètement x1, et B choisit secrètement x2.
3. A envoie à B a^{x1}, et B calcule $K=(a^{x1})^{x2}=a^{x1x2}$ [p].
4. B envoie à A a^{x2}, et A calcule $K=(a^{x2})^{x1}=a^{x1x2}$ [p].
5. A et B sont donc en possession d'une même clé secrète K, qu'ils ne se sont pas échangés directement.

- *Si quelqu'un a espionné leurs conversations, il a en sa possession p,a, a^{x1} et a^{x2}.*
- *Pour obtenir K, il doit pouvoir calculer x1, en connaissant a,p et a^{x1}.*
- *Autrement dit, il doit pouvoir résoudre l'équation (en x) y=ax [p]. Quand les valeurs de p, a et x sont très grandes, il s'agit d'un problème très difficile.*

Chiffrement symétrique ou conventionnelle : *Les règles à respecter*

- Le chiffre doit être poly-alphabétique pour éviter l'analyse de fréquences
- La clef doit être de grande longueur pour lutter contre la cyclicité
- Elle doit être à usage unique (masque jetable)
- Elle doit être générée aléatoirement pour éviter la méthode du va-et-vient

Chiffrement symétrique : Avantages - inconvénients

- Potentiellement incassable
- Traitements faciles à mettre en oeuvre
- Rapidité (1000 x Algo à biclefs)

- ✓ Problème de la distribution des clefs
- ✓ Réservée à une communauté fermée d'utilisateurs

Crypto à clés publiques

- Chaque utilisateur a une paire de clés
  - Une clé secrète
  - Une clé publique

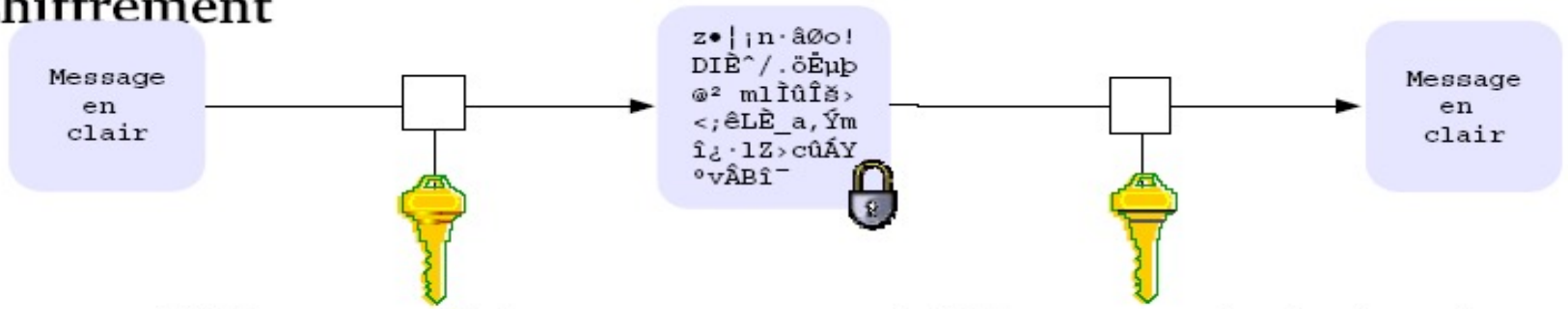
- Une sert à chiffrer, l'autre à déchiffrer
- Cryptographie « asymétrique »

Algorithmes à clef publique ou asymétriques

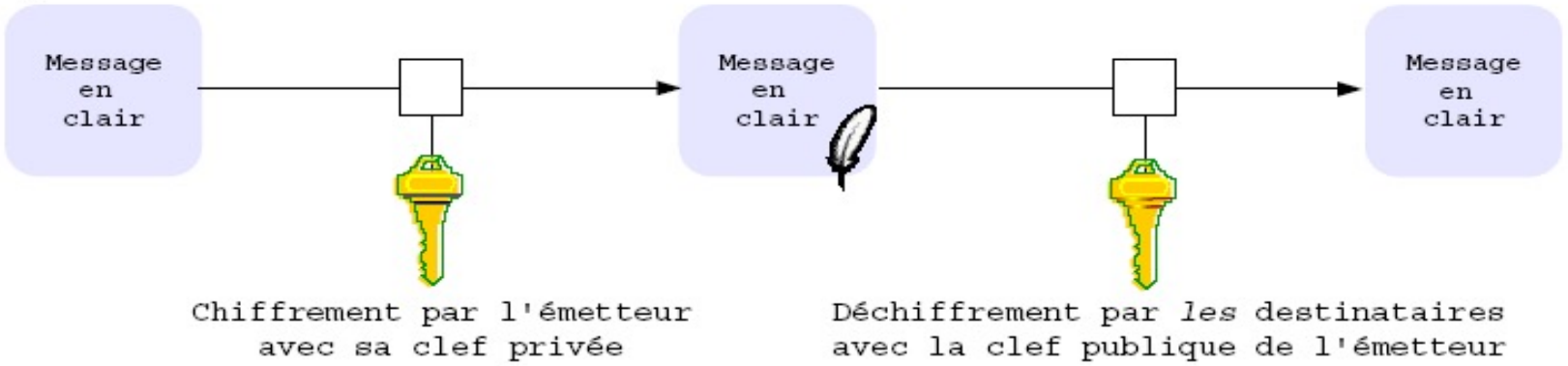
- Le principe des algorithmes de chiffrement à clés asymétriques a été introduit en 1976 par Diffie et Hellman. Ils ont été conçus pour utiliser des clés qui possèdent 2 propriétés essentielles :
  - Les clés sont crées **par couple** souvent appelé bi-clé. Ce bi-clé est tel que tout texte chiffré par l'une quelconque des deux clés n'est déchiffrable que par l'autre clé. C'est cette caractéristique qui a donné leur nom aux algorithmes de chiffrement asymétrique
  - La connaissance d'une des deux clés ne permet pas de déduire l'autre.

