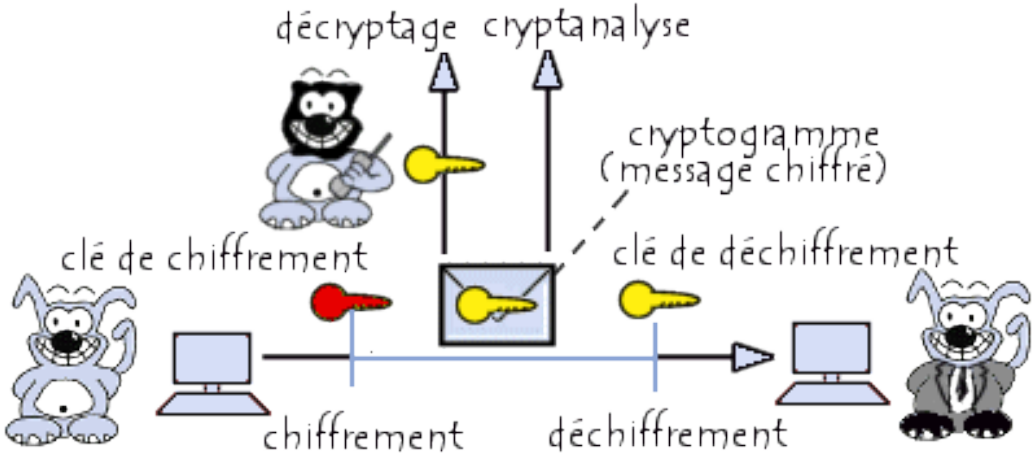
Sécurité des Systèmes d'Information
Cryptographie

Martin Peres

Doctorant de Francine Krief au LaBRI

October 6, 2013

Sommaire



Source: commentcamarche.net

Cryptanalyse: Décryptage d'un message sans connaissance préalable de la clé

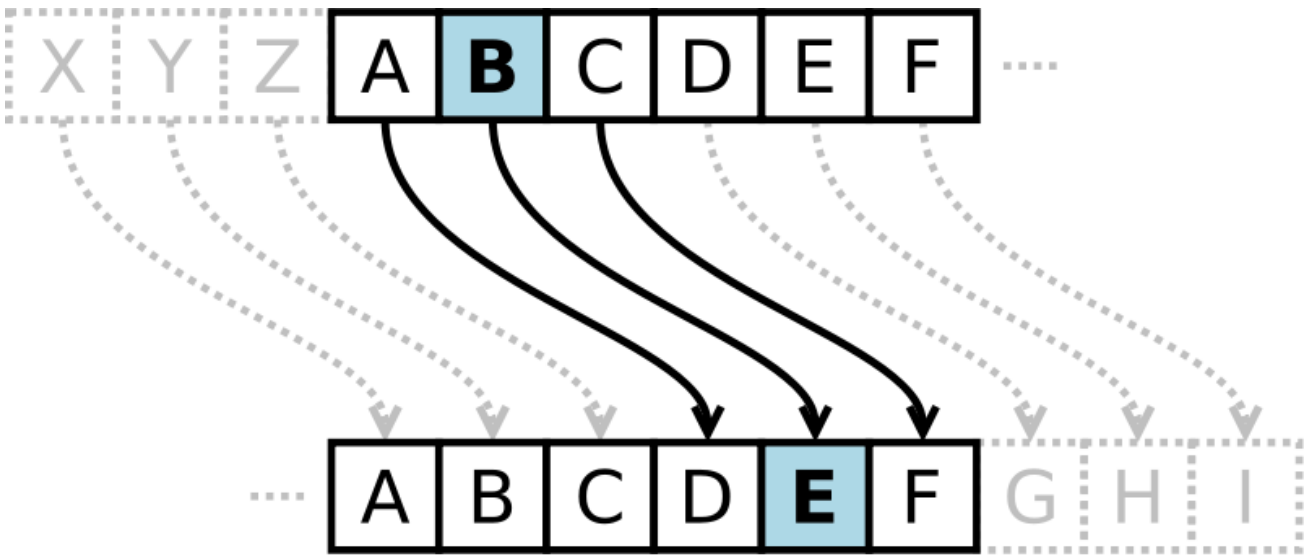
Sommaire

Cryptographie “Humaine”

- Chiffre de César
- Vigenère

Chiffre de César

- Décalage constant entre les lettres



Chiffre de César - Cryptanalyse

- Attaque par analyse fréquentielle
- car il n'y a pas équiprobabilité d'apparition d'une lettre

Probabilité d'apparition par caractère (%)

Langue	A	B	C	D	E	F	G	H
Francais	9.42	1.02	2.64	3.39	15.87	0.95	1.04	0.77
Anglais	8.08	1.67	3.18	3.99	12.56	2.17	1.80	5.25

