

Sécurité Informatique: Cryptography

Systèmes symétriques
et asymétriques

Fonctions de hachage

Signature numérique

Introduction

Confiance et Internet

Dans la vie courante la plupart des transactions reposent sur une « confiance » acquise par une relation en face à face ou un contact physique .

Dans le cybermonde cette relation de proximité est rompue.

Comment établir une relation de confiance indispensable à la réalisation de transactions à distance entre personnes qui ne se connaissent pas ?

Ce cours a pour but de répondre à cette question.

Problématique

Failles dans les protocoles de communication

Toute information circulant sur Internet peut être capturée et enregistrée et/ou modifiée

Problème de confidentialité et d'intégrité

Toute personne peut falsifier son adresse IP (*spoofing*) ce qui engendre une fausse identification

Problème d'authentification

Aucune preuve n'est fournie par Internet quant à la participation dans un échange électronique

Problème d'absence de traçabilité

Cryptographie

Le mot « Cryptographie » est composé des mots grecques :

CRYPTO = caché

GRAPHY = écrire

C'est donc l'art de l'écriture secrète.

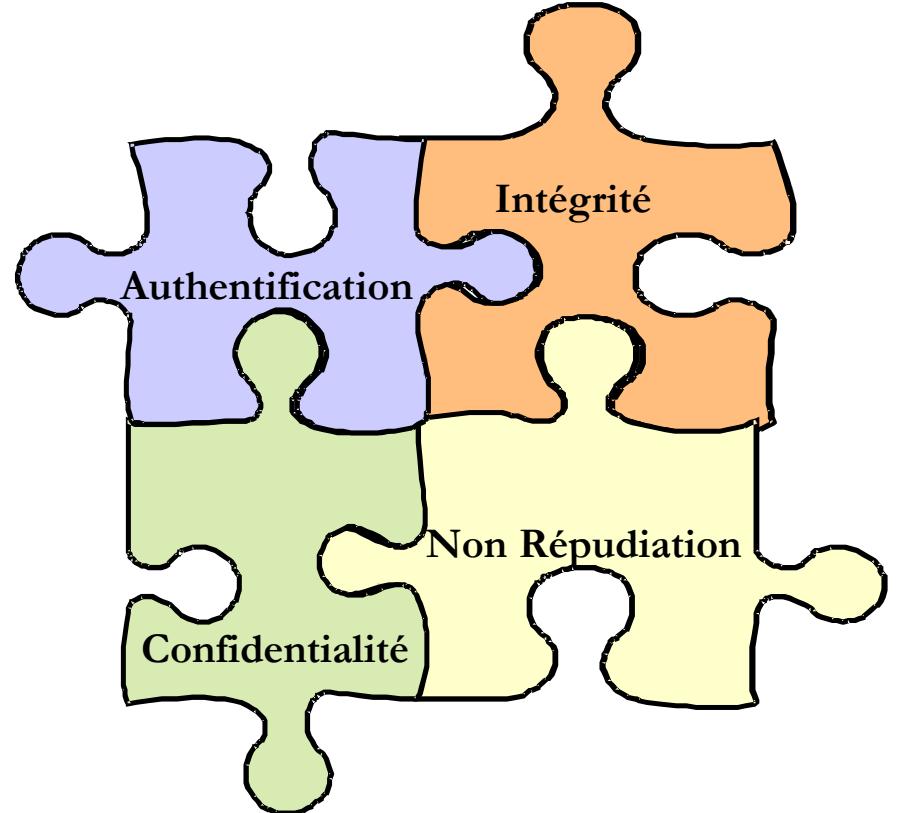
C'est une science permettant de préserver la confidentialité des échanges.

Cryptanalyse

La cryptanalyse est l'art de décrypter des messages chiffrés.

Cryptographie

Science mathématique permettant d'effectuer des opérations sur un texte intelligible afin d'assurer une ou plusieurs propriétés de la sécurité de l'information.



Cryptographie

Objectifs

Parmi les objectifs de la cryptographie :

- Garantir la confidentialité
- Vérifier l'intégrité des données
- Gérer l'authentification
- Assurer la non-répudiation

Cryptographie

Authentification

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée .

Confidentialité

Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables

Contrôle d'intégrité

Permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)

Non réputation

Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication

Confidentialité et chiffrement

Confidentialité

La confidentialité est la propriété qui assure que l'information est rendu inintelligible aux individus, entités, et processus non autorisés.

Chiffrement / déchiffrement

Le chiffrement est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire. Le déchiffrement est l'opération qui permet de restaurer le message original à partir du message chiffré.

Confidentialité et chiffrement

Clé de chiffrement

Dans la cryptographie moderne, l'habileté de maintenir un message chiffré secret, repose non pas sur l'algorithme de chiffrement (qui est largement connu), mais sur une information secrète dite CLE qui doit être utilisée avec l'algorithme pour produire le message chiffré.

Selon que la clé utilisée pour le chiffrement et le déchiffrement est la même ou pas, on parle de système cryptographique symétrique ou asymétrique.

Chiffrement Symétrique par substitution

Chiffrement de César

Le chiffre de César consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 rangs vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre):

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Chiffrement Symétrique par substitution

