UNIVERSITÉ M'HAMED BOUGARA DE BOUMERDES
FACULTÉ DES SCIENCES
DÉPARTEMENT D'INFORMATIQUE

LICENCE 3
MODULE: SÉCURITÉ INFORMATIQUE

Cours 2
Introduction à la cryptographie

Plan du cours

1. INTRODUCTION/TERMINOLOGIE /HISTOIRE
2. CRYPTOGRAPHIE CLASSIQUE: CHIFFREMENT DE CESAR
3. CRYPTOGRAPHIE MODERNE
    1. Système cryptographique symétrique
    2. Système cryptographique asymétrique
4. FONCTIONS DE HACHAGE ET SIGNATURE ÉLECTRONIQUE
5. LES CERTIFICATS NUMÉRIQUES

Introduction

- Sécuriser quoi?
  - Contenu: l'information qui circule dans le réseau
  - Contenant: les vecteurs supports de cette communication
    - Les systèmes d'exploitations des machines hôtes, les applications (clients, serveurs, applications réparties, les protocoles de communications …)

- Ceci dans le but d'assurer confidentialité, intégrité, authentification et non répudiation de l'information

Introduction

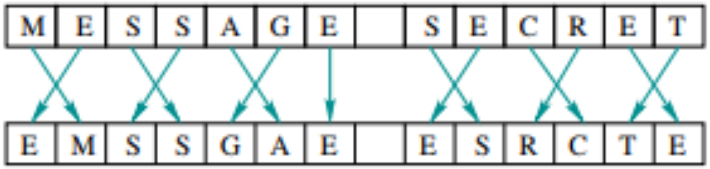
- Comment assurer la confidentialité d'une information ?
- Il existe deux façons de protéger une information: la stéganographie et la cryptographie

- **La stéganographie :** écriture couverte
  - L'information est dissimulée au sein d'une autre information afin de la rendre invisible.
  - Exemples :
    - Message couvert : tablette couverte de cire, crâne du messager
    - Message invisible : encre sympathique
    - Message illisible : Micro-film sous forme de point

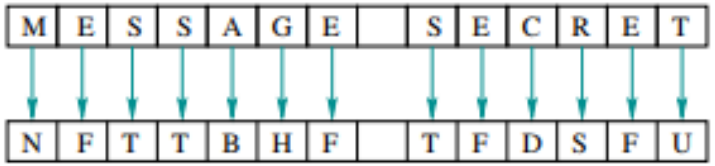
  - Connaissance de l'existence de l'information = Connaissance de l'information

Introduction

- **La cryptographie** : écriture cachée
  - L'information est modifiée selon une méthode préétablie afin de la rendre incompréhensible.
  - Il existe deux grandes catégories:
    - **par transposition** : l'ordre des éléments d'une information est modifiée (caractères d'une phrase, pixels d'une image, ...)



    - **par substitution** : les éléments d'une information sont remplacés par d'autres



Terminologie

- La **cryptologie** est la science du secret. Elle se divise en deux disciplines :
  - La **cryptographie** qui est l'étude des algorithmes permettant de protéger (cacher) de l'information.
  - la **cryptanalyse** comprend l'ensemble des moyens qui permettent d'analyser une information préalablement chiffrée afin de la déchiffrer (en se basant sur les failles des algorithmes utilisés).

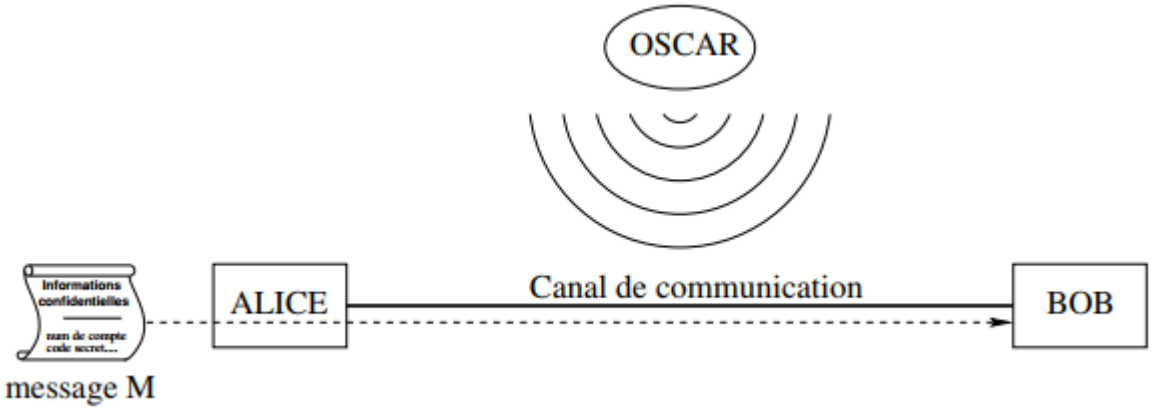
- Le **chiffrement**: processus de transformation d'une information (quelque soit sa nature: texte, voix, son, image, etc.) de telle manière à la rendre incompréhensible pour toute personne autre que son émetteur et récepteur.

- Le **déchiffrement:** processus permettant de retrouver l'information en clair à partir de l'information chiffrée.

Terminologie

- Protagonistes traditionnels :
  - **Alice** et **Bob** : souhaitent se transmettre des informations
  - **Oscar** : un opposant qui souhaite espionner Alice et Bob

- Objectif fondamental de la cryptographie:
  - permettre à Alice et Bob de communiquer sur un canal peu sûr et
  - Oscar ne doit pas comprendre ce qui est échangé.



Terminologie

- **Texte clair**: information qu'Alice souhaite transmettre à Bob (un message M)

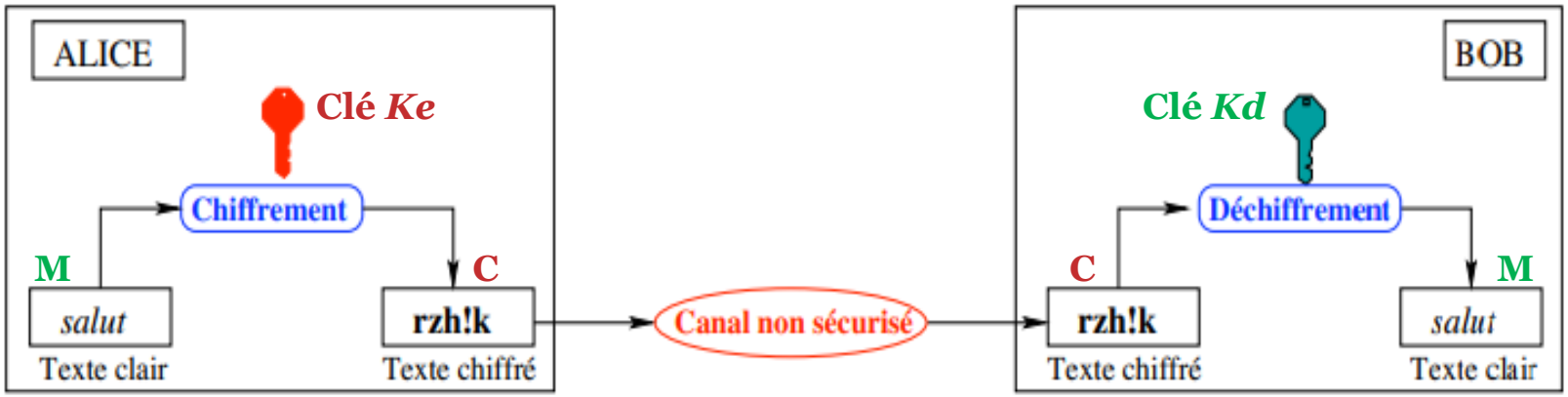
- **Chiffrement**: processus de transformation d'un message M de telle manière à le rendre incompréhensible
  - Basé sur une fonction de chiffrement **E**
  - On génère ainsi un message chiffré (appelé cryptogramme) **C = E(M)**

- **Déchiffrement**: processus de reconstruction du message clair à partir du message chiffré
  - Basé sur une fonction de déchiffrement **D**
  - On a donc D(C) = D(E(M)) = M

- **Clé**: l'information permettant de chiffrer/déchiffrer un message.
  - **E** et **D** sont généralement paramétrées par des clés **Ke** et **Kd** :

$E_{ke}(M) = C$ $D_{kd}(C) = M$

Terminologie (pour résumer)



- Deux catégories de systèmes cryptographiques :
  - Systèmes à clé secrète (ou symétriques) ($Ke = Kd = K$)
  - Systèmes à clé publique (ou asymétriques) ($Ke \neq Kd$)

Un peu d'histoire

- Antiquité: cryptographie artisanale
  - **1900 Av J.C**
    Un scribe égyptien utilise des hiéroglyphes non standards pour communiquer.
  - **1500 av J.C**
    Un potier babylonien code la recette d'un vernis sur une tablette d'argile en supprimant certaines consonnes et en modifiant l'orthographe des mots.
  - **500 av J.C**
    L'expéditeur d'un message enroulait une bande de papyrus parallèles sur un bâton de diamètre défini, appelé *scytale*. Il écrivait ensuite son message transversalement dans le sens du bâton. En déroulant la bande, le message devenait inintelligible, à part pour la personne qui possédait un bâton de même diamètre.
  - **50 av J.C**
    Jules César, pour communiquer avec ses troupes, utilise un cryptage par substitution rudimentaire (un simple décalage des lettres de l'alphabet).

