



Université
De Boumerdes

Cryptographie

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes



Université
De Boumerdes

- 1. Introduction, définition et Historique**
- 2. Cryptographie actuelle**
- 3. Signature et certificats numériques**
- 4. Applications de la cryptographie**



Université
De Boumerdes

Introduction et Historique

Historique et introduction



Historique et introduction

- Lorsque **Jules César** envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers.
- Il remplaçait donc tous les **A** contenus dans ses messages par des **D**, les **B** par des **E**, et ainsi de suite pour tout l'alphabet.
- Seule la personne connaissant la règle du « **décalage par trois** » pouvait déchiffrer ses messages.

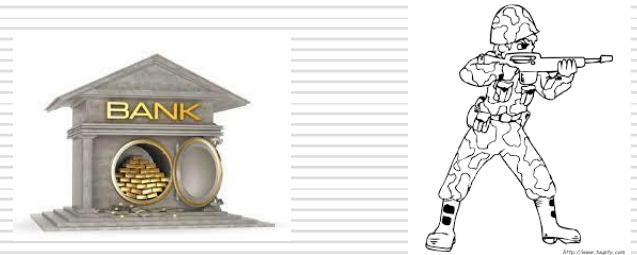
Historique et introduction

Et voilà comment tout a commencé...

Historique et introduction

De nos jours on retrouve de la cryptographie dans :

- Armée.
- Système bancaire.
- Internet (achat, identification).
- Téléphone portable.
- TV payante.
- Carte d'identité électronique.
- Vote électronique.



Historique et introduction

Pour protéger une information :

Stéganographie

Cryptographie

Transposition

Substitution

Historique et introduction

La stéganographie : écriture couverte



Durant l'antiquité, certains généraux rasaient le crâne de leurs esclaves, leur tatouaient un message et attendaient que les cheveux repoussent pour faire passer des informations importantes.

Historique et introduction

La stéganographie : écriture couverte

L'information est dissimulée au sein d'une autre information afin de la rendre invisible.

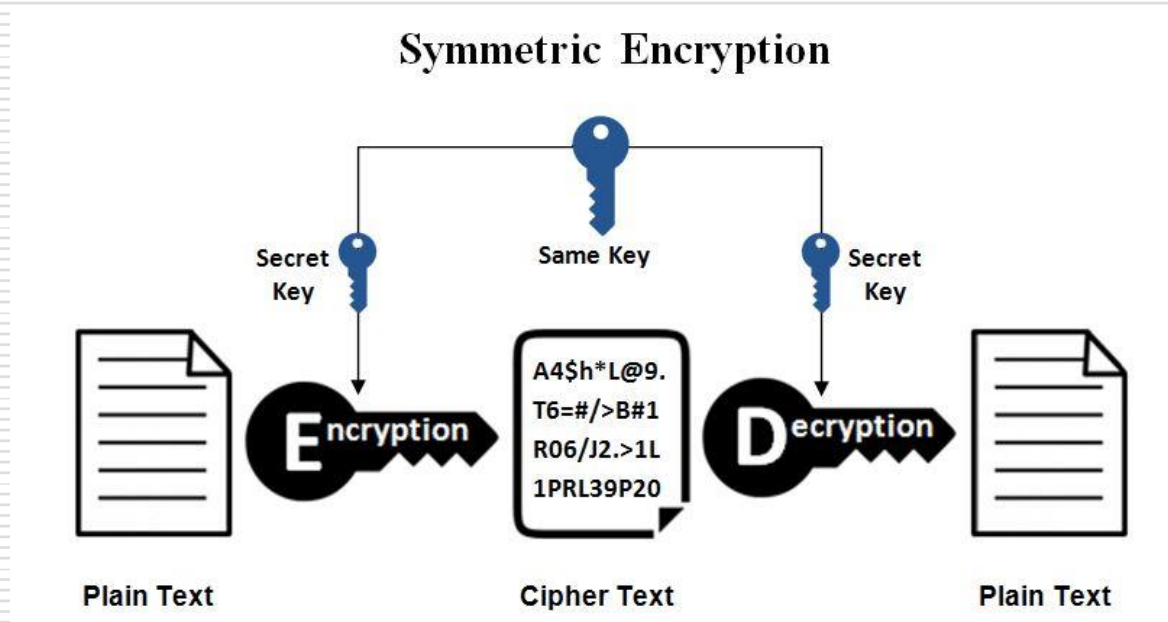


Stéganographie

Historique et introduction

La cryptographie :

L'information est modifiée selon une méthode préétablie afin de la rendre incompréhensible.



Historique et introduction

La cryptographie : Il existe deux grandes catégories :

➤ **Par transposition** : l'**ordre** des éléments d'une information est modifiée (**décalage** des caractères d'une phrase, pixels d'une image, ...)

➤ **Par substitution** : les éléments d'une information sont **remplacés** par d'autres (**remplacer** tous les A par B, B par C, etc...)

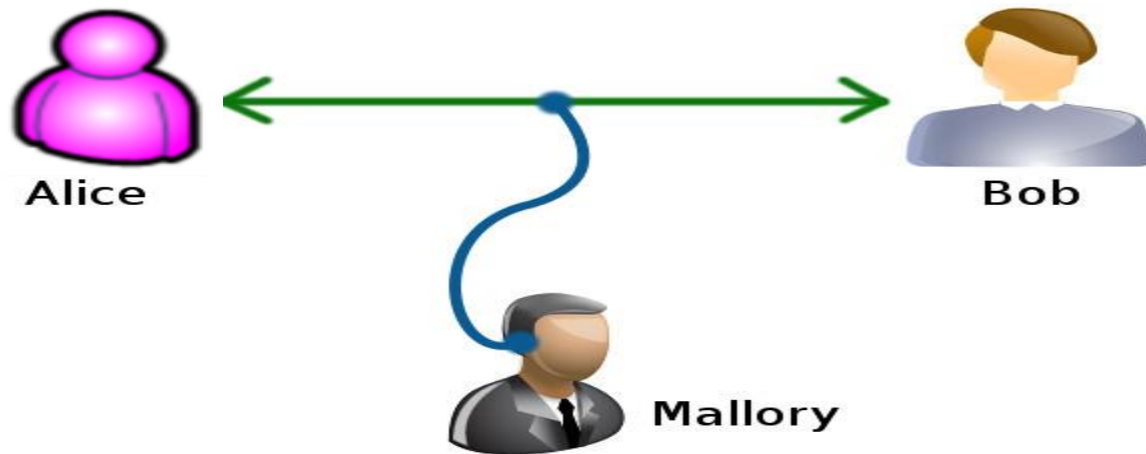


Cryptographie

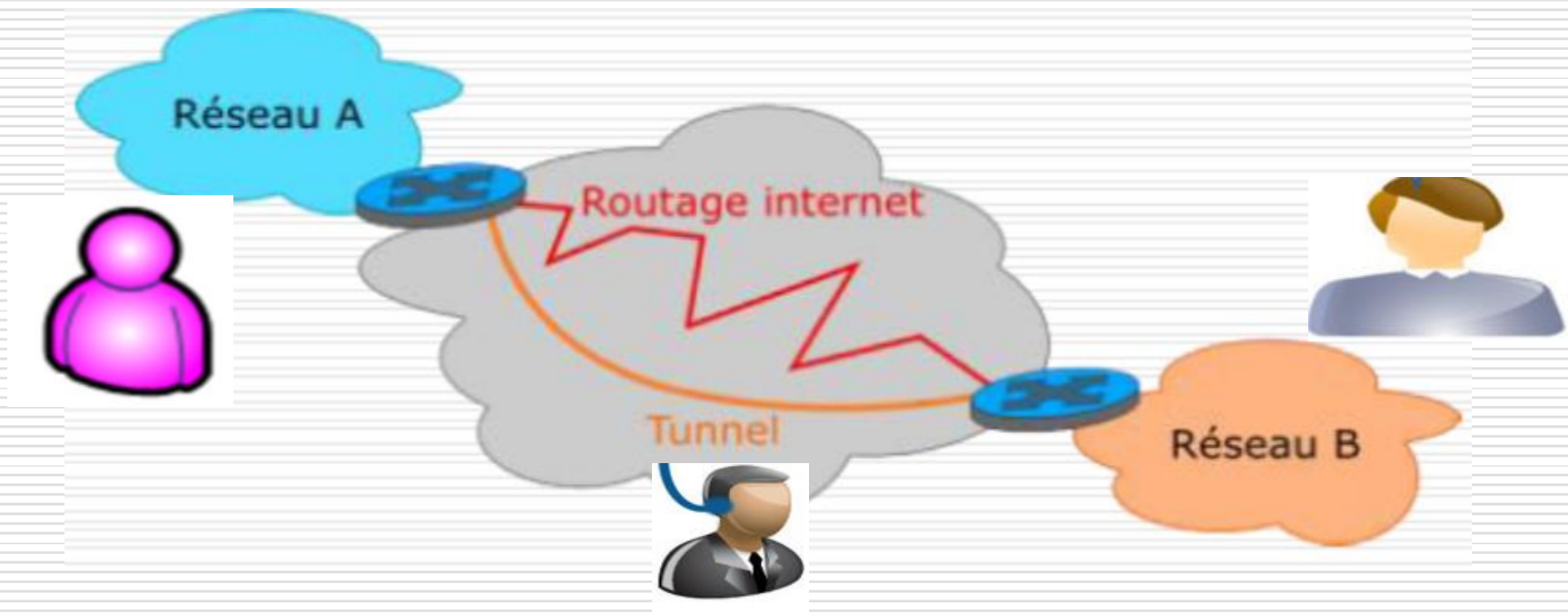
Définitions

Protagonistes traditionnels

- **Alice ou Anne** et **Bob** souhaitent se transmettre des données
- **Oscar ou Mallory**, un opposant qui souhaite espionner Alice et Bob.



Définitions



Définitions

Message clair 'M': Cette expression désigne le message original n'ayant subi aucune modification

Clé: La clé désigne l'information permettant de chiffrer et de chiffrer/déchiffrer un message

Chiffrement:

Fonction 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 **$C = E(M)$**

Définitions

Déchiffrement:

Fonction de reconstruction du message clair à partir du message chiffré :

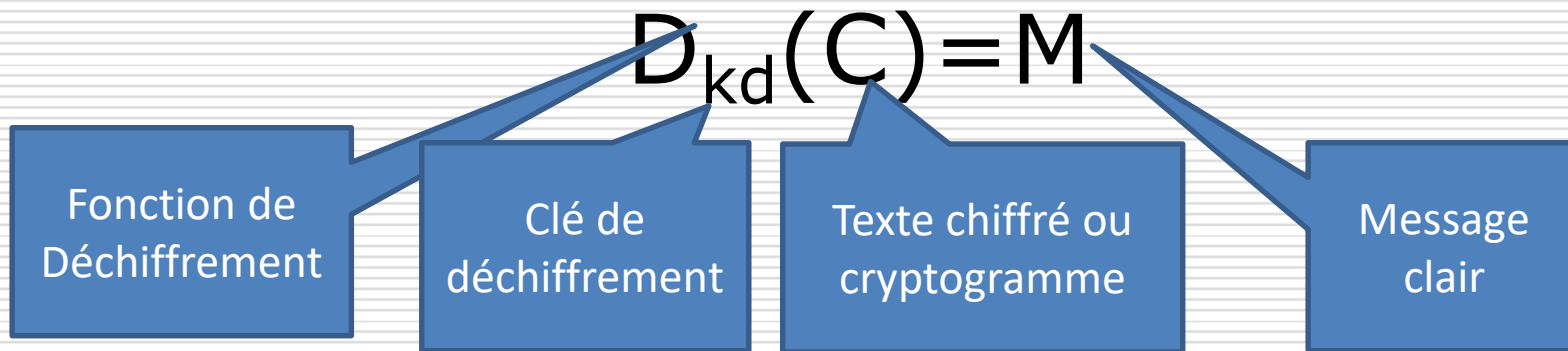
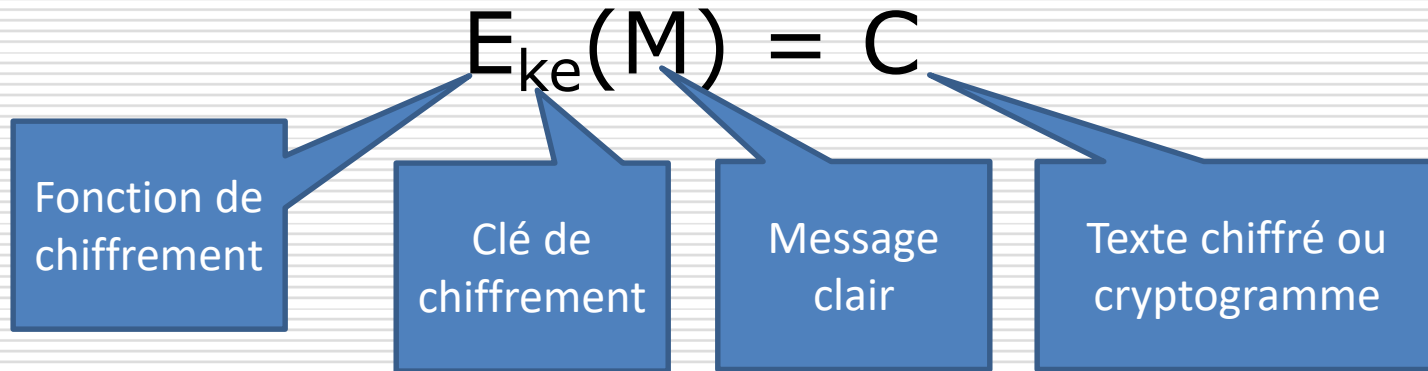
Basé sur une fonction de déchiffrement D

On a donc $D(C) = D(E(M)) = M$

En pratique : E et D sont généralement paramétrées par des clefs K_e et K_d :

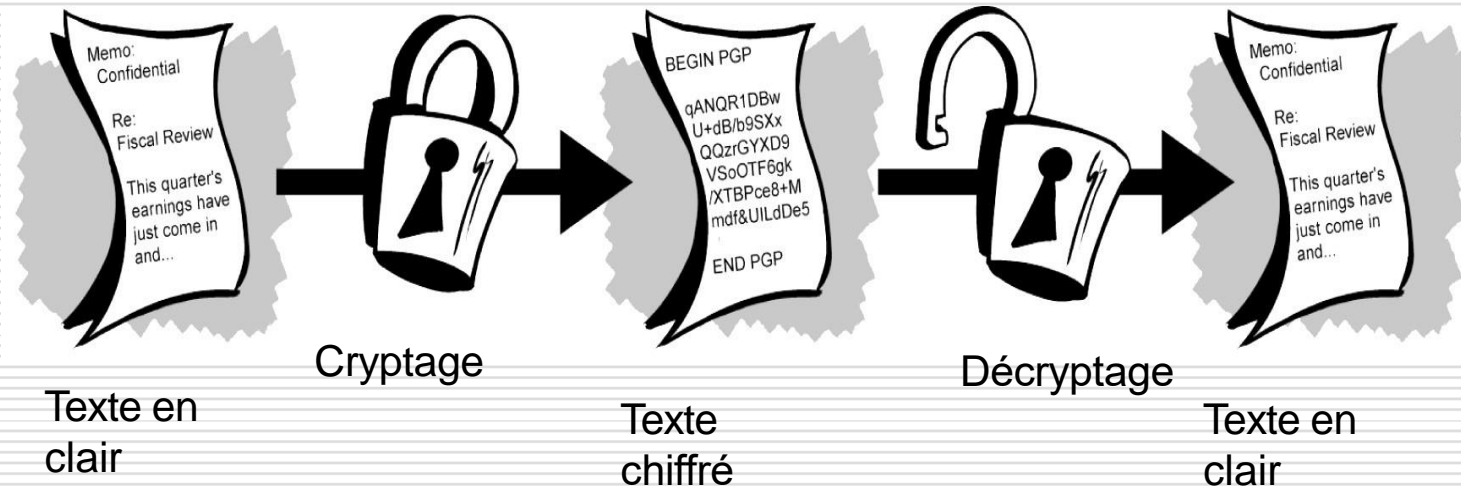
- $E_{ke}(M) = C$
- $D_{kd}(C) = M$

Définitions



Définitions

Cryptage et décryptage



Définitions

Cryptographie et cryptanalyse

- **La cryptographie** est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.
- **La cryptanalyse** est l'étude des informations cryptées, afin d'en découvrir le secret.
- **La cryptologie** englobe la cryptographie et la cryptanalyse