Chiffrement de Vigenère

Le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

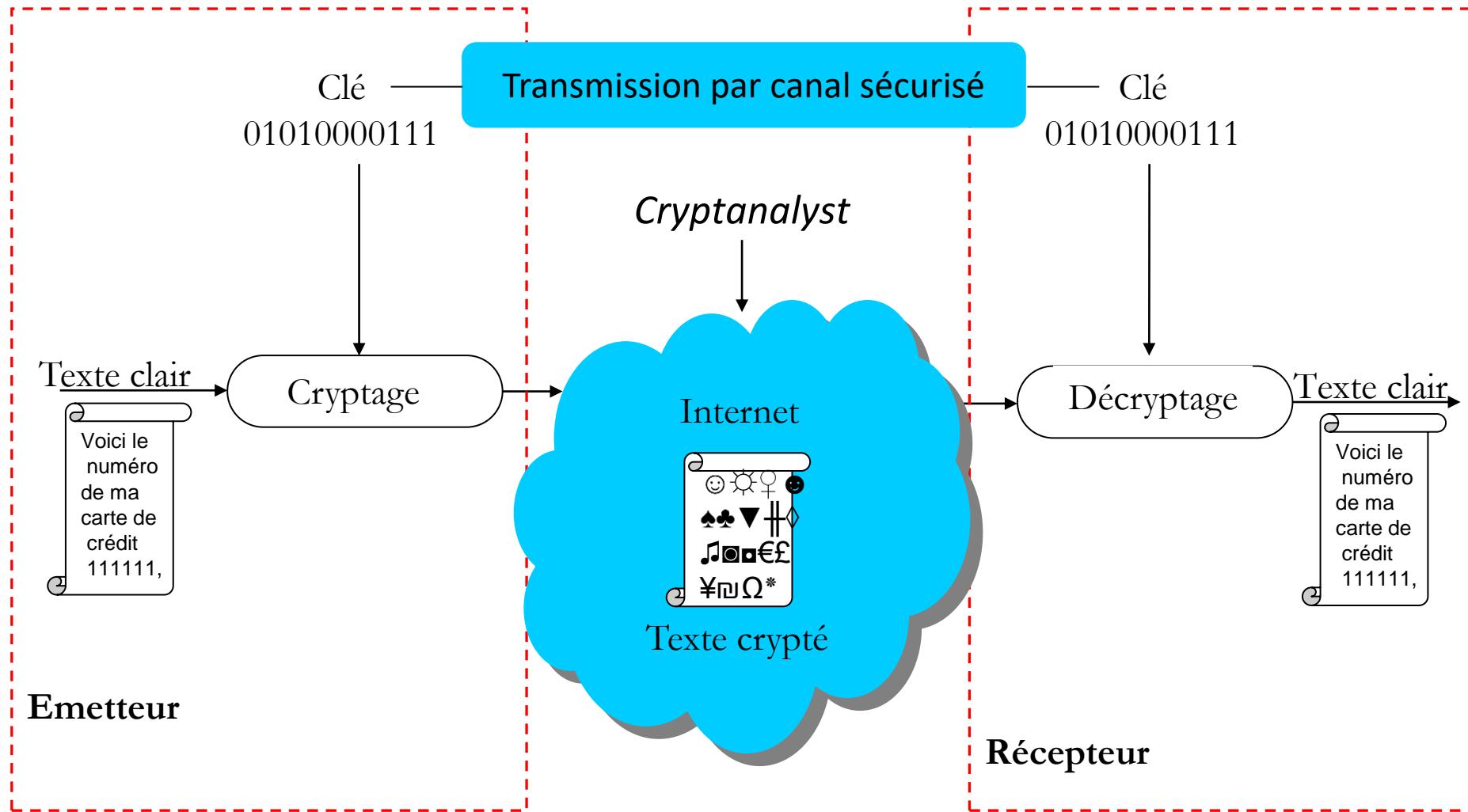
Chiffrement Symétrique par substitution

Exemple Chiffrement de Vigenère

chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

Chiffrement Symétrique



Confidentialité et chiffrement

Chiffrement symétrique

Dans le chiffrement symétrique, une même clé est partagée entre l'émetteur et le récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour chiffrer le message et par le récepteur pour le déchiffrer en utilisant un algorithme de chiffrement symétrique.



Chiffrement de Vernam

Plaintext: $m = 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0$

Clé : $K = 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1$

Cipheretext: $c = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1$

Comme vous le voyez il n' ya 4 possibilités

a	b	xor
0	0	0
0	1	1
1	0	1
1	1	0



$$\begin{aligned}m &= 010101110 \\k &= 010100101\end{aligned}$$

$$\mathbf{c} = m \oplus k = 011001011$$

$$\begin{aligned}k &= 010100101 \\c &= 011001011\end{aligned}$$

$$m = c \oplus k = 001101110$$

Confidentialité et chiffrement

Algorithmes de chiffrement symétriques

Il existe deux types d'algorithmes de chiffrement symétrique :

1. **Chiffrement par bloc** : division du texte clair en blocs fixe, puis chiffrement bloc par bloc

- DES: IBM, Standard NIST 1976
- 3DES: W. Diffie, M. Hellman, W. Tuchmann 1999.
- IDEA: Xuejia Lai et James Massey en 1992
- Blowfish: Bruce Schneier en 1993
- AES (Rijndael): Joan Daemen et Vincent Rijmen 2000

2. **Chiffrement par flux** : le bloc a une dimension unitaire (1 bit, 1 octet, ...), ou une taille relativement petite

- RC4: Ron Rivest 1987
- SEAL: Don Coppersmith et Phillip Rogaway pour IBM 1993.

• Blocks Ciphers

DES

Blocks de 64 bits
Clé de 64 bits

Mais en réalité c'est 56 bits qui sont utilisés

AES

Blocks de 128 bits
Clé de 128, 192 ou 256 bits



2 puissance 256

Chiffrement Symétrique

- Exigences:
 - Un algorithme de cryptage solide.
 - Une clé secrète partagée et connue entre l'émetteur et le récepteur.

$$Y = E_K(X)$$

$$X = D_K(Y)$$

- Suppose que l'algorithme de cryptage est connu à l'avance.
- Les clés sont distribuées à travers des canaux sécurisés.
- Exemples :
 - Algorithmes : DES, IDEA, AES
 - Taille des clés : 64-128-192-256-... bits

Introduction à DES

Aperçus générale

DES (Data Encryption Standard) est l'un des algorithmes pionnier de chiffrement symétrique. Il est basé sur un ensemble de permutations et substitutions comme présenté ci-dessous.

C'est un algorithme qui opère sur des blocs de 64 bits, et utilise une clé de 56 bits qui était suffisante à l'époque. Il a été définis officiellement dans FIPS46-3. Il est constitué d'une permutation initiale, un calcul médian en fonction de la clé et une permutation finale.

Confidentialité et chiffrement

Sécurité de DES

DES fut raisonnablement sûr à l'époque de son invention. RSA Security a lancé le DES Challenge qui a permis de mettre fin à la robustesse de DES à la cryptanalyse :

- DES Challenge I 1997: DESCHALL a cassé la clé DES en 96 j
- DES Challenge II-1 1998: Distributed.net a réussi à casser la clé DES en 41j
- DES Challenge II-2 1998: EFF Deep Crack a cassé la clé DES en 56h
- DES Challenge III 1999: Deep Crack et Distributed.net ont cassé la clé DES en 22h15

En 2000 AES deviens le standard à la place de DES

Les modes d'opération du chiffrement symétrique

Dans le chiffrement symétrique l'algorithme opère sur un bloc. Pour chiffrer un ensemble de blocs constituants le message à chiffrer il est nécessaire de définir une stratégie d'opération sur la succession des blocs à chiffrer.