Un peu d'histoire

- Mécanisation de la cryptographie et de la cryptanalyse
  - Enigma (1918). Un ingénieur hollandais (H Alexander), dépose un brevet de machine à chiffrer éléctromécanique : ENIGMA. Elle fera un succès commercial mais sera reprise par les Allemands durant la seconde guerre mondiale.

- Cryptographie moderne
  - Cryptographie à clé secrète : DES (1977), AES(2000)
  - Cryptographie à clé publique: RSA (1976)

Cryptographie classique

Chiffrement de César

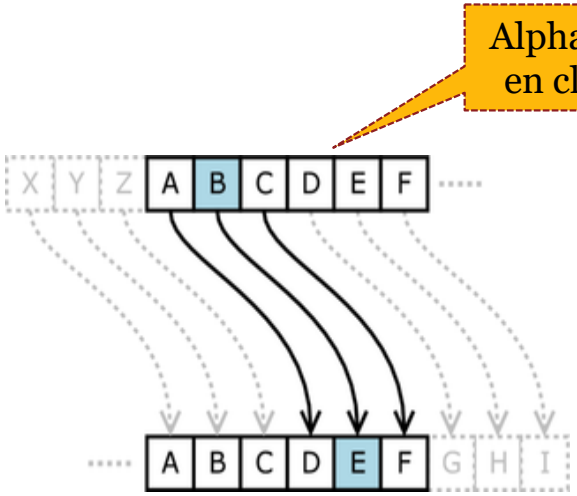
- **Principe**
  - Chiffrement mono-alphabétique: chaque lettre est remplacée par une autre lettre (crypto par substitution)
  - Consiste simplement à décaler l'alphabet clair
  - Le décalage k est la clé du chiffrement/déchiffrement (même clé)
  - Formules chiffrement/déchiffrement $\begin{cases} E_K(M) = M + K \mod n \\ D_K(C) = C - K \mod n \end{cases}$

Chiffrement de César

- **Exemple**
  - Alphabet: lettres de la langue Française (n=26)
  - Décalage: k=3
  - Texte clair: SECURITE

  - On écrit les alphabets clair et chiffré comme suit :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC



  - Il suffit alors de remplacer les lettres du message clair à l'aide de l'alphabet chiffré :

SECURITE → **VHFXULWH**

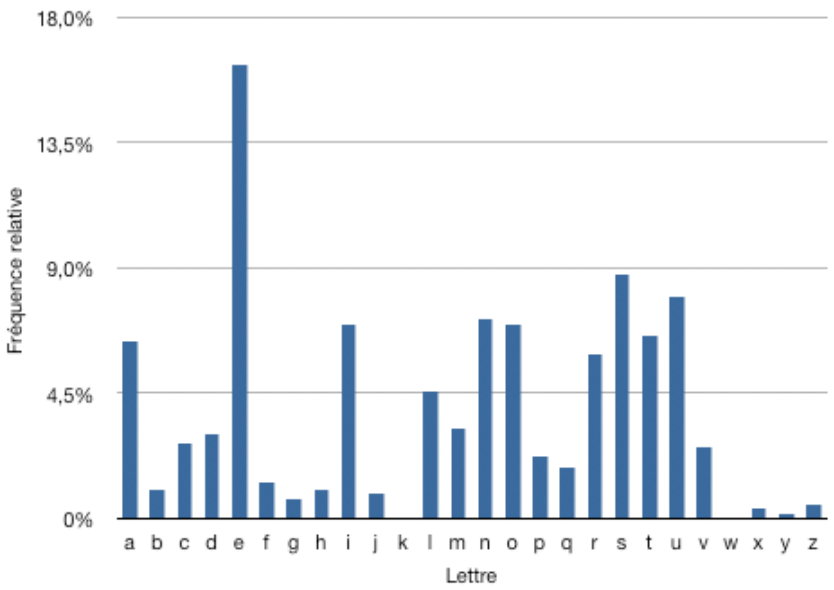
Chiffrement de César

- **Cryptanalyse**
  - Seulement *n* façons différentes de chiffrer un message
    - avantage de la simplicité
    - code très peu sûr (recherche exhaustive facile)
  - Dans l'exemple de l'alphabet de la langue Française, étant donné un message chiffré, il suffit de tester les 26 clés possibles pour retrouver le message clair → relativement très simple!!
  - Solution: utiliser un alphabet chiffré aléatoirement
    - Le nombre de possibilités devient *n!*
    - Par exemple pour n=26, le nombre de possibilités est de l'ordre de $4*10^{26}$
    - Cependant, il est encore possible de casser ce chiffrement en un temps très réduit → analyse des fréquences

Chiffrement de César

- **Cryptanalyse**
  - Idée: analyse des fréquences d'apparition des lettres
    - Mesurer la fréquence d'apparition de chaque lettre d'un texte chiffré
    - Comparer avec la table des fréquences des lettres
    - Déduire l'alphabet chiffré
    - Déchiffrer les messages

  - C'est *Al Kindi*, un savant arabe, (800) qui explique sans son ouvrage de cryptanalyse la méthode de l'étude des fréquences.



Autres systèmes …

- Plusieurs autres systèmes classiques
  - Les homophones
  - Chiffre affine
  - Chiffre de Playfair
  - Chiffre de Hill
  - Chiffre de Vigenère (poly-alphabétique)
  - Chiffre de Vernam (masque jetable)
  - Transpositions
  - Machines à retor (machine Enigma)
  - *etc.*

Cryptographie moderne

Principe d'Auguste Kerckhoffs

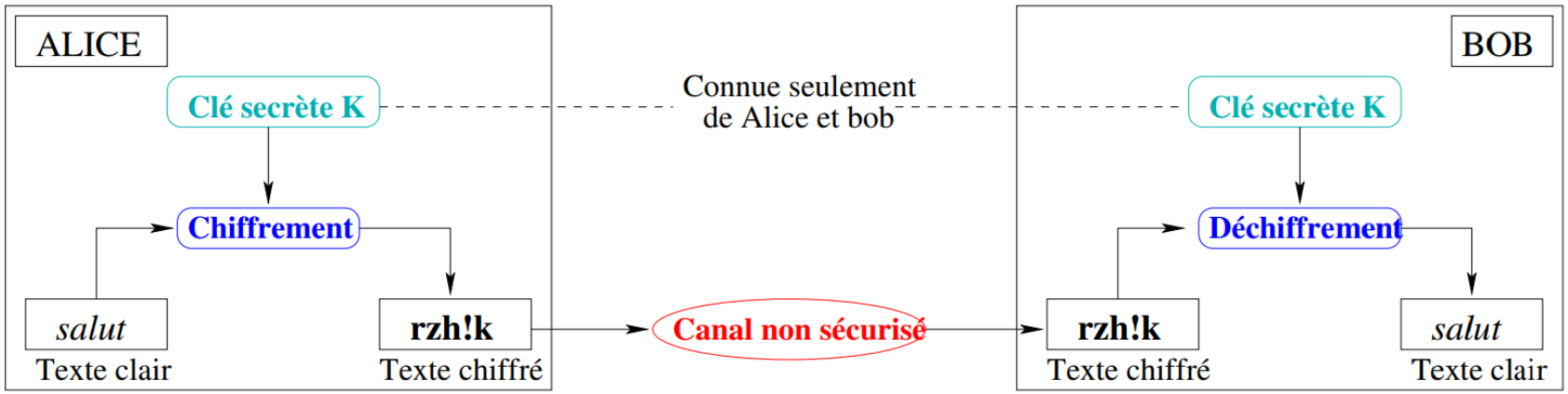
1. La sécurité repose sur le secret de la clé et non sur le secret de l'algorithme

