Cryptographie

module complémentaire

DUT SRC – IUT d'Arles – 2010-2011

xavier.heurtebise@univ-provence.fr

http://x.heurtebise.free.fr

Objectifs de ce cours (PPN)

1. **Comprendre les concepts essentiels de cryptographie**
   - chiffrement et déchiffrement
   - hachage
   - cryptographie à clé publique/privée
   - signature
   - zero-knowledge

2. **Comprendre les protocoles et modes de fonctionnement**
   - étude des protocoles élémentaires (SSL, TLS, HTTPS)
   - algorithmes usuels rencontrés dans le domaine des services
   - modes de protection des données
   - attaques existantes
   - autorités de certification

Organisation du cours

- Le cours de cryptographie s'organise provisoirement en :

1. 2h de CM
2. 3h de TD
3. 5h de TP
4. 2 évaluations :
   a. Contrôle continu de 2h (coefficient 2)
   b. Compte rendu de TP (coefficient 1)

Total : 12h

Plan

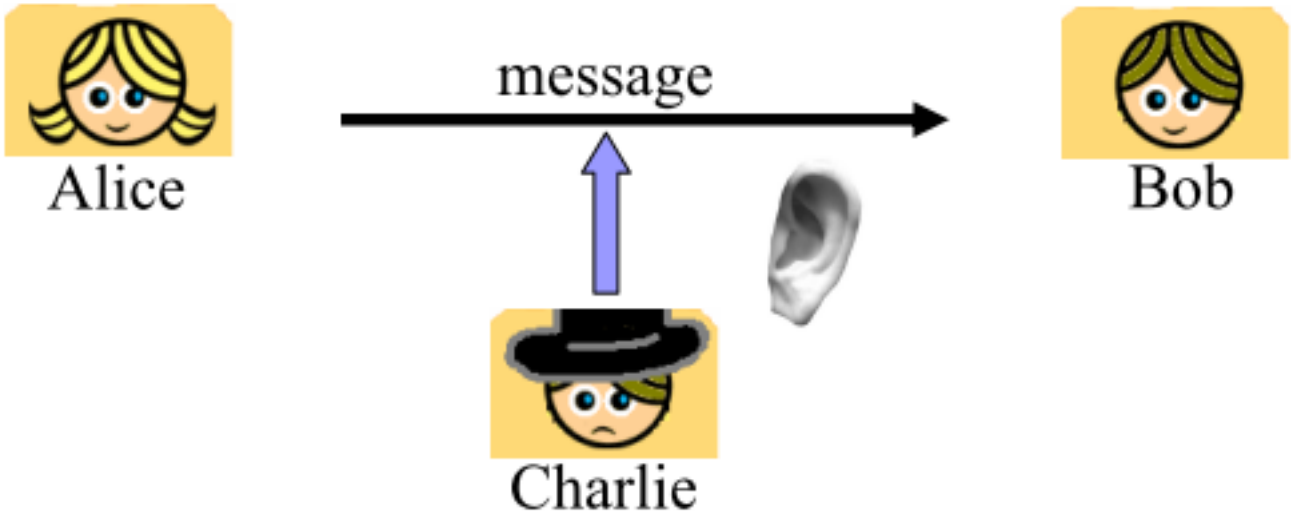
1. **Introduction**
   - Terminologie
   - Mécanismes et services de sécurité
2. **Algorithmes de cryptographie**
   - Chiffrement simple
   - Chiffrement symétrique
   - Chiffrement asymétrique
3. **Intégrité et authentification**
   - Fonctions de hachage, scellement et signature
   - Authentification mutuelle et échange de clefs de session
   - Principe de certification
4. **Protocoles sécurisés**
5. **Législation française**
6. **Conclusion**

Chapitre 1

INTRODUCTION

Menaces : utilité de la cryptographie

- **Attaques passives**

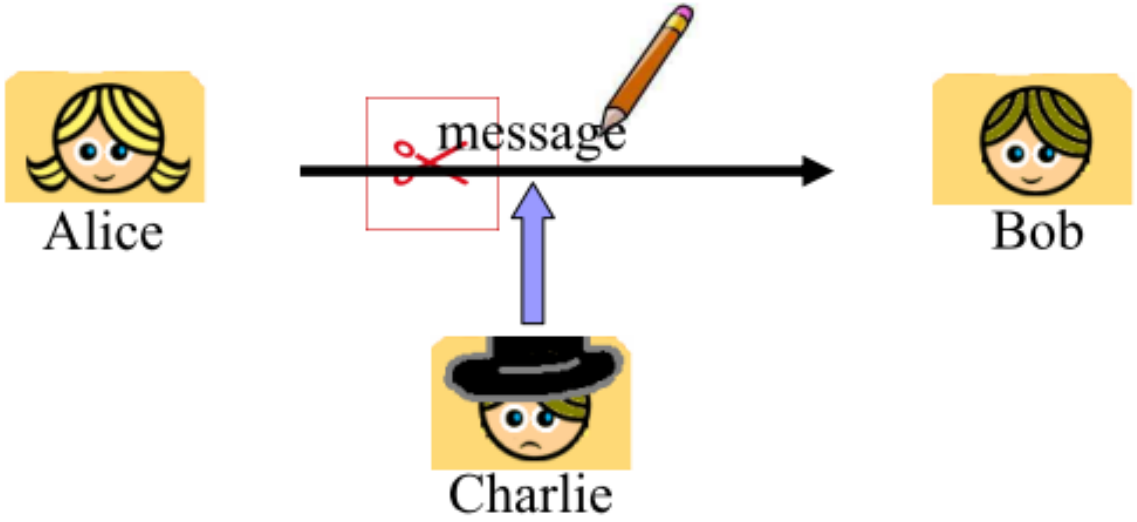


- Menace contre la **confidentialité** de l'information :

→ une information sensible parvient à une personne autre que son destinataire légitime

Menaces : utilité de la cryptographie

- **Attaques actives : interventions sur la ligne**



  - Menace contre l'**intégrité** et l'**authenticité** de l'information
  - Exemples :
    - Impersonification : modification de l'identité de l'émetteur / récepteur
    - Altération des données (modification du contenu)
    - Destruction des données
    - Retardement de la transmission
    - Répudiation du message = l'émetteur nie l'envoi du message

Services de sécurité

- Fournir un certain nombre de services de sécurité

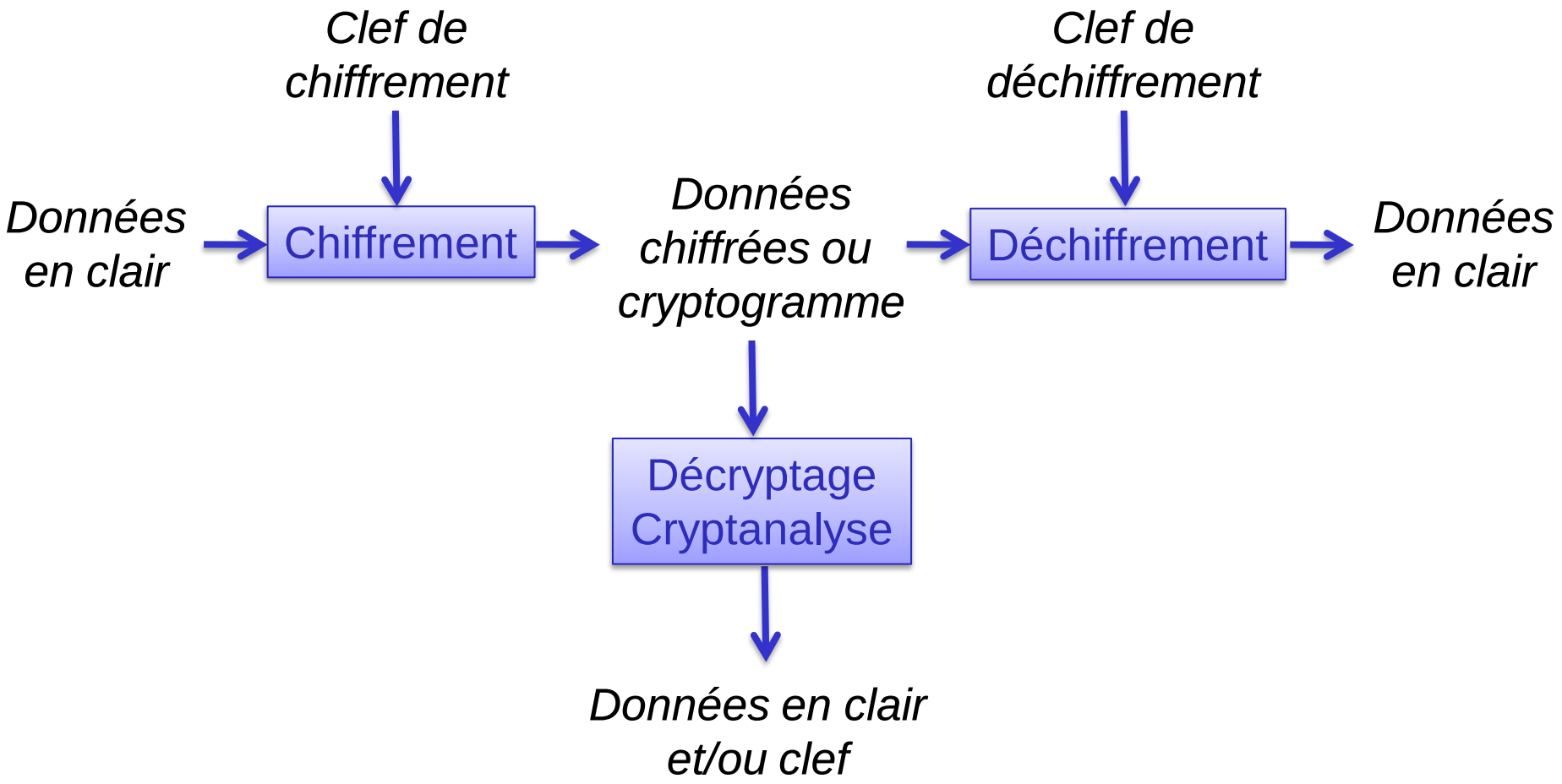
1. ***Confidentialité***
   - Fait de garder quelque chose privé et secret vis-à-vis de tout le monde sauf de ceux qui sont autorisés à le voir.
2. ***Intégrité***
   - Assurance que les données n'ont pas été modifiées (par des personnes non autorisées) pendant le stockage ou la transmission
3. ***Authentification*** de l'origine des données ou d'un tiers
   - Assurance qu'un tiers non autorisé n'est pas à l'origine des données
4. ***Non-répudiation***
   - Assurance que l'émtteur ne puisse pas nier l'envoi d'un message.
5. ***Preuves à divulgation nulle de connaissance***
   - Désigne un protocole sécurisé dans lequel un tiers veut prouver au second tiers qu'il connait une information, mais sans lui dévoiler.