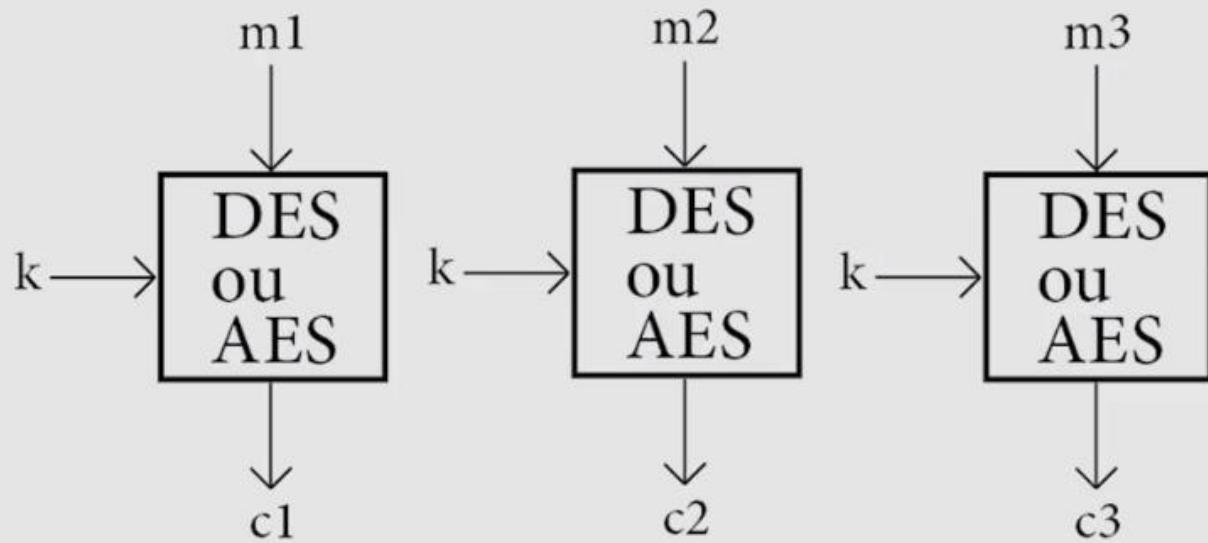
Il existe quatre modes définis dans FIPS 81 (1980)

- Electronic Code Book (ECB),
- Cipher Block Chaining (CBC),
- Cipher FeedBack (CFB) et
- Output FeedBack (OFB).

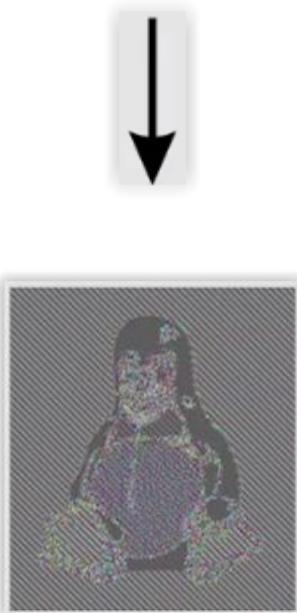
Electronic Code Book (ECB)



m est découpé en 3 blocs: m_1, m_2, m_3

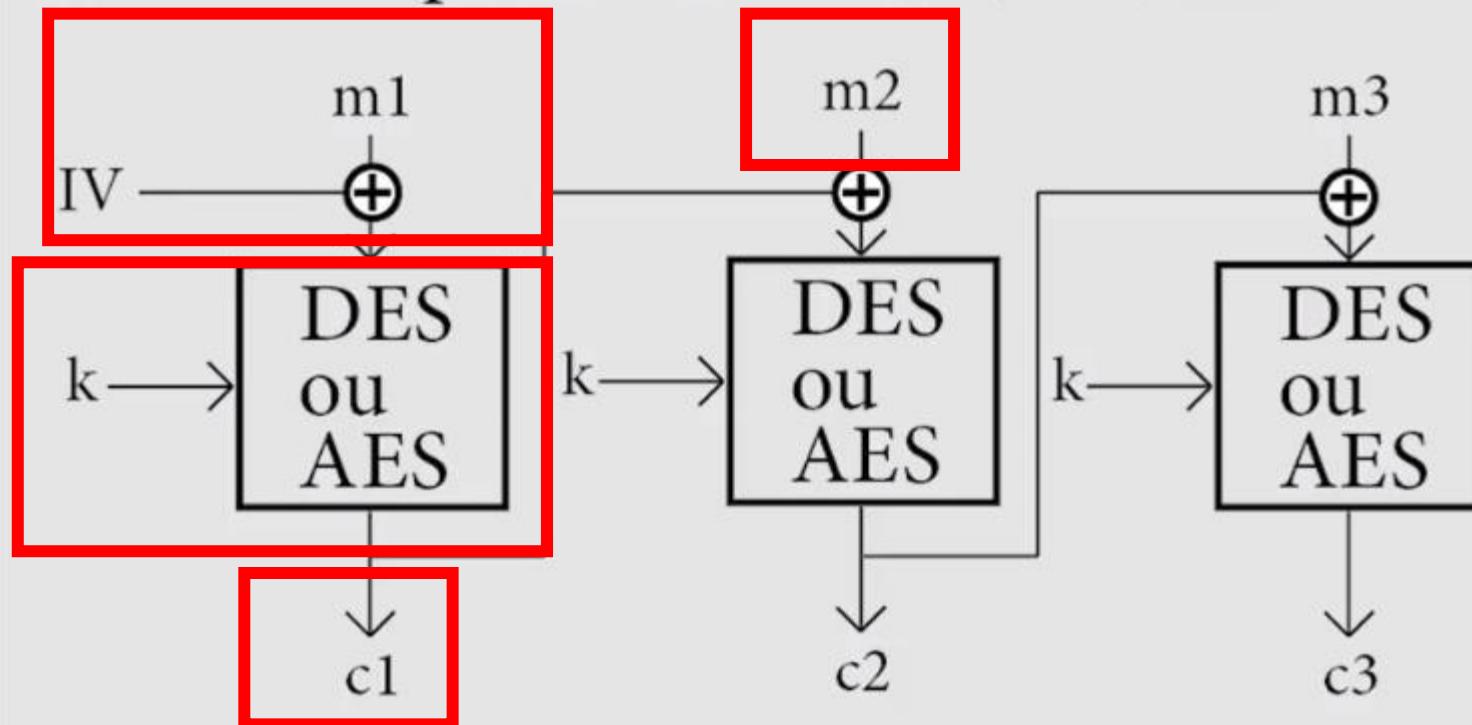


c est construit avec les 3 blocs c_1, c_2 et c_3



Cipher Block Chaining (CBC)

m est découpé en 3 blocs: m_1, m_2, m_3



c est construit avec les 3 blocs c_1, c_2 et c_3



Confidentialité et chiffrement

Chiffrement asymétrique

Dans un système asymétrique, le récepteur génère une paire de clés asymétrique : une clé publique qui est diffusée à tout le monde et une clé privée maintenue secrète chez le récepteur. La particularité de cette paire de clé est que tout message chiffrée avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante. D'où la confidentialité des messages chiffré avec la clé publique d'un récepteur. Bien évidemment la clé privée correspondante ne peut être calculée à partir de la clé publique correspondante.



Confidentialité et chiffrement

Algorithmes de chiffrement asymétrique

RSA: Rivest, Shamir et Adleman 1978

El Gamal Diffie et Hellman 1976

RSA : Rivest Shamir et Adleman 1978

Principe de RSA

RSA est fondé sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.