2. Le déchiffrement sans la clé doit être impossible (en un temps raisonnable)

3. Trouver la clé à partir du clair et du chiffré est impossible (en un temps raisonnable)

Cryptographie symétrique

- Principe
  - Appellations: Cryptographie à clé secrète / symétrique / à clé privée
  - La même clé pour chiffrer et déchiffrer un message ($Ke = Kd = K$)
  - Les deux communicants doivent être en possession de cette clé. (clé convenue **secrètement** par Alice et Bob)



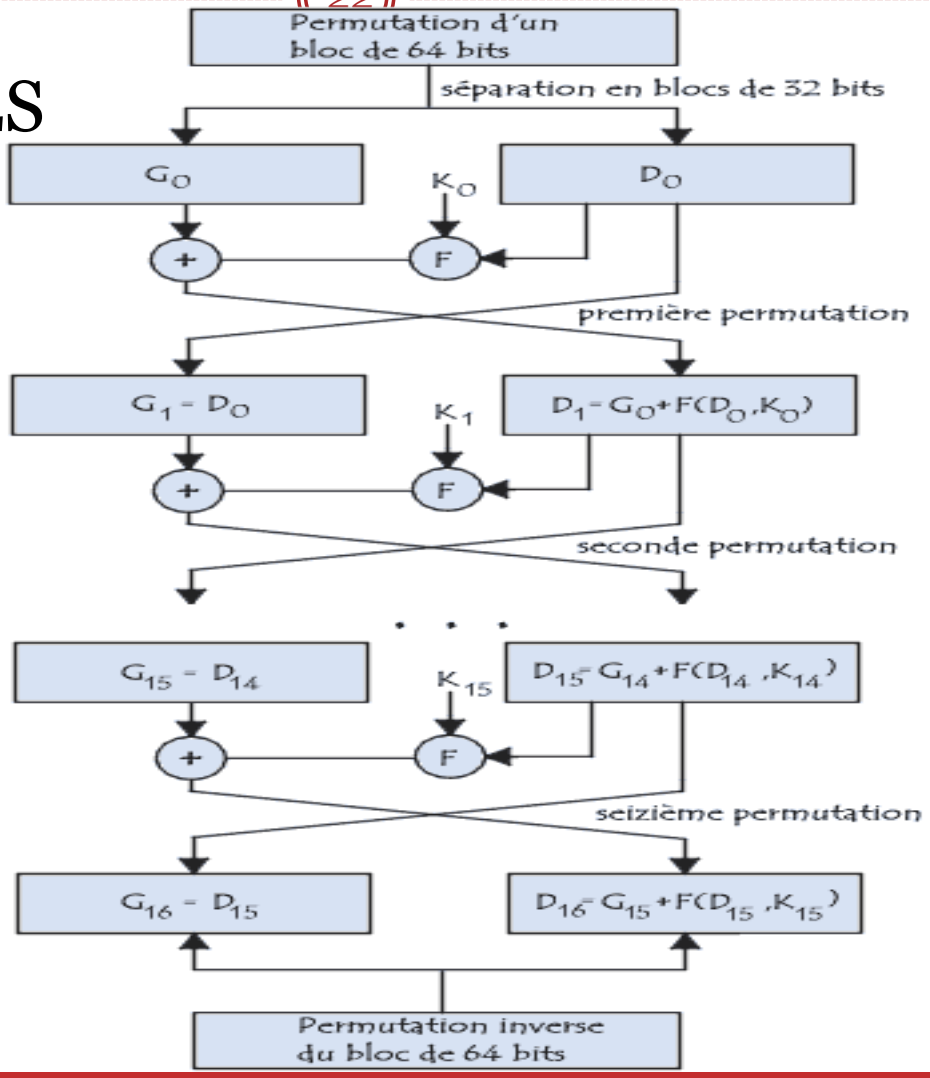
Cryptographie symétrique

- Systèmes symétriques : DES, 3DES, AES

- Exemple DES (Data Encryption Standard)
  - Chiffrement par blocs: découpage du message en clair, en blocs de 64 bits.
  - Code les blocs séparément puis les concatène
  - Clé de 64 bits (56bits + 8bits de parité)
  - 16 étapes du chiffrement et du déchiffrement et utilisation des clés (16 sous-clés de 48 bits) et des permutations
  - Algorithme facile à réaliser matériellement

Cryptographie symétrique

- Algorithme DES



Cryptographie symétrique

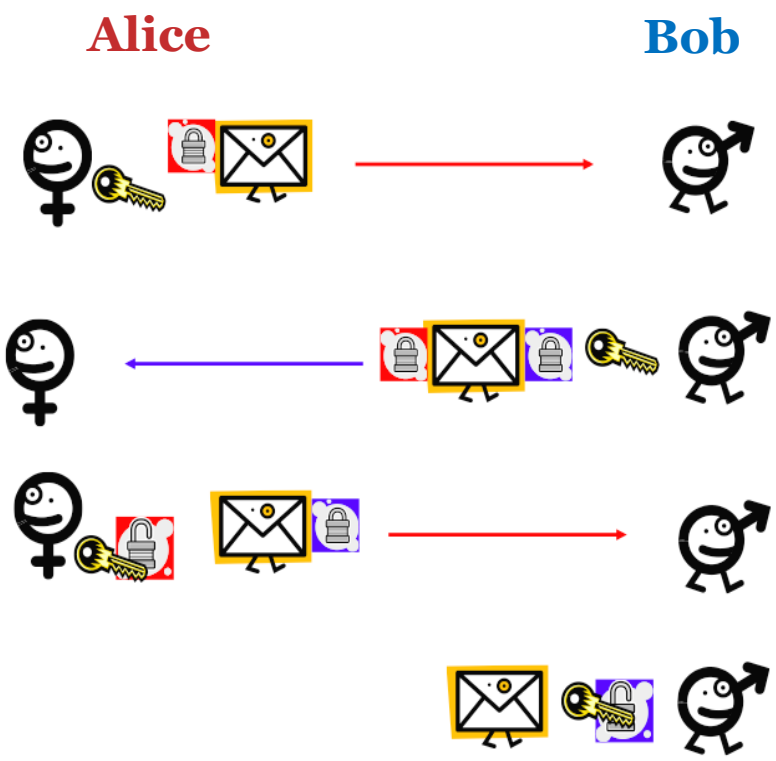
- Avantage:
  - En pratique : grande efficacité en terme de temps de calcul
- Inconvénient :
  - la clé *K* doit rester secrète → problème de l'échange des clés.
  - Comment s'échanger la clé secrète de façon sécurisée? Surtout si:
    - La clé doit être changée souvent
    - Le nombre de communicants devient grand
    - L'un des communicants est malintentionné
- Solution: **schéma à double chiffrement** (travaux de Diffie et Hellman)

Cryptographie symétrique

- **Echange de clé: Schéma à double chiffrement**

  - **Principe**

    - Alice met son colis dans une boite qu'elle ferme avec un cadenas et l'envoie à Bob.
    - Bob reçoit le colis, rajoute un cadenas à la boite et renvoie le tout à Alice
    - Alice retire son cadenas avec sa clé et renvoie la boite à Bob.
    - Bob peut maintenant ouvrir la boite avec sa clé et profiter du colis