Mécanismes et services de sécurité

- **Moyens mis en œuvre :**
  - Mécanismes de sécurité construits au moyen d'outils cryptographiques (fonctions, algorithmes, générateurs aléatoires, protocoles…)
    - Chiffrement / déchiffrement
    - Scellement et signature
    - Certification
    - Protocoles d'authentification mutuelle avec échange de clefs

- **Cryptologie**
  - Science regroupant :
    - La cryptographie
    - Et la cryptanalyse

Principe d'une transmission sécurisée



Cryptographie

- **Définition :**
  - Conception de mécanisme de cryptologie destinés à garantir les notions de sécurité à des fins de :
    - **confidentialité**,
    - d'**authenticité**
    - et d'**intégrité** de l'information,
  - mais aussi pour d'autres notions comme :
    - l'**anonymat**
    - et la **non-répudiation** de l'information

Cryptanalyse

- **Définition :**
  - Reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques.

- **Pourquoi ?**
  - Tout cryptosystème doit nécessairement être **résistant** aux méthodes de cryptanalyse.
  - Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un crypto-système, on dit alors que l'algorithme de chiffre-ment a été « **cassé** ».

- On appellera « **attaque sur texte** » une méthode de cryptanalyse permettant de déchiffrer un message donné.

Cryptanalyse

- **Méthodes d'attaque :**
  - attaque texte chiffré seul (*cyphertext-only attack*) :
    - l'attaquant possède une copie du texte chiffré.
  - attaque texte clair connu (*known plaintext attack*) :
    - l'attaquant possède une copie du texte clair et une copie du texte chiffré.
  - attaque texte clair choisi (*chosen plaintext attack*):
    - l'attaquant possède temporairement un accès à la machine de chiffrement. Il peut choisir librement un texte clair et le chiffrer.
  - attaque texte chiffré choisi (*chosen cyphertext attack*) :
    - l'attaquant possède temporairement un accès à la machine de déchiffrement et peut choisir des textes chiffrés et les déchiffrer.
  - attaque par force brute (*brute force attack*) :
    - on essaie toutes les clés possibles.
  - attaque par devinette (*riddle attack*) :
    - Soit un espace de clé défini. Si un utilisateur utilise un sous-espace seulement (par exemple seulement des mots français) on peut facilement faire une recherche sur les mots français. Ceci réduit grandement le nombre de clés possibles.

Chapitre 2

ALGORITHMES DE CRYPTOGRAPHIE

Confidentialité et algorithmes

- **Il existe trois types d'algorithmes**

1. Algorithmes de substitution ou chiffrement simple
2. Algorithmes symétriques ou à clef privée
3. Algorithmes asymétriques ou à clef publique

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Définition :**

Le chiffrement **simple** ou **par substitution** qui consiste à remplacer dans un message une ou plusieurs entités par une ou plusieurs autres entités.

Exemples d'entité : lettre, octet, entité de 8/16/24/32 bits ou +

- **Types de chiffrement par substitution :**

monoalphabétique	remplacer chaque lettre du message par une autre lettre
polyalphabétique	utiliser une suite de chiffres monoalphabétique réutilisée périodiquement
homophonique	faire correspondre à chaque lettre du message un ensemble possible d'autres caractères
polygrammes	substituer un groupe de caractères dans le message par un autre groupe de caractères

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Exemples d'algorithmes de chiffrement simples**
  - Décalage de lettres dans l'alphabet
    - ROT13
    - Chiffre de César
    - Chiffre de Vigenère
  - Remplacement des lettres par des symboles
    - Code Morse
    - Code musical
    - Alphabet des templiers

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Exemple de chiffrement monoalphabétique :**
  - Alphabet Morse :
    - code permettant de transmettre un teste à l'aide de séries d'impulsions courtes et longues
      - 1835 : télégraphie
      - Aujourd'hui : application militaire, aviation, transpondeurs…

Morse Code Table

A	.-	N	-.	1	.----	.	.-.-.-
B	-...	O	---	2	..---	,	--..--
C	-.-.	P	.--.	3	...--	?	..--..
D	-..	Q	--.-	4	....-	(	-.--.
E	.	R	.-.	5	.....	)	-.--.-
F	..-.	S	...	6	-....	-	-....-
G	--.	T	-	7	--...	"	.-..-.
H	....	U	..-	8	---..	_	..--.-
I	..	V	...-	9	----.	'	.----.
J	.---	W	.--	0	-----	:	---...
K	-.-	X	-..-	/	-..-.	;	-.-.-.
L	.-..	Y	-.--	+	.-.-.	$	...-..-
M	--	Z	--..	=	-...-		

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Exemple de chiffrement monoalphabétique :**
  - Alphabet Morse :
    - Soit le texte en clair :

      JE SUIS VENU, J'AI VU, J'AI VAINCU

    - Et le texte codé en Morse :

      .--- . ... ..- .. ..- . -. ..- --.--
      .--- .- .. ...- ..- --.--
      .--- .- .. ...- .- .. -. -.-. ..-

  - Chiffre de César :
    - Décalage de lettres de *n* rangs dans l'alphabet
    - Soit le texte en clair

      JE SUIS VENU, J'AI VU, J'AI VAINCU

    - Et le texte codé avec le « chiffre de César » ***n* = 3** :

      MH VXLV YHQX, M'DL YX, M'DL YDLQFX

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Etude du « Chiffre de César » :**
  - Avantage
    - Très simple, rapide à mettre en œuvre
    - Relativement efficace pendant la période de l'antiquité.
  - Inconvénient
    - A l'apogée de la civilisation musulmane, les mathématiciens arabes trouvèrent un moyen de casser le cryptage des textes cryptés avec une substitution alphabétique.
  - Comment ont-ils fait ?
    - Ils ont utilisés une caractéristique propre à chaque langue : la fréquence d'utilisation de chaque lettre de l'alphabet.

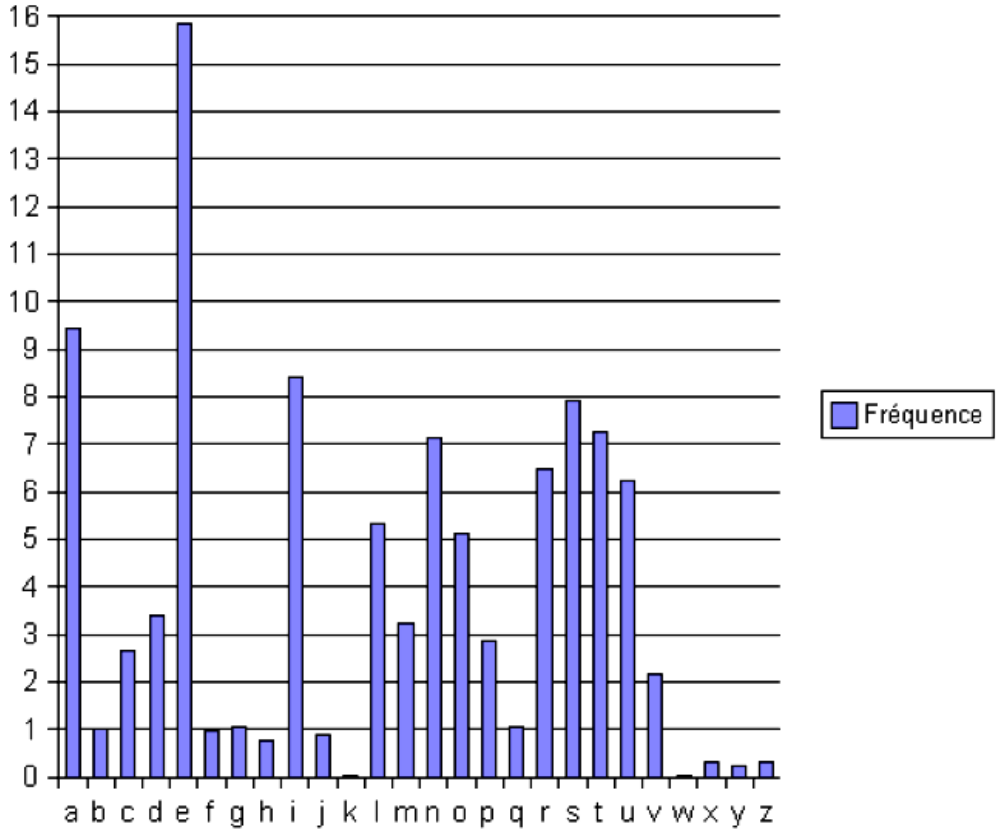
Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Etude du « Chiffre de César »:**
  - Table des fréquences pour l'alphabet français

Résultats tirés du livre « ***Histoire des codes secrets*** »de Simon Singh



Histogramme des fréquences.

Chiffrement par substitution

Chiffrement

- **Substitution**
  - Défiinition
  - Types
  - Algorithmes
  - Exemples
    - Morse
    - César
  - Limites
- **Symétrique**
- **Asymétrique**

- **Limites du chiffrement par substitution**

  - Le chiffrement de par substitution se casse facilement, car les lettres sont toujours codées de la même façon.

  - Si l'attaquant ne possède que le message chiffré, il réalisera une cryptanalyse de la fréquence de chaque symbole ou chaque groupe de symboles pour tenter d'en extraire le message en clair.