Principe

Chiffrement



Signature

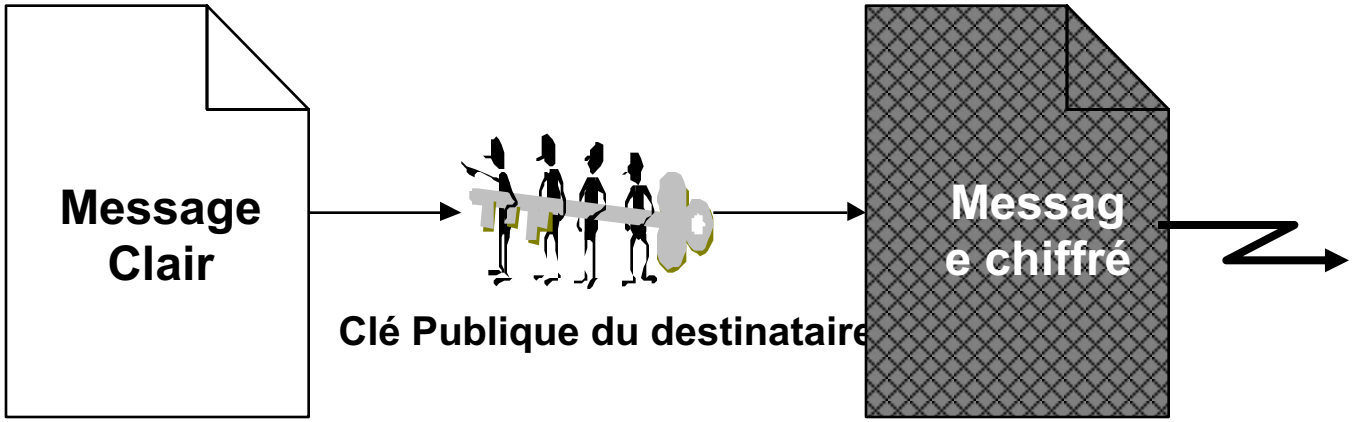


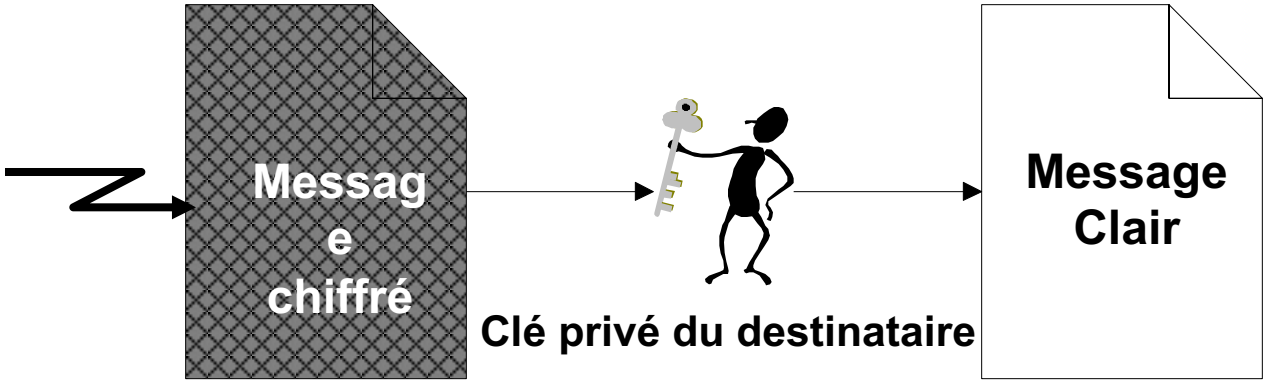
Algorithmes Asymétriques

- **Deux clés : clé publique / clé privé.**
- **Traitement relativement lent.**

- Exemple :
  - RSA (Rivest Shamir Adleman).
- Usage:
  - authentification,
  - signature
  - échange de clés.

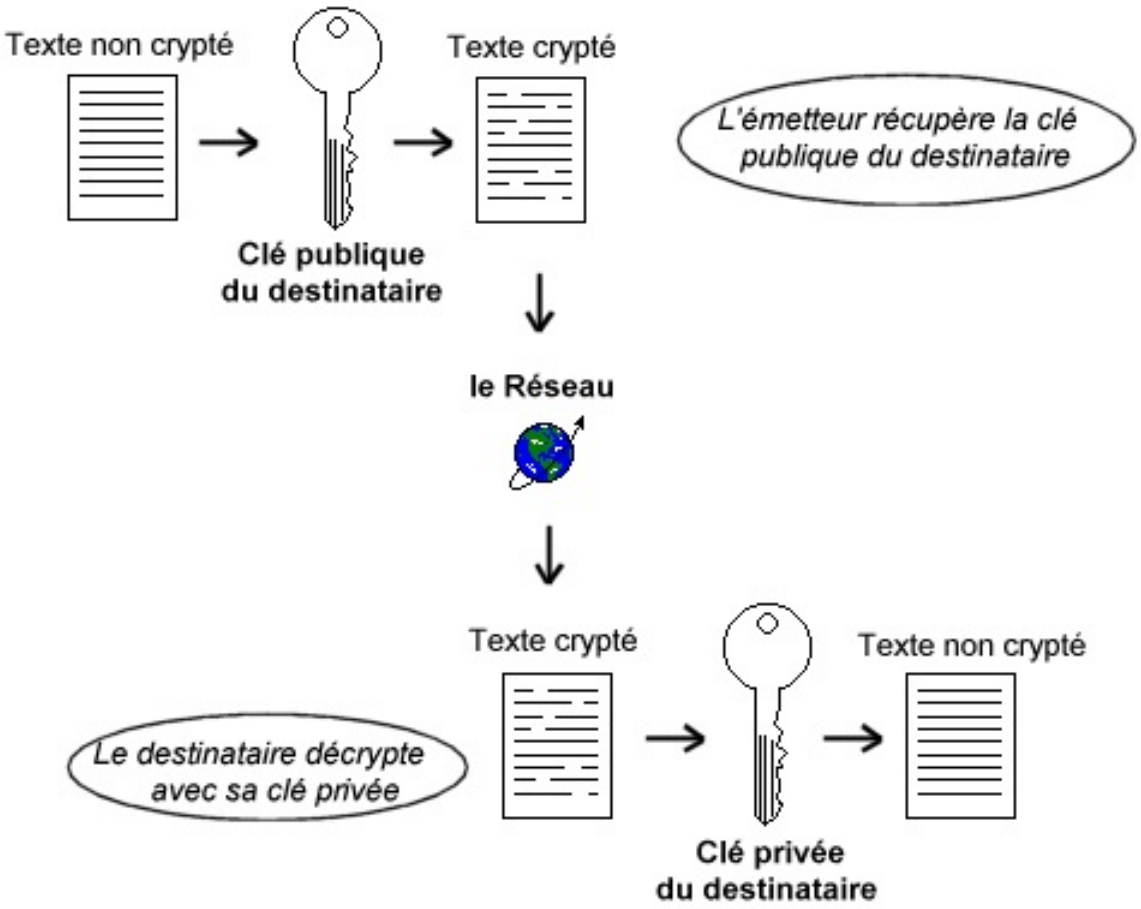
Algorithme Asymétrique.