Cryptographie asymétrique

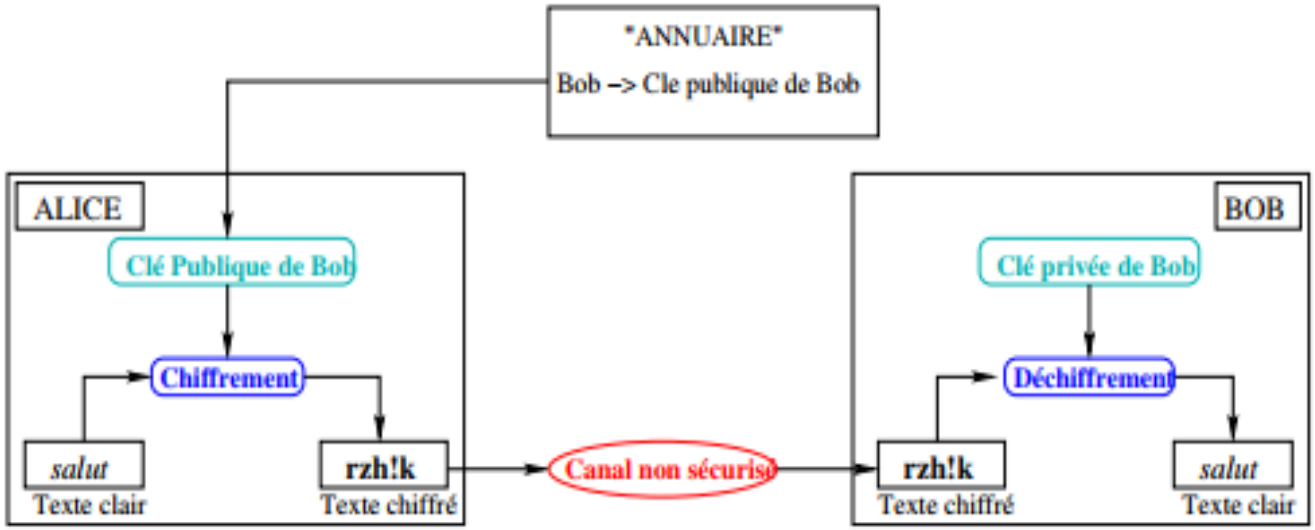
- **Motivations**
  - Systèmes cryptographiques à clé secrète
    - pratiquement sûrs
    - efficaces en termes de temps de calcul.
  - Mais nouvelles interrogations :
    - Avant d'utiliser un système de chiffrement à clé secrète, comment convenir d'une clé ?
    - Comment établir une communication sécurisée entre deux entités sans échange préalable de clé ?
      $\Longrightarrow$ Solution apportée par Diffie et Hellman
  - Encore des problèmes!!
    - Les échanges ne peuvent se faire qu'en présence des deux parties communicantes
    - Solution: **systèmes cryptographiques à clé publique**

Cryptographie asymétrique

- **Principe**
  - Appellations: Cryptographie asymétrique / à clé publique
  - Deux clés différentes ($Ke \neq Kd$)
    - Ke publique (connue de tous) → pour chiffrer
    - Kd privée (gardée secrète) → pour déchiffrer
  - Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante.
  - Chaque communicant doit être en possession d'un couple de clés (publique, privée)
    - Alice (Pub_A, $Priv_A$)
    - Bob (Pub_B, $Priv_B$)

Cryptographie asymétrique

- **Principe**
  - Bob possède une clé publique permettant de chiffrer des messages, et une clé privée permettant de les déchiffrer. Il doit être impossible de déchiffrer un message à partir de la seule clé publique
  - Alice a accès à la clé publique de Bob et peut lui envoyer un message à tout moment
  - Bob peut facilement déchiffrer le message grâce à sa clé privée.



Cryptographie asymétrique

- Cryptographie à clé publique se base sur des problèmes mathématiques réputés difficiles.

- But: Trouver des fonctions mathématiques :
  - Faciles à utiliser dans un sens
  - Très difficile à inverser, à moins de connaître un paramètre secret (clé)

- Les algorithmes se basent sur des concepts mathématiques tels que:
  - La factorisation de grands nombres premiers (**RSA**),
  - Le problème des logarithmes discrets (**ElGamal**),
  - Les courbes elliptiques (**ECC**)
  - Cryptographie quantique

Cryptographie asymétrique

- Exemple RSA
  - 1975 : Diffie, Hellman et Merkle inventent le principe de la cryptographie à clé publique. Mais aucun exemple concret n'est proposé.
  - 1977: Ronald **R**ivest, Adi **S**hamiret Leonard **A**dleman inventent le premier protocole de cryptographie à clé publique: RSA. Il est basé sur le principe de la factorisation de grands nombres entiers par des nombres premiers.

Cryptographie asymétrique

- Exemple RSA: Principe
  - Alice choisit deux grands nombres premiers **p** et **q** et calcule : n = p*q et z=(p-1)(q-1).
  - Elle choisit un entier **e** qui n'a pas de facteur commun avec z (premiers entre eux).
  - Elle calcule **d** tel que (e*d-1) est exactement divisible par z.
  - Elle déduit : Clé publique = (n,e) et clé privée =(n,d)
  - Bob peut chiffrer le message destiné à Alice grâce à la clé publique de cette dernière. Mais il ne peut plus le déchiffrer, car RSA est impossible à inverser, à moins de connaître **p** et **q**.
  - Alice reçoit le message chiffré de Bob et peut le déchiffrer grâce à sa clé privée.
  - Formules:
    - Chiffrement (par Bob): $\mathbf{c = m^e \bmod n}$
    - Déchiffrement (par Alice): $\mathbf{m = c^d \bmod n}$

Cryptographie asymétrique

- Exemple RSA: calcul
  - Prenons $p = 47$ et $q = 59$.
  - On calcule $n = p*q = 47*59 = 2773$ et z=2668
  - On choisit **e**, premier par rapport à z . Ex : $e = 17$.
  - On calcule alors, par l'algorithme d'Euclide étendu, d tel que $e*d \equiv 1 \bmod z$, soit $d = 157$.
  - Donc,
    - Clé publique : $(n, e) = (2773, 17)$
    - Clef privée : $(n, d) = (2773, 157)$
  - Chiffrement du message m = 01000010 = 66 :
    $C \equiv \boldsymbol{m^e} \bmod n \equiv \mathbf{66^{17}} \bmod 2773 = 872$
  - Déchiffrement de C :
    $m = \boldsymbol{c^d} \bmod n \equiv \mathbf{872^{157}} \bmod 2773 \equiv 66$

Cryptographie asymétrique

- Exemple RSA
  - Le vrai but de l'attaquant : découvrir le texte en clair
    - Calculer d à partir de $(n, e) \Leftarrow\Rightarrow$ factoriser n.
  - Toujours d'actualité : Casser RSA est aussi dur que factoriser n
  - Afin de prouver la robustesse de leur algorithme de chiffrement face aux avancées mathématiques sur le problème de la factorisation d'entier, la société RSA propose un défi en mars 1991. Ils fabriquent puis publient une liste de nombres n, dont la taille varie entre 100 et 617 chiffres, et proposent une prime, se montant à $200 000 pour le plus grand de ces nombres, à la première personne qui trouvera sa factorisation.
  - Cette liste de nombres reste la référence pour réaliser les records de factorisation d'entiers

Cryptographie asymétrique

Taille de n	Date	Auteurs
100 chiffres	1er avril 1991	Lenstra
110 chiffres	14 avril 1992	Lenstra, Manasse
120 chiffres	9 juillet 1993	Denny, Dodson, Lenstra, Manasse
129 chiffres	26 avril 1994	Atkins, Graff, Lenstra, Leyland
130 chiffres	10 avril 1996	Cowie, Dodson, Elkenbracht-Huizing, Lenstra, Montgomery, Zayer
140 chiffres	2 février 1999	Cavallar, Dodson, Lenstra, Leyland, Lioen, Montgomery, Murphy, te Riele, Zimmermann
155 chiffres	22 août 1999	Cavallar, Dodson, Lenstra, Lioen, Montgomery, Murphy, te Riele, Aardal, Gilchrist, Guillerm, Leyland, Marchand, Morain, Muffett, Putnam, Putnam, Zimmermann
158 chiffres	19 janvier 2002	Bahr, Franke, Kleinjung
160 chiffres	1er avril 2003	Bahr, Franke, Kleinjung, Lochter, Böhm
174 chiffres	3 décembre 2003	Franke, Kleinjung, Montgomery, te Riele, Bahr, NFSNET
176 chiffres	2 mai 2005	Aoki, Kida, Shimoyama, Ueda
200 chiffres	9 mai 2005	Bahr, Böhm, Franke, Kleinjung
232 chiffres	12 décembre 2009	Kleinjung, Aoki, Franke, Lenstra, Thomé, Bos, Gaudry, Kruppa, Montgomery, Osvik, te Riele, Timofeev, Zimmermann
240 chiffres	2 décembre 2019	Boudot, Gaudry, Guillevic, Heninger, Thomé, Zimmermann
250 chiffres	28 février 2020	Boudot, Gaudry, Guillevic, Heninger, Thomé, Zimmermann

Tableau 1 – Records de factorisation d'entier depuis l'instauration du challenge RSA.