Vigenère

- version améliorée du chiffre de César
- introduit la notion de clé
- le décalage dépend de la clé

```
message en clair :    ENSEIRB    | 4 13 ...
clé de chiffrement :  CLE        | 2 11 ...
-------------------------------------------
message chiffré :     GYWGTVD    | 6 24 ...
```

Vigenère - Cryptanalyse

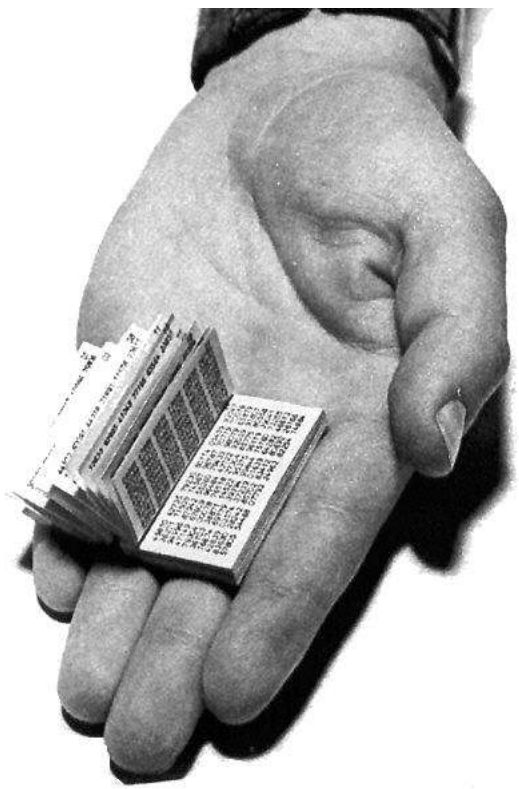
- recherche de répétitions dans le texte et leurs espacements
- la longueur de la clé est probablement multiple du PPCD des espacements
- le texte doit ensuite être découpé pour revenir à une sécurité équivalente au chiffre de César
- C'est le test de Kasiski

Conclusion sur la longueur des clés

- Vigenère est n fois plus dur à craquer que César (n = len(cle))
- le texte doit ensuite être découpé et chaque lettre du mot de passe craqué par analyse fréquentielle
- pour éviter les répétitions, la clé doit être au moins aussi longue que le texte

One-Time Pad

- Cryptographie prouvée incassable
- nécessite la création de livres “clés”
- la clé doit être générée de façon purement aléatoire



Sommaire

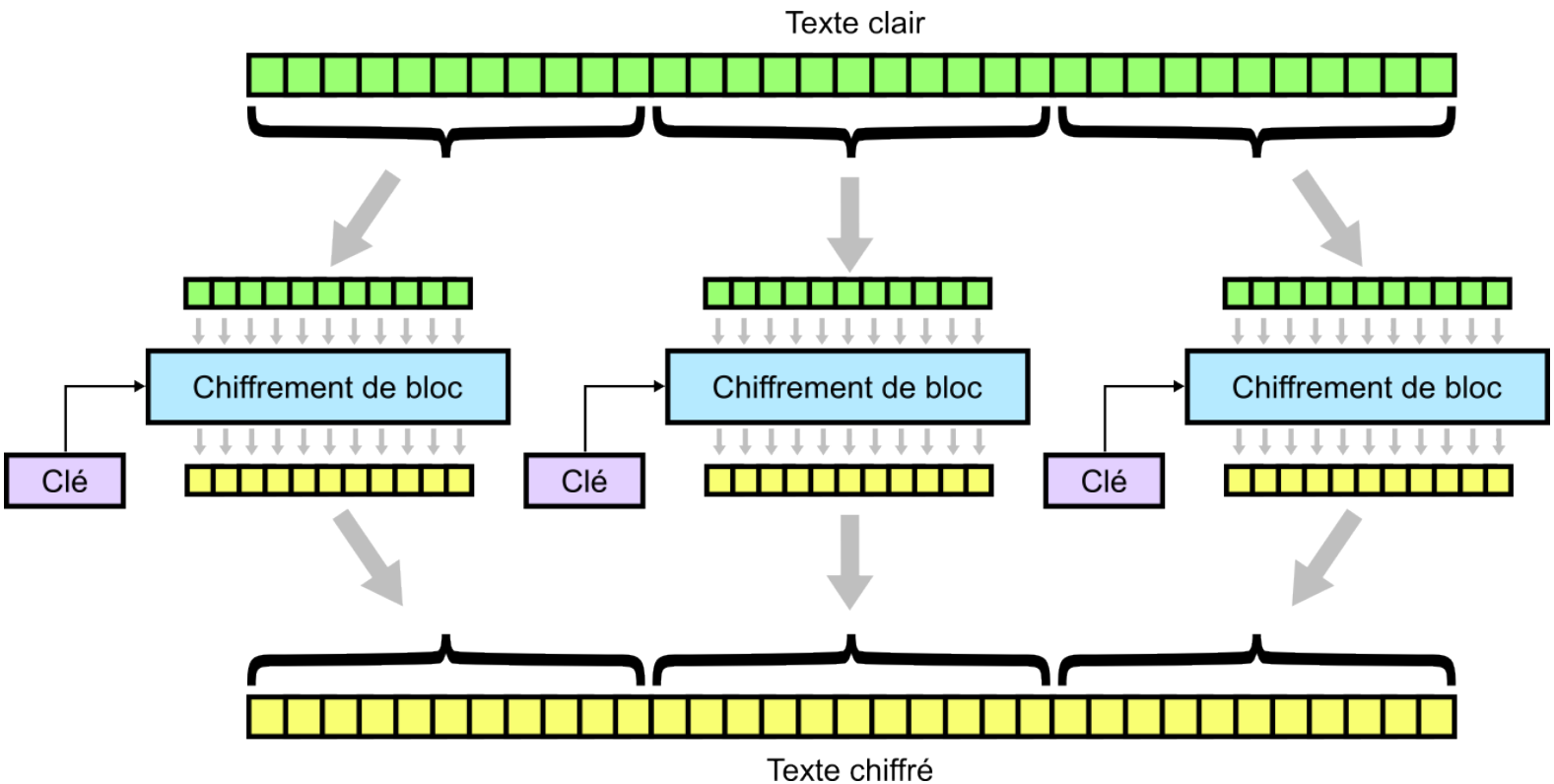
Cryptographie symétrique (dite à clé privée)