Technique A Clé Publique

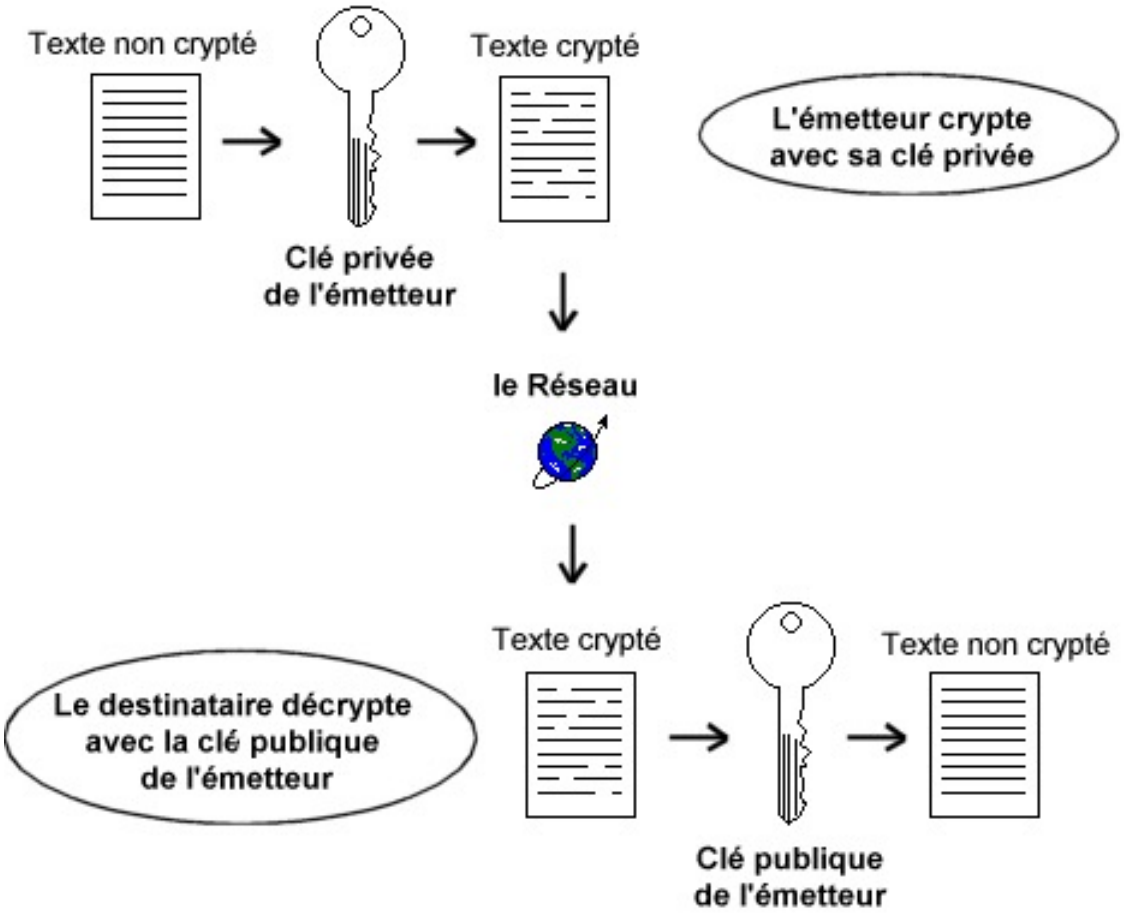
Confidentialité



Le Texte est totalement CONFIDENTIEL car le destinataire est le seul a avoir la CLÉ PRIVÉE

Technique A Clé Publique

Authentification



On est sûr de l'identité de l'émetteur car il est le seul à pouvoir chiffrer un message avec cette clé privée

Chiffrement asymétrique - RSA

- Soit M le message à chiffrer et C le message chiffré.
- Pour chiffrer le message, on calcule :
  - $C = M^e$ modulo n.
- Pour déchiffrer on calcule :
  - $M = C^d$ modulo n.
- La clé publique est :
  - le couple (e,n)
- La clé privée est :
  - le couple (d,n).

Chiffrement asymétrique - RSA

- Comment procède-t-on pour former les couples publique *(e,n)* et privé *(d,n)*

  - On choisit au hasard 2 grands nombres premiers *p* et *q*.
  - On calcule $n = p.q$
  - On pose $j = (p-1).(q-1)$
  - On sélectionne e tel que : *e* et *j* soient premiers entre eux avec $1 < e < j$.
  - On calcule *d* tel que : $e.d = 1 \bmod j$ (*e* et *d* sont inverses l'un de l'autre modulo *j*)

Par exemple …

p = 32 769 132 993 266 709 549 961 988 190 834 461
413 177 642 967 992 942 539 798 288 533

q = 3 490 529 510 847 650 949 147 849 619 903 898 133
417 764 638 493 387 843 990 820 577
et donc

n = 114 381 625 757 888 867 669 235 779 976 146 612
010 218 296 721 242 362 562 561 842 935 706 935
245 733 897 830 597 123 563 958 705 058 989 075
147 599 290 026 879 543 541

Chiffrement asymétrique - RSA

- **Pour percer RSA, il “ suffit ” de pouvoir factoriser n.**

  En effet, n est connu et si on le factorise, on obtient p et q puis j et connaissant j et d, on obtient e. Mais, la factorisation de n n’est pas une chose facile.

  La factorisation de grands nombres suffit ,à elle seule, à dissuader de nombreuses tentatives.

- **En pratique, il y a deux difficultés pour implémenter RSA.**

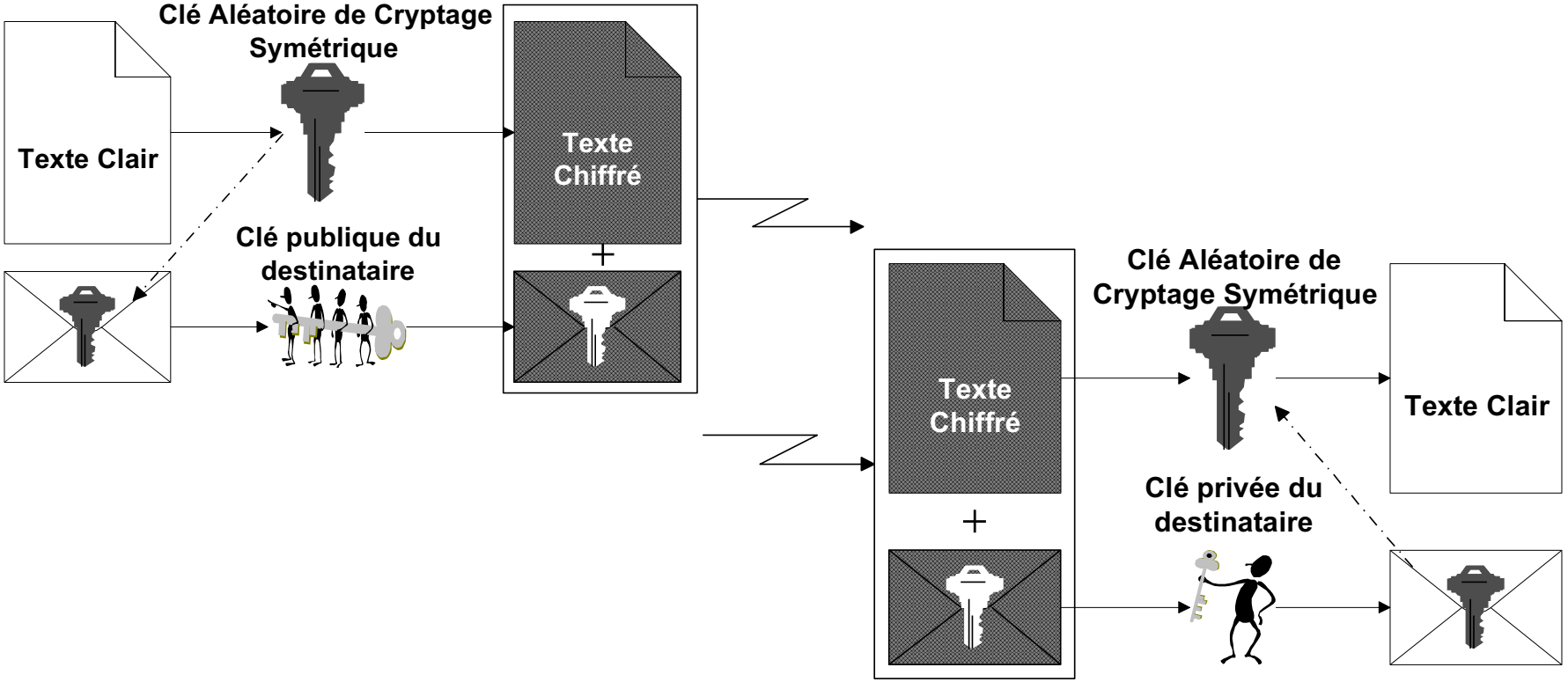
  La première est la génération de grands nombres premiers (p et q) et la seconde est l’élévation de nombre à des puissances très grandes. Un standard de RSA est PKCS 1.