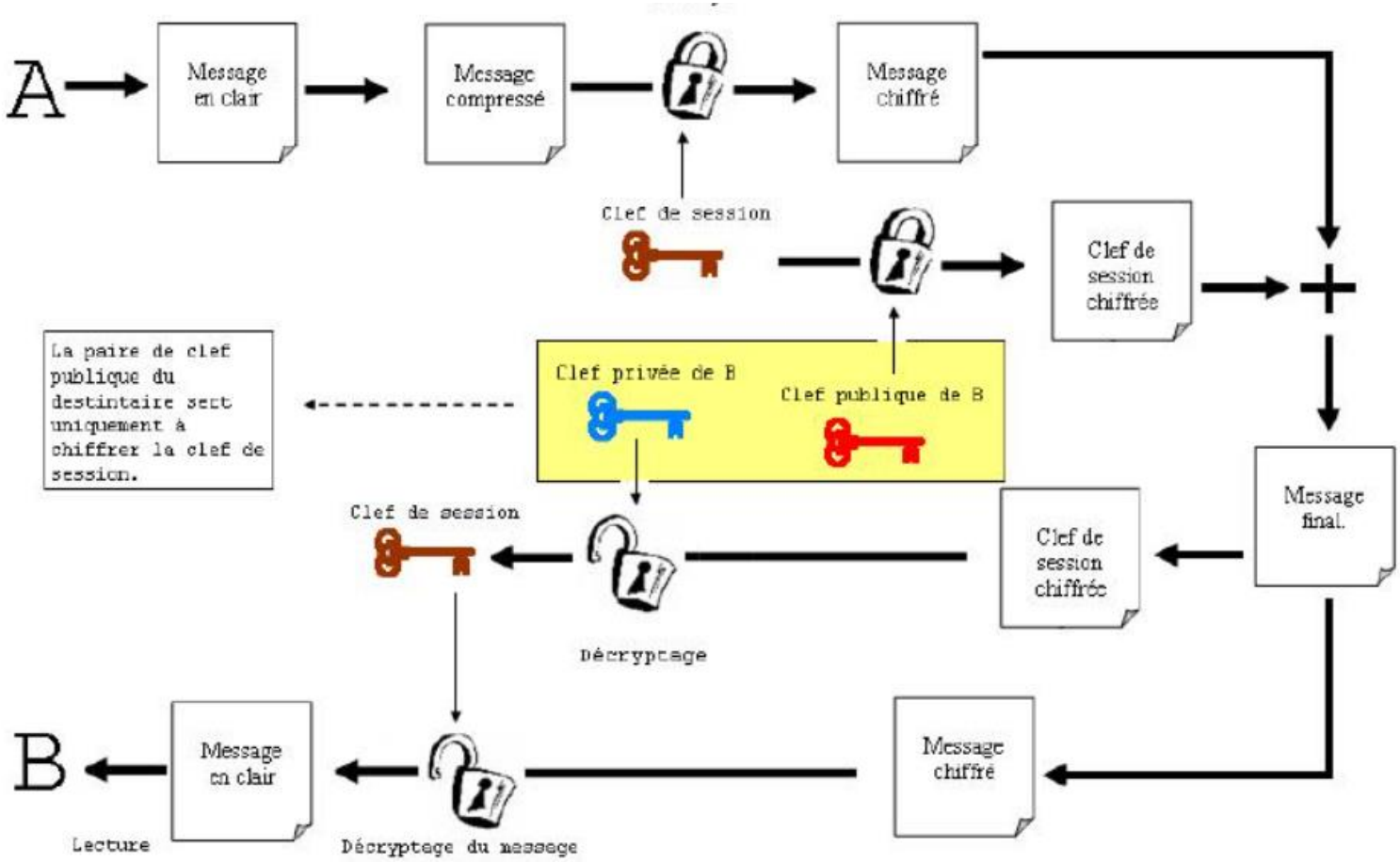
Cryptographie asymétrique

- La taille des clés s'étend de 512 bits à 2048 bits en standard
- Le chiffrement asymétrique est environ **1000** fois plus lent que le chiffrement symétrique.
- Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires. En effet, chaque utilisateur possède une paire (*pub, priv*) et tous les transferts de message ont lieu avec ces clés.
- La distribution des clés est grandement facilitée car l'échange de clés secrètes n'est plus nécessaire. Chaque utilisateur conserve sa clé secrète (privée) sans jamais la divulguer. Seule la clé publique devra être distribuée.

Cryptographie hybride

- Profiter des avantages des deux systèmes:
  - Chiffrer le message avec une clé de session (symétrique)
    - Plus rapide
  - Chiffrer la clé de session avec une clé publique (asymétrique)
    - Résoudre le problème d'échange de clés
- Exemple: PGP (Pretty Good Privacy)

Cryptographie hybride



Signature numérique

- Sécuriser un échange ➔ assurer les propriétés fondamentales:
  - Confidentialité
  - Authentification
  - Intégrité
  - Non-répudiation

- La notion de confidentialité ne suffit pas pour répondre aux questions :
  - qui m'a réellement envoyé ce message ?
  - quelqu'un a-t-il pu usurper son identité ?
  - ai-je bien reçu le message complet ?
  - quelqu'un a-t-il pu remplacer le message initial par un autre ?

- Solution: **signature numérique**

Signature numérique

- Notion de signature (au sens habituel=manuscrite)
  - La signature ne peut être imitée, le signataire est donc le seul à pouvoir signer :
    - Signature = Authentification
  - Le document signé ne peut être partiellement ou totalement modifié :
    - Signature = intégrité
  - La signature ne peut être reniée :
    - Signature = Non répudiation
  - La signature appartient à un seul document.

Signature numérique

- La signature électronique (ou numérique) dépend du signataire et du document
- Objectifs d'une signature électronique
  - Une signature est authentique.
  - Une signature ne peut être falsifiée (imitée).
  - Une signature n'est pas réutilisable sur un autre document.
  - Un document signé est inaltérable.
  - Une signature ne peut pas être reniée.

- Réalisation: système asymétrique + fonction de hachage

Signature numérique

- **Fonction de hachage**
  - Ce sont des fonctions à sens unique :
    - pour un entier x, il est facile de calculer H(x),
    - mais étant donnée H(x), il est pratiquement impossible de déterminer x
  - La fonction de hachage permet d'extraire une empreinte (un hash / condensé) qui caractérise les données
    - Une empreinte a toujours une taille fixe indépendamment de la taille des données (qui est variable)
    - Il est pratiquement impossible de trouver deux données ayant la même empreinte
  - Exemples de fonctions de hachage :
    - MD5 : Message Digest 5, il génère une empreinte de 128 bits.
    - SHA-1 : Secure Hash Algorithm, il génère une empreinte de 160 bits.
    - SHA-2: génère une empreinte de 256, 384 ou 512 bits

Signature numérique

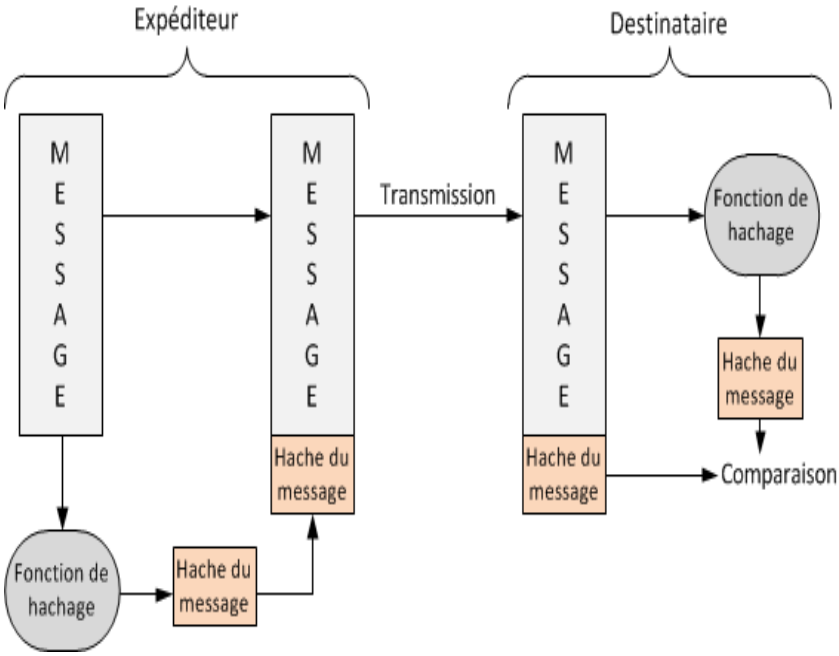
- **Fonction de hachage: propriétés**
  - Propriétés de base : compression et facilité de calcul
  - Résistance à la préimage
    - étant donné y, il est difficile de trouver x tel que y = H(x)
  - Résistance à la seconde préimage
    - étant donné x, il est difficile de trouver x' ≠ x tel que H(x) = H(x')
  - Résistance à la collision
    - il est difficile de trouver x et x' tels que H(x) = H(x').