Crypto-graphiquement parlant, on peut dire que multiplier deux grands nombres premiers est une fonction à sens unique: Il est facile de multiplier deux nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.

RSA : Rivest Shamir et Adleman 1978

Principe de RSA

RSA est fondé sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.

Crypto-graphiquement parlant, on peut dire que multiplier deux grands nombres premiers est une fonction à sens unique: Il est facile de multiplier deux nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.

RSA : Rivest Shamir et Adleman 1978

Algorithme RSA

Initialisation

Choisir deux nombres premiers, p et q , les deux étant plus grands que 10Exposant100.

Calculer $n = p \cdot q$ (n est le modulus)

Choisir e aléatoire tel que e et $((p - 1) \cdot (q - 1))$ n'aient aucun facteur commun excepté 1

Trouver d tel que : $ed \equiv 1 \pmod{(p - 1)(q - 1)}$.

Clé publique : (n, e) .

Clé privée : (n, d) ou (p, q, d) si on désire garder p et q .

RSA : Rivest Shamir et Adleman 1978

Algorithme RSA

Chiffrement/Déchiffrement

L'expéditeur crée le texte chiffré c à partir du message m : $c = m^{expe} \text{ mod}(n)$, où (n,e) est la clé publique du destinataire

Le destinataire reçoit c et effectue le déchiffrement : $m = c^{expd} \text{ mod}(n)$, où (n,d) est la clé privée du destinataire.

RSA : Rivest Shamir et Adleman 1978

Sécurité de RSA

Ce qui est connus est la clé publique (e, n)

Pour déchiffrer un message m , il faut connaître d tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$

Pour calculer d il faut donc connaître p et q

Or on sait que $n = pq$ et on connaît n

Il faut donc factoriser n en ses facteurs premiers p et q

Or personne n'a pu le faire en un temps raisonnable.

Signature Numérique

La signature numérique est un moyen essentiel pour garantir l'authenticité et l'intégrité des données dans un monde numérique en évolution rapide.

Principes de la Signature Numérique

1

Authentification

La signature numérique permet de vérifier l'identité de l'émetteur d'un message ou d'un document.

2

Intégrité des données

Elle garantit que les données n'ont pas été modifiées depuis leur signature initiale.

3

Non-Répudiation

Elle empêche l'émetteur de nier avoir envoyé le message ou le document signé.

Fonctionnement de la Signature Numérique

1. Clé Privée

L'émetteur utilise sa clé privée pour signer le message ou le document.

2. Clé Publique

La signature est vérifiée à l'aide de la clé publique de l'émetteur.

3. Hash Cryptographique

Un hash cryptographique est utilisé pour garantir l'intégrité des données.

Avantages de la Signature Numérique

Fiabilité



La signature numérique offre un niveau élevé de fiabilité et de confiance dans les communications et les transactions en ligne.

Efficacité



La signature numérique permet d'économiser du temps et des ressources en automatisant les processus de validation.

Gain de Place



Elle élimine le besoin de documents papier et de stockage physique, réduisant ainsi les coûts.

Utilisations de la Signature Numérique



INSTANT DOWNLOAD



Contrats Électroniques

Les signatures numériques sont couramment utilisées pour sécuriser les contrats électroniques et les accords commerciaux.

Communications Electroniques

Elles garantissent l'authenticité et l'intégrité des e-mails et des documents électroniques.

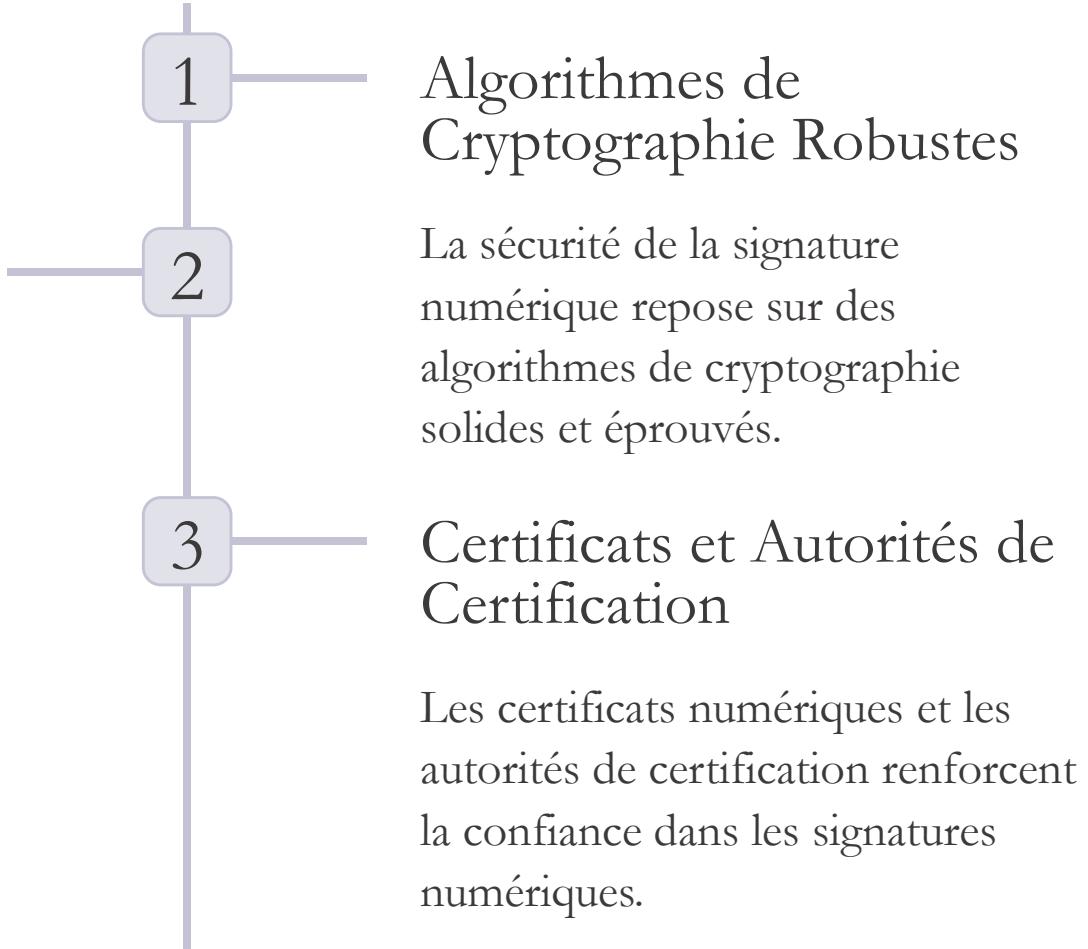
Développement de Logiciels

Elles sont utilisées pour vérifier l'authenticité et l'intégrité des logiciels téléchargés.