Définitions

Cryptographie

Exemple: Chiffrement de César

Chiffrement de César

Consiste à décaler l'alphabet clair. Le décalage est la clé du chiffrement

Exemple :

On veut chiffrer le mot *CRYPTOGRAPHIE* avec un décalage de 3. Pour cela on écrit les alphabets clair et chiffré comme suit :

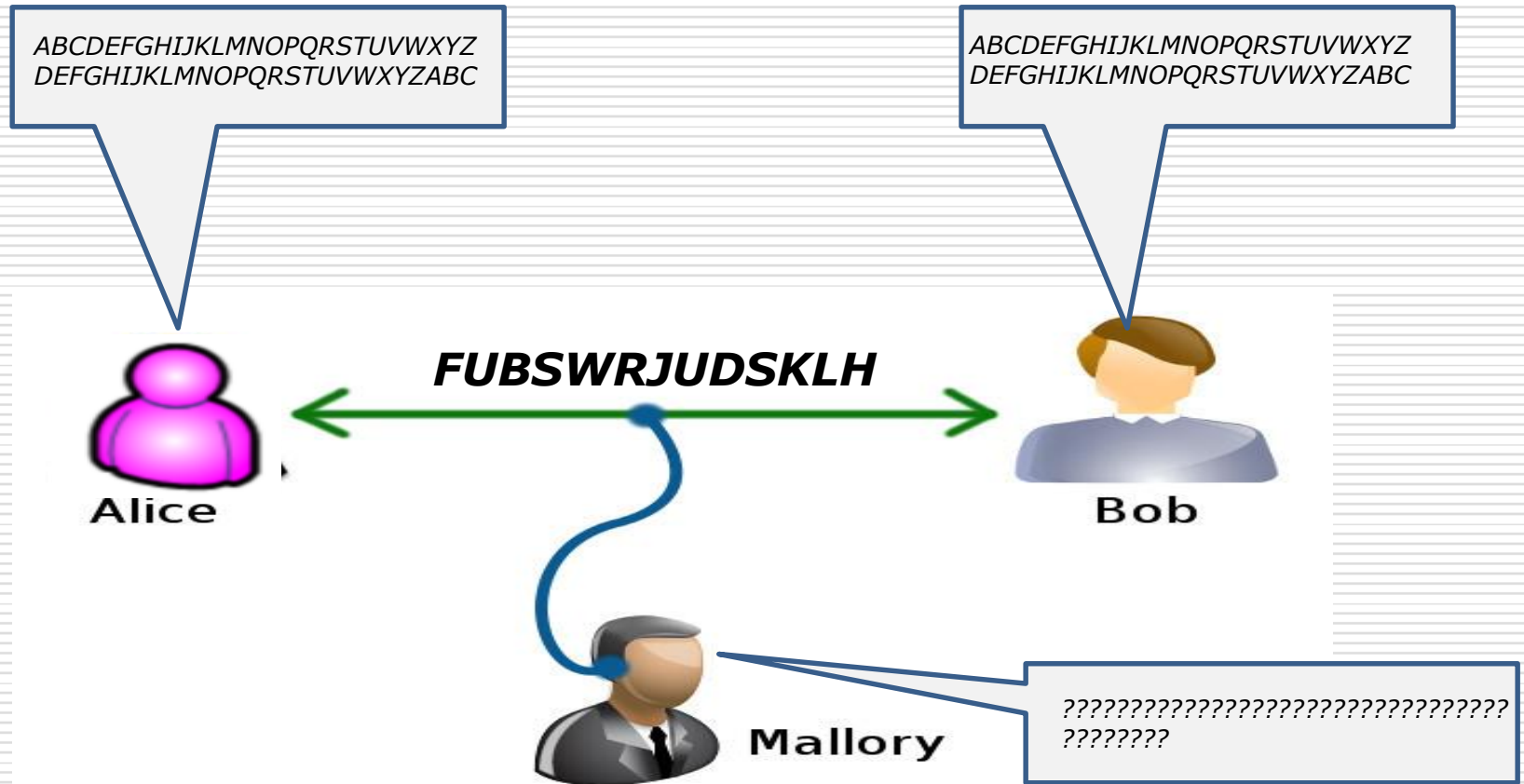
ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

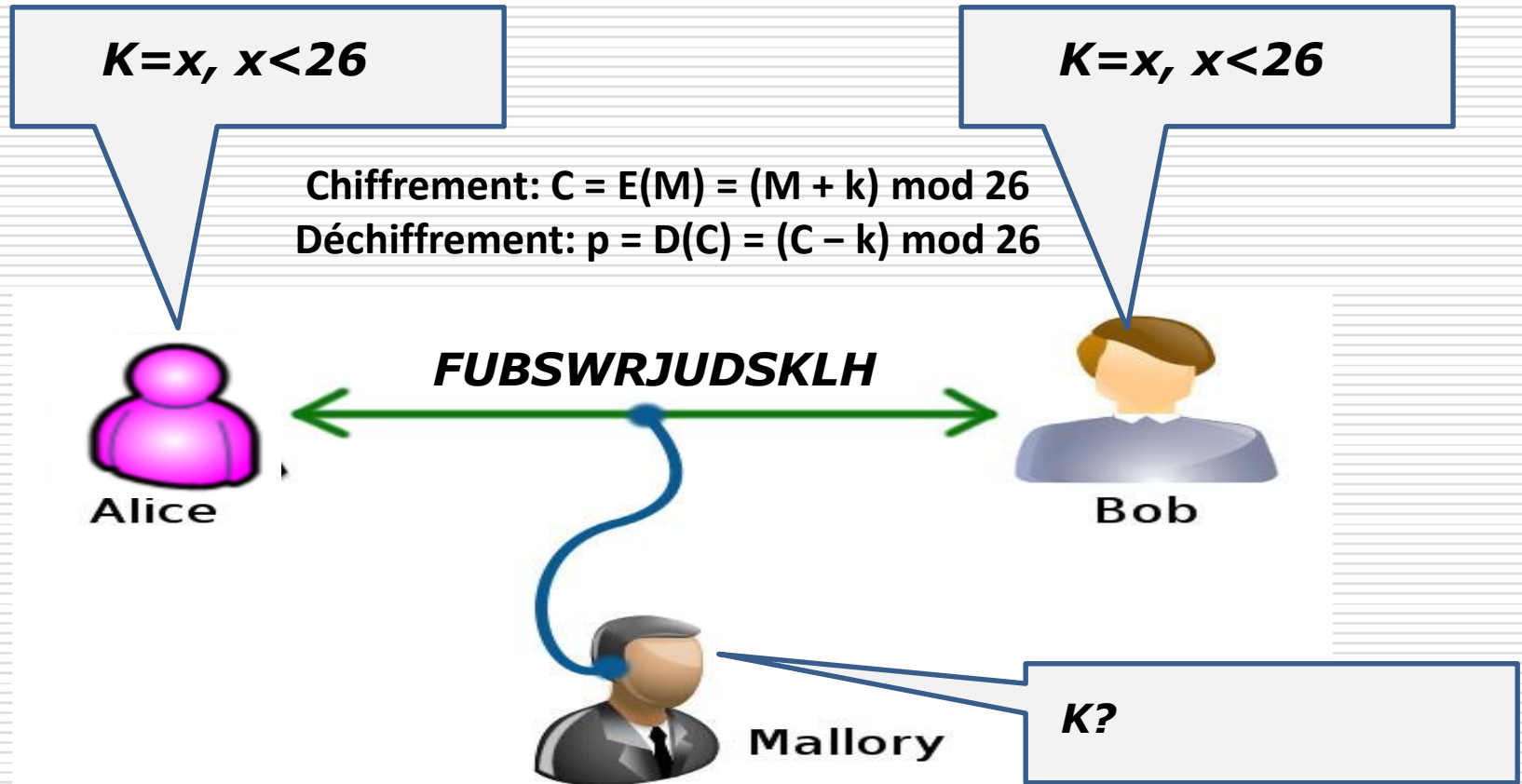
Et on remplace:

CRYPTOGRAPHIE ---> FUBSWRJUDSKLH

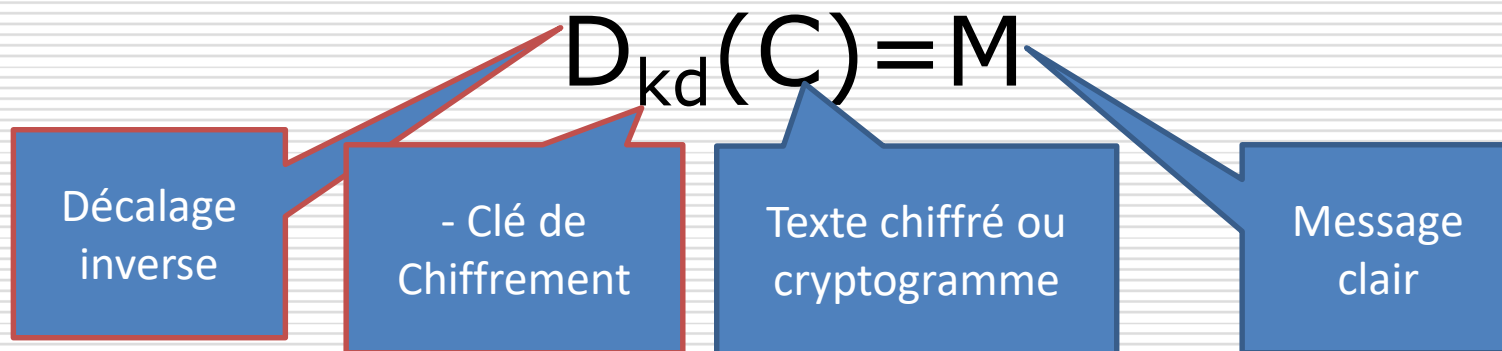
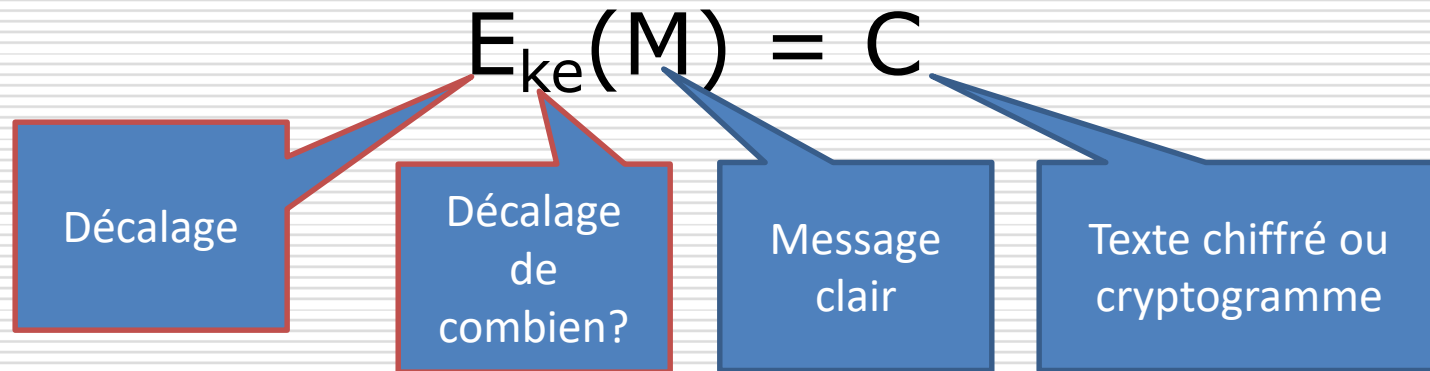
Chiffrement de César



Chiffrement de César



Chiffrement de César



Chiffrement de César

Cryptanalyse

Faiblesse du chiffre de César:

- Il n'y a que 26 clés possibles !
- Donc étant donné un message chiffré, il suffit de tester les 26 clés possibles pour retrouver le message clair.
- Cela se fait en quelques minutes !!

Solution:

Utiliser un alphabet chiffré aléatoirement

Chiffrement de César

Substitution aléatoire

Exemple :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
OHGFEDCBUKJPNMIQRXSTLZXYWV

Dans ce cas, le nombre de clés possibles passe à
400 000 000 000 000 000 000 000 000 000 !!!

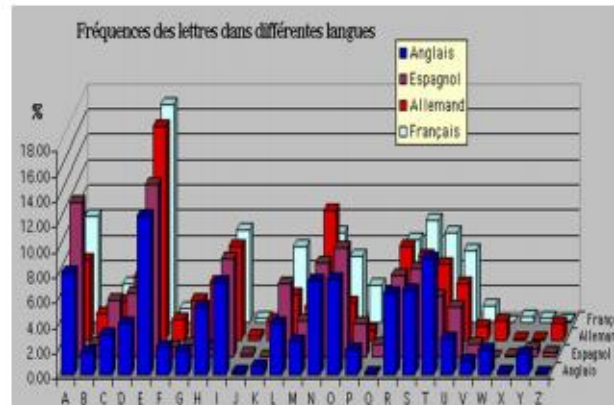
Cryptanalyse:

Il est évident impossible de tester toutes les clés possibles, même une machine est incapable de le faire en un temps raisonnable (**300 000** ans pour un ordinateur très puissant !!).

Chiffrement de César

Substitution aléatoire: cryptanalyse

Rang ↕	Caractère ↕	Nombre d'occurrences ↕	Pourcentage ↕		Rang ↕	Caractère ↕	Nombre d'occurrences ↕	Pourcentage ↕
1	e	115 024 205	12,10	↔	1	h	115 024 205	12,10
2	a	67 563 628	7,11	↔	2	j	67 563 628	7,11
3	i	62 672 992	6,59	↔	3	e	62 672 992	6,59
4	s	61 882 785	6,51	↔	4	k	61 882 785	6,51
5	n	60 728 196	6,39	↔	5	u	60 728 196	6,39
6	r	57 656 209	6,07	↔	6	p	57 656 209	6,07
7	t	56 267 109	5,92	↔	7	w	56 267 109	5,92
8	o	47 724 400	5,02	↔	8	x	47 724 400	5,02
9	l	47 171 247	4,96	↔	9	r	47 171 247	4,96
10	u	42 698 875	4,49	↔	10	v	42 698 875	4,49
11	d	34 914 685					34 914 685	3,67
12	c	30 219 574					30 219 574	3,18
13	m	24 894 034					24 894 034	2,62
14	p	23 647 179					23 647 179	2,49
15	é	18 451 937					18 451 937	1,94
17	g	11 684 140					11 684 140	1,23
18	b	10 817 171					10 817 171	1,14
19	v	10 590 858					10 590 858	1,11
20	h	10 583 562					10 583 562	1,11
21	f	10 579 192					10 579 192	1,11
28	q	6 140 307					6 140 307	0,65



Statistique selon la langue
française

Statistique du texte chiffré

Chiffrement de César

Substitution aléatoire: cryptanalyse

Pourtant il est possible là encore de casser ce chiffrement en quelques minutes !!