  → c'est ce que l'on appelle « **attaque texte chiffré seul** »

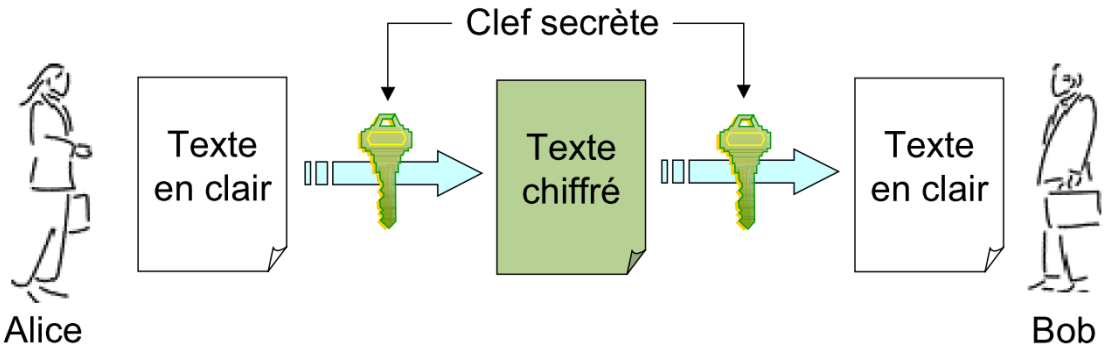
Chiffrement symétrique

Chiffrement

- **Substitution**
- **Symétrique**
  - Définition
  - Principe
  - Problèmes
  - Algorithmes
- **Asymétrique**

- **Définition :**

Le chiffrement **symétrique** (ou *chiffrement à clé privée*) consiste à utiliser la même clé pour le chiffrement et le déchiffrement.



- **Principe :**
  - Le chiffrement symétrique consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles.
  - On donne le message à quelqu'un et on lui fournit la clé privée, pour qu'il puisse déchiffrer le message.

Chiffrement symétrique

Chiffrement

- **Substitution**
- **Symétrique**
  - Définition
  - Principe
  - Problèmes
  - Algorithmes
- **Asymétrique**

- **Problèmes :**
  - Longueur de la clé privée :
    - Selon *Claude Shannon* (années 40) :

      pour être totalement sûr, les systèmes à clefs privées doivent utiliser **des clefs d'une longueur au moins égale à celle du message à chiffrer**.
  - Canal sécurisé :
    - Le chiffrement symétrique impose d'avoir un **canal sécurisé pour l'échange de la clé**, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.
  - Nombres de clés :
    - Pour un groupe de *N* personnes utilisant un cryptosystème à clés secrètes avec un niveau de sécurité maximal, il est nécessaire de distribuer un **nombre de clés égal à *N * (N-1) / 2***.

Chiffrement symétrique

Chiffrement

- **Substitution**
- **Symétrique**
  - Définition
  - Principe
  - Problèmes
  - Algorithmes
- **Asymétrique**

- **Algorithmes existants :**
  - Algorithme de chiffrement à flot ou en continu
    - Agissent sur un bit à la fois
    - Le plus courant :
      - RC4 (longueur de clef variable) et RC5
  - Algorithme de chiffrement par blocs
    - Opère sur le message en clair par blocs de *n* bits
    - Exemples :
      - DES (clef de 56 bits codée sur 64 bits)
      - IDEA ou CAST-128 (clef de 128 bits)
      - Blowfish (longueur de clef variable, jusqu'à 448 bits)
      - AES (Rijndael, longueur de clef variable : 128, 192 ou 256 bits)
  - Fonction de hashage
    - Calcul d'un condensé de n bits d'un message de *m*>*n* bits
    - Exemples :
      - CRC32, MD5, SHA192,…

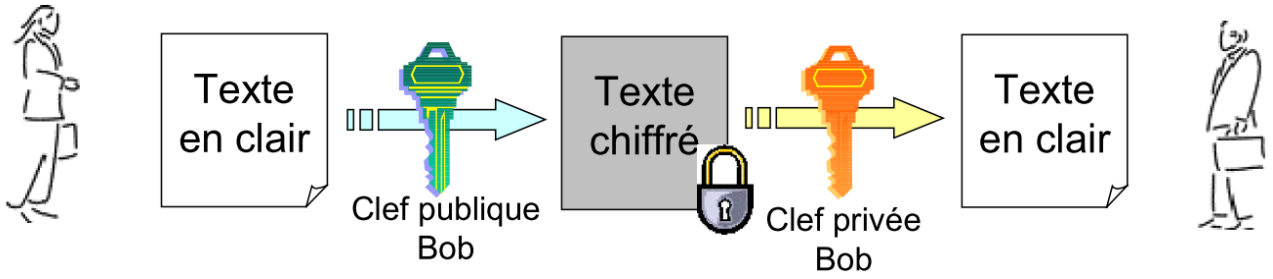
Chiffrement asymétrique

Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

- **Définition :**

Le chiffrement **asymétrique** (ou *chiffrement à clés publiques*) consiste à utiliser une clé publique pour le chiffrement et une clé privée pour le déchiffrement.



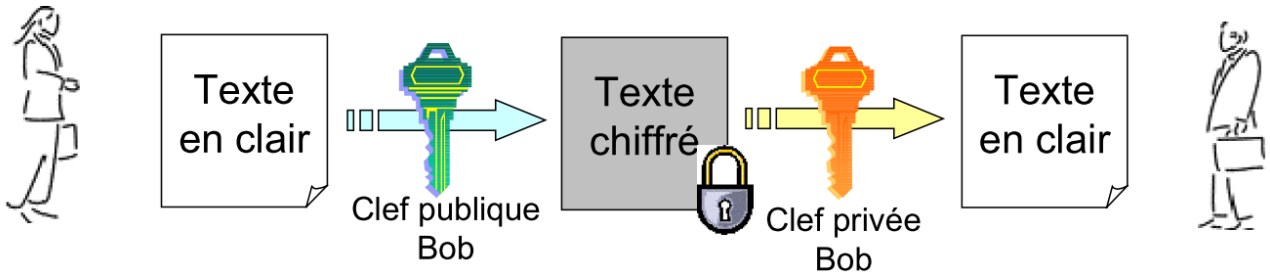
- **Principe :**
  - Les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée).
  - Ils en déduisent chacun automatiquement un algorithme (il s'agit de la clé publique).
  - Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

Chiffrement asymétrique

Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

- **Principe (suite) :**
  - Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire.
  - Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).



- **Historique :**
  - Concept inventé par Diffie & Hellman, 1976
  - Algorithmes :
    - Basés sur des problèmes difficiles à résoudre
    - Trop lents pour une utilisation intensive

Chiffrement asymétrique

Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

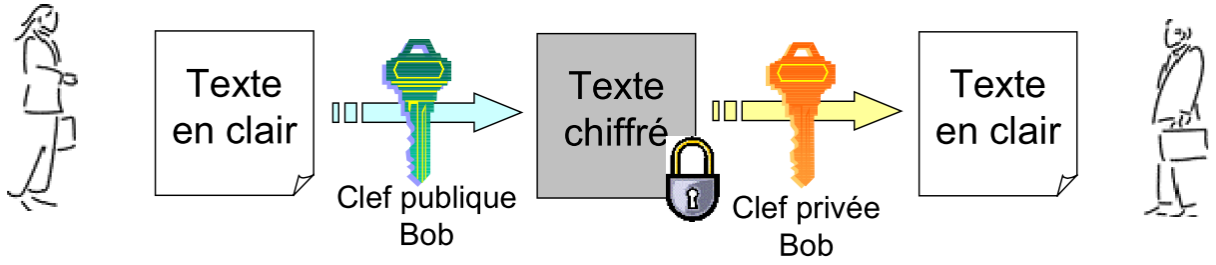
- **Problème :**
  - Algorithmes plus lents que ceux à clef privée
    - Rarement utilisé pour chiffrer les données
    - Mais utilisé pour :
      - *chiffrer une clef de session secrète*
      - *établir une signature*
  - Certains algorithmes sont uniquement adaptés au chiffrement, d'autres à la signature (DSA)
  - Seuls trois algorithmes sont adaptés à la fois au chiffrement et à la signature :
    - RSA, 1978
    - ElGamal
    - Rabin

Chiffrement asymétrique

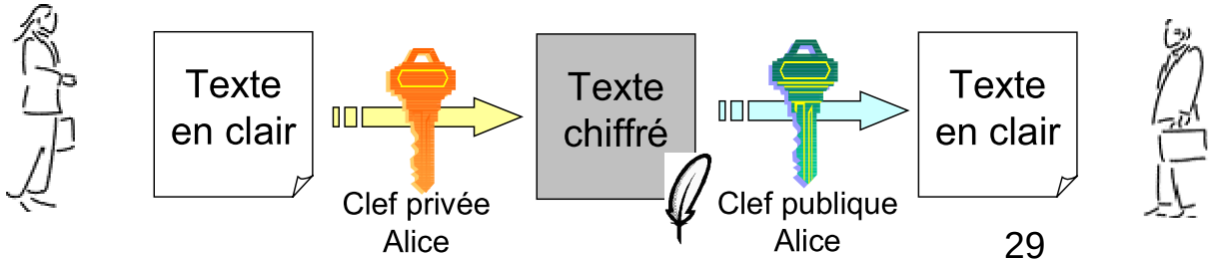
Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

- **Différence entre chiffrement et signature :**
  - Chiffrement :
    - Clef **publique** utilisée pour le chiffrement, seul le détenteur de la clef privée peut déchiffrer



  - Signature :
    - Clef **privée** utilisée pour le chiffrement, seul son détenteur peut chiffrer, mais tout le monde peut déchiffrer (et donc en fait vérifier la « **signature** »)