- La même clé est utilisée pour le chiffrement/déchiffrement
- 3 types de chiffrement: ECB, CBC et flux

Source: commentcamarche.net

Chiffrement symétrique "Electronic Code Book" (ECB)

- découpage en bloc indépendants
- chiffrement de chaque bloc



ECB : Pros

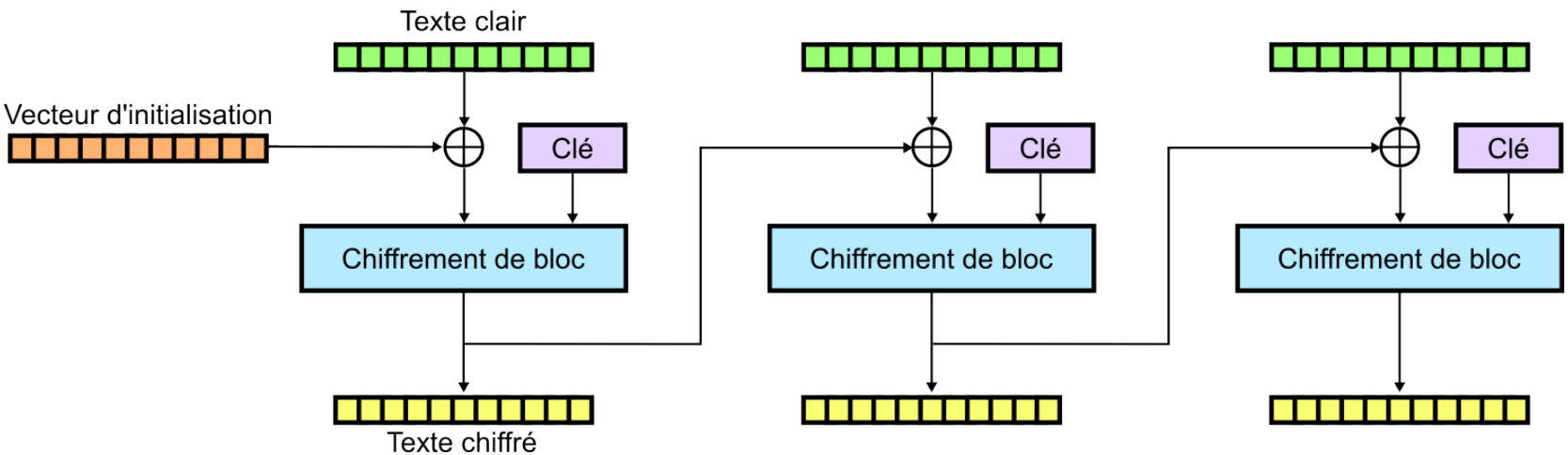
- Décodage partiel possible
- Plus grande résistance à la corruption

ECB : Coins

- Plus grande répétition : Cryptanalyse plus facile

Chiffrement symétrique "Cipher Block Chaining" (CBC)