Dans la langue française, par exemple, on sait que la fréquence d'apparition de chaque lettre est à peu près stable. Il suffit donc à:

- Mesurer la fréquence d'apparition de chaque lettre d'un texte chiffré
- Comparer avec la table des fréquences des lettres françaises
- Dédurre l'alphabet chiffré

Autres systèmes classiques

- Les homophones (solution pour attaque par stat)
- Chiffre affine (polynôme)
- Chiffre de Playfair (Chiffrement polygraphique)
- Chiffre de Hill (Matrices)
- Chiffre de Vigenère (amélioration du chiffre de César)
- Chiffre de Vernam (masque jetable)
- Transpositions
- ...
- La machine Enigma
- ...

Définitions

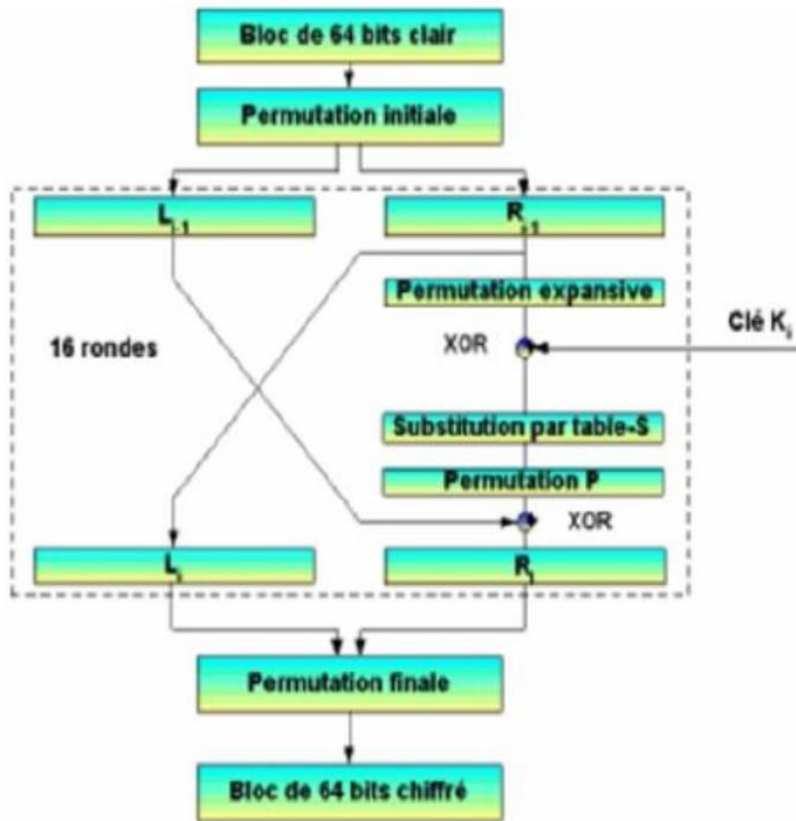
Cryptographie

Cryptographie moderne

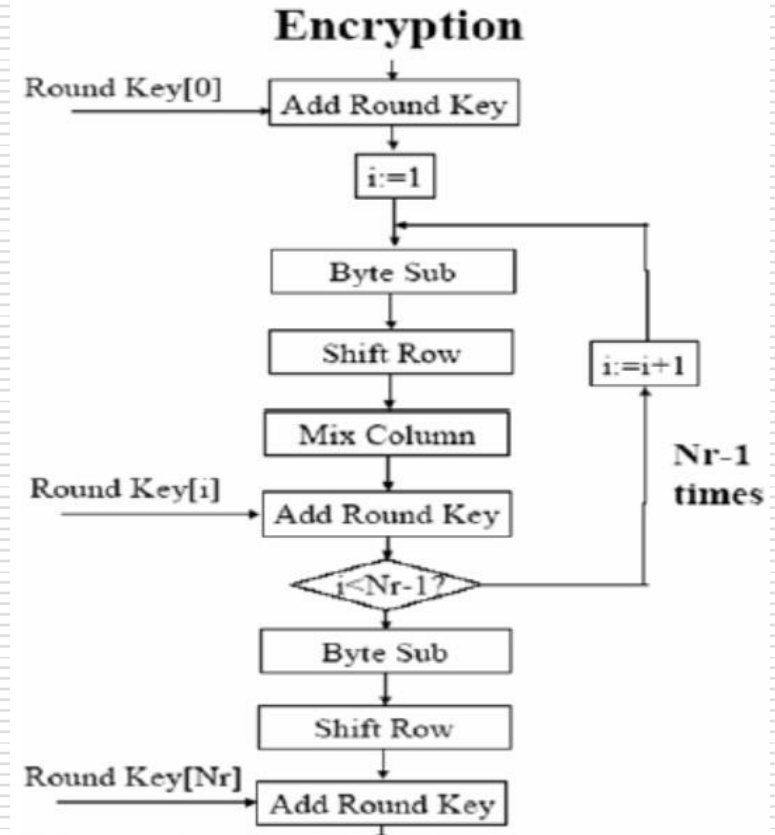
Cryptographie symétrique

- Ou cryptographie à clé privée
- On utilise la même clé pour chiffrer et déchiffrer un message (**$k_e = k_d = k$**).
- Les deux communicants doivent être en possession de cette clé.
- La norme de cryptage de données (**DES, 3DES, AES**) sont un exemple de ce type de système largement utilisé par le gouvernement fédéral des Etats-Unis.

Cryptographie symétrique

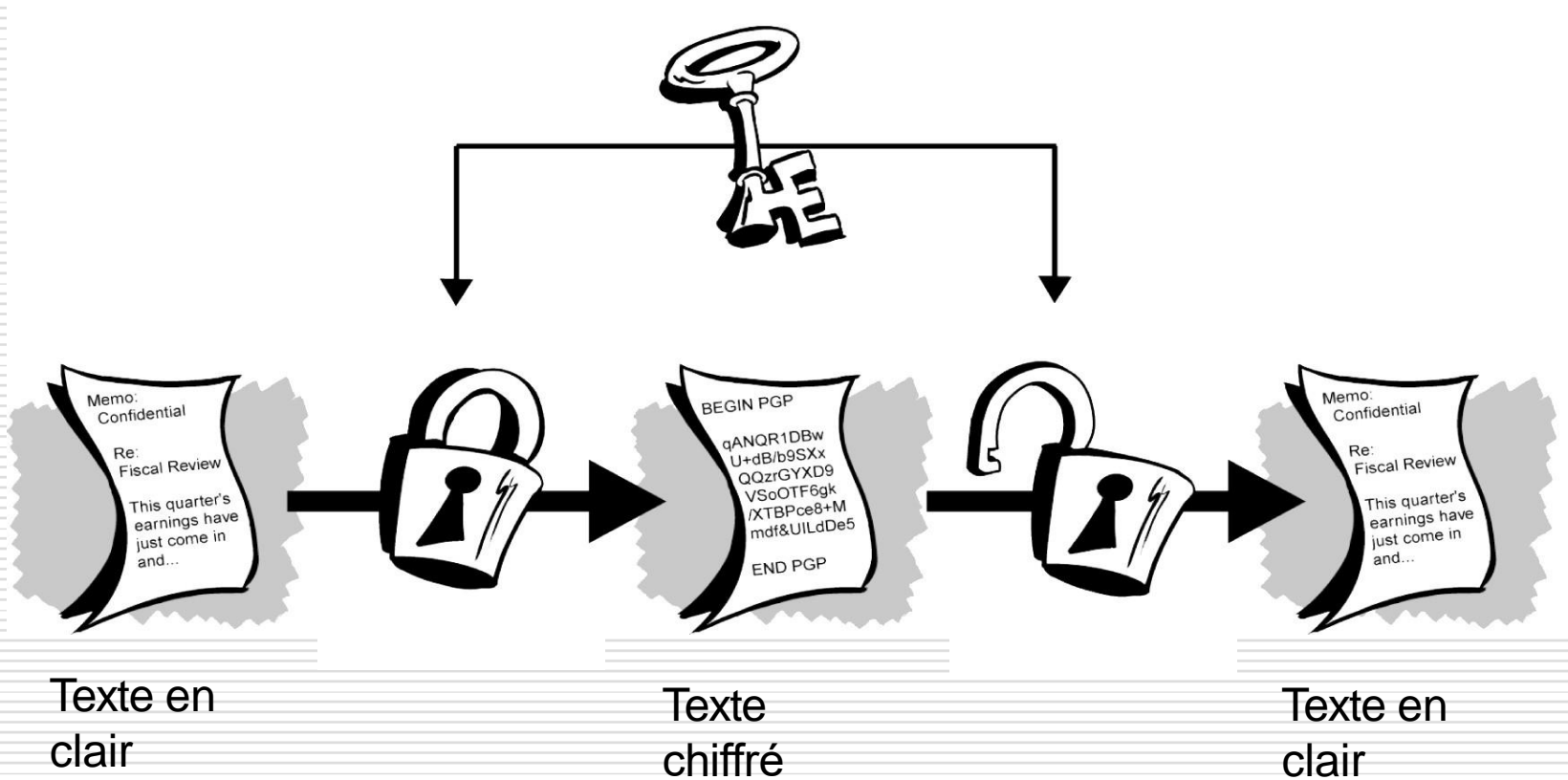


DES



AES

Cryptographie symétrique



Cryptographie symétrique

Avantages et inconvénients

Avantage:

- Il est très rapide

Inconvénient:

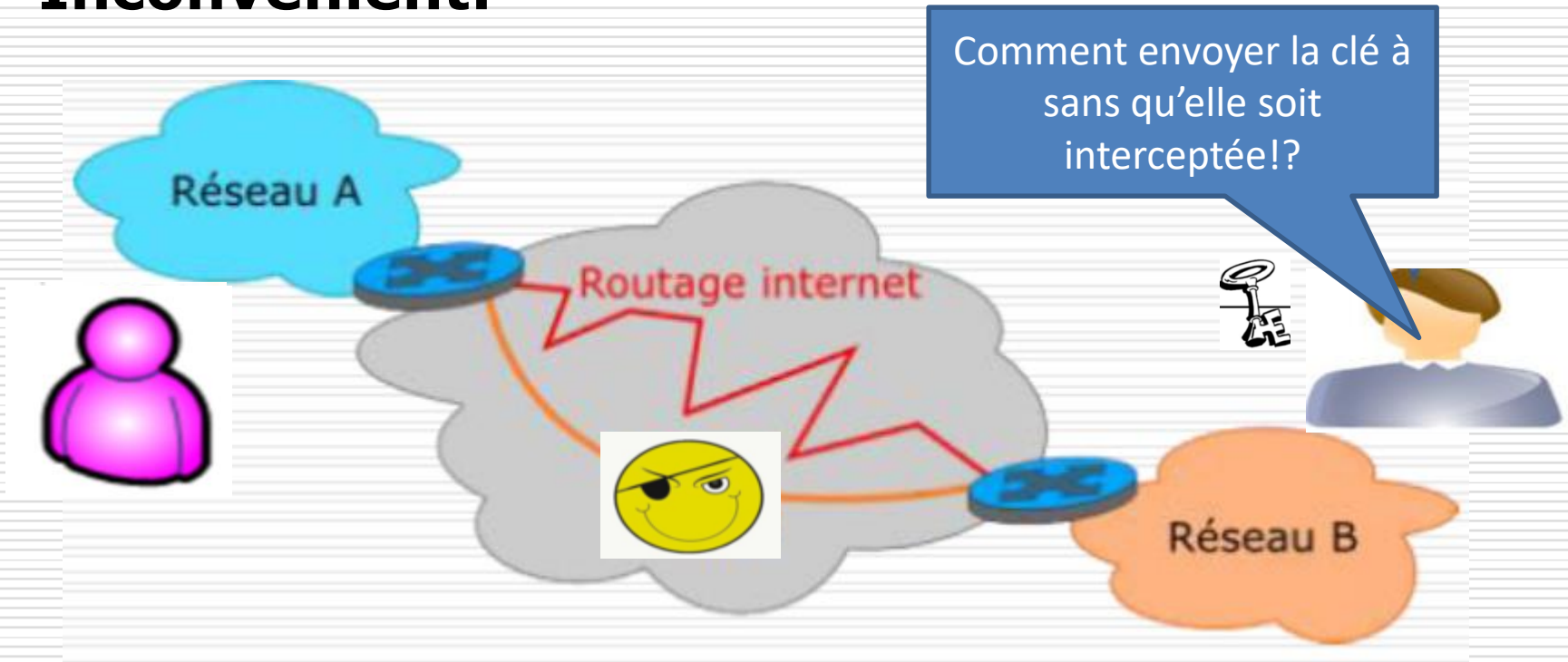
- La **distribution des clés** reste le problème majeur du cryptage conventionnel surtout lorsque Le nombre de communicants devient grand.

Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?

Cryptographie symétrique

Avantages et inconvénients

Inconvénient:



Au début des années 70, la solution fut trouvée (des recherches depuis les années 50).

Cryptographie symétrique

Comment partager un secret ?

Comment cet homme peut-il traverser la rivière avec tous ses animaux ?



Cryptographie symétrique

Comment partager un secret ?