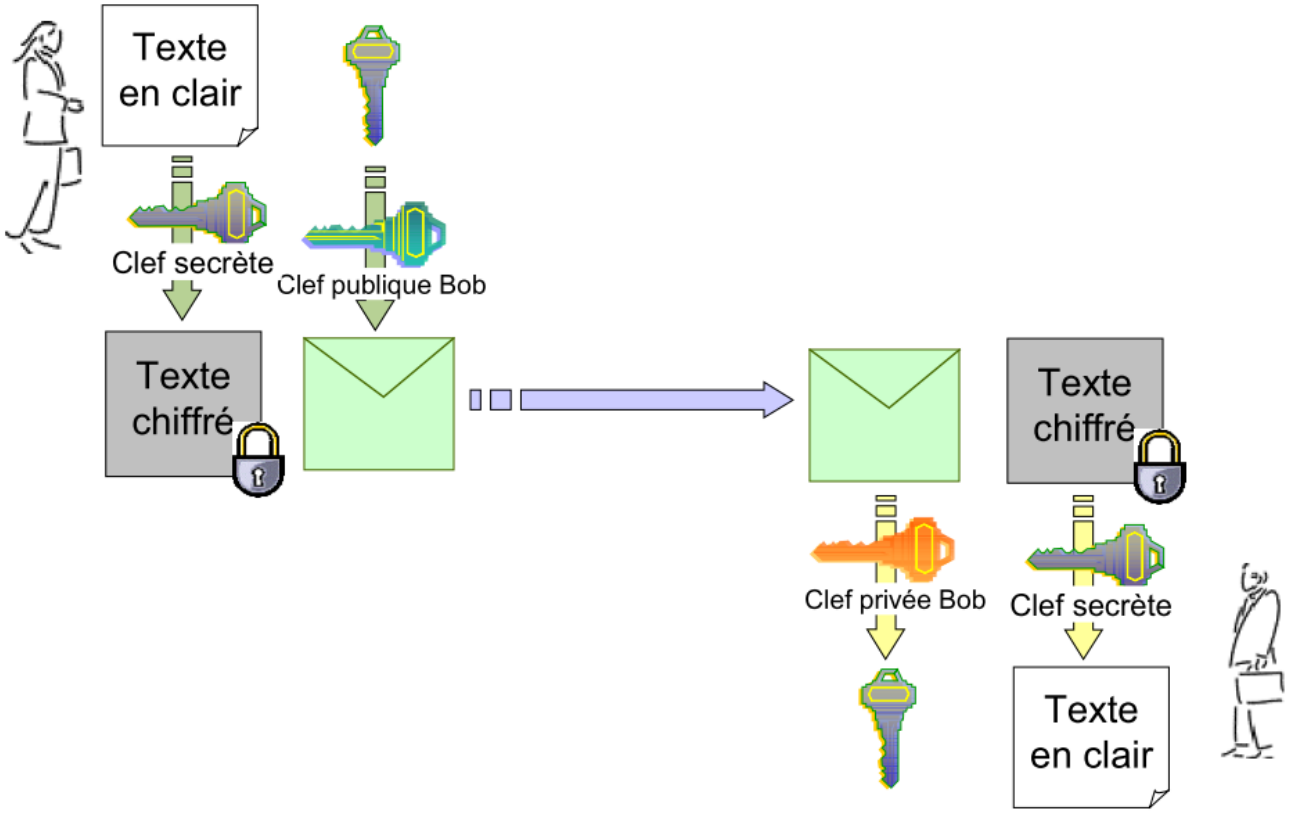


Chiffrement asymétrique

Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

- **Chiffrement de la clef publique à l'aide de la clé secrète :**



Chiffrement asymétrique

Chiffrement

- **Substitution**
- **Symétrique**
- **Asymétrique**
  - Définition
  - Principe
  - Historique
  - Problèmes
  - Chiffrement et signature
  - Chiffrement croisé
  - Longueurs des clés

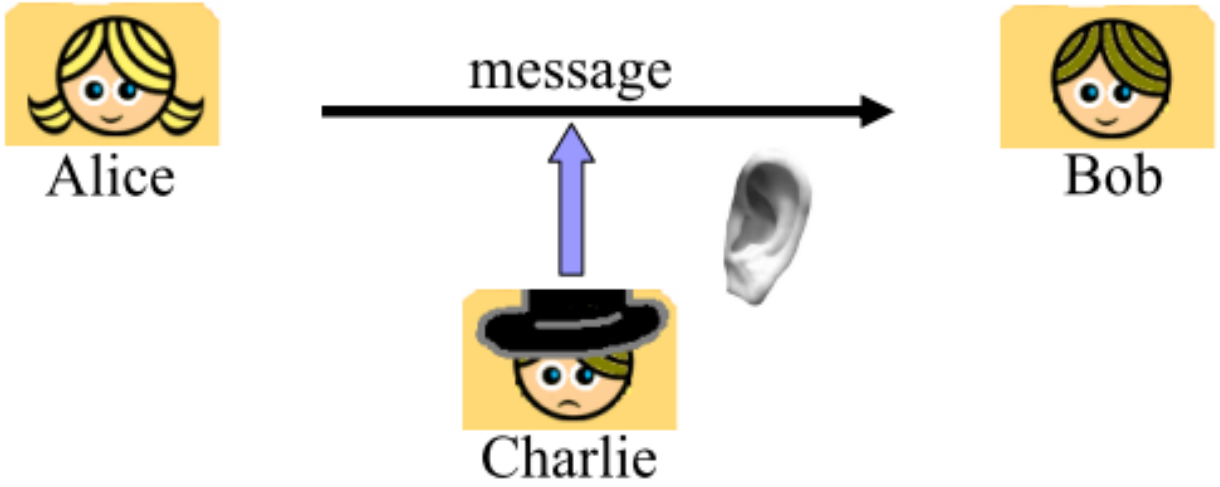
- **Choix des longueurs de clefs :**
  - Attention :
    - Ne pas mélanger les longueurs de clefs publiques et secrètes (en général différentes)
    - Les algorithmes reposent sur des principes différents et utilisent donc comme clef des éléments présentant des caractéristiques (notamment longueur) différentes
  - Cryptanalyse et comparaisons de résistance :
    - Pour des clefs secrètes de longueur *n* bits, la référence est la recherche exhaustive (brute force), qui nécessit 2^{n-1} essais en moyenne
    - Pour des clefs publiques *n*, l'attaquant doit résoudre le problème mathématique sur lequel repose l'algorithme :
      - Factorisation (RSA) : $O(x^n)$, avec n = 1024 bits

Chapitre 3

INTÉGRITÉ ET AUTHENTIFICATION

Introduction

- **Services souhaités par la cryptographie**

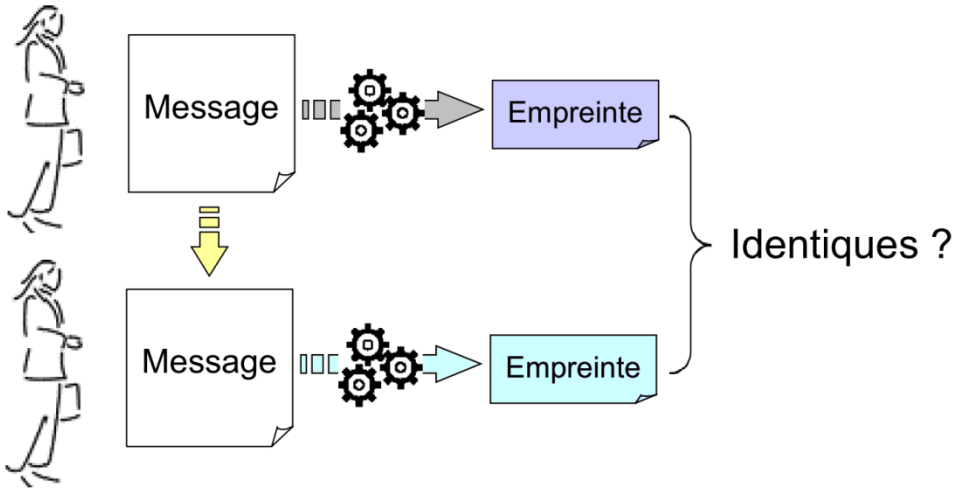


- Confidentialité :
  - Rendre le message secret entre deux tiers
- Authentification :
  - Le message émane t-il de l'expéditeur anoncé ?
- Intégrité :
  - Le message a-t-il été modifié durant le transfert ?

Vérification d'intégrité

- **Définition**
  - Garantir l'intégrité d'un message, c'est vérifier que le message envoyé n'a pas été altéré (intentionnelement ou de manière fortuite) durant la transmission.

- **Principe**
  - Le destinataire calcule le condensé (ou empreinte) du message reçu et le compare avec le condensé accompagnant le message envoyé par l'expéditeurs.



  - Le destinataire et l'expéditeur utilise la même fonction de hachage.
  - Si les deux condensés sont différents, alors le message a été falsifié durant la communication

Authentification

- **Définition**
  - Action de s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication ou d'un fichier.

- **Remarques**
  - Authentification de l’origine des données et intégrité sont inséparables
  - Authenticité = authentification + intégrité
  - « authentification » souvent utilisé pour désigner en fait l’authenticité

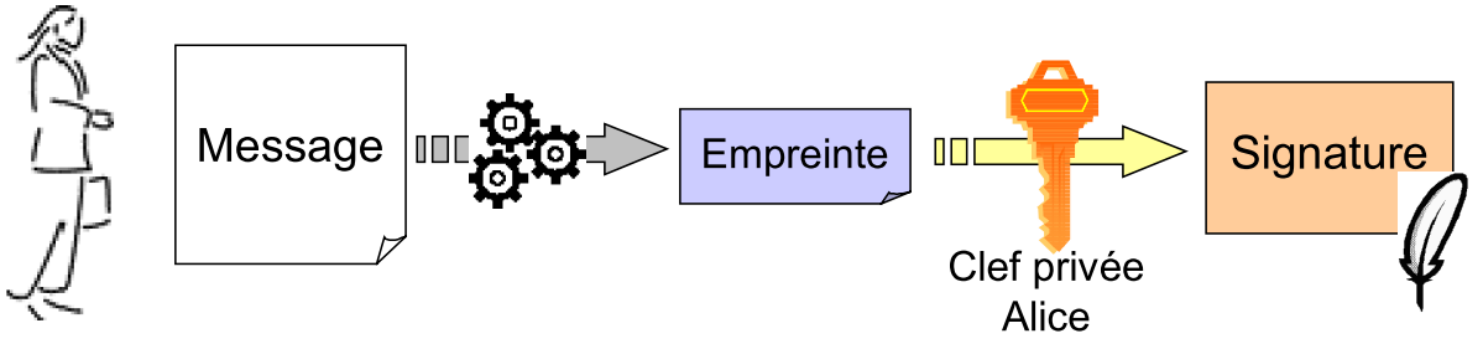
Signature

- **Définition**
  - La **signature électronique** (ou *signature numérique*) est un procédé permettant de :
    - garantir l'**authenticité** de l'expéditeur,
    - de vérifier l'**intégrité** du message reçu.
  - Elle assure également une fonction de non-répudiation qui permet d'assurer que l'expéditeur a bien envoyé le message.