Inconvénients

- Avec les algorithmes asymétriques, **le temps pour les opérations de chiffrement et de déchiffrement est long.**

- *Ainsi sur un ordinateur courant, RSA (algorithme asymétrique) est de 100 à 1000 fois plus lent que le Triple DES (algorithme symétrique*).

Méthode plus rapide : Chiffrement mixte



Analyse comparée des méthodes

La sécurité d'un système de cryptologie va reposer sur plusieurs facteurs.

- L'un d'entre eux est la difficulté de décrypter (Déchiffrer sans posséder la clé de déchiffrement) l'information.
- Plus la clé utilisée sera longue plus le décryptage sera difficile, la limite étant la puissance actuelle des calculateurs, avec un algorithme de chiffrement solide (bon mathématiquement) et une implémentation correcte (sans bogue).

- **On considère actuellement que pour une communication chiffrée il faut au moins utiliser une longueur de clé de 128 bits pour le chiffrement à clés symétriques et une longueur de clé de 1024 bits pour le chiffrement à clés asymétriques.**

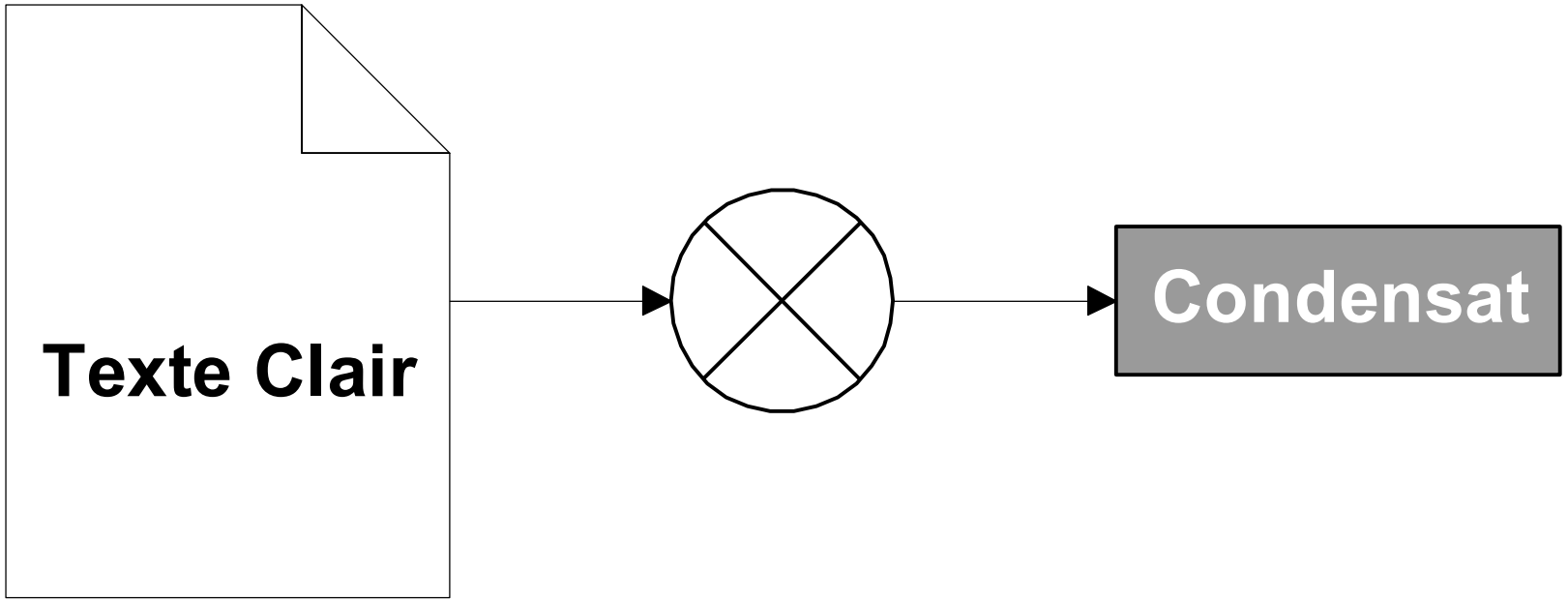
SOLUTION ALTERNATIVE

Fonction de hachage et Signature numérique

- Une fonction de hachage calcule le résumé d'un texte. Ce résumé doit être à sens unique, pour éviter de reconstituer le message initial connaissant seulement le résumé.
  - Il doit être très sensible, c'est-à-dire qu'une petite modification du message entraîne une grande modification du résumé.
  - En expédiant un message accompagné de son résumé (on dit aussi son haché), on peut s'assurer de l'intégrité du message, en recalculant le résumé à l'arrivée.

- C'est le principe de la **SIGNATURE NUMERIQUE**

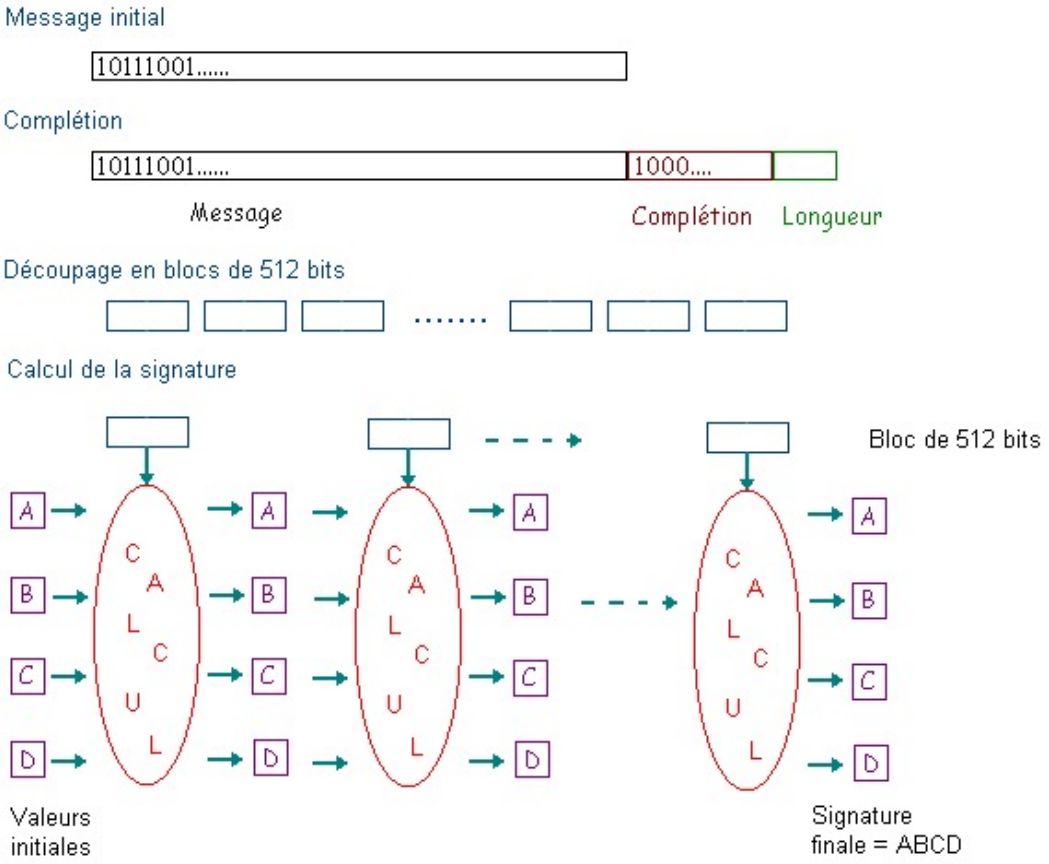
Fonction de hashage



Fonction de hashage

- H (M) = C
  - M est de taille quelconque
  - C est de taille fixe (16 ou 20 octets)
    - C est appelé condensât, ou empreinte, ou fingerprint, ou message digest
- Fonction à sens unique
- Si H (M_1) = C_1 ,
  - il est très difficile de trouver :
    M_2 différent de M_1 tel que H (M_2) = C_1
- **Usage : checksums, « intégrité »**