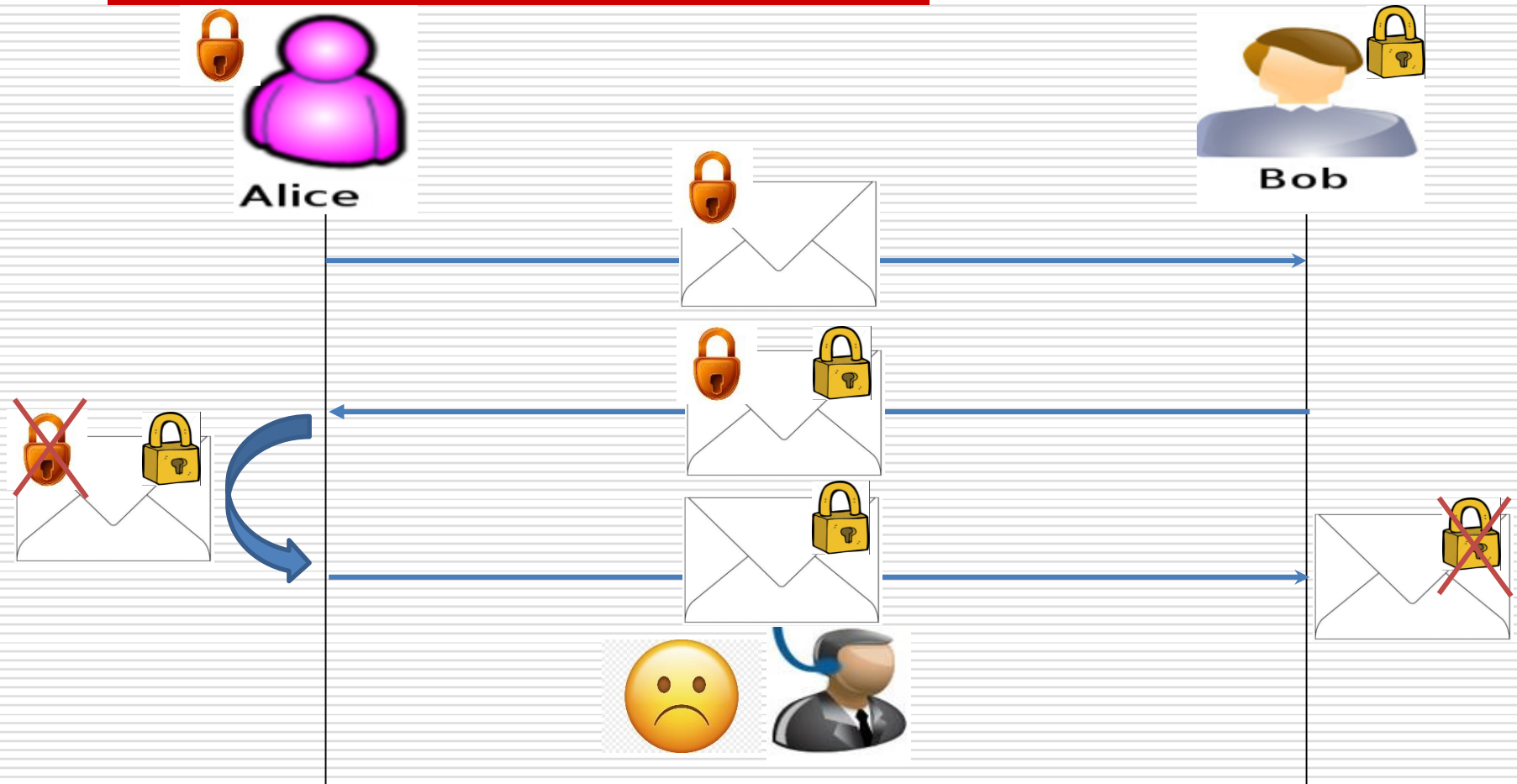
Exemple du facteur :

On suppose que Alice veut envoyer un colis secret à Bob par la poste, mais que leur facteur ne peut s'empêcher de lire les correspondances non closes. Comment peut elle lui envoyer ?



Cryptographie symétrique

Comment partager un secret ?



Cryptographie symétrique

Comment partager un secret ?

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

Remarque

A aucun moment le facteur n'a été en mesure d'ouvrir la boîte

Cryptographie symétrique

Problème?

➤ Encore et toujours des problèmes !!

En particulier l'**ordre** dans lequel sont effectués les chiffrements et les déchiffrements successifs joue un rôle crucial, sans parler **du flux!!!**

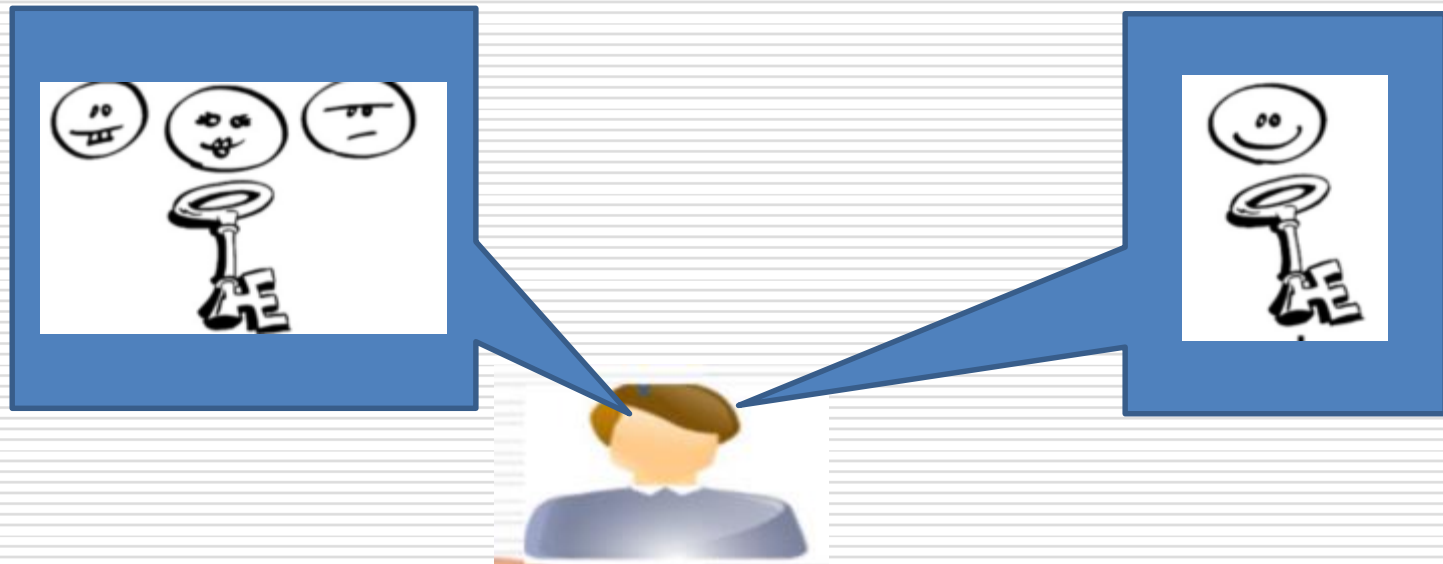
De plus les échanges ne peuvent se faire qu'en **présence de deux parties.**

De là va apparaître la cryptographie asymétrique (à clé publique).

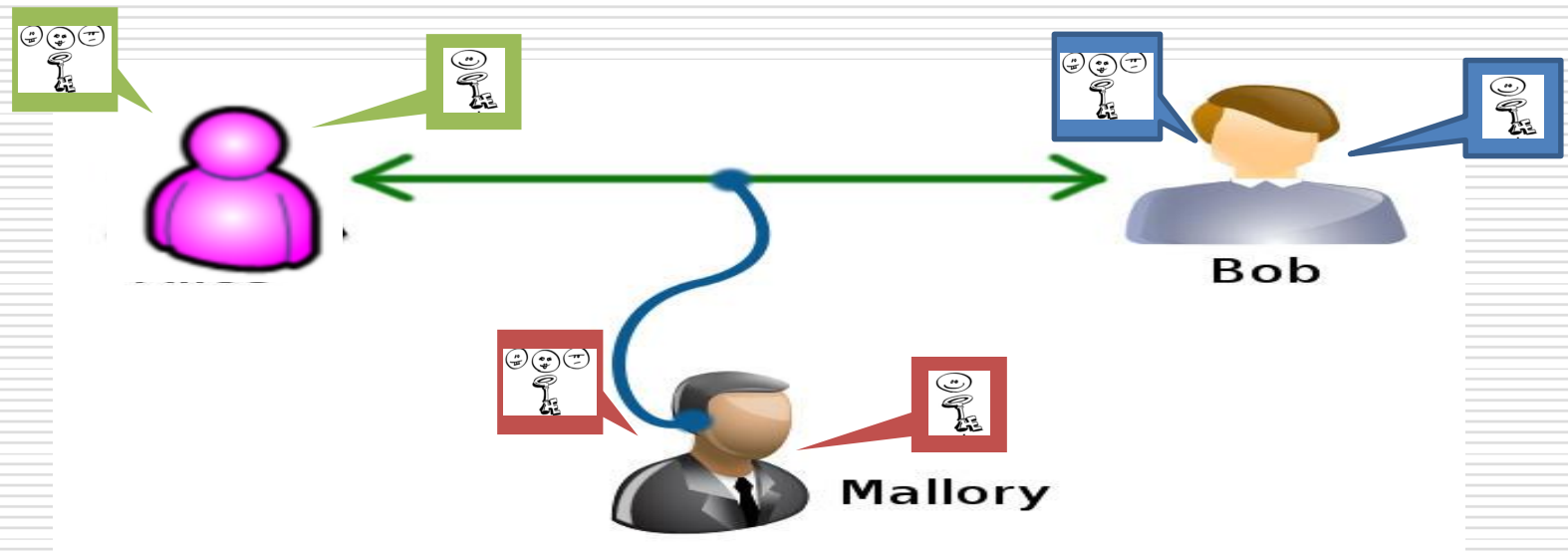
Cryptographie asymétrique

- Chaque entité possède une paire de clés :
Une clé publique, connue par toutes les autres entités et utilisée pour chiffrer un message donné,
Une clé privée qui ne doit être connue que par l'entité qui possède la paire en question, et qui est utilisée pour déchiffrer un message
- Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

Cryptographie asymétrique



Cryptographie asymétrique



Cryptographie asymétrique

- Bob laisse ses cadenas en libre accès à la poste

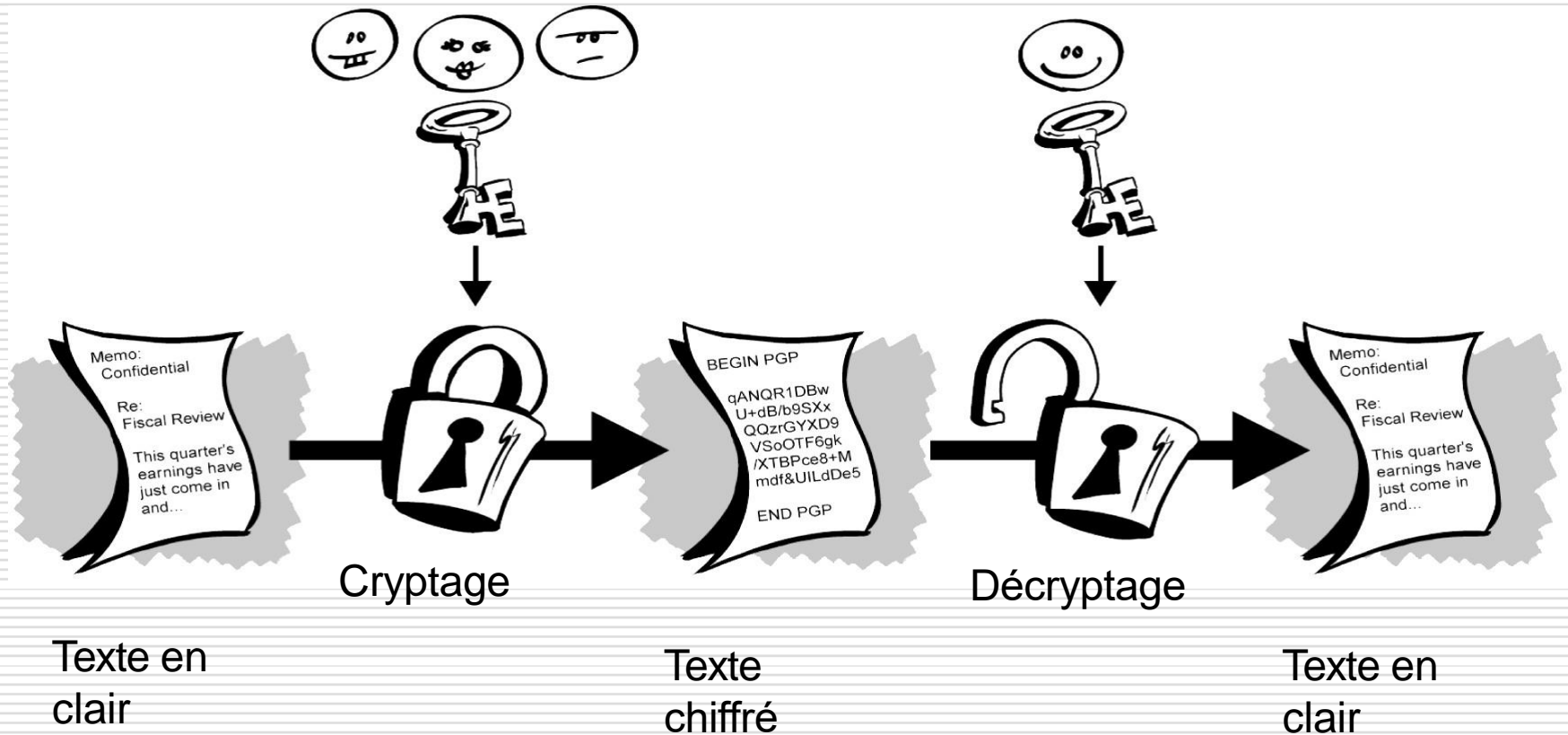


- Alice peut à tout moment venir à la poste prendre un cadenas et envoyer un message à Bob

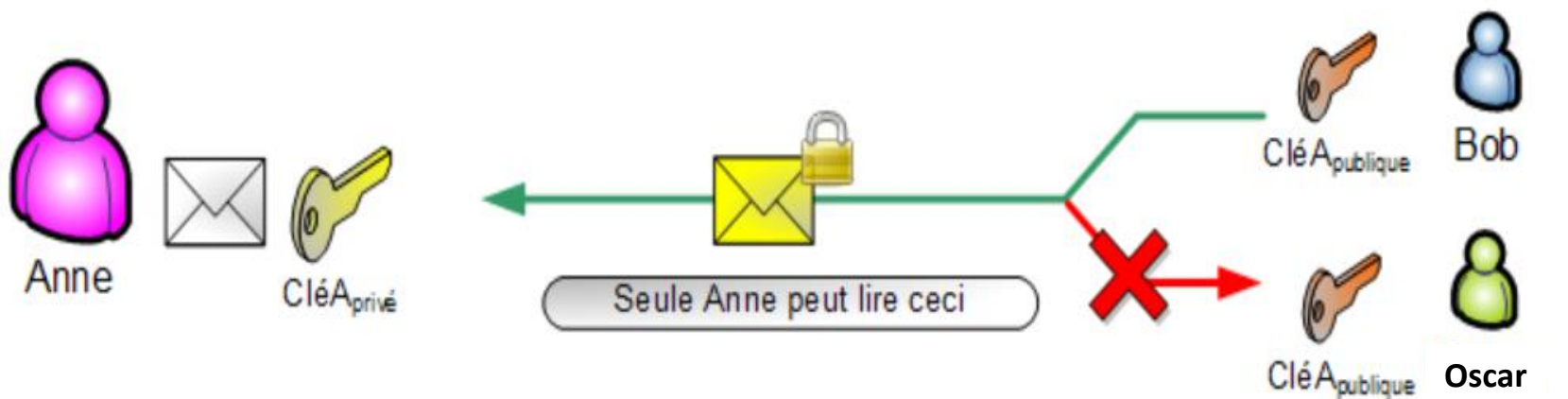
- Bob peut facilement ouvrir son cadenas avec sa clé et récupérer le message.



Cryptographie asymétrique



Cryptographie asymétrique



Cryptographie asymétrique

Difficulté : Il faut avoir un système de cryptage ayant des clés k_e et k_d différentes.