* Si y est tel que $y = H(x)$, alors x est appelé *préimage* de y

Signature numérique

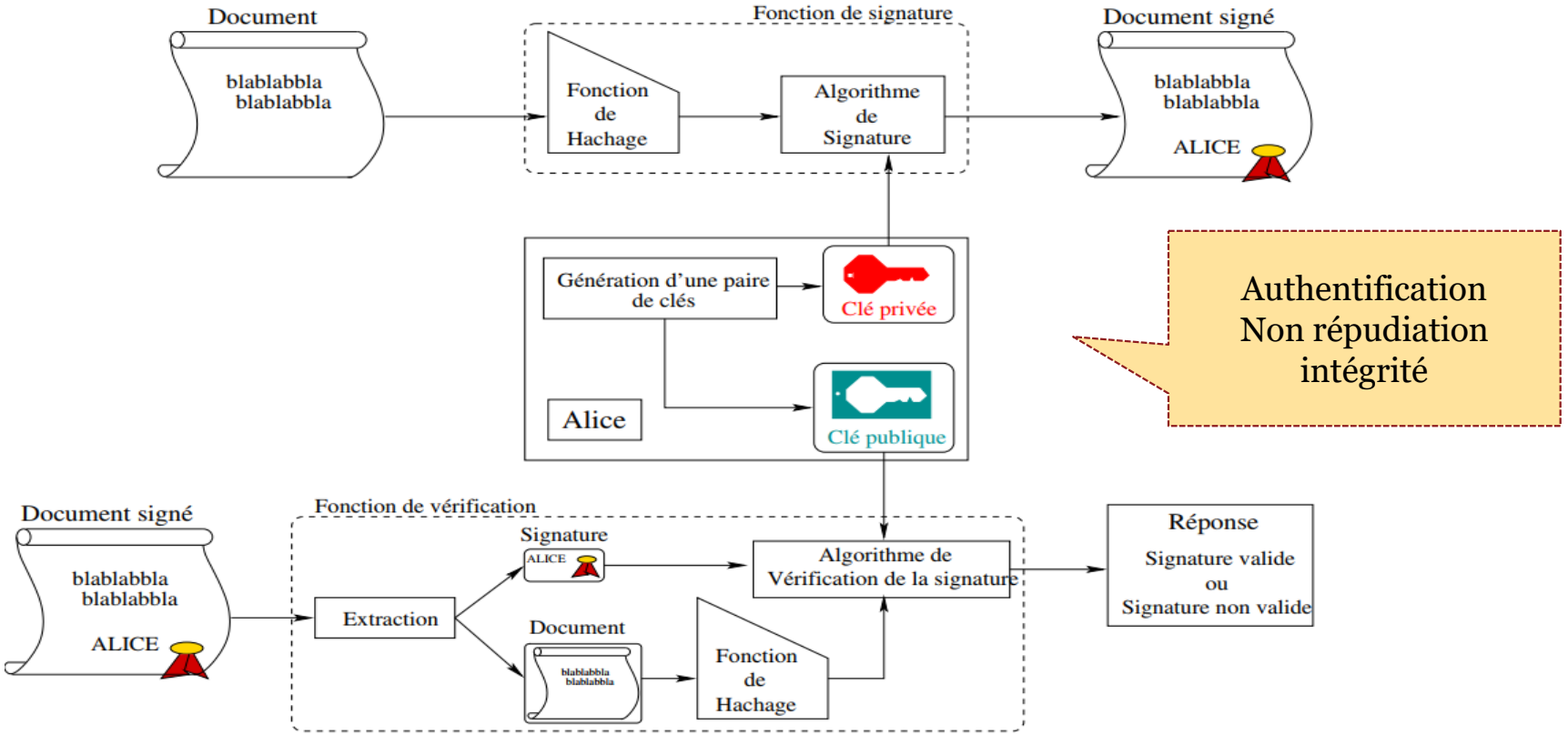
- **Fonction de hachage: Principe**

  - Alice calcule une empreinte sur un texte clair en appliquant une fonction de hachage.
  - Alice envoie le texte clair ainsi que l'empreinte (hash) du message
  - Bob, qui possède la même fonction de hachage, recalcule l'empreinte sur le texte reçu et la compare avec celle reçue:
    - Si les deux empreintes sont les mêmes alors le message est intègre
    - sinon il ne l'est pas.



Signature numérique

- **Principe de la signature numérique**
  - Au lieu de chiffrer tout le message, seule l'empreinte est chiffrée → devient la signature



Encore un problème …

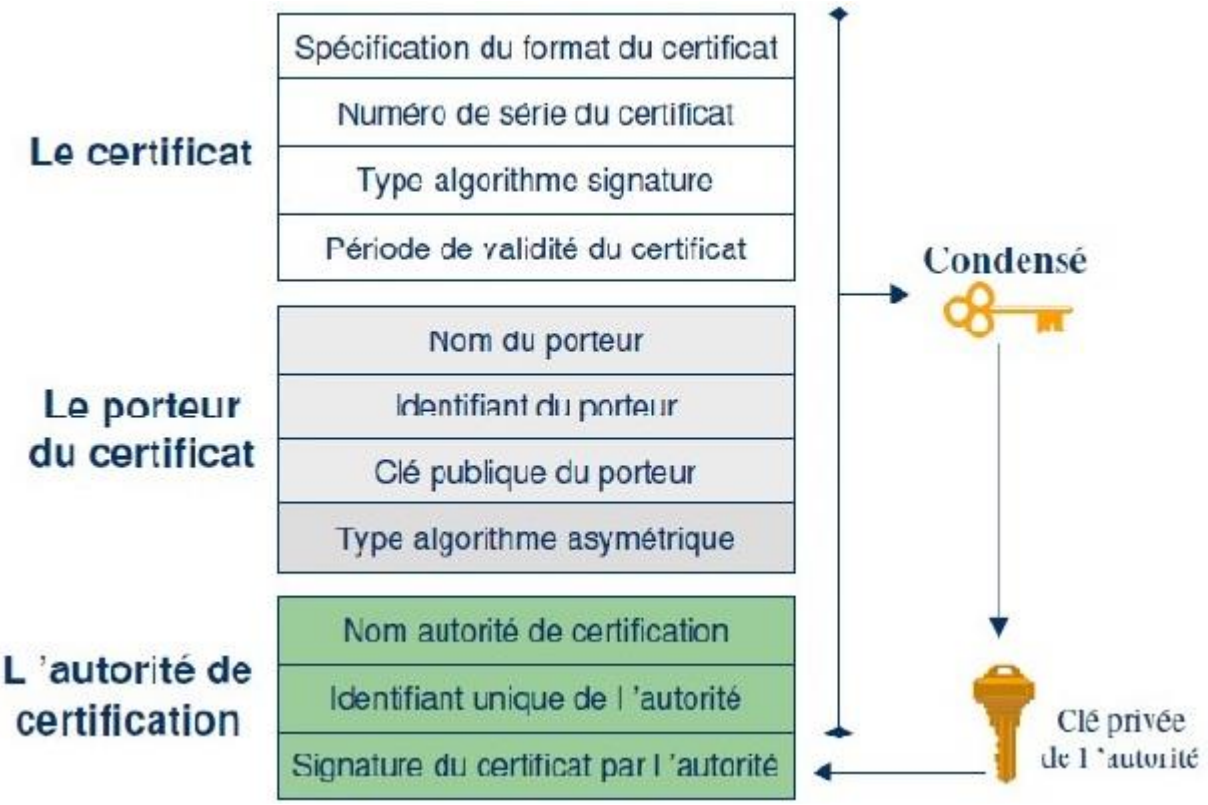
- Comment récupérer et être sûr d'une clé publique ?
  - Oscar peut se faire passer pour le destinataire en plaçant une fausse clé publique (comportant le nom et l'ID du vrai destinataire)
  - Les données chiffrées avec cette fausse clé seront interceptées par Oscar (une personne non autorisée)
  - Il faut un moyen de prouver la correspondance entre une clé publique et une personne (à qui elle est associée)
  - Solution: **Certificats numériques**