Sécurité de la Signature Numérique

Protection des Clés Privées

Il est essentiel de protéger les clés privées contre l'accès non autorisé.



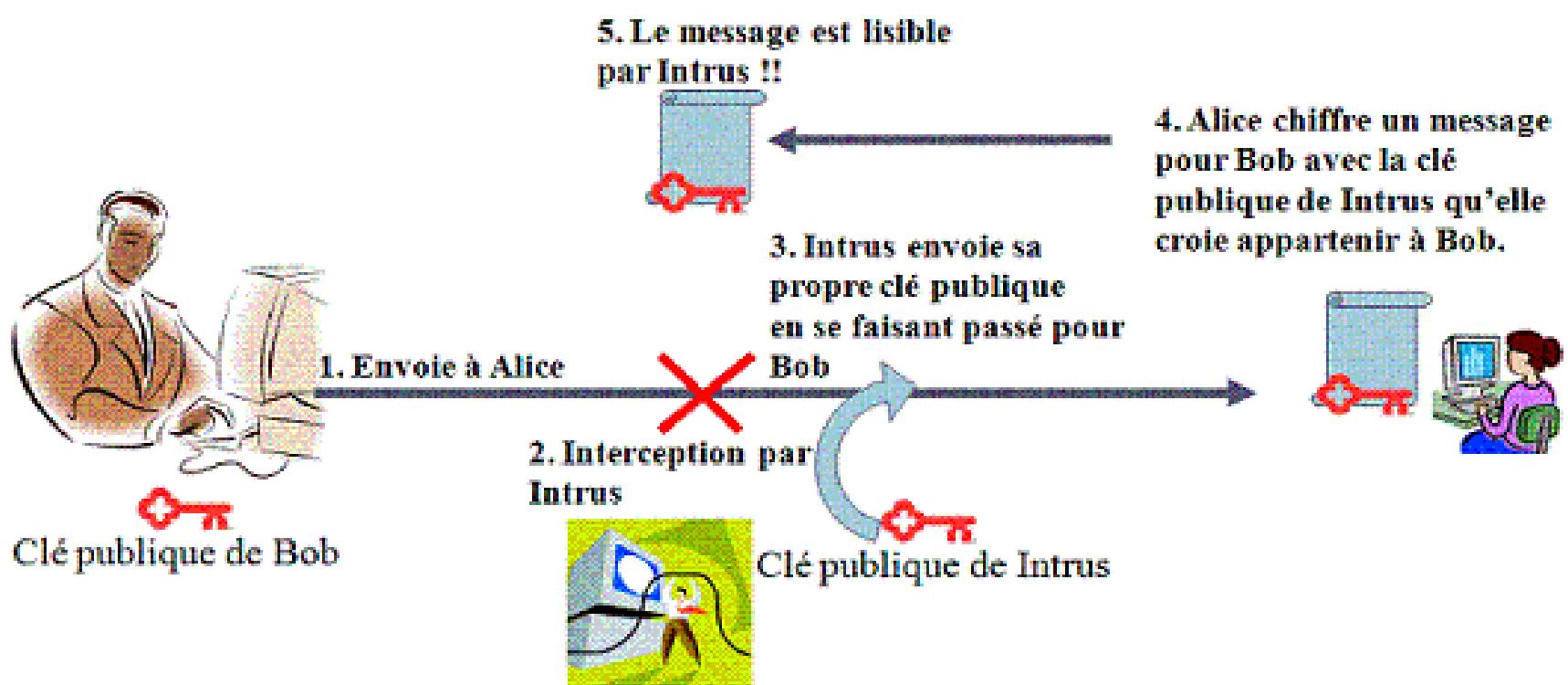
Systèmes asymétriques : limites



Systèmes asymétriques : limites

Comment garantir qu'une clé publique correspond bien à l'entité avec qui on communique ?

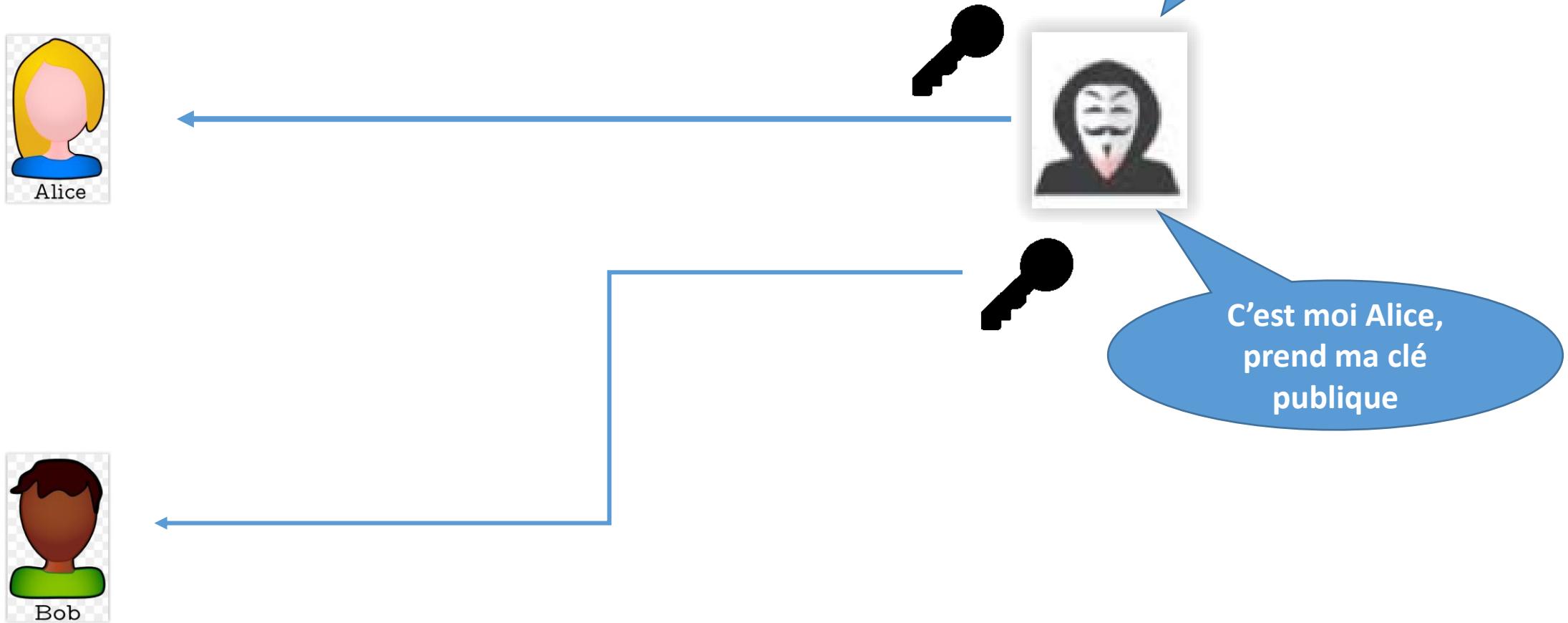
Jusque là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type "Man in the Middle". Une telle attaque est illustrée dans le scénario ci-après.