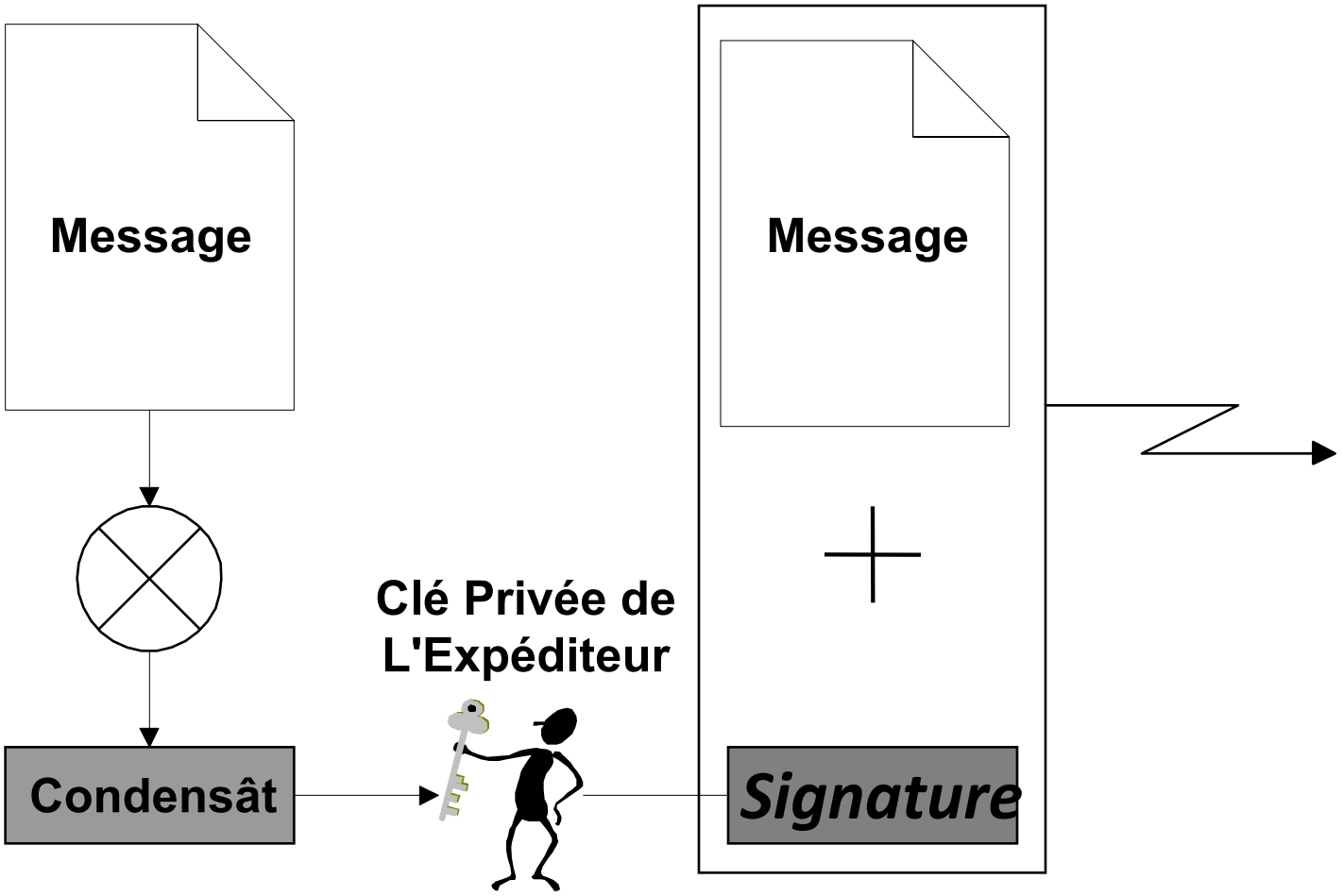
fonction de hachage : le MD5



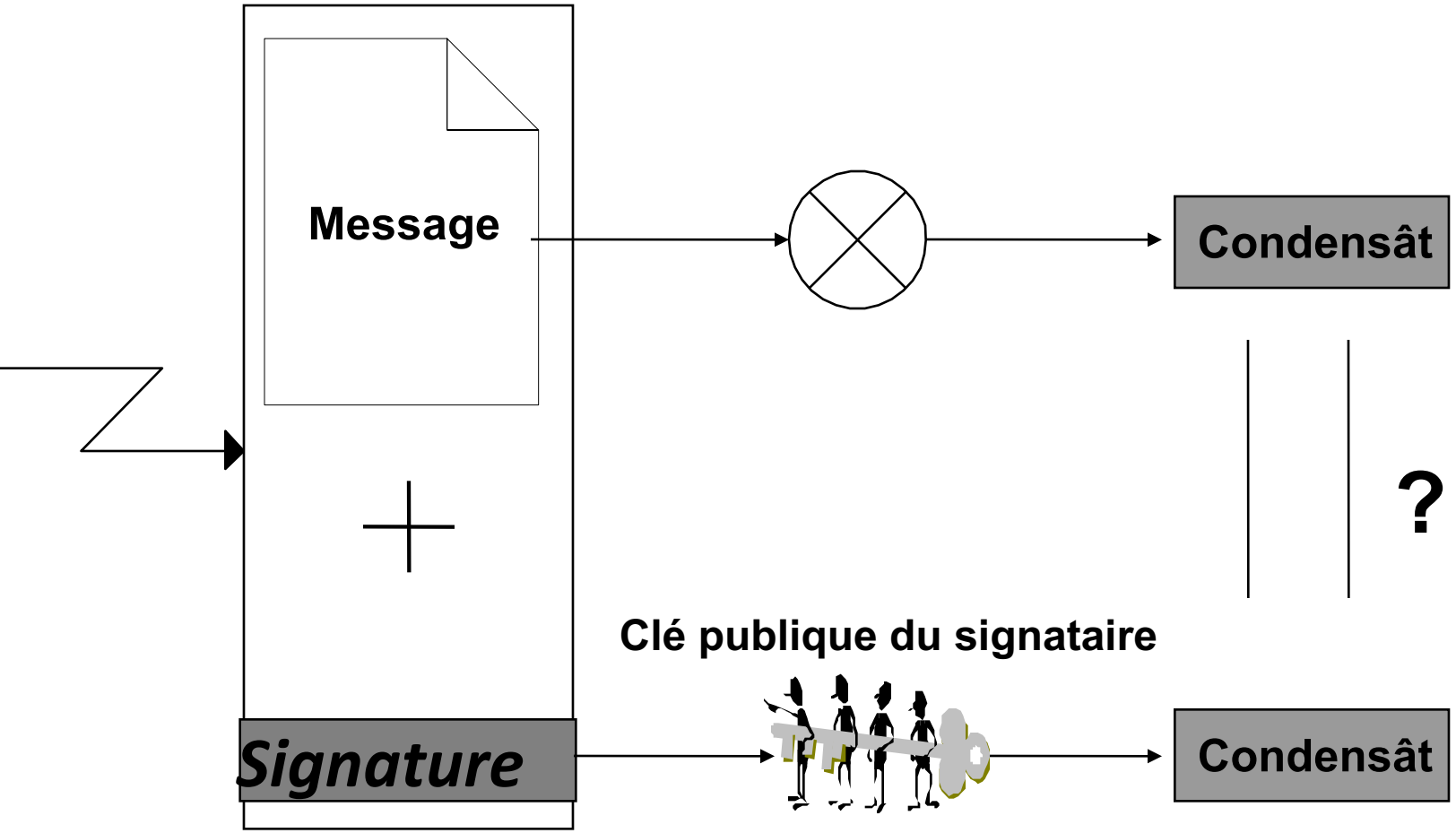
Description du fonctionnement du MD5

- Initial :
- A=01234567
  B=89abcdef
  C=fedcba98
  D=76543210

Signature : expéditeur (1/2)



Signature : destinataire (2/2)

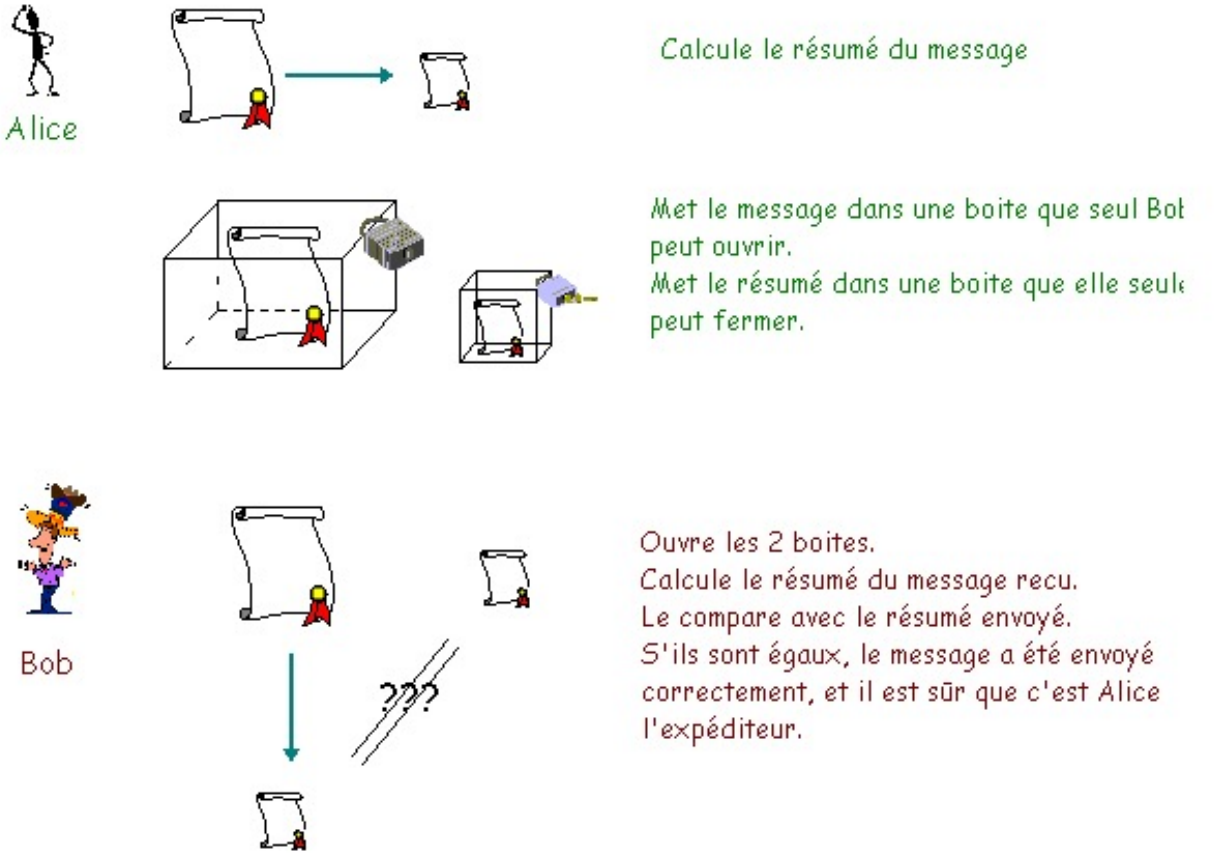