But: Trouver des fonctions mathématiques:

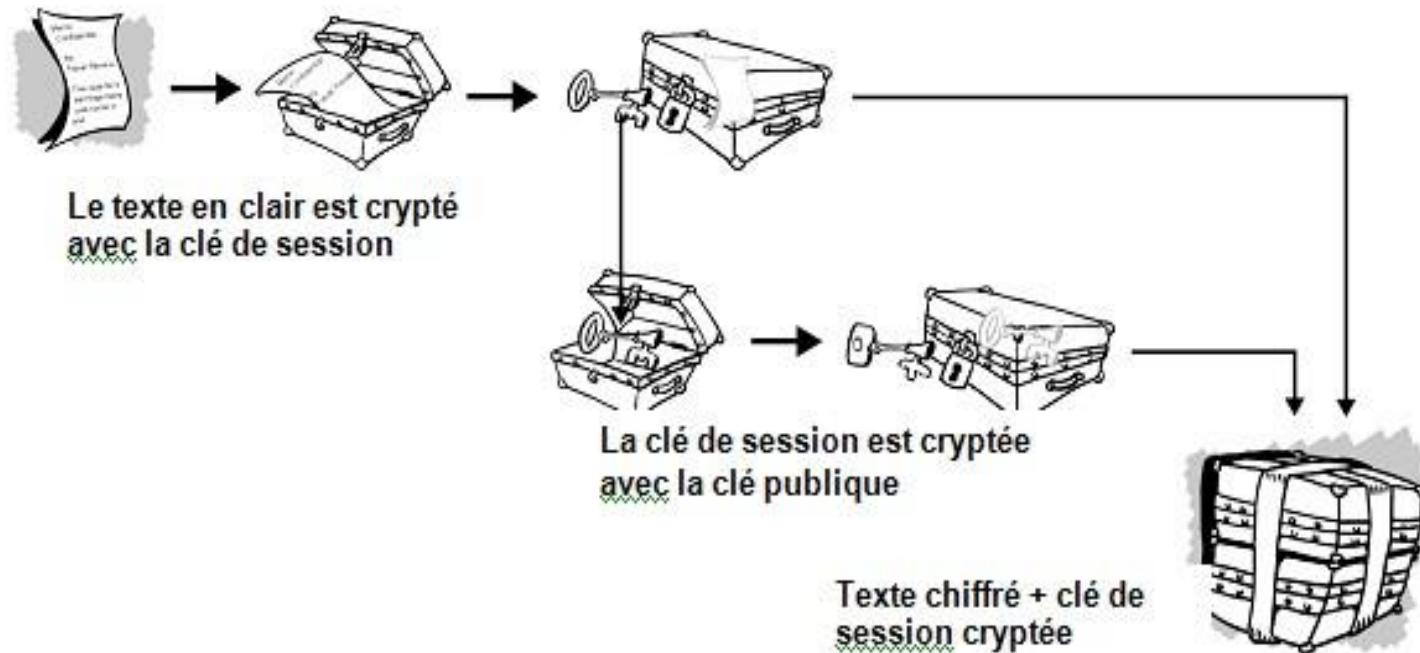
- Faciles à utiliser dans un sens
- Très difficile à inverser

Problème: Très gourmand en calcul surtout avec un grand message à chiffrer!!! **1000 fois plus lent** que AES.

Solution: Le chiffrement asymétrique est utilisé pour distribuer des clés symétriques.

Cryptographie asymétrique

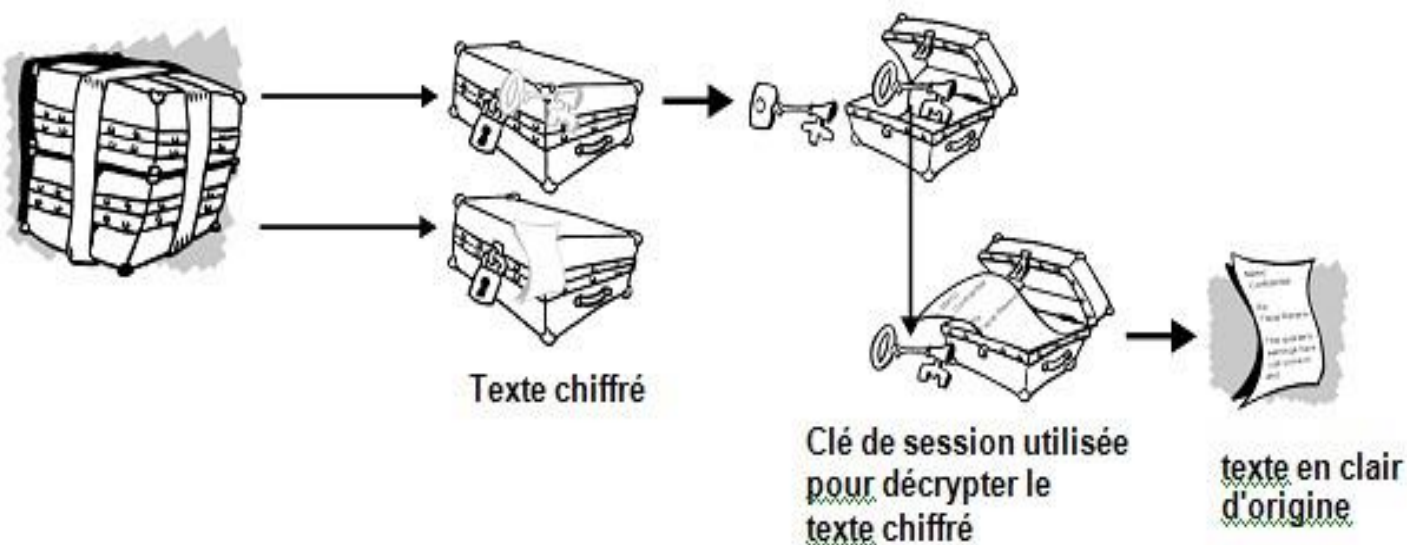
Exemple dans le système PGP



Fonctionnement du cryptage PGP

Cryptographie asymétrique

Exemple PGP



Fonctionnement du décryptage PGP

Cryptographie asymétrique

- L'exponentiation de grands nombres premiers (**RSA**),
- Le problème des logarithmes discrets (**ElGamal**),
- Le problème du sac à dos (**Merkle-Hellman**).

Cryptographie asymétrique

RSA: le premier protocole a clef publique

- Alice choisit deux grands nombres premiers p et q et calcule : **$n = p \times q$** 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 $(ed-1)$ est exactement divisible par z .
 - **Elle déduit :**
- Clé publique = (n, e) et clé privée = (n, d)

Cryptographie asymétrique

RSA: le premier protocole a clef publique

- Grâce à sa clé public, Bob peut chiffrer son message avec la formule RSA. 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 p et q .

Bob veut envoyer un message m à Alice :
chiffrement : **$c = m^e \bmod n$**

Alice reçoit le message c et calcule :

déchiffrement : **$m = c^d \bmod n = (m^e \bmod n)^d \bmod n$**

Cryptographie asymétrique

RSA: le premier protocole a clef publique

➤ **Exemple:**

$p=5, q=7, m=12$

Exemple :

$p=5, q=7$, donc $n=35$ et $z=24$

Alice choisit $e=5$ et déduit $d=29$

Bob : (chiffrement) : $m=12$, $me=248832$, $c=me \bmod n = 17$.

Alice : (déchiffrement) : $c=17$,
 $cd=4819685721067509141182522307200$
 0

$m = cd \bmod n = 12$.

Cryptographie asymétrique

Challenge RSA

Factoriser le nombre:

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

et utiliser cette factorisation pour déchiffrer un Message codé avec RSA.

100\$ était offert au premier qui parviendrait à déchiffrer le message.

Cryptographie asymétrique

Challenge RSA

- Le but de ce concours était de tester la robustesse de RSA.
- Il aura fallu 17 ans pour qu'une équipe de 600 personnes remporte le concours !!!

Cryptographie asymétrique

Un nouveau challenge est lancé

Nouveau challenge RSA

```
25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357
```

Récompense 200 000\$!!!



Comment assurer les autres objectifs
de sécurité???

Comment assurer les autres objectifs de sécurité???

- Jusqu'à présent, on a traité uniquement la confidentialité !!!!!
- Et les autres objectifs ?
 - **L'authentification**
 - **L'intégrité des données,**
 - **Non répudiation**
- **Solution :**

Signature numérique

Signature numérique

➤ L'un des principaux avantages de la cryptographie de clé publique est qu'elle offre une méthode d'utilisation des signatures numériques.

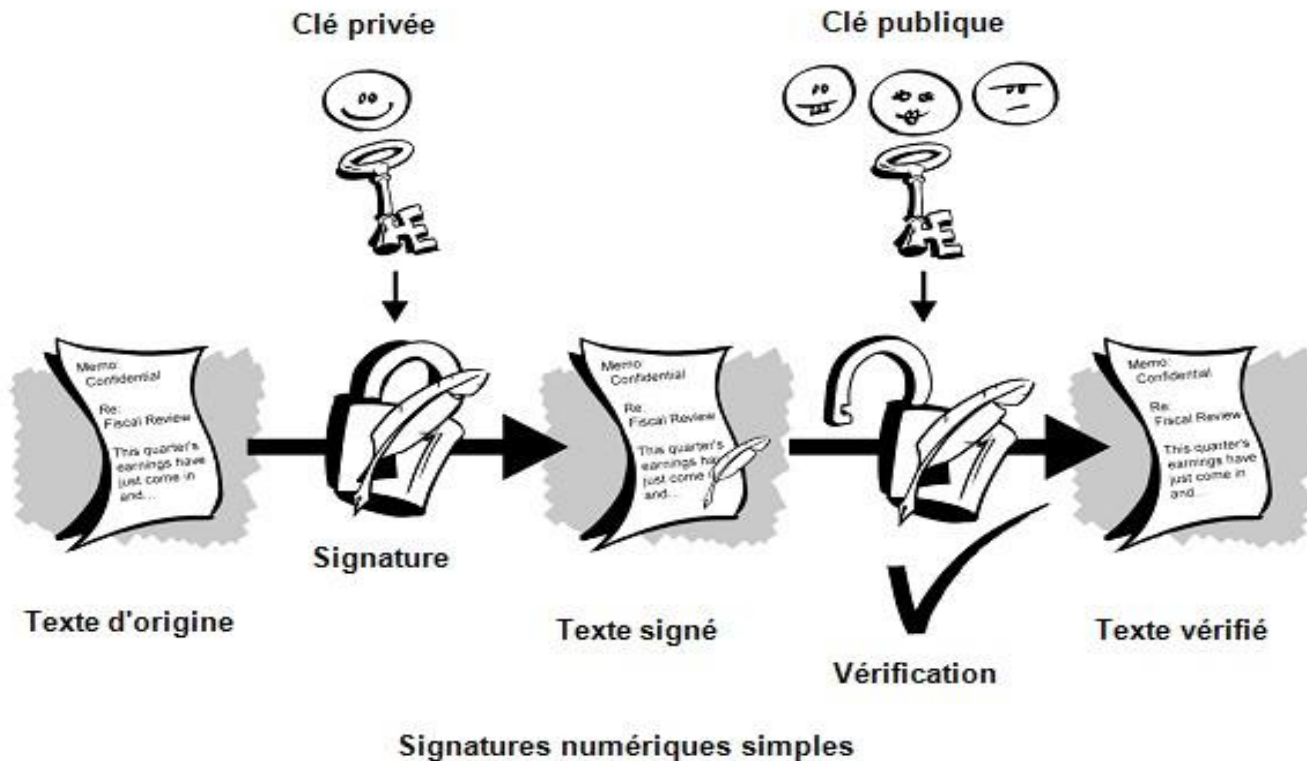
C'est une chaîne de données qui associe un message (dans sa forme numérique) à l'entité dont il est originaire.

➤ Les signatures numériques sont largement utilisées dans la sécurité informatique, dans **l'authentification** ou **l'intégrité des données**, et la **non répudiation**

Signature numérique



Signature numérique



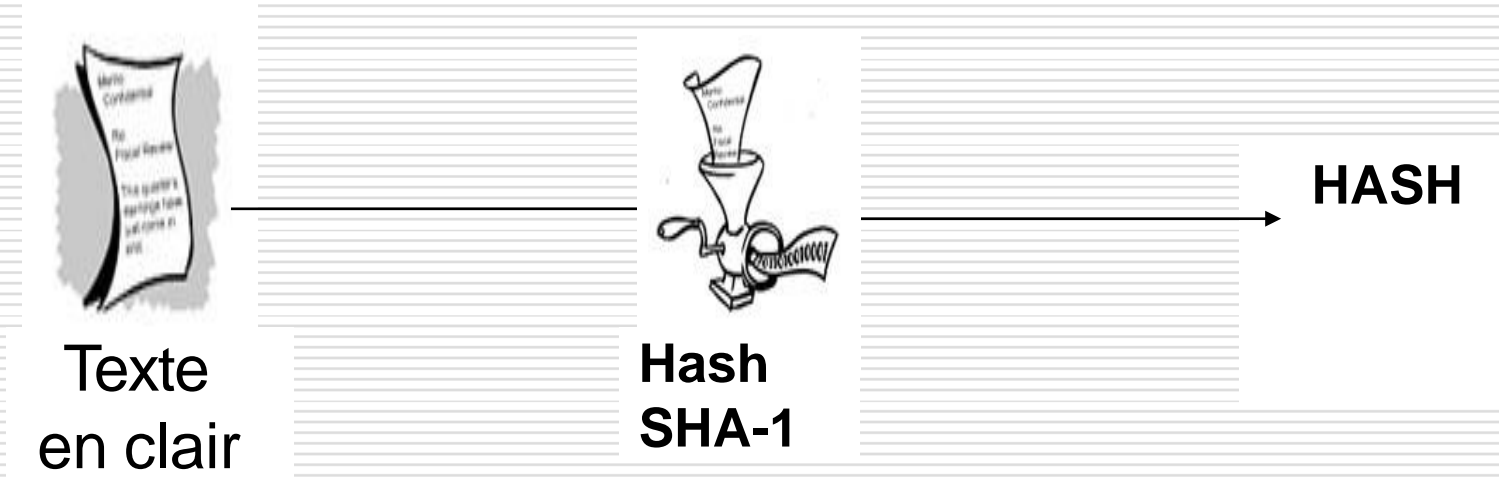
Signature numérique



Problème: Très gourmand en calcul surtout avec un grand message à chiffrer!!!