Certification numérique

La solution au problème dit "man in the middle" est l'usage d'un certificat numérique qui assure la liaison entre l'identité et la clé publique correspondante dans un document numérique signé par une tierce partie de confiance dite autorité de certification.

Systèmes asymétriques : limites



La certification numérique

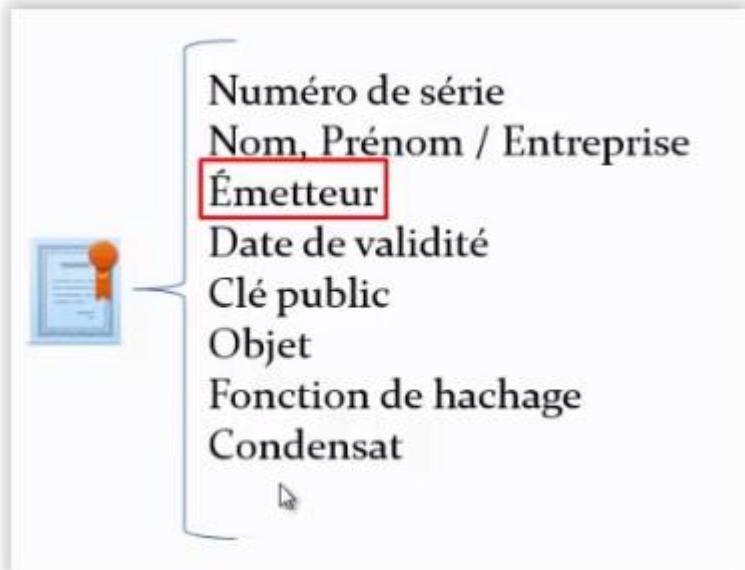
Certificat numérique

Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations.

C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.

Un certificat est signé numériquement par une autorité de certification à qui font confiance tous les usagers et dont la clé publique est connue par tous d'une manière sécurisée.

La certification numérique



La certification numérique

Structure d'un certificat X.509

Version

Numéro de série

Algorithme de signature du certificat

Signataire du certificat

Validité (dates limite)

Pas avant

Pas après

Détenteur du certificat

Informations sur la clé publique

Algorithme de la clé publique

Clé publique

Identifiant unique du signataire (Facultatif)

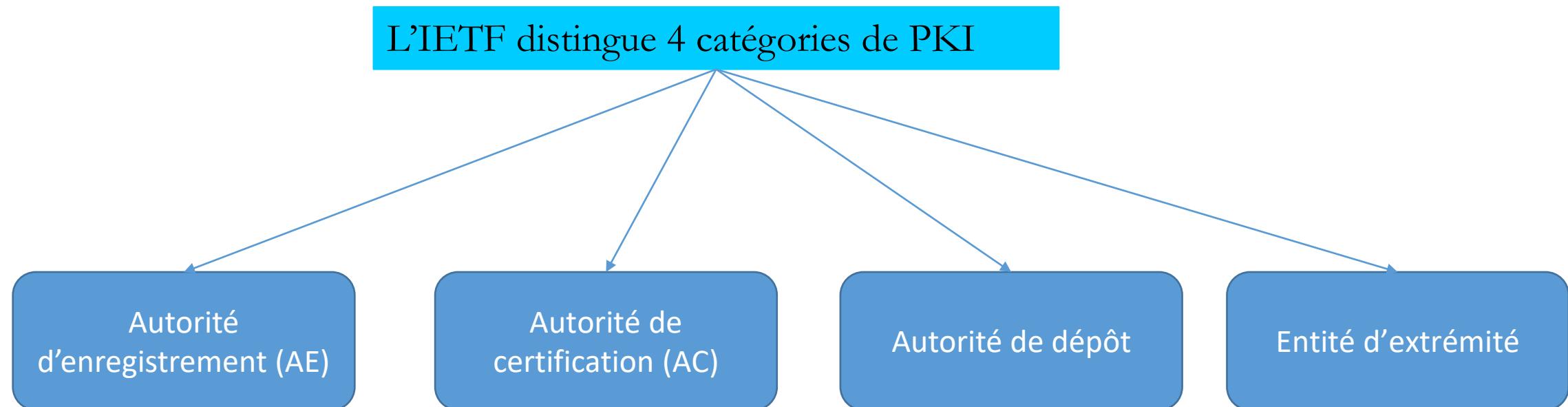
Identifiant unique du détenteur du certificat (Facultatif)

Extensions (Facultatif)

Liste des extensions...