Signature

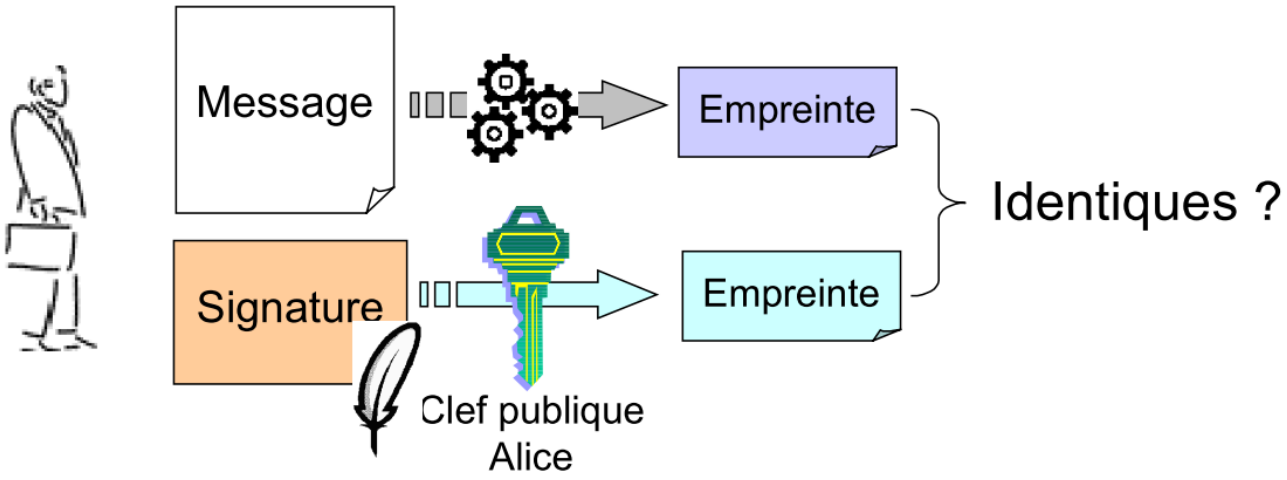
- **Principe de la signature**
  1. La **signature électronique** utilise une fonction de hachage permettant d'obtenir un condensé (appelé **empreinte**) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense.

  2. Ensuite, l'empreinte est chiffrée avec la clé privée de l'émetteur : on obtient alors la **signature électronique**.



Signature

- **Principe de la vérification**
  - Pour vérifier que la correspondance entre un message et une signature donnée, il suffit de vérifier l'égalité entre :
    1. L'empreinte du message, en utilisant la fonction de hachage qui a été utilisée pour calculer la signature,
    2. Et l'empreinte issue du déchiffrement de la signature avec la clé publique de l'émetteur de la signature.



Signature

- **Propriétés d'une signature**
  1. Elle ne peut être contrefaite
  2. Elle n'est pas réutilisable
  3. Un message signé est inaltérable
  4. La signature ne peut être reniée

- **Remarques**
  - Sur un support électronique :
    - La signature doit dépendre du message,
    - sinon il y a risque de copie et/ou de réemploi

  - **Signer ≠ chiffrer !**

Signature

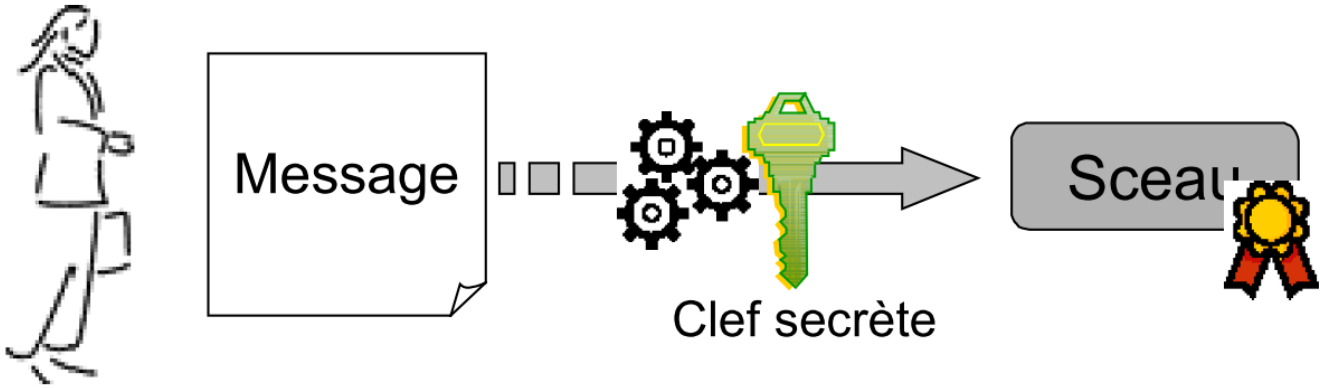
- **Algorithmes les plus couramment utilisés**
  - **DSA (Digital Signature Algorithm) :**
    - Algorithme de signature standardisé par le NIST aux Etats-Unis
    - Fonction de hachage : SHA-1 (empreinte sur 160 bits)
    - Chiffrement asymétrique : ElGamal
  - **RSA :**
    - Norme de fait
    - Fonction de hachage : MD5 (empreinte sur 128 bits) ou SHA-1
    - Chiffrement asymétrique : RSA

Scellement

- **Définition**
  - **Le scellement des données** permet de garantir que le condensé utilisé pour vérifier l'intégrité des données a bien été envoyé par le bon expéditeur.
  - Pour cela, on utilise un chiffrement asymétrique pour chiffrer le condensé : le condensé est alors **signé**. Le condensé ainsi signé est appelé **sceau** ou **code d'authentification de message (*Message Authentification Code*, MAC)**.
- **Remarque**
  - Tout comme la signature électronique, le scellement fournit les services suivants :
    - L'**authentification** de l'origine des données,
    - L'intégrité des données.
  - Cependant, le scellement ne fournit pas la non-répudiation.

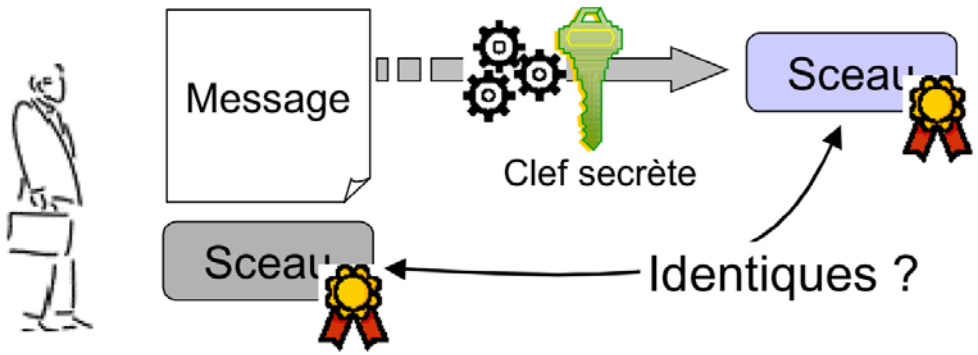
Scellement

- **Principe du scellement**
  - La création du sceau se fait en deux étapes :
    1. Utilisation d'une fonction de hachage permettant d'obtenir un condensé du message
    2. Obtention du sceau par chiffrement du condensé à l'aide de la clé secrète (ou privée) de l'émetteur du message



Scellement

- **Principe de vérification**
  - A la réception du message, il suffit au destinataire de :
    - Déchiffrer le sceau avec la clé publique de l'expéditeur,
    - Puis de comparer ce condensé avec celui obtenu à l'aide de la fonction de hachage (la même que celle utilisée par l'expéditeur) appliqué au message