Signature numérique

Fonction de hachage



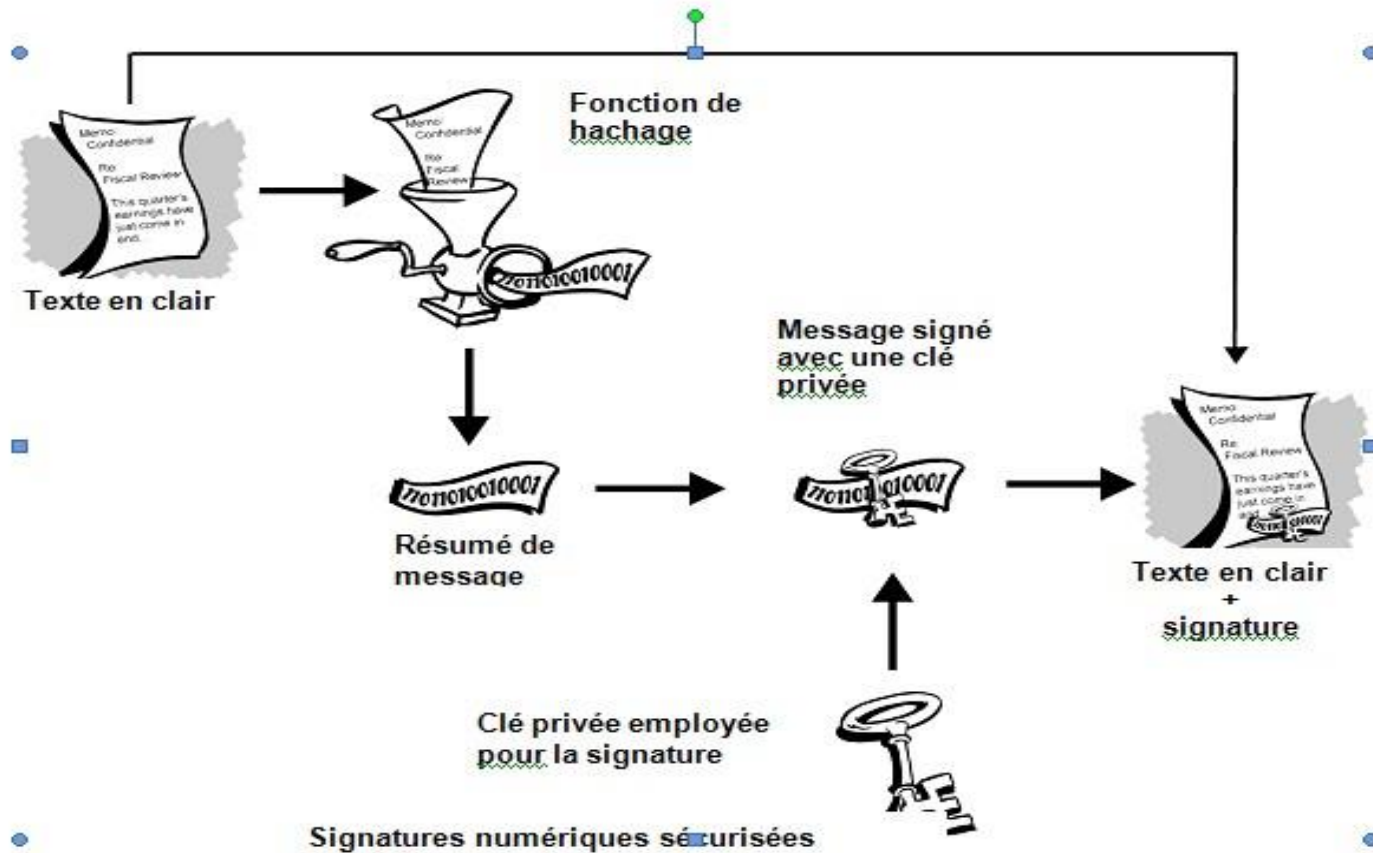
Signature numérique

Fonction de hachage

- Le système précédent est **lent** et produit un **volume important de données**.
- L'ajout d'une **fonction de hachage** à sens unique permet d'améliorer le schéma précédent.
- Cette fonction traite une entrée de longueur variable et donne en sortie un élément de longueur fixe, à savoir 160 bits.
- En cas de modification des données, la fonction de hachage donne une valeur de sortie différente.

Signature numérique


Fonction de hachage: Exemple PGP



Signature numérique

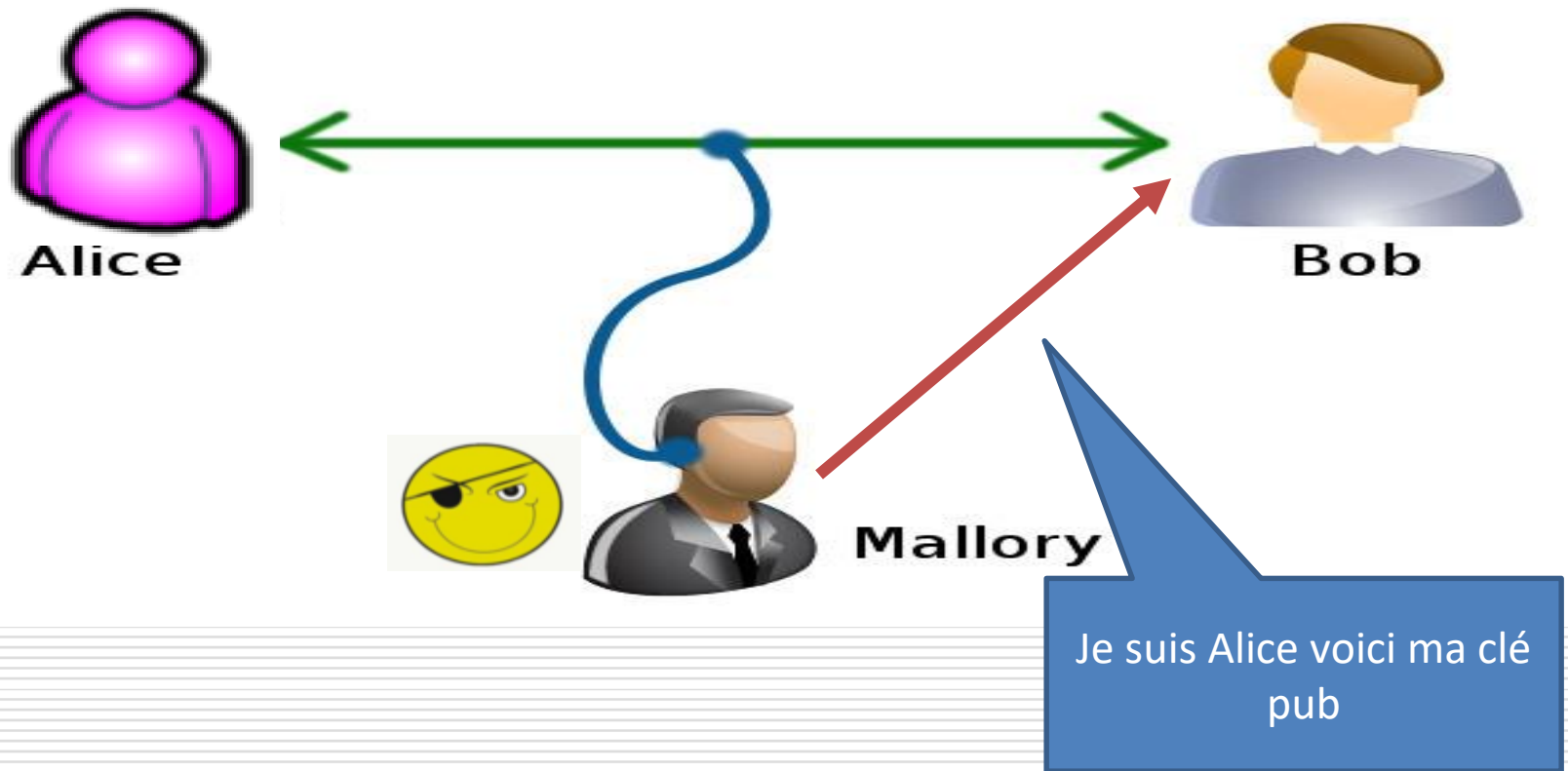
Exemples de fonctions de Hashage

- **MD5** : Message Digest 5, il génère une empreinte de 128 bits.
- **SHA-1** : Secure Hash Algorithm, il génère une empreinte de 160 bits..



Un autre Problème avec La Cryptographie asymétrique

Problème avec la Cryptographie asymétrique

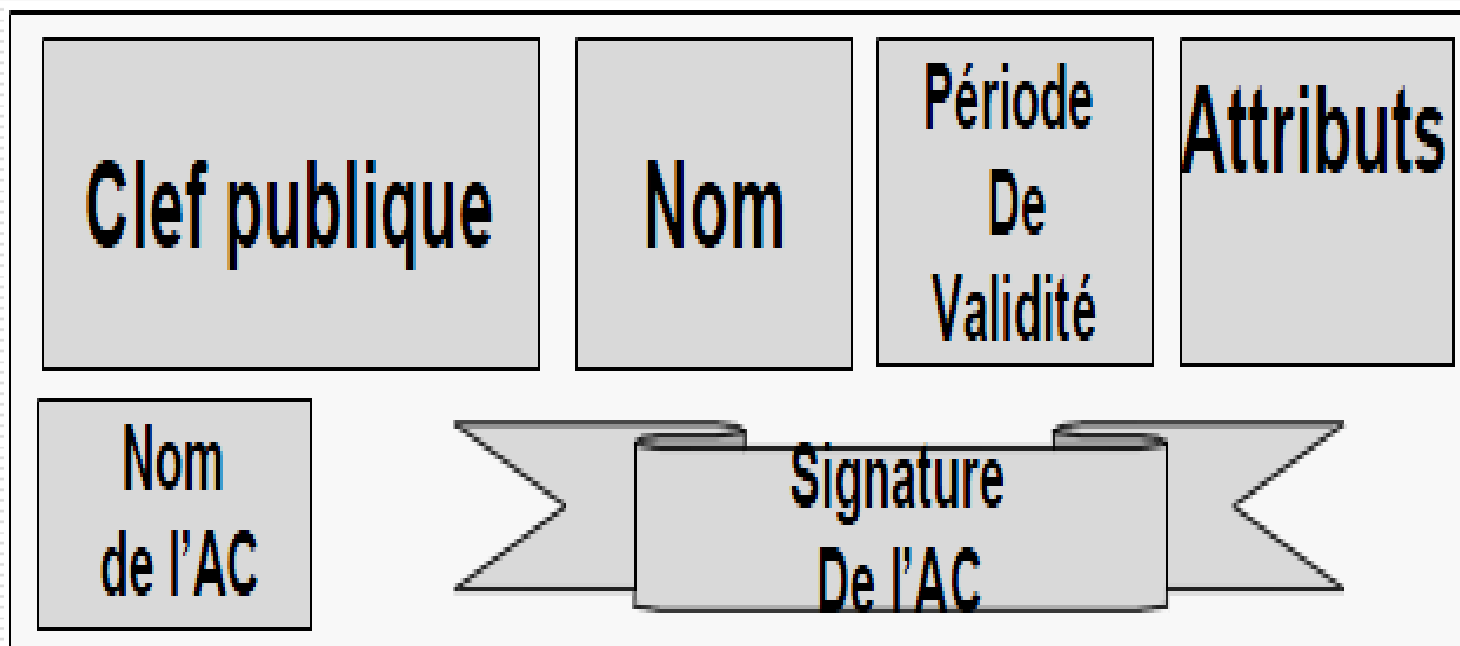


Problème avec la Cryptographie asymétrique

- Une personne peut placer une fausse clé (celle du pirate par exemple) comportant le nom et l'ID utilisateur du destinataire.
- Les données cryptées (et interceptées) vers le détenteur réel de cette clé erronée sont dorénavant entre de mauvaises mains.
- Donc les utilisateurs doivent constamment vérifier qu'ils cryptent vers la clé du bon utilisateur.
- **Solution:** l'utilisation des **Certificats numériques**

Certificats numériques

Les certificats sont émis par une autorité de certification (Certificate Authority – CA)



Certificats numériques

Les certificats sont émis par une autorité de certification (Certificate Authority – CA)

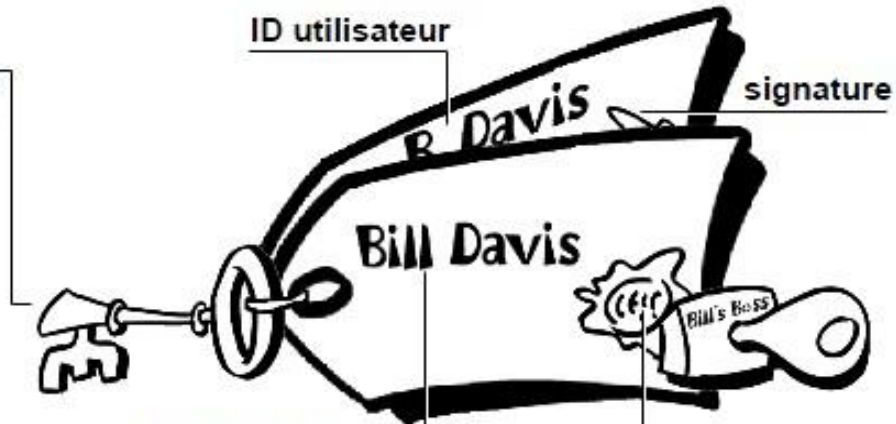


Certificats numériques

Exemple certificat PGP

clé publique

- numéro de version de PGP
- heure de création de la clé
- durée de validité de la clé
- type de clé (DH, RSA)
- clé elle-même



ID utilisateur

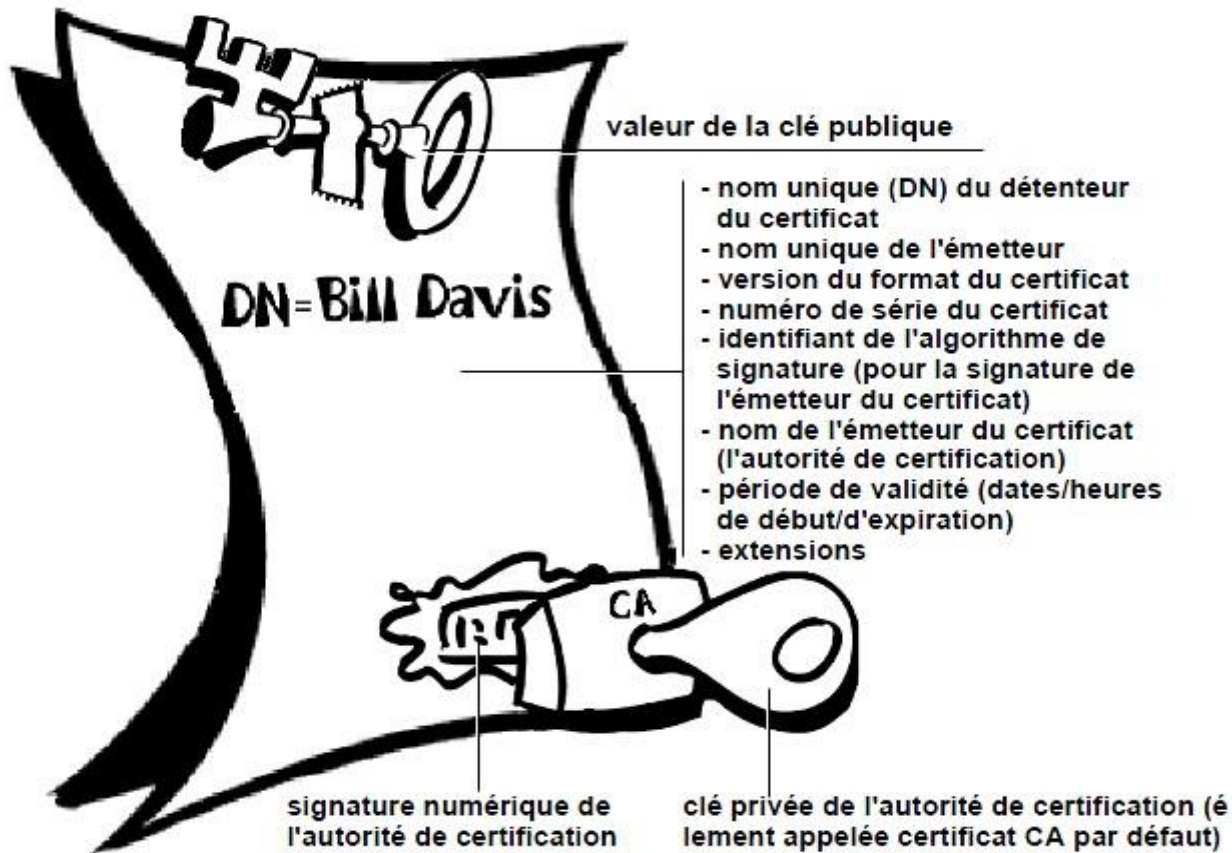
- chaîne de caractères identifiant le détenteur de la clé

signature

- certification de l'association de l'ID utilisateur à la clé
- numéro de version
- algorithme de résumé de message
- calcul de résumé de message
- résumé de message signé
- ID de la clé du signataire

Certificats numériques

Exemple certificat X.509



Certificats numériques

- Les certificats numériques simplifient la tâche qui consiste à déterminer si une clé publique appartient réellement à son détenteur supposé.
- Un certificat correspond à une référence. Il peut s'agir par exemple de votre **permis de conduire**, de votre **carte de sécurité sociale** ou de votre **certificat de naissance**.
- Chacun de ces éléments contient des informations vous identifiant et **déclarant qu'une autre personne a confirmé votre identité**.