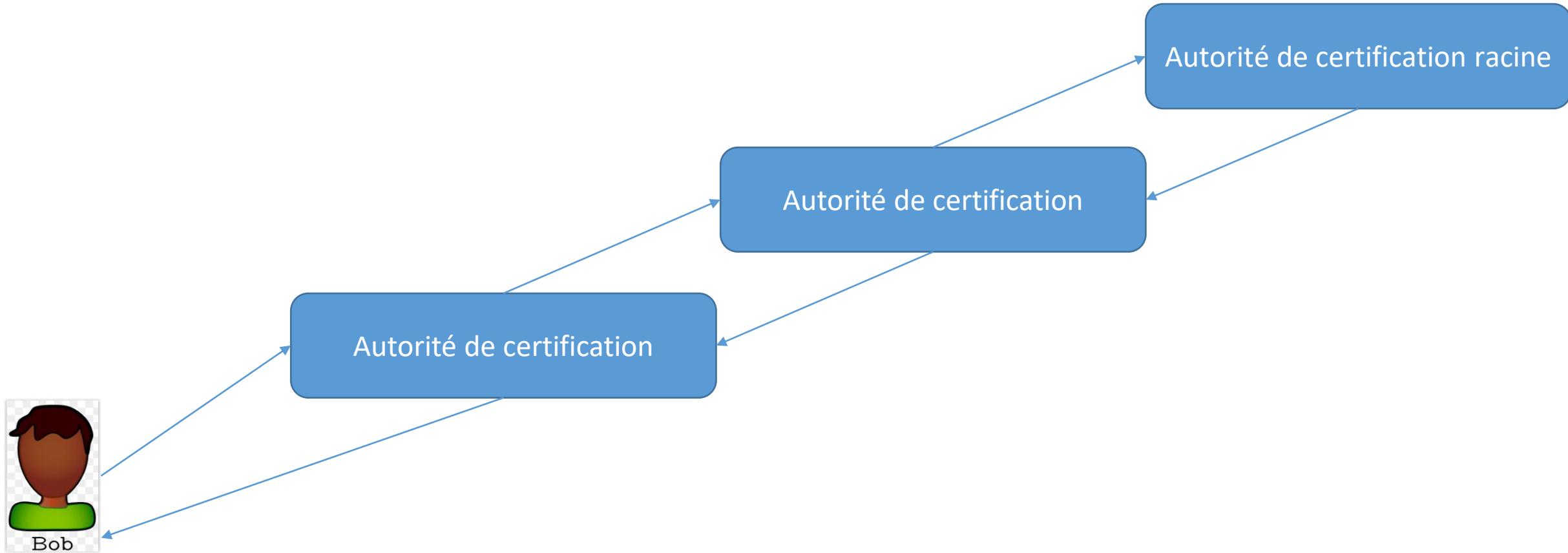
La certification numérique

Les PKI: Public Key Infrastructure/ Infrastructure à clés publiques



La certification numérique

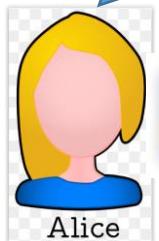
Les autorités de certification



La certification numérique

Comment ça se passe

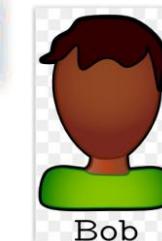
Je veux discuter avec
toi en HTTPS



Attestes que
c'est lui ?

Autorité de
certification

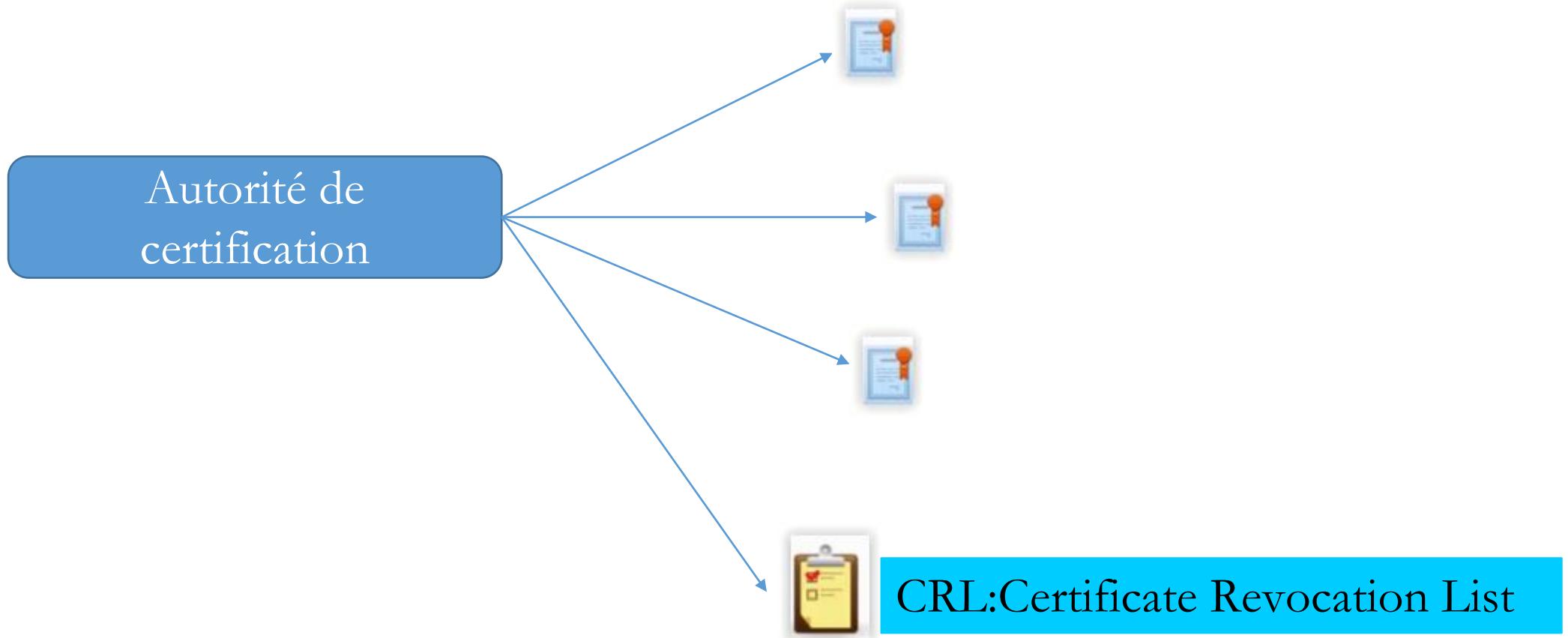
Ok, Voici le certificat qui
prouve bien que je suis celui
que vous recherchez et maclé
publique