Clés + Signature

- La signature associée aux techniques précédentes permet de mettre en œuvre les services:
  - Intégrité du message
  - Authentification
  - Non-répudiation

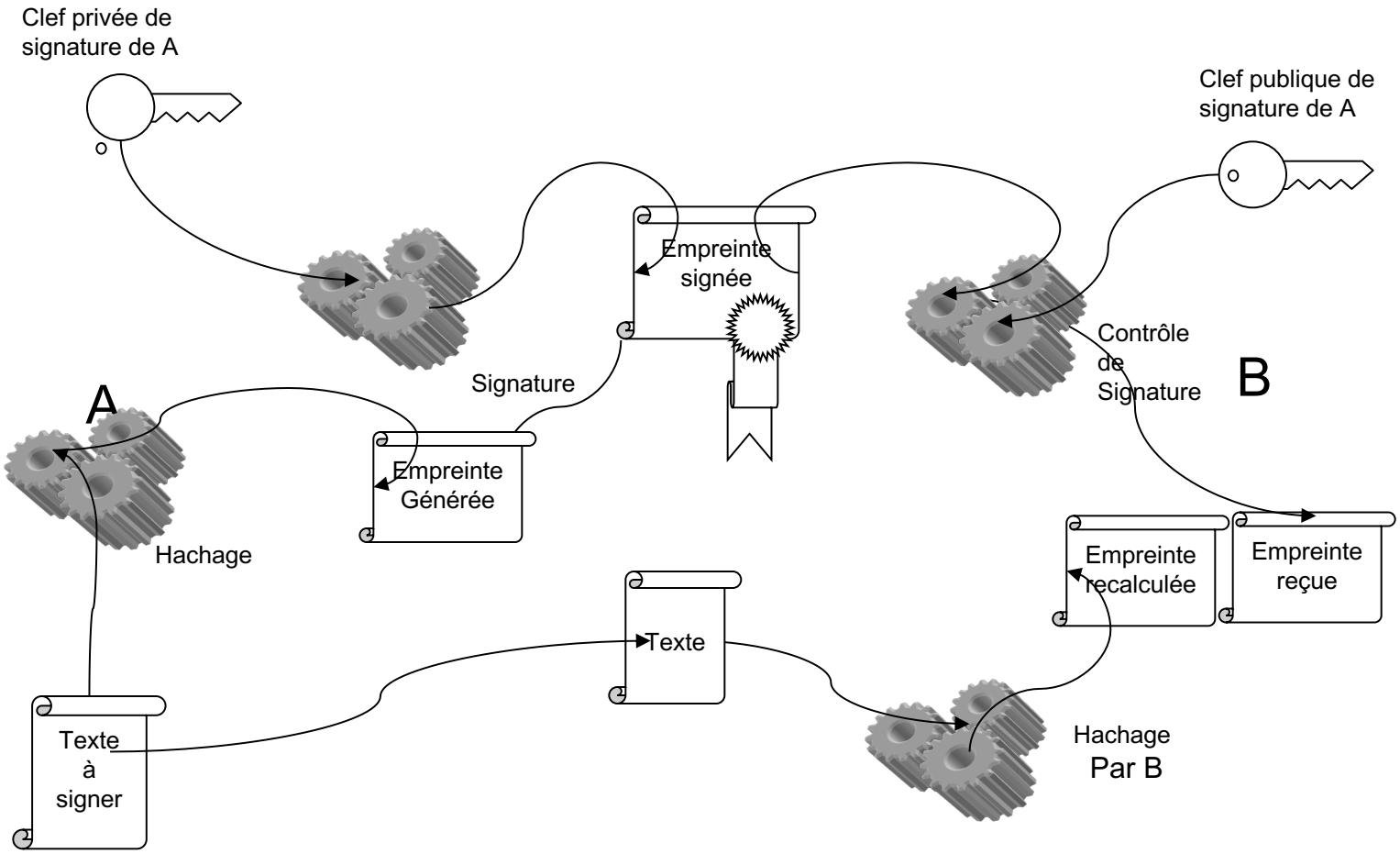
  Avec Génération d'une clé de chiffrement symétrique pour le service de Confidentialité