Certificats numériques

Un certificat numérique contient des données similaires à celles d'un certificat physique.

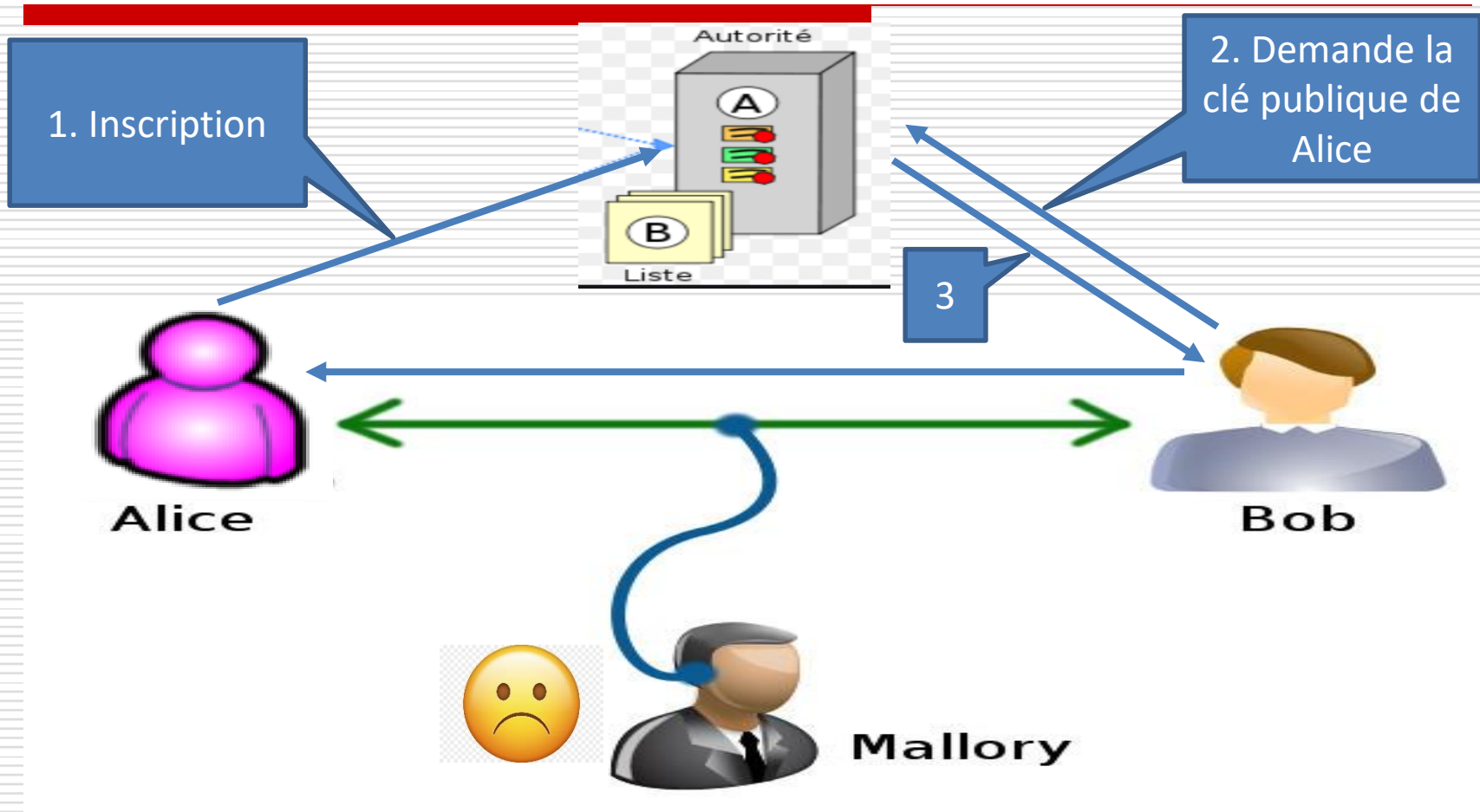
Un certificat numérique se compose de:

- **Une clé publique.**
- Des informations sur le certificat. (Informations sur l'« **identité** » de l'utilisateur: nom, ID utilisateur, etc.)
- Une ou plusieurs **signatures numériques**.

La signature numérique d'un certificat permet de déclarer que ses informations ont été attestées par une autre personne ou entité.

Certificats numériques

Principe



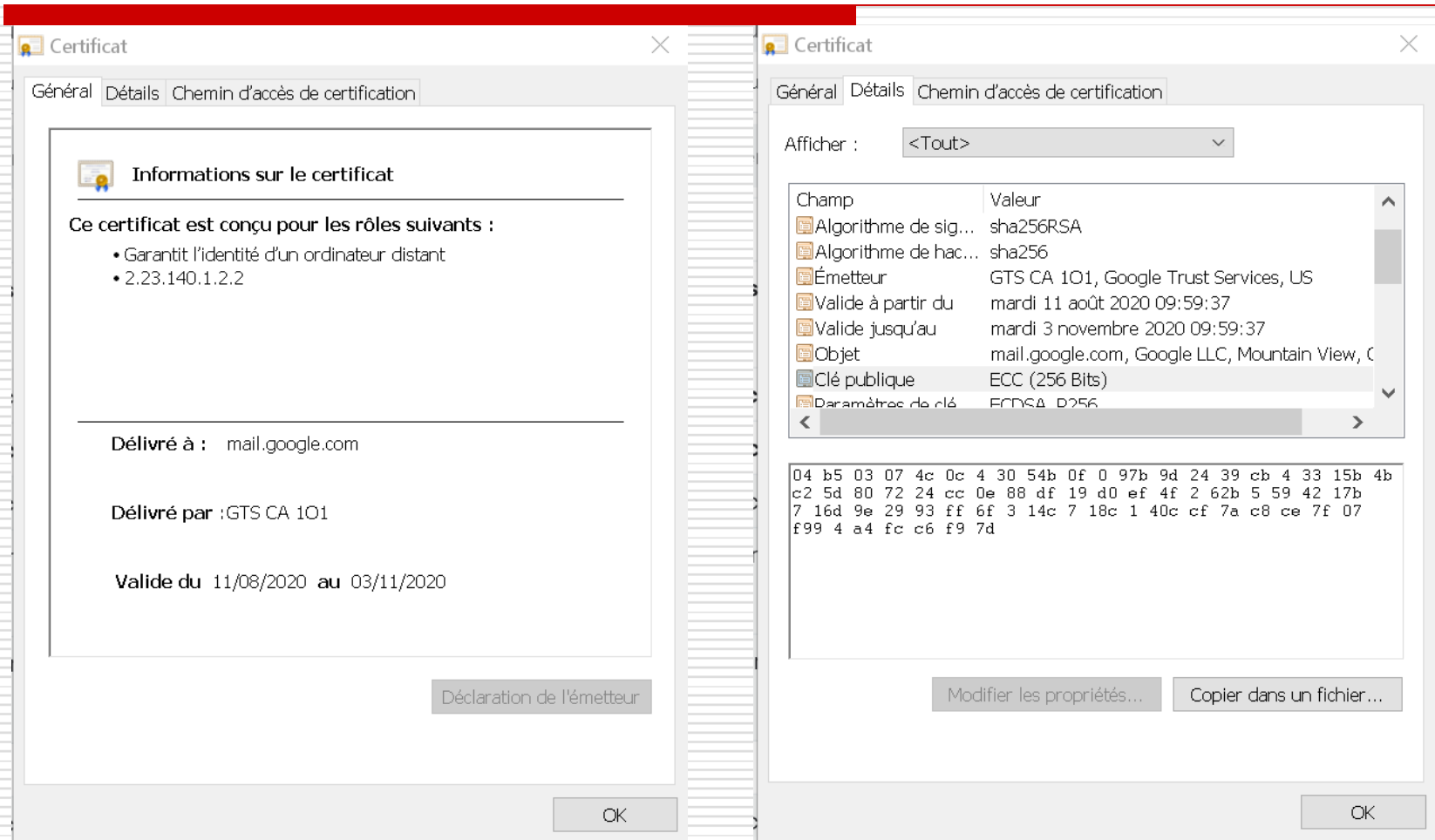
Certificats numériques

Principe

- Alice fait une requête de certification d'une clé publique auprès d'une autorité de certification.
- Cette dernière vérifie la véracité des infos contenues dans ce certificat (authentications des infos) puis le certificat est émis dans un annuaire
- Bob récupère la clé publique d'Alice via l'annuaire, récupère aussi un certificat anti-signé via l'autorité de certification et vérifie son intégrité grâce à la signature de la CA.

Certificats numériques

Principe



PKI (Public Key Infrastructure)

Infrastructure à clefs publiques

Nature : Infrastructure (ensemble d'éléments, protocoles et services)

Rôle : Gestion des clés publiques à grandes échelle

- Enregistrement et émission
- Stockage et distribution
- révocation et vérification de statut
- Utilisation de certificats

PKI (Public Key Infrastructure)

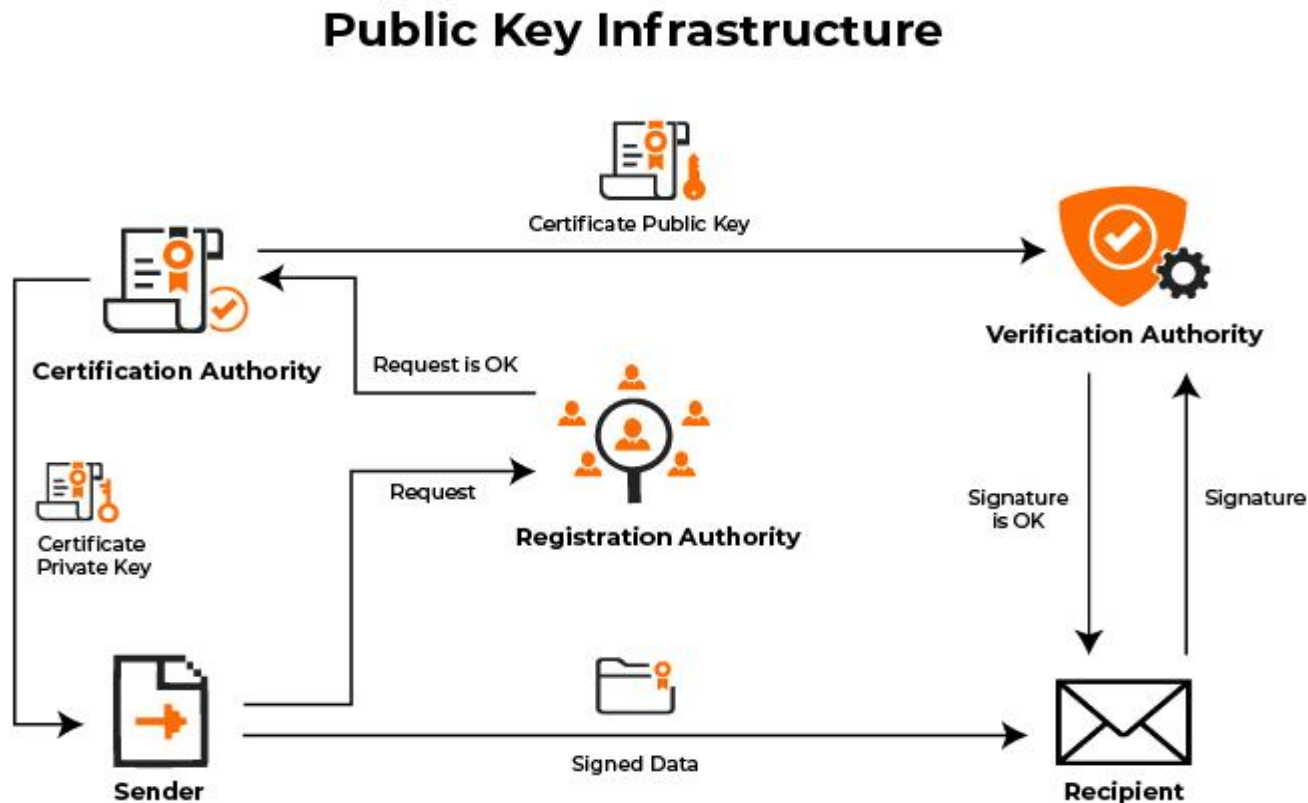
Infrastructure à clefs publiques

C'est toute l'infrastructure nécessaire au fonctionnement d'une ou plusieurs ACs pour délivrer des certificats :

- **Matériel** : ordinateurs, locaux...
- **Informatique** : logiciels
- **Humain** : les employés
- **Organisationnel** : procédures de révocation...
- **Administratif** : désignation d'un responsable
- **Financier** : assurance des risques en cas de dommage par utilisation de certificat

PKI (Public Key Infrastructure)

Infrastructure à clefs publiques



Résumé

- **Confidentialité (chiffrement hybride):**
 - Clé (de session) Symétrique pour chiffrer les messages
 - Clé Asymétrique pour chiffrer la clé symétrique

- **Intégrité, Authentification, Non répudiation:**
 - Fonctions de hachage pour la signature numérique
 - Certificats pour authentifier les clés publiques

Autres systèmes de chiffrement

- L'échange de clés Diffie-Hellman
- Cryptographie à seuil
- Cryptographie Quantique (utiliser les propriétés de la physique quantique)
- MAC (Code d'Authentification de Message)
- ECC (La cryptographie sur les courbes elliptiques)
- TESLA
- ...

Utilisations de la cryptographie



Les applications et les Communications sécurisées



Les Communications sécurisées

Le protocole SSH (Secure Shell)

Les protocoles d'accès distant à une machine tels que Telnet, rlogin, etc.. Sont limités:

- Circulation des **mots de passe en clair**
- Authentification faible basée sur le numéro IP
- Commandes à distance non sécurisées.
- Transferts de fichiers non sécurisés.

Solution: l'utilisation du protocole SSH



SSH utilise la cryptographie asymétrique (**RSA**) et symétrique

Le protocole SSH

Principe

Le serveur a un couple de clefs stocké dans /etc/ssh et généré lors de son lancement.