Oui c'est bien lui

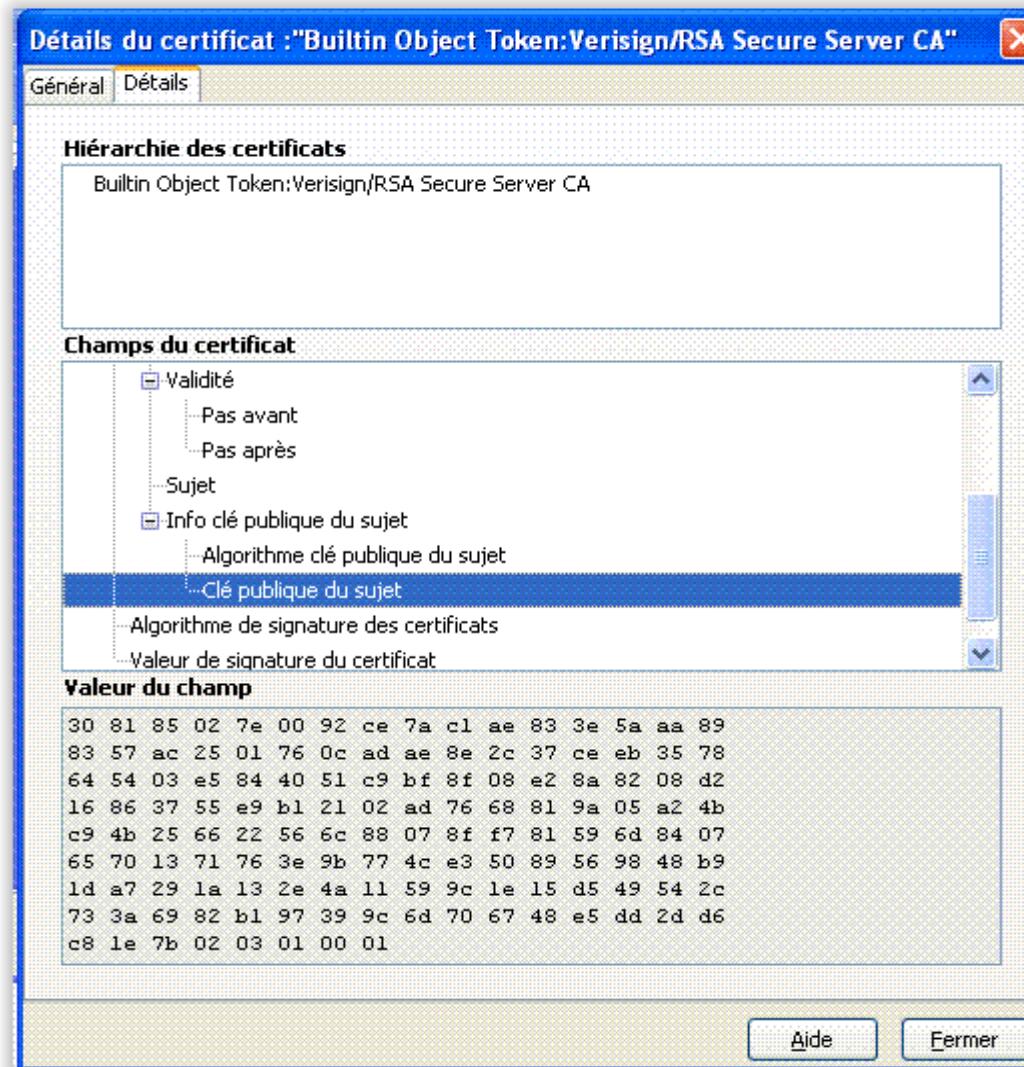
La certification numérique

Révocation de certificats



La certification numérique

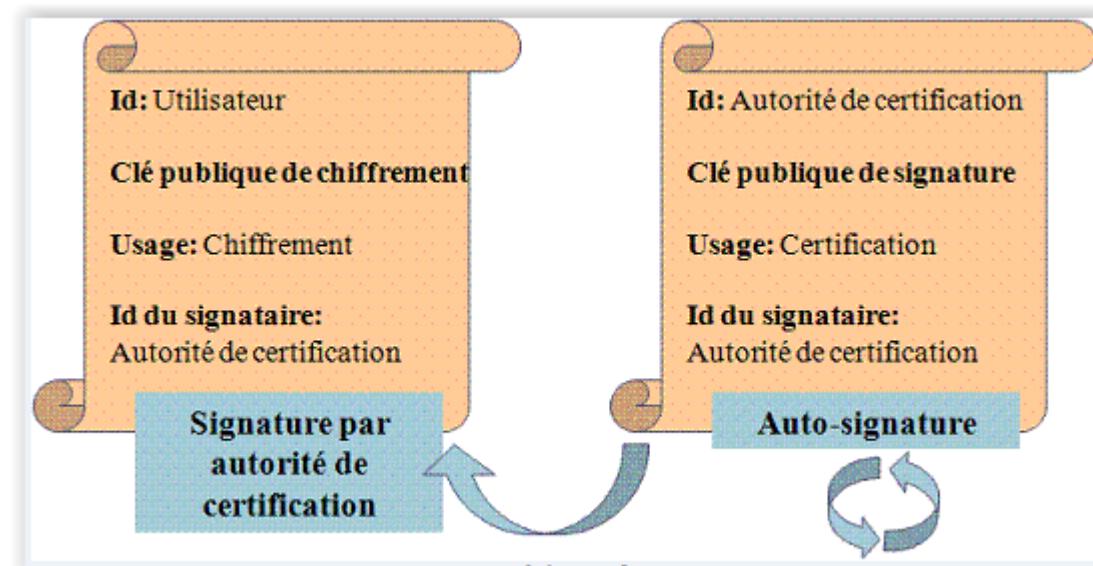
La figure suivante illustre un tel certificat inclus dans un navigateur web



La certification numérique

Autorité de certification

Une autorité de certification est toute entité qui délivre des certificats de clé publique



La certification numérique

Auto signature

Une autorité de certification auto-signé son certificat numérique. ceci ne posant pas de problème puisque la clé publique d'une autorité de certification est censée connue d'une manière sécurisée (remise en main propre pas exemple).

Autorité de certification et confiance

L'autorité de certification certifie la correspondance Clé publique – Identité pour l'ensemble d'une population. Ceci mène à faire régner la confiance par transitivité :

- A fait confiance à l'Autorité de Certification
- L'Autorité de Certification délivre un certificat à B
- A est assuré de l'identité de B

Normes et Protocoles de la Signature Numérique

Normes	Protocoles
PKCS#7	HTTPS
XAdES	S/MIME
PAdES	XML-DSig

Secure Socket Layer : SSL

Aperçus générale

SSL/TLS est un protocole de sécurisation des échanges développé par Netscape. Il assure les transactions Client / Serveur sur Internet. Il a été intégré dans les navigateurs web depuis 1994. La version 3.1 est baptisée Transport Layer Security TLS. Cette version a été standardisée à l'IETF: RFC 2246. Le protocole fonctionne au dessus de la couche TCP

Secure Socket Layer : SSL

Services de sécurité assurés par SSL

Confidentialité

- Obtenue par chiffrement symétrique

Intégrité

- En utilisant des MAC : MD5(128 bits), SHA1(160 bits)

Authentification

- Identification des deux entités (client optionnel) basée sur les certificats X.509
- Authentification de l'origine des données basée sur des MAC

Secure Socket Layer : SSL

Déroulement du protocole SSL

SSL se déroule en deux phases

- Phase 1: authentification du serveur
- Phase 2: authentification du client

Testez vos connaissances

Chiffrement symétrique

Garantie la confidentialité du message chiffré

Utilise une paire de clés publique/privée

Assure la non répudiation

Repose sur la confidentialité de la clé utilisée

Repose sur la confidentialité de l'algorithme de chiffrement utilisé

Testez vos connaissances

RSA

Est un système cryptographique asymétrique

Repose sur la difficulté de factoriser un grand nombre en ses facteurs premiers

Repose sur la difficulté du logarithme discret

Permet de faire une signature digitale

Ne peut pas être utilisé pour assurer la confidentialité

Testez vos connaissances

Pour garantir la non-répudiation de l'origine, on peut utiliser

Un chiffrement RSA avec la clé privée de l'émetteur

Un MAC

Une signature digitale

Un chiffrement RSA avec la clé publique de l'émetteur

Un échange de clé Diffie-Hellman

Testez vos connaissances

L'objectif d'un certificat numérique est d'assurer

La confidentialité de la signature numérique du porteur du certificat

L'authenticité de la clé publique correspondante à la clé privée du porteur du certificat

La correspondance entre l'identité et la clé publique correspondante à la clé privée du porteur du certificat

L'authenticité de la signature numérique de l'autorité de certification

Testez vos connaissances

Le protocole SSL/TLS permet d'assurer

Le contrôle d'intégrité

La confidentialité des échanges entre le client et le serveur

L'authentification de l'origine de données

L'authentification du serveur optionnellement

L'authentification du client optionnellement