Signature numérique



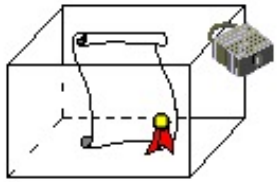
- **la fonction de hachage (signature),**
- **couplée à la cryptographie à clé publique,**
- **permet d'authentifier l'expéditeur.**

Utilisation de la signature électronique

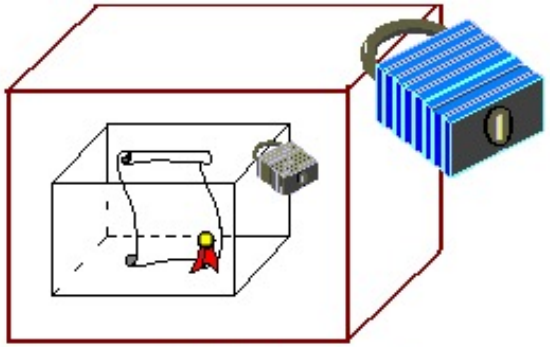


Authentification forte

Alice

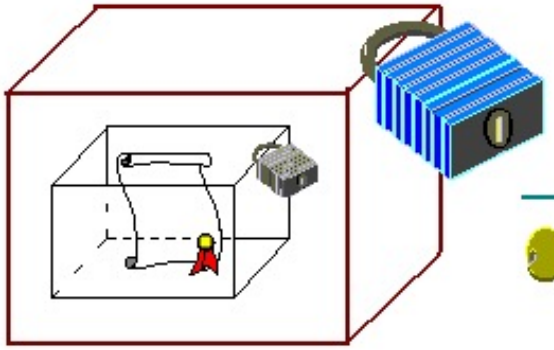


enferme le message dans une boite à l'aide de sa clé privée (authentification de l'expéditeur)

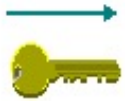


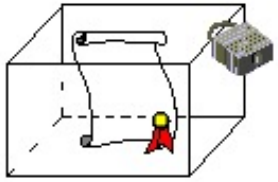
enferme cette boite dans une autre boite avec la clé publique de Bob (chiffrement, seul Bob peut ouvrir)

Bob



recoit le message chiffré et authentifié





ouvre la premičre botie avec sa clé privée (déchiffrement)

ouvre la deuxičme boite avec la clé publique d'Alice (authentification)

Les règles à respecter

- Réserver une biclef à un usage donné (ne pas chiffrer et signer avec la même)
- S'assurer du réel propriétaire de la clef publique utilisée.
- S'assurer des dates de validité de la clef

➢ **SOLUTION → Utilisation de certificats**

(Avantages – inconvénients) des biclefs

- Il n'y a plus d'échanges préalable de clefs
- Echanges « n vers n », plus « 1 vers 1 »
- Bien adapté au commerce électronique

- ✓ Fiabilité des clefs publiques
- ✓ Sécurité dépendant de l'évolution technologique et des connaissances.

Signature et authentification électroniques

- Signature électronique :
  - être sûr de l'expéditeur.
- Certificat électronique :
  - être sûr du destinataire.
- Autre alternative :
  - S'identifier auprès d'un tiers.

Gestion des clés
(infrastructure à clés publiques : PKI)

- Dans un système utilisant un chiffrement à clés asymétriques, un utilisateur a un couple de clés.
  - *La clé privée reste toujours avec l'utilisateur et la clé publique est publiée dans un annuaire publique.*
- Un nouvel utilisateur aura uniquement besoin de son couple de clés et de publier sa clé publique dans l'annuaire pour pouvoir communiquer avec l'ensemble des autres entités.

Gestion des clés
(infrastructure à clés publiques : PKI)

- **Ce type de système introduit un nouveau problème :**
- l'utilisation d'un couple de clés entraîne la nécessité de publication, en toute confiance, de la clé publique. Cette publication doit offrir l'assurance que :
  - **la clé est bien celle appartenant à la personne avec qui les échanges sont envisagés ;**
  - **le possesseur de cette clé est « digne de confiance » ;**
  - **la clé est toujours valide.**

- Cette notion de confiance est résolue avec les **certificats** et les **autorités de certification**.

Notion de certificat

Un certificat est un document électronique, résultat d'un traitement fixant les relations qui existent entre une clef publique, son propriétaire (une personne, une application, un site) et l'application pour laquelle il est émis :

- pour une personne il prouve l'identité de la personne au même titre qu'une carte d'identité, dans le cadre fixé par l'autorité de certification qui l'a validé ;
- pour une application il assure que celle-ci n'a pas été détournée de ses fonctions ;
- pour un site il offre la garantie lors d'un accès vers celui-ci que l'on est bien sur le site auquel on veut accéder.

C'est un **protocole normalisé X509** *(RFC2459)* - (ITU-T X.509 international standard V3 - 1996)

- Il existe des applications ou des systèmes de cryptologie qui ne s'appuie pas sur les certificats X509 (PGP par exemple).

Informations dans un certificat

Version	Indique à quelle version de X.509 correspond ce certificat.
Serial number	Numéro de série du certificat (propre à chaque autorité de certification).
Signature Algorithm	Type de signature utilisée.
Issuer	Distinguished Name (Subject) de l'autorité de certification qui a émis ce certificat.
Validity	Période de validité.
Subject	Distinguished Name du propriétaire de ce certificat.
Subject public key info	Infos sur la clef publique de ce certificat.
X509v3 Extensions	Extensions génériques optionnelles, introduites avec la version 3 de X.509.
Signature	Signature numérique de l'AC sur l'ensemble des champs précédents.

Autorité de Certification

- **Une Autorité de Certification est une organisation qui délivre des certificats électroniques à une population.**

- Une AC possède elle-même un certificat (autosigné ou délivré par une autre AC) et utilise sa clé privée pour créer les certificats qu'elle délivre.
- N'importe qui peut se déclarer Autorité de Certification. Une AC peut être organisationnelle (exemple : UCAD), spécifique à un corps de métiers (exemple : notaires) ou encore institutionnelle.