Certificats numériques

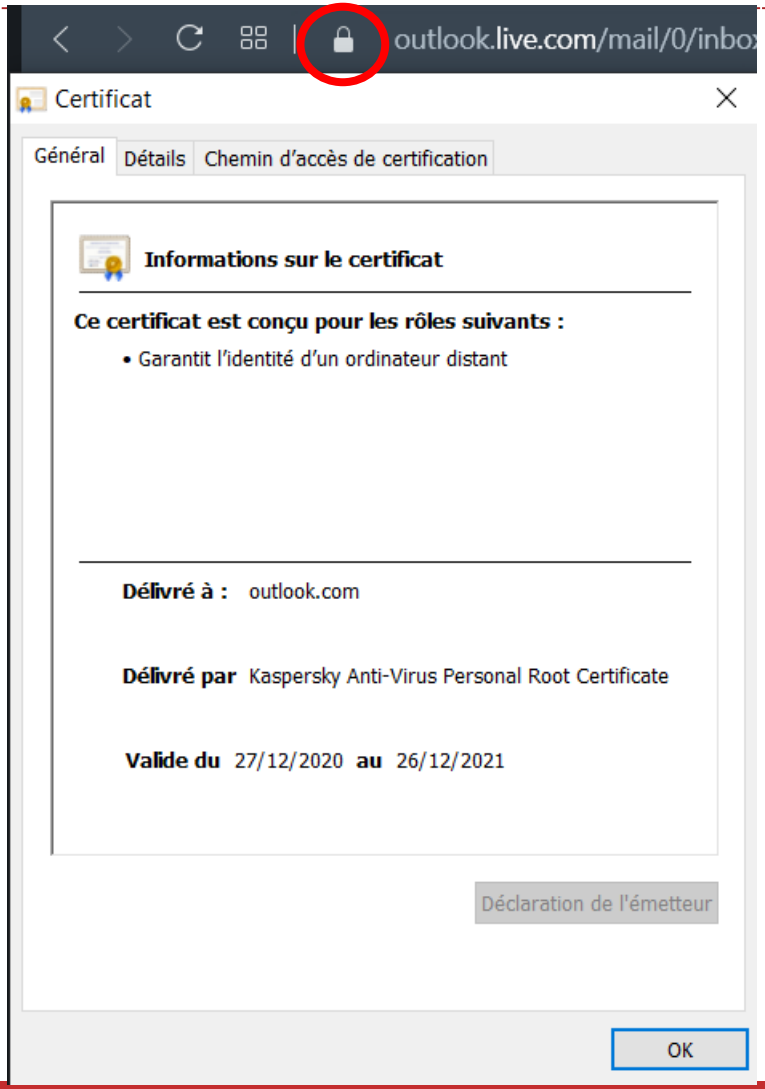
- **Principe**
  - Le certificat = Structure de données
    - Permet de lier une clé publique à différents éléments, au moyen de la signature d'une autorité de confiance
    - Un certificat contient
      - une clé publique
      - Il contient aussi des données d'identité
        - Pour une personne : état civil, adresse, mail…
        - Pour un serveur : nom de domaine, adresse IP, mail de l'administrateur etc…
      - Dates de validité
      - Type d'utilisation autorisée
      - *Etc*
  - Les certificats sont émis par une autorité de certification (Certificate Authority – CA)
    - Garantit l'exactitude des données
    - Certificats vérifiables au moyen de la clé publique de la CA

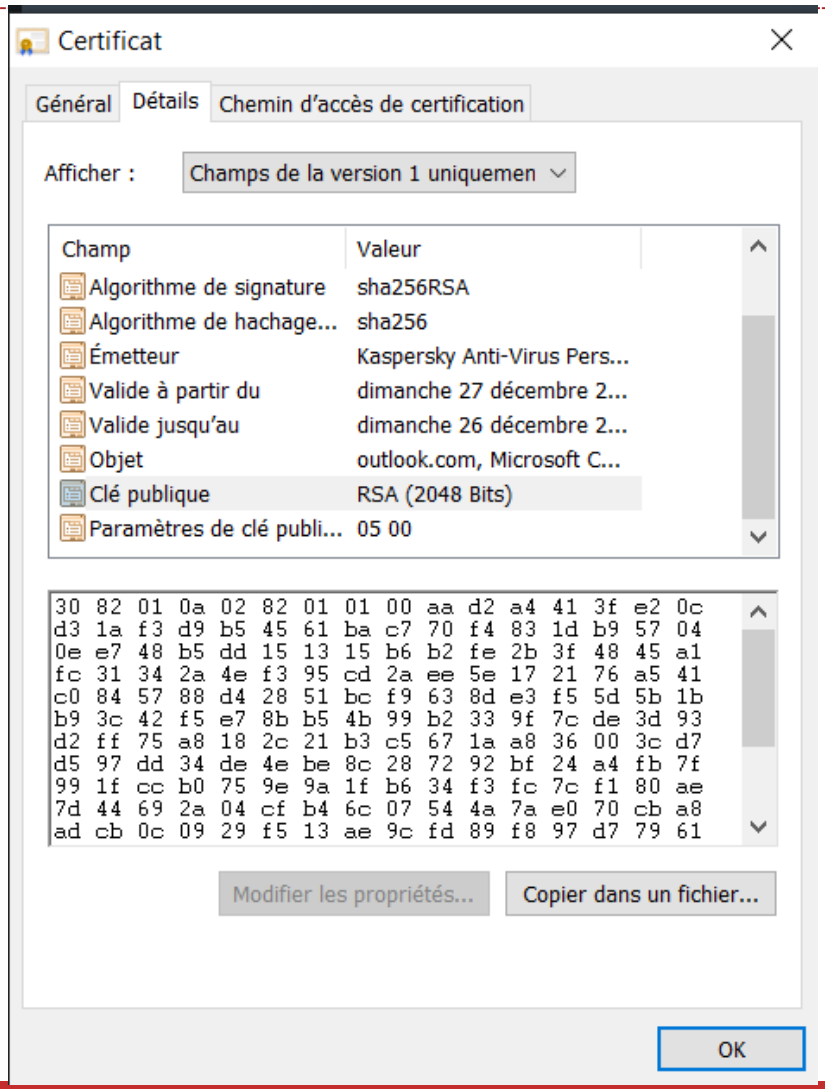
Certificats numériques

- **Structure générale**



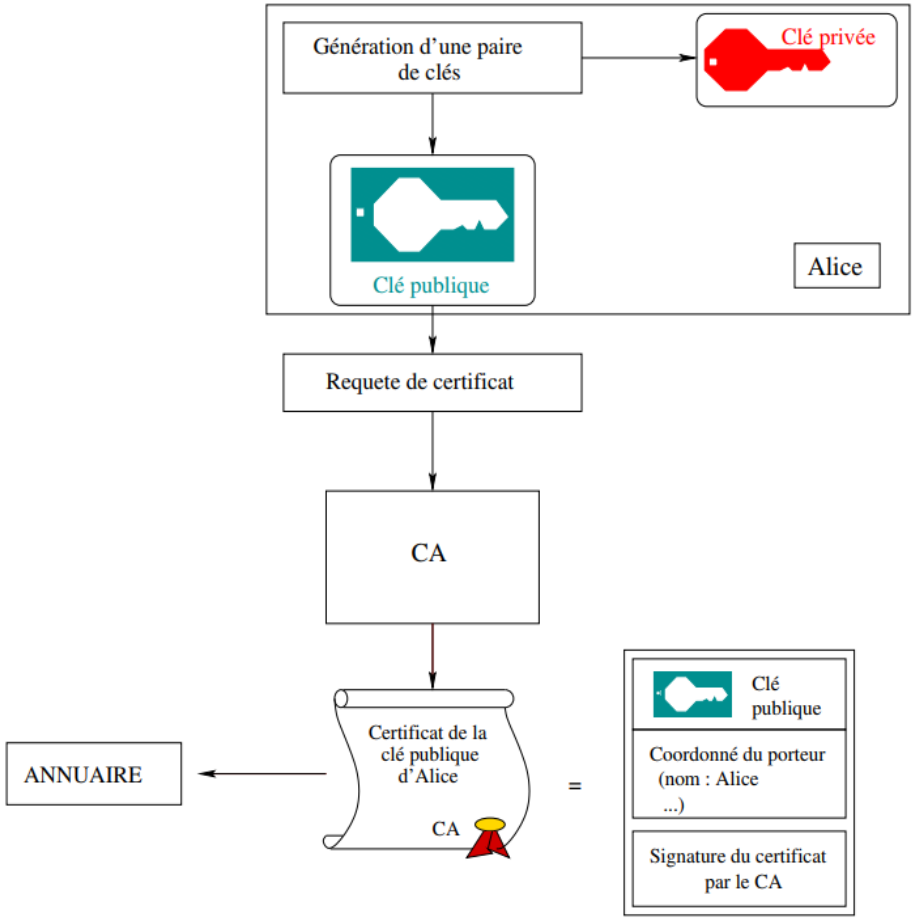
Certificats numériques





Certificats numériques

- **Principe simplifié: création d'un certificat**
  - Alice génère ses clés (publique, privée)
  - Elle émet une requête au CA pour un certificat de sa clé publique
  - CA valide la clé, authentifie Alice et génère un certificat
  - le certificat est signé par le CA
  - Cette signature certifie l'origine du certificat et son intégrité.
  - Le certificat est publié dans un annuaire publique