1. Lorsqu'un client SSH se connecte au serveur, ce dernier envoie sa clé publique au client.
2. Le client génère une clé secrète (chiffrement symétrique), et l'envoie au serveur, en cryptant l'échange avec la clé publique du serveur.
3. Le serveur déchiffre la clé secrète avec sa clé privée.

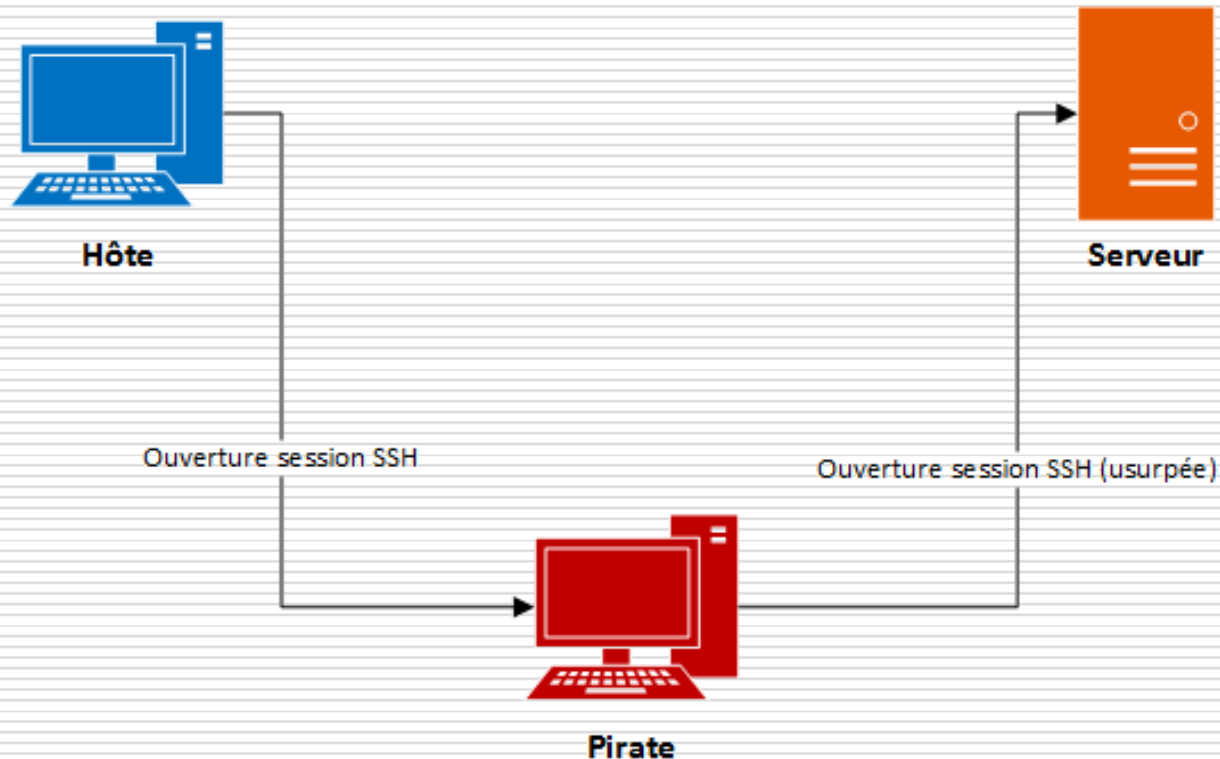
Le protocole SSH

Principe

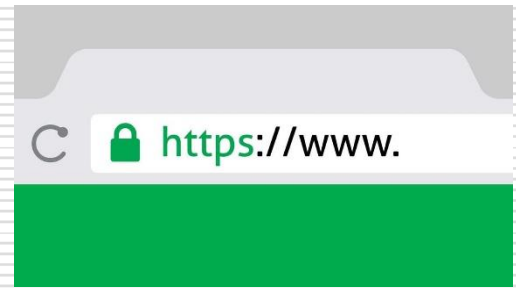
4. Pour prouver au client qu'il est bien le bon serveur (authentification du serveur), il crypte un message standard avec la clé secrète et l'envoie au client.
5. Si le client retrouve le message standard en utilisant la clé secrète, il a la preuve que le serveur est le vrai.
6. Une fois la clé secrète échangée, le client et le serveur peuvent alors établir un canal sécurisé (grâce à la clé secrète partagée).

Faible du protocole SSH

➤ Attaque à base de la méthode Man In The Middle



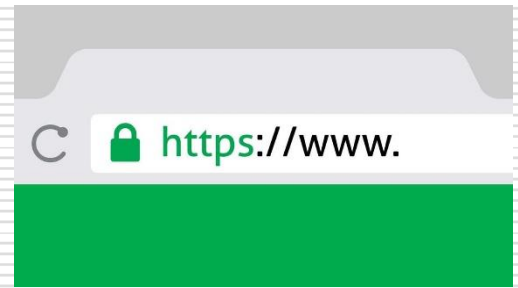
SSL/TLS



SSL(Secure Socket Layer):

- Se situe entre la couche application et la couche transport.
- Garantit l'authentification, l'intégrité et la confidentialité.
- Développé par netscape et largement utilisé pour la sécurisation des sites www (https).
- La dernière version est SSL 3.0

SSL/TLS



TLS (Transport Layer Security)

- TLS 1.0 remplace SSL (very few differences).
- TLS 1.1 est la dernière version
- Tous les serveurs Web et les navigateur supportent la version TLS 1.1

Réseau VPN

(réseau privé virtuel)



- . permet d'établir des communications sécurisées en s'appuyant sur un réseau existant non sécurisé.

VPN utilise le protocole IPSEC qui est composé de quatre protocoles :

➤ **Le protocole AH** (Authentication Host)
ce protocole permet de garantir l'authenticité des paquets échangés en leur inscrivant une somme de contrôle (entête du paquet + données du paquet) chiffrée.

Réseau VPN

(réseau privé virtuel)



- **Le protocole ESP** (Encapsuling Security Payload) :
Ce protocole permet de chiffrer toutes les données du paquet garantissant leur confidentialité
- **Le protocole IPComp** :
Ce protocole permet de compresser un paquet avant de le chiffrer avec ESP
- **Le protocole IKE** (Internet Key Exchange) :
Ce protocole est utilisé pour l'échange des clés pour les différents chiffrements.

Réseau VPN

(réseau privé virtuel)

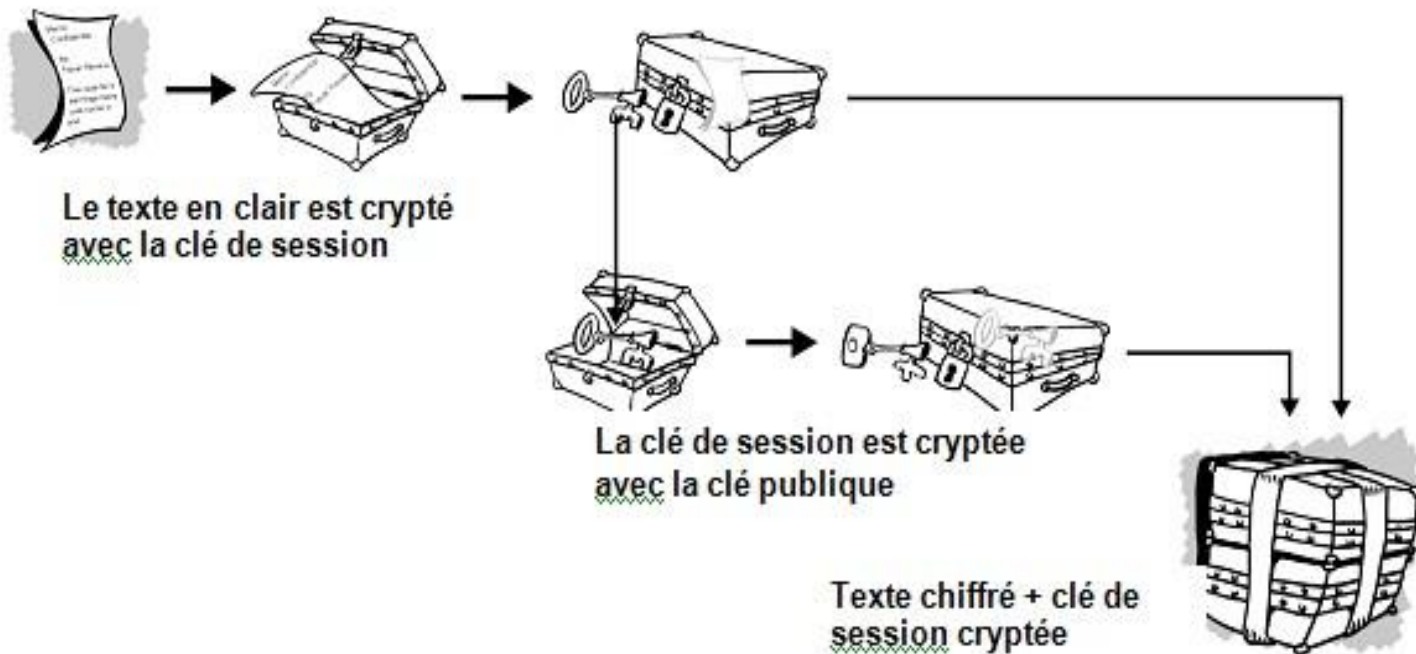


VPN utilise aussi les protocoles:

- **PPTP** (point to point tunnelling protocol)
- **L2TP** (Layer 2 tunnelling protocol)

Les applications sécurisées

L'outil PGP



Fonctionnement du cryptage PGP

L'outil PGP



- Est un logiciel de cryptographie qui est bien adapté à l'utilisation sur Internet.
- PGP est une combinaison des fonctionnalités de la cryptographie de clé publique et de la cryptographie de clé secrète : **C'est un système hybride**
- PGP utilise en plus la **compression des données** afin de renforcer la sécurité des informations, de réduire le temps de transmission et d'économiser l'espace disque.

L'outil PGP

Chiffrement et déchiffrement

PGP crée une **clé de session** à usage unique. Cette clé correspond à un **nombre aléatoire**, généré par les déplacements aléatoires de la souris et les séquences de frappes de touche.

Pour crypter un texte clair, la clé de session utilise un Algorithme de chiffrement symétrique conventionnel (DES, AES,...).

Une fois les données codées, la clé de session est chiffrée à l'aide de la clé publique du destinataire (à l'aide d'une méthode de chiffrement asymétrique).

L'outil PGP

Chiffrement et déchiffrement



La clé de session chiffrée ainsi que le texte chiffré est transmis au destinataire.

Le processus de décryptage est inverse : le destinataire utilise sa clé privée pour récupérer la clé de session temporaire qui permettra ensuite de déchiffrer le texte chiffré.

Le protocole Kerberos



Kerberos est un protocole d'authentification réseau .

Kerberos utilise un système de tickets au lieu de mots de passe en texte clair. Ce principe renforce la sécurité du système et empêche que des personnes non autorisées interceptent les mots de passe des utilisateurs.

L'ensemble repose sur un chiffrement symétrique (clefs privées).

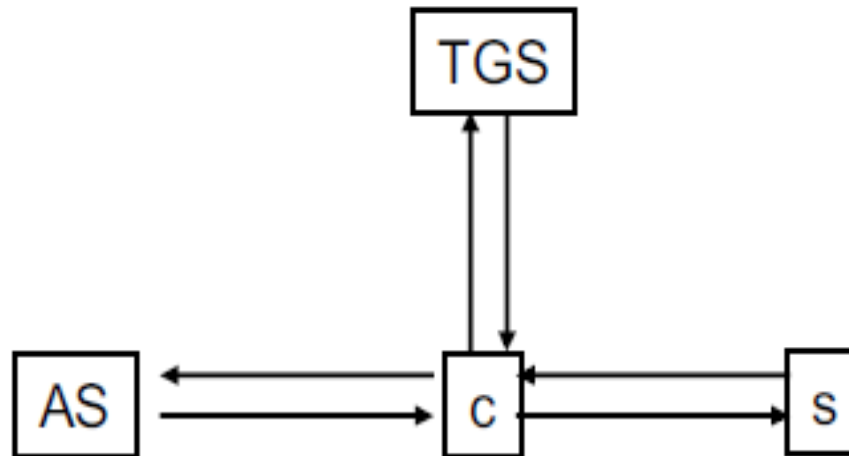
Le protocole Kerberos éléments



Dans un réseau simple utilisant Kerberos, on distingue:

- **Le client** (C), il a sa propre clé privée *KC*
- **Le centre de distribution de clés** (KDC pour *key distribution center*), il connaît les clés privées *KC* et *KTGS* (appelé aussi *AS: Authentication Server*)
- **Le serveur de tickets** (TGS pour *ticket granting server*), il a une clé privée *KTGS* et connaît la clé privée *KS* du serveur
- **Le serveur** (S), il dispose aussi d'une clé privée *KS*

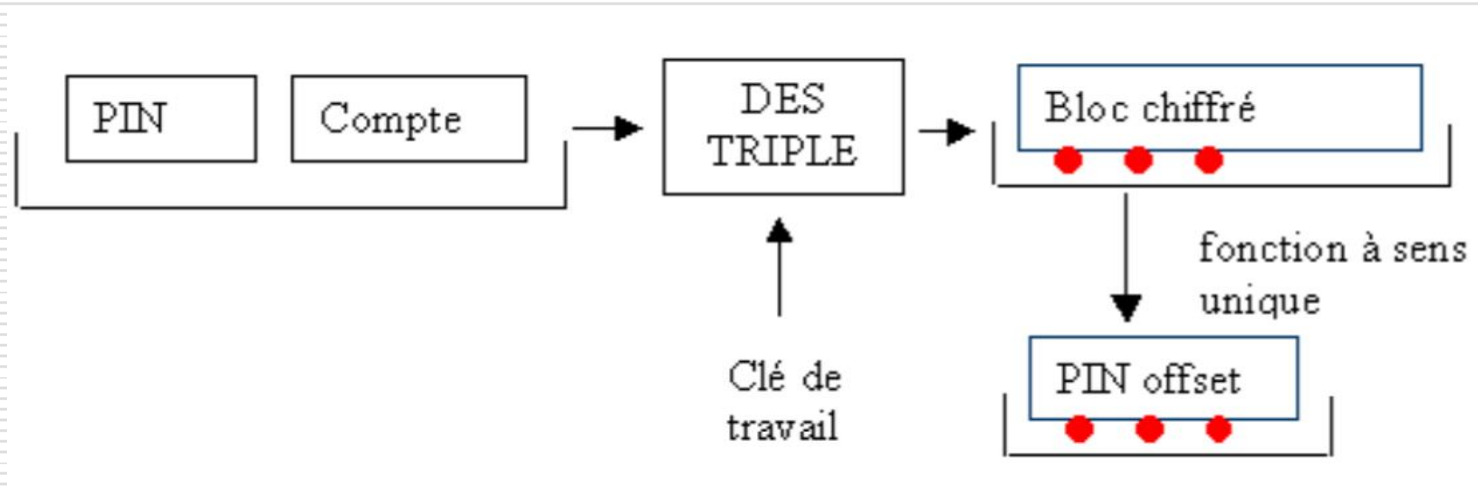
Le protocole Kerberos éléments



Le protocole des cartes bancaires



Fabrication de la carte



Utiliser OpenSSL pour les Tps Crypto Hybride



Enfin!!!