Certification

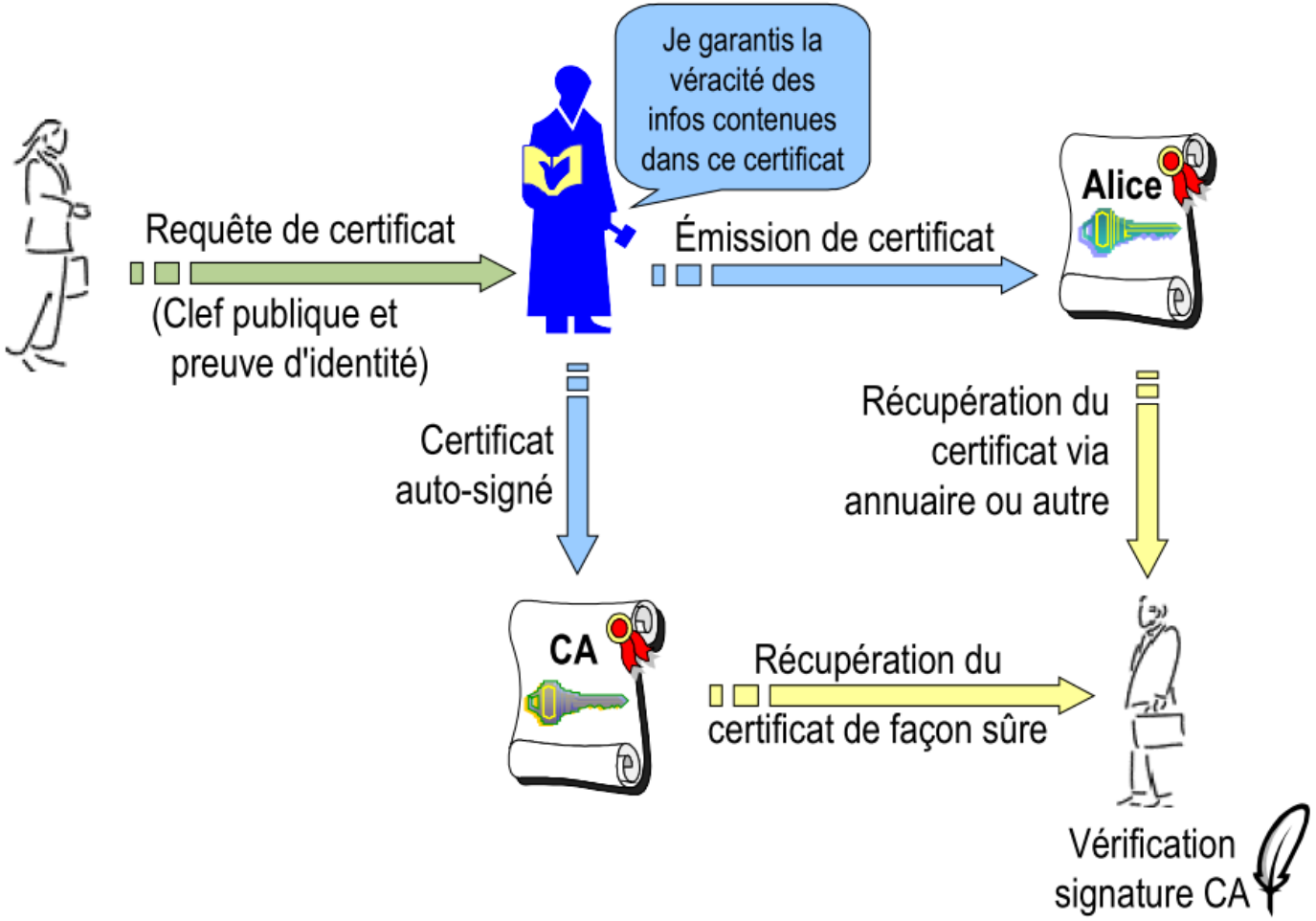
- **Définition**
  - Un **certificat** permet d'associer une clé publique à une entité, au moyen de la signature d'une autorité de confiance (appelé autorité de certification, souvent notée CA pour **Certification Authority**), afin d'en assurer la validité :
    - Nom du propriétaire de la clef
    - Dates de validité
    - Type d'utilisation autorisée
    - …

Certification

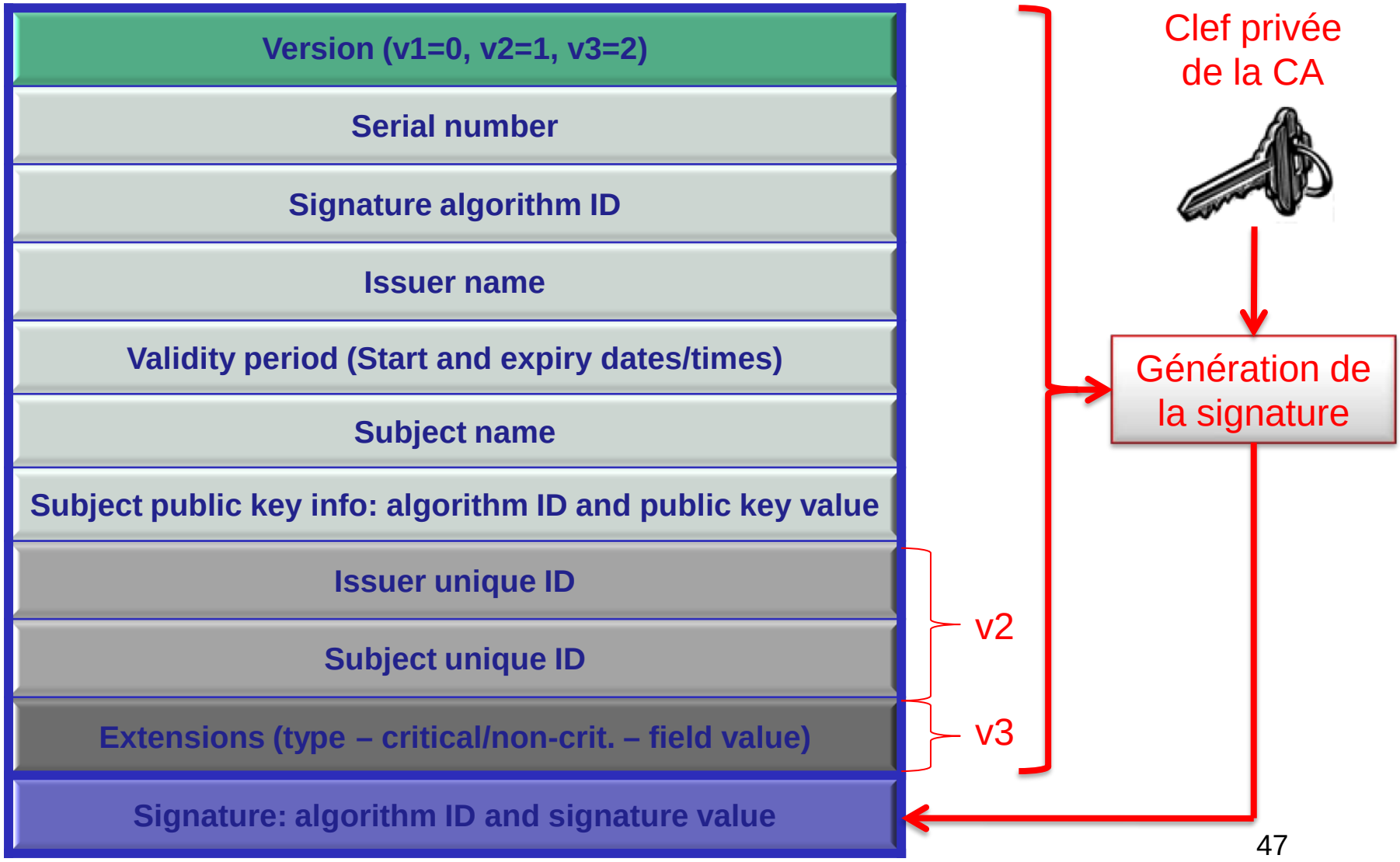
- **Emission et vérification des certificats**
  - Les certificats sont émis par une autorité de certification
    - ***Certificate Authority – CA***
    - Garantit l'exactitude des données (identification du propriétaire de la clef)
    - Certificats vérifiables au moyen de la clef publique de la CA (seule clef à stocker de façon sûre)
    - Format actuel du certificat : X.509v3, profil PKIX
  - Listes de révocation
    - ***Certificate Revocation LIST – CRL***
    - Permettre de révoquer des certificats avant leur expiration normale

Certification

- **Emission et vérification des certificats**



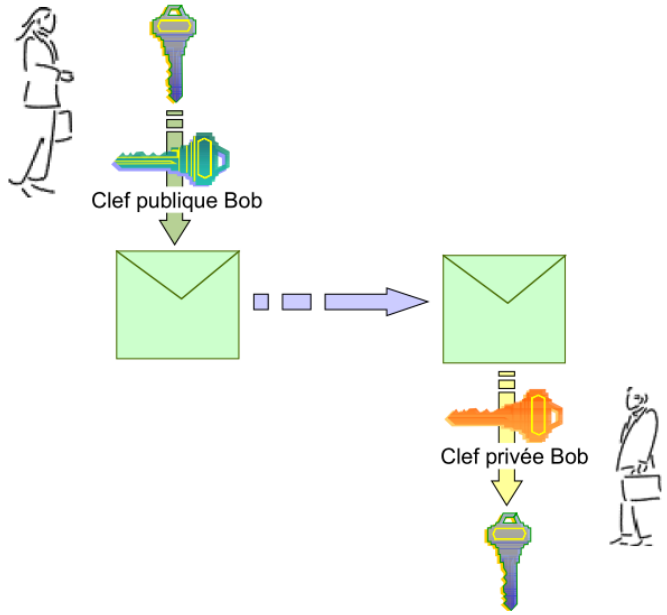
Certificats X.509v3



Clefs de session

- **Définition**
  - Un **clé de session** est une clé secrète utilisée pour chiffrer chaque jeu de données dans un système de transaction ou de communication.
  - Une clé de session différentes est utilisée pour chaque session de communication.

- **Principe**
  - On crypte une clé de session avec la clé publique du destinataire,
  - Le décryptage est fait avec sa clé privée,
  - Les échanges sont ensuite cryptés et décryptés à l'aide de la clé de session.