Certificats numériques

- **Vérifier l'authenticité du tiers de confiance**
  - Chaque CA possède lui-même un certificat
    - La clé privée associée permet de signer les certificats émis par le CA
    - Ce certificat est signé par un autre CA etc…
      - ==⇒ Chaîne de certificats
  - Le dernier certificat de la chaîne est signé par lui-même
    - On parle de certificat *auto-signé* ou certificat *racine*

Certificats numériques

- **PKI = Public Key Infrastructure**
  - Ensemble d'infrastructures permettant de réaliser effectivement des échanges sécurisés.
    - Ensemble de technologies, organisations, procédures et pratiques qui supporte l'implémentation et l'exploitation de certificats basés sur la cryptographie à clé publique
  - PKI ne distribue pas des clés mais des certificats
  - Les fonctions d'une PKI
    - émettre des certificats à des entités préalablement authentifiées ;
    - révoquer des certificats, les maintenir ;
    - établir, publier et respecter des pratiques de certification pour établir un espace de confiance ;
    - rendre les certificats publics par le biais de services d'annuaires
    - éventuellement, gérer les clés et fournir des services d'archivage.

Certificats numériques

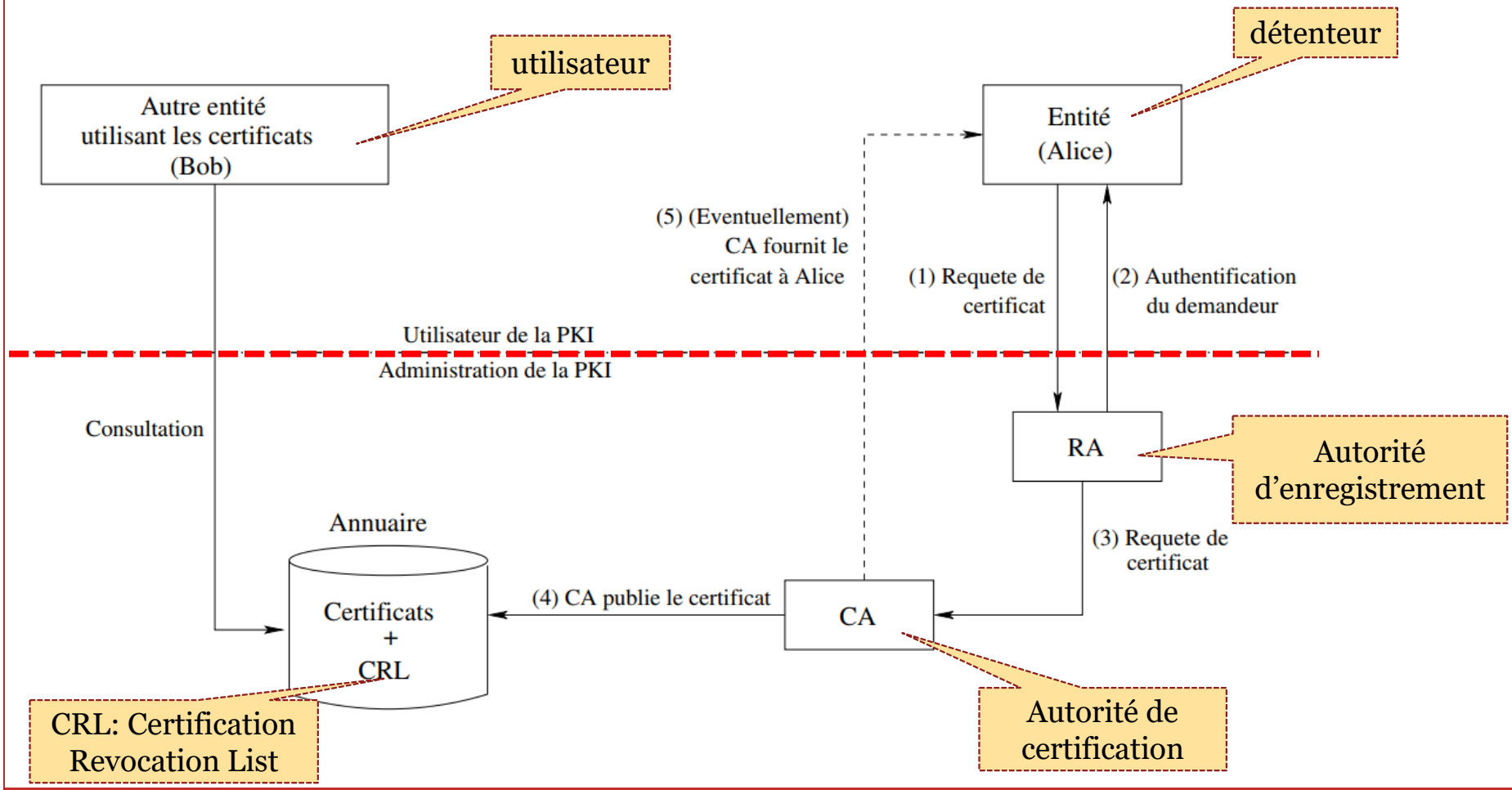
- **Acteurs d'une PKI**
  - Détenteur d'un certificat
    - entité qui possède une clé privée
    - le certificat numérique contient la clé publique associée.
  - Utilisateur d'un certificat
    - récupère le certificat
    - utilise la clé publique dans sa transaction avec le détenteur.
  - L' Autorité de Certification (CA)
    - Ensemble de ressources défini par son nom et sa clé publique qui :
      - génère des certificats ;
      - émet et maintient les informations sur les CRL (liste de révocation de certificats)
      - publie les certificats non encore expirés ;
      - maintient les archives des certificats expirés/révoqués.
    - Entité juridique et morale d'une PKI

Certificats numériques

- **Acteurs d'une PKI**
  - Autorité d'enregistrement (RA)
    - Intermédiaire entre le détenteur de la clé et le CA.
    - Vérifie les requêtes des utilisateurs
    - Transmet les requêtes au CA
    - Chaque CA a une liste de RA accrédités.
    - Un RA est connu d'un CA par son nom et sa clé publique.
    - CA vérifie les informations du RA par le biais de sa signature
  - Dépôt ou Annuaire (Repository)
    - Distribue les certificats et les CRL.
    - Accepte les certificats et les CRL d'autres CA et les rend disponibles aux utilisateurs.
    - Connu par son adresse et son protocole d'accès.
  - Archive
    - stockage sur le long terme des informations pour le compte d'un CA.
    - permet de régler les litiges en sachant quel certificat était valable à telle époque.

Certificats numériques

- **Acteurs d'une PKI**



Certificats numériques

- Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse.

- Les deux formats les plus utilisés aujourd'hui sont :
  - X.509, défini dans la RFC 52804 ;
    - Ne peut contenir qu'un seul identifiant, et cet identifiant doit contenir de nombreux champs prédéfinis, et ne peut être signé que par une seule autorité de certification.
  - OpenPGP, défini dans la RFC 48805.
    - peut contenir plusieurs identifiants, lesquels autorisent une certaine souplesse sur leur contenu, et peuvent être signés par une multitude d'autres autorités de certification, ce qui permet alors de construire des toiles de confiance.

Pour résumer

- Chiffrement (symétrique, asymétrique) → confidentialité
- Signature numérique → authentification + intégrité + non répudiation
- Combinaison des deux → un schéma qui assure les 4 objectifs de la sécurité
- La cryptographie offre une variété de méthodes à combiner selon les besoins en sécurité