- Selon le crédit accordé à l'AC, les certificats délivrés auront un champ d'applications plus ou moins importants :
  - limité à l'intérieur d'un organisme
  - échanges inter-organismes
  - …

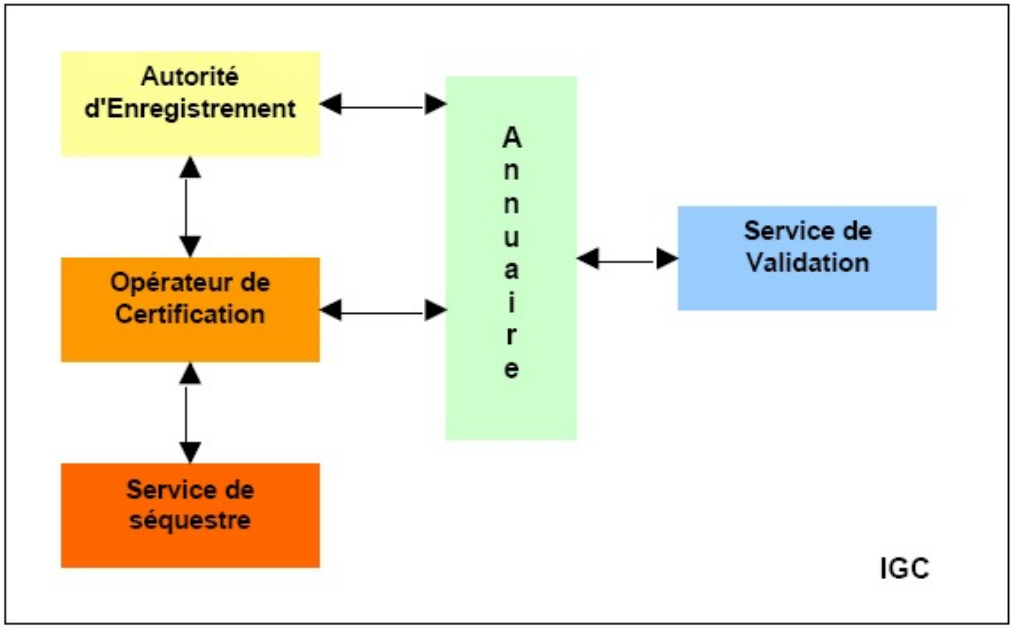
Infrastructure de Gestion de clés (IGC)

On parle aussi d'"Infrastructure à clés publiques" (**ICP**) ou de "Private Key Infrastructure" (**PKI**).

- L'IGC est constituée de l'ensemble des matériels, logiciels, personnes, règles et procédures nécessaire à une Autorité de Certification pour créer, gérer et distribuer des certificats X509.
- Une IGC est donc une structure à la fois technique et administrative permettant une mise en place, lors de l'échange de clef, de ***relations de confiance entre des entités morales et/ou physiques et/ou logiques***.
- Les fonctions principales d'une IGC sont :
  - Emettre et révoquer des certificats
  - Publier les certificats dans un annuaire
  - Éventuellement, fournir un service de séquestre et de recouvrement des clés privées

Infrastructure de Gestion de clés (IGC)

- autorité de certification (**AC**)
- Une autorité d'enregistrement (**AE**)
- Un opérateur de certification (**OC**)
- Un annuaire de publication de certificats
- Un service de validation
- Éventuellement, un service de séquestre de clés



Certificat numérique ou électronique

Un certificat numérique peut être considéré comme un passeport ou une carte d'identité nationale utilisée dans le domaine du numérique.

Cette pièce d'identité sur Internet contient de nombreuses informations personnelles et/ou professionnelles telles que le nom, le prénom, l'adresse, la date de naissance et le pays de résidence d'une personne mais aussi des informations sur l'organisme tels que le nom de la société, son numéro de registre et bien d'autres encore.

Une partie des fichiers de cet ensemble de données numériques est dite publique et contient en même temps une partie privée.

On parle alors de « clé publique » et de « clé privée » dont cette dernière ne sera jamais échangée.

Par ailleurs, le certificat électronique comporte aussi le nom de l'autorité émettrice de la pièce qui garantit la validité et l'authentification des informations.

Le certificat électronique

est donc un fichier informatique attestant du lien entre les données de vérification de signature électronique et un signataire) ;

- ✓ Le certificat, qui représente votre identité numérique, est un fichier informatique qui associe vos données d'identification physiques à un résultat mathématique infalsifiable.
- ✓ Selon les niveaux de sécurité choisis, ce fichier, votre signature électronique, sera soit sauvegardé dans l'ordinateur, soit mis sur une clé USB protégée ou bien mis sur une carte à puce et sera ensuite apposé sur les documents à signer.

Classes de Certificat électronique

Classe I

Ne garantit pas l'identité du titulaire du certificat mais seulement l'existence de son adresse e-mail.

Classe II

Garantit les informations du titulaire et de son entreprise (contrôlées par l'autorité de certification sur pièces justificatives transmises par voie postale).

Classe III

Idem à la Classe II, assure un contrôle supplémentaire de l'identité du titulaire.

Classe III Plus

Il impose que le certificat soit remis en face à face sur un matériel certifié conforme.

Usages du Certificat Electronique

Certificat d'authentification

- Ex. Accès au poste de travail
- Ex. Accès à une application en ligne

Certificat de signature

- Ex. Email
- Ex. Fichiers

Certificat de chiffrement

- Ex. Email
- Ex. Fichiers

Mise en oeuvre : Le protocole SSL

- ✓ Le protocole *Secure Sockets Layer* (SSL) est un ensemble de règles gouvernant l'authentification serveur, l'authentification client et les communications encryptées entre des serveurs et des clients.
- ✓ SSL est largement utilisé sur Internet, particulièrement pour les interactions mettant en œuvre l'échange d'informations confidentielles telles que les numéros de cartes de crédit.
  - ➢ **SSL requiert un certificat SSL serveur, au minimum.**
- ✓ Comme partie du processus de négociation, le serveur présente son certificat au client afin d'authentifier son identité.
- ✓ Le processus d'authentification utilise le chiffrement par clef publique et les signatures numériques pour confirmer que ce serveur est bien celui-ci qu'il prétend être.

Utilisation des certificats SSL

Certificats de serveur SSL :

- Utilisé pour identifier les serveurs auprès des client via SSL (authentification serveur). L'authentification serveur peut être utilisée avec ou sans authentification client. L'authentification serveur est obligatoire lors de l'établissement d'une connexion SSL chiffrée.

Les sites internet de commerce électronique (communément appelé e-commerce) supportent habituellement l'authentification serveur par certificat, au minimum, pour établir une session SSL chiffrée et assure les clients qu'ils traitent avec un site identifié comme étant celui d'une entreprise donnée.

La session SSL assure que les informations personnelles renseignées par le client et transmises par le réseau, telles que son numéro de carte de crédit, ne seront pas aisément interceptées.

Utilisation des certificats SSL

Certificats de client SSL :

- Utilisés pour identifier des client auprès de serveurs via SSL (authentification client). Généralement, l'identité du client est présumée être la même que celle d'un être humain, tel qu'un employé dans une entreprise.

- ✓ Une banque donne un certificat client SSL à l'un de ses usagers qui lui permet de s'identifier auprès du serveur de la banque et d'accéder à ses comptes.
- ✓ Une compagnie peut donner un certificat client SSL à l'un de ses nouveaux employés qui lui permet de s'identifier auprès du serveur de l'entreprise et d'obtenir accès aux ressources disponibles sur ce serveur.