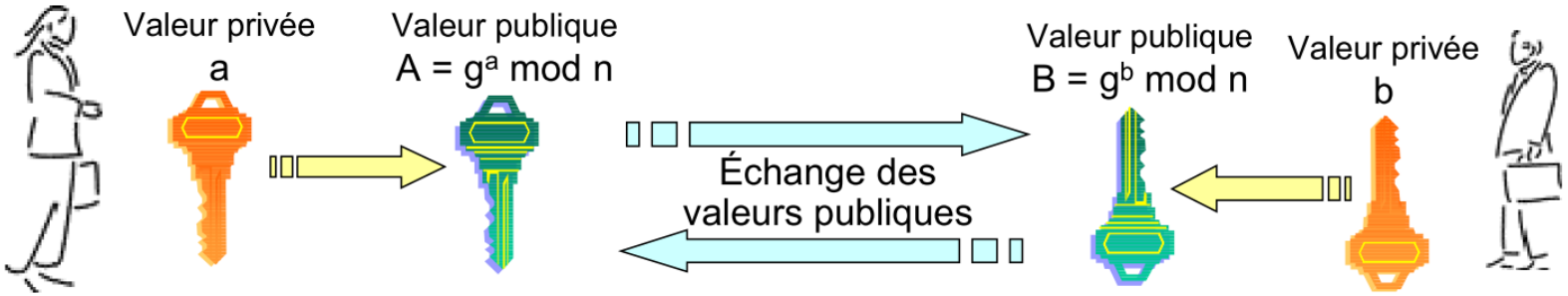


Clefs de session

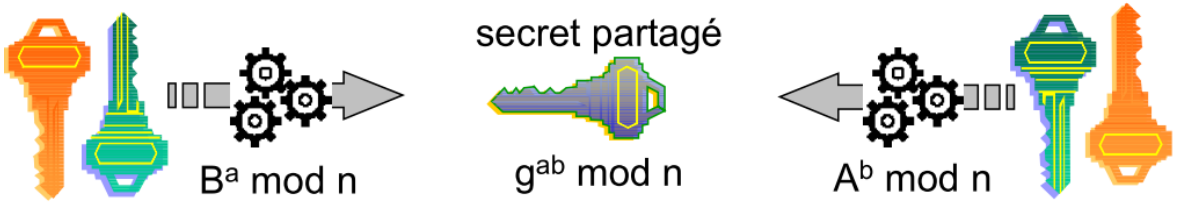
- **Intérêt**
  - Permet d'étendre l'authentification à l'ensemble de la comminucation, sans à avoir besoin d'envoyer la clé pour chaque message.
- **Problème**
  - L'échange de clefs doit être authentifié pour éviter les attaques
- **Solution**
  - Utilisation d'une protocole d'authentification mutuelle avec échange de clefs tout-en-un
- **Types d'échange de clefs**
  - Transport
    - Exemple : transport RSA (utilisé par SSL)
  - Génération
    - Exemple : Diffie-Hellman

Clefs de session

- **Principe du protocole Diffie-Hellman**
  1. Echange de valeurs publiques



  2. Génération d'un secret partagé



  3. Un espion ne peut reconstituer le secret partagé à partir des valeurs publiques**.**

Clefs de session

- **Propriétés du protocole Diffie-Hellman**
  - Problème : sensible à l'attaque de l'intercepteur
    - L'attaquant evoir sa valeur publique à la place de deux tiers en communication : il partage donc un secret avec chaque tiers
  - Solution : authentifier les valeurs publiques
    - Exemple : utilisation de certificats
  - Résultat : protocole Diffie-Hellman authentifié

- **Propriété de Perfect Forward Secrecy (PFS)**
  - La découverte du secret à long terme ne compromet pas les clefs de session
  - Car le secret à long terme n'intervient pas dans la génération ou la protection en confidentialité des clefs

Chapitre 4

PROTOCOLES SÉCURISÉS

Introduction

- **Protocoles sécurisés**
  - Inclus dans la couche application

Modèle TCP/IP	Pile de protocoles
4 – couche application	HTTP, SMTP, FTP, SSH, IRC, SNMP, DHCP, POP3 …
	HTML, MIME, ASCII
	TLS, SSL, NetBIOS, SET, Secure Shell SSH, RTSP, S-HTTP
3 – couche de transport	TCP, UDP, SCTP, RTP, DCCP …
2 – couche internet	IPv4, IPv6, ARP, IPX …
1 – couche d'accès réseau	Ethernet, 802.11 WiFi, Token ring, FDDI …
	Câble, fibre optique, ondes radio ….

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

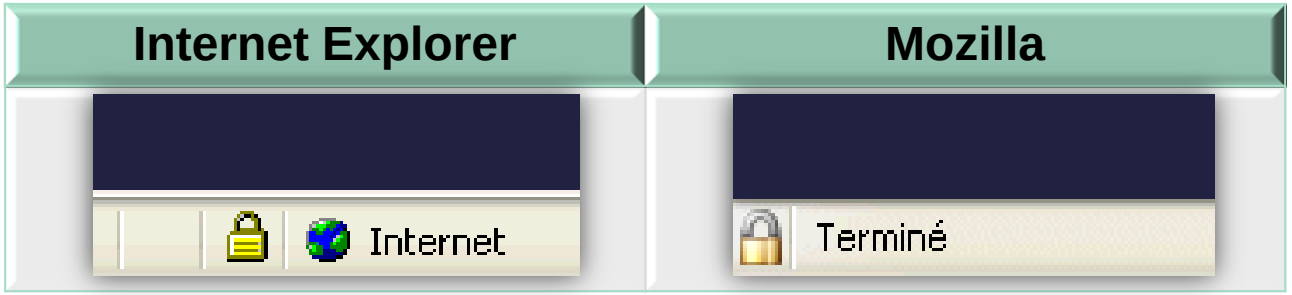
- **Introduction à SSL**
  - SSL = Secure Sockets Layers
  - Standard SSL :
    - mis au point par Netscape,
    - en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.
  - Procédé de :
    - sécurisation des transactions effectuées via Internet.
    - cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet.
  - Principe :
    - Etablir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **Propriétés**
  - Système SSL indépendant du protocole utilisé, pouvant sécuriser :
    - des transactions faites par le protocole HTTP,
    - des connexions via le protocole FTP, POP ou IMAP.
  - SSL est transparent pour l'utilisateur.
  - SSL supporté par la quasi intégralité des navigateurs.



  - URL d'un serveur web securisé par SSL :
    - Commence par https://
    - Le « s » signifie « secured / sécurisé ».

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **SSL 2.0**
  - Principe de la création de la clé de session :
    1. Connexion du client au site marchand sécurisé par SSL :
       - Demande de authentification.
       - Envoi de la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.
    2. Réponse du serveur au client :
       - Envoi un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA),
       - Envoi du nom du cryptosystème le plus haut dans la liste avec lequel il est compatible.
    3. Réponse du client au serveur :
       - Vérification de la validité du certificat
       - Création d'une clé secrète aléatoire
       - Chiffrement de la clé à l'aide de la clé publique du serveur
       - Envoi du résultat (la clé de session) au serveur
       - Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **SSL 3.0**
  - Authentification mutuelle entre le serveur et le client
- **TLS 1.0**
  - Correspondant à SSL 3.1
  - SSL 3.0 et TLS 1.0 non interopérables
    - Compatibilité ascendant de TLS avec SSL.
  - TLS diffère de SSL pour générer les clés symétriques :
    - Génération plus sécurisée dans TLS que dans SSL 3.0
  - Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
  - Nouvelles versions :
    - TLS 1.1 en 2006
    - TLS 1.2 en 2008

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Introduction**
  - Protocole Telnet
    - Permet d'effectuer ces tâches distantes possédaent l'inconvénient majeur de faire circuler en clair sur le réseau les informations échangées.
    - Attaques faciles
      - Ainsi, un pirate situé sur un réseau entre l'utilisateur et la machine distante a la possibilité d'écouter le traffic,
      - le pirate obtient un accès à un compte sur la machine distante et peut éventuellemen et étendre ses privilèges sur la machine afin d'obtenir un accès administrateur (root).
  - Protocole SSH (Secure Shell)
    - Permet à des utilisateurs (ou bien des services TCP/IP) d'accéder à un machine à travers une communication chiffrée (appelée tunnel).

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Le protocole SSH**
  - SSH = Secure Shell
  - Mis au point en 1995 par le Finlandais Tatu Ylönen.
  - Intérêt :
    - Permet à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :
      - Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité.
      - Le client et le serveur s'authentifient mutuellement.

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Le protocole SSH**
  - Version 1 : SSH1
    - proposée dès 1995
    - alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec.
    - faille permettant à un pirate d'insérer des données dans le flux chiffré.
  - Version 2 : SSH2
    - proposée en 1997
    - solution de transfert de fichiers sécurisé
      - SFTP, Secure File Transfer Protocol.

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Fonctionnement de SSH**
  - Etablissement d'une connexion SSH :
    1. Le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
    2. Le client s'authentifie auprès du serveur pour obtenir une session.

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Mise en place du canal sécurisé**
  1. phase de négociation entre le client et le serveur :
     - s'entendre sur les méthodes de chiffrement à utiliser.
  2. le serveur envoie sa clé publique d'hôte (host key) au client.
  3. le client génère une clé de session de 256 bits chiffrée grâce à la clé publique du serveur
  4. envoie au serveur la clé de session chiffrée ainsi que l'algorithme utilisé.
  5. le serveur déchiffre la clé de session grâce à sa clé privée
  6. le serveur envoie un message de confirmation chiffré à l'aide de la clé de session.
  7. Les communications sont chiffrées grâce à un algorithme de chiffrement symétrique en utilisant la clé de session

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **L'authentification**
  - Une fois la connexion sécurisée mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès.
  - Il existe plusieurs méthodes :
    - La plus connue : le traditionnel mot de passe.
      1. Le client envoie au serveur en mode « sécurisé » :
         - un nom d'utilisateur ,
         - et un mot de passe
      2. Le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide
    - La moins connue : l'utilisation de clés publiques.
      1. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge,
      2. Si ce dernier parvient à déchiffrer le challenge avec sa clé privée, le serveur va donner un accès au client

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Introduction**
  - S-HTTP (Secure HTTP) :
    - procédé de sécurisation des transactions HTTP
    - mis au point en 1994 par l'EIT (Enterprise Integration Technologies).
    - Fournit une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de :
      - leur numéro de carte bancaire,
      - ou de tout autre information personnelle.

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Fonctionnement de S-HTTP**
  - Messages S-HTTP basés sur trois composantes :
    1. Le message HTTP
    2. Les préférences cryptographiques de l'envoyeur
    3. Les préférences du destinataire
  - Décryptage S-HTTP par le destinataire :
    1. Analyse des en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message.
    2. Puis déchiffrement du message grâce à :
       - Ses préférences cryptographiques actuelles et précédentes,
       - Les préférences cryptographiques précédentes de l'expéditeur

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Complémentarité de S-HTTP et SSL**
  - SSL et S-HTTP
    - SSL :
      - Couche de chiffrement.
      - Indépendant de l'application utilisée.
      - Chiffre l'intégralité de la communication.
    - S-HTTP :
      - Combinaison de HTTP avec couche de chiffrement
      - Marquage individuel des documents HTML à l'aide de certificats.
      - Très fortement lié au protocole HTTP.
      - Chiffre individuellement chaque message.
    - Complémentarité :
      - SSL permet de sécuriser la connexion internet,
      - tandis que S-HTTP permet de fournir des échanges HTTP sécurisés.

Protocole SET

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**
  - Introduction
  - Principe
- **S/MIME**

- **Introduction**
  - SET :
    - Secure Electronic Transaction
    - Protocole de sécurisation des transactions électroniques
    - Mis au point par Visa et MasterCard
    - S'appuie sur le standard SSL.
  - SET est basé sur l'utilisation de :
    - une signature électronique au niveau de l'acheteur,
    - et une transaction mettant en jeu :
      - non seulement l'acheteur et le vendeur,
      - mais aussi leurs banques respectives.

Protocole SET

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**
  - Introduction
  - Principe
- **S/MIME**

- **Principe d'une transaction sécurisée avec SET**

1. Les données sont envoyées par le client au serveur du vendeur

2. Le vendeur ne récupère que la commande.

3. Le numéro de carte bleue est envoyée directement à la banque du commerçant pour :
   - être en mesure de lire les coordonnées bancaires de l'acheteur,
   - et donc contacter sa banque afin de les vérifier en temps réel.

- **Nécessité d'une signature électronique :**
  - Au niveau de l'utilisateur de la carte
  - Pour certifier qu'il s'agit bien du possesseur de cette carte.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Introduction**
  - Standard MIME :
    - Permettre d'inclure dans les message électroniques des fichiers attachées autres que des fichiers texte.
  - S/MIME :
    - **S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtension
    - Procédé de sécurisation des échanges par courrier électronique, encapsulé au format MIME.
    - Assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des messages électroniques.
    - Historique :
      - Mis au point à l'origine par la société RSA Data Security.
      - Ratifié en juillet 1999 par l'IETF, S/MIME est devenu un standard, dont les spécifications sont contenues dans les RFC 2630 à 2633.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Principe**
  - Chiffrement à clé publique :
    - Permet ainsi de chiffrer le contenu des messages,
    - Mais ne chiffre pas la communication.
  - Chiffrement du message électronique :
    - Utilisation d'une clé de session
      - Pour chiffrer chaque partie du message
      - Insérée, dans l'en-tête de chaque partie, sous forme chiffré à l'aide de la clé publique du destinataire
    - Intérêt :
      - Seul le destinataire peut ainsi ouvrir le corps du message, à l'aide de sa clé privée.
      - Ceci assure la confidentialité et l'intégrité du message reçu.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Principe**
  - Signature du message :
    - Chiffrée à l'aide de la clé privée de l'expéditeur.
    - Intérêt :
      - Toute personne interceptant la communication peut lire le contenu de la signature du message,
      - Mais seul l'expéditeur est capable de chiffrer un message (avec sa clé privée) déchiffrable à l'aide de sa clé publique.
      - Garantit au destinataire l'identité de l'expéditeur.

Protocole S/MIME

Protocoles

- SSL
- SSH
- S-HTTP
- SET

- S/MIME
  - Introduction
  - Principe
  - Exemple

```
MIME-Version: 1.0
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="----D7B623C746311F5D683A038DC482F307«

This is an S/MIME signed message

------D7B623C746311F5D683A038DC482F307
Content-Type: text/plain

Ceci est le texte d'origine qui est signé.
------D7B623C746311F5D683A038DC482F307
Content-Type: application/x-pkcs7-signature;
name="smime.p7s«
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smime.p7s"

MIIGgQYJKoZIhvcNAQcCoIIGcjCCBm4CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHAaCCA7wwggO4MIICoKADAgECAgEMMA0GCSqGSIb3DQEBBAUAMIGrMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGRlJBTkNFMQ4wDAYDVQQHEwVQQVJJUzEZMBcGA1UE
ChMQVEhFIFNJR05BVFVSRSBDQTEaMBgGA1UECxMRU2lnbmF0dXJlIFNlcnZpY2Ux
HDAaBgNVBAMTE1NpZ25hdHVyZSBBdXRob3JpdHkxJjAkBgkqhkiG9w0BCQEWF2F1
dGhvcml0eUBzaWduYXR1cmUub3JnM…ygIVIs1VsPQ==

------D7B623C746311F5D683A038DC482F307--
```

Chapitre 5

LÉGISLATION FRANÇAISE

Vue d'ensemble

- **Il existe des lois sur Internet :**
  - Souvent inadéquates
  - Chaque pays a sa propre législation
  - Exemple, la France :
    - Il y a quelques années; interdiction de tout chiffrage (excepté la signature depuis 1990), car les politiciens considéraient que le citoyen ne pouvait pas avoir accès à des moyens cryptographiques pouvant servir aux militaires.
    - La politique française s'est assouplie depuis mais reste encore en marge par rapport à des pays comme les Etats-Unis qui laisse la liberté à ses citoyens de crypter à loisir.
    - Textes législatifs et réglementaires
      - Loi n°90-1170 du 29 décembre 1990, modifiée par la loi n°96-659 du 26 juillet 1996 (décrets d'application début 1998)
      - Deux nouveaux décrets et un arrêté le 17 mars 1999.
      - http://www.internet.gouv.fr/francais/commerce/textesref.htm

Vue d’ensemble

- **Il existe des lois sur Internet :**
  - Problème :
    - L'Etat n'a plus aucun contrôle sur le contenu des échanges :
      - piratage (pour les transactions bancaires),
      - Mafia,
      - terrorisme (échange de données mettant en jeu la sécurité nationale).
  - Commerce électronique :
    - besoin des services de la cryptographie pour assurer au client qu'il va être livré et pour s'assurer qu'il va être payé
  - Solution :
    - Les clés paraissent donc être le meilleur moyen de garantir l'identification.

Vue d’ensemble

- **La DCSSI** *(ex-SCSSI)*
  - **D**irection **C**entrale de la **S**écurité des **S**ystèmes d’**I**nformation
  - C’est le service à qui adresser les déclarations et demandes d’autorisations.
  - http://www.scssi.gouv.fr
- Principe actuel
  - On distingue différents régimes en fonction de la finalité des moyens ou prestations de cryptologie et du niveau correspondant

Finalités

- **Utilisation**
  - Personnelle
  - Collective (pour un domaine ou un type d'utilisateur donné)
  - Générale (potentiellement n'importe qui)
- **Fourniture**
  - Vente, location ou gratuit
- **Importation**
  - Hors Communauté Européenne
- **Exportation**
  - Hors Communauté Européenne

Régimes

- **Dispense de toute formalité préalable**
  - La liberté est totale d'utiliser, de fournir, d'importer ou d'exporter le moyen ou la prestation considérés
- **Déclaration**
  - Simplifiée ou non
  - Un formulaire administratif doit être transmis à la DCSSI un mois à l'avance
- **Autorisation**
  - Partie administrative et partie technique
  - La DCSSI dispose de quatre mois pour notifier sa décision. Une absence de notification à l'expiration de ce délai vaut autorisation

Synthèse

Synthèse du nouveau cadre législatif et réglementaire				
Finalités	**Fonctions offertes**			
	authentification signature Intégrité non répudiation	confidentialité		
		L ≤ 40 bits	*40 bits < L ≤ 128 bits*	*L > 128 bits*
Utilisation	libre	libre	libre ou déclaration *(1)*	autorisation
Fourniture	déclaration simplifiée	déclaration	déclaration	autorisation
Importation	libre	libre	libre ou déclaration *(1)*	autorisation
Exportation	libre	autorisation	autorisation	autorisation

(1) La déclaration est nécessaire uniquement pour un matériel ou un logiciel qui n'a pas fait l'objet préalablement d'une déclaration par leur producteur, un fournisseur ou un importateur, et si ledit matériel ou ledit logiciel n'est pas exclusivement destiné à l'usage privé d'une personne physique

Chapitre 6

CONCLUSION

Conclusion

- **Cryptologie = cryptographie + cryptanalyse**

  - La cryptographie doit fournir un certain nombre de services de sécurité :
    1. Confidentialité
    2. Intégrité
    3. Authentification
    4. Non répudiation

  - La cryptanalyse sert à vérifier l'efficace des méthodes de cryptographie contre les attaques.

Conclusion

- **Trois méthodes de cryptographie :**
  - Simple ou par substitution :
    - simple, rapide, mais facilement attaquable
  - Symétrique ou à clé privée/secrète :
    - Shannon : clé privée de longueur égale au moins au message
    - Canal sécurisé pour le transport de la clé privée
    - Avoir N * (N – 1) / 2 clés pour un groupe de N personnes.
    - Facilement attaquable si la clé privée est interceptée avec le message.
  - Asymétrique ou à clé publique :
    - Algorithmes complexes et plus lents que ceux à clef privée
    - Utilisé pour chiffrer une clef de session ou pour établir une signature.

Conclusion

- **Pour satisfaire les critères de sécurité d'une communication entre deux tiers :**
  - La vérification d'intégrité :
    - comparaison des condensés du message reçu et du message envoyé.
  - L'authentification :
    - s'assurer de l'identité d'une entité ou de l'origine d'une communication/fichier.
    - Authenticité = authentification + intégrité
  - La signature électronique :
    - garantir l'authenticité de l'expéditeur,
    - vérifier l'intégrité du message reçu,
    - assurer une fonction de non-répudiation.
  - Le certificat :
    - associer une clé publique à une entité, au moyen de la signature d'une autorité de confiance/certification afin d'en assurer la validité

Conclusion

- **Pour satisfaire les critères de sécurité d'une communication entre deux tiers :**
  - Le scellement des données :
    - garantir que le condensé utilisé pour vérifier l'intégrité des données a bien été envoyé par le bon expéditeur.
    - sceau = condensé signé à l'aide d'un chiffrement
  - La clé de session = clé secrète
    - utilisée pour chiffrer chaque jeu de données dans un système de transaction ou de communication.
    - différente à chaque communication
- **Plusieurs protocoles, situés dans la couche d'application :**
  - SSL / TLS
  - SSH
  - S-HTTP
  - SET
  - S/MIME