- découpage en bloc
- la valeur du bloc chiffré dépend du bloc précédent



CBC : Pros

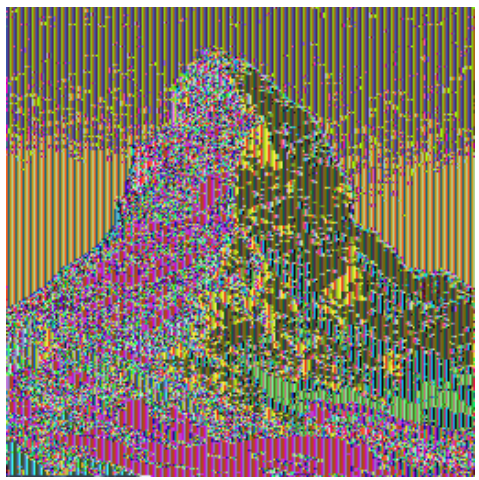
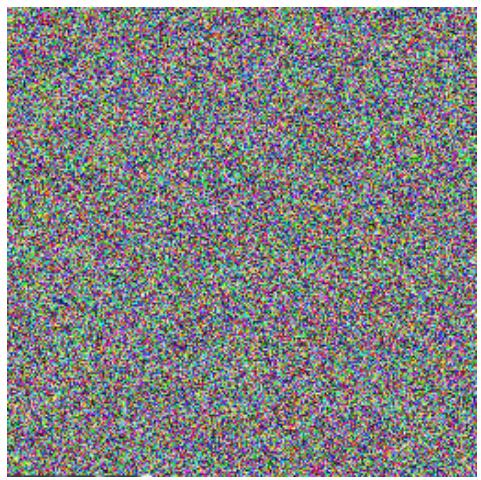
- Moins de chance de répétition : Cryptanalyse plus dure

CBC : Coins

- Décodage partiel impossible
- Non-résistance à la corruption

Comparaison des 2 modes de chiffrement

- Image 1: Image originale
- Image 2: Image chiffrée en ECB
- Image 3: Image chiffrée en CBC

Chiffrement symétrique par flot (Stream Cipher)

- pas de découpage en blocs
- traite les données dès qu’elles arrivent

Stream Cipher : Pros

- Faible latence (granularité = 1 octet)
- Faible consommation mémoire

Stream Cipher : Coins

- Généralement facilement cassable
- Décodage partiel impossible
- Non-résistance à la corruption

Liste d'algorithmes de chiffrement symétrique

- RC4 (Flux): Taille de clé arbitraire. Considéré comme peu sûr.
- DES: clés de 56 bits, cassable en environ une journée
- tripleDES: clés de taille 168, 112 ou 56 bits. Considéré comme sûr jusqu'en 2030
- AES: clés de taille 128 bits. C'est l'algorithme le plus populaire
- Blowfish: clés de taille 1-448 bits. Pas breveté

Réalisation d'un algo de chiffrement symétrique simple

- Besoin d'une opération de base
- Toute transformation doit être réversible

Input		Output		
A	B	A AND B	A OR B	A XOR B
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Chiffrement d'un message simple

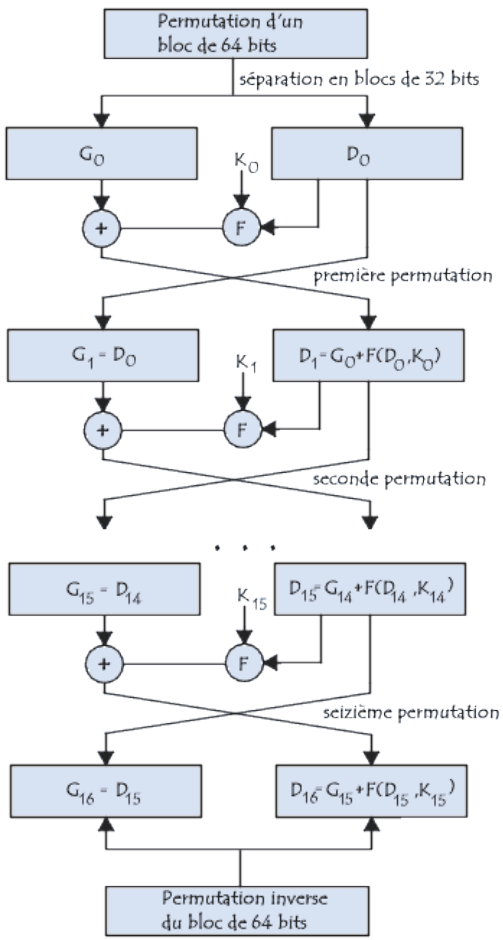
- Clé: 42
- Message: 1337

Xor Lookup Table

xor		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0001	1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
0010	2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
0011	3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
0100	4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
0101	5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
0110	6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
0111	7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
1000	8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
1001	9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
1010	10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
1011	11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
1100	12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
1101	13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
1110	14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
1111	15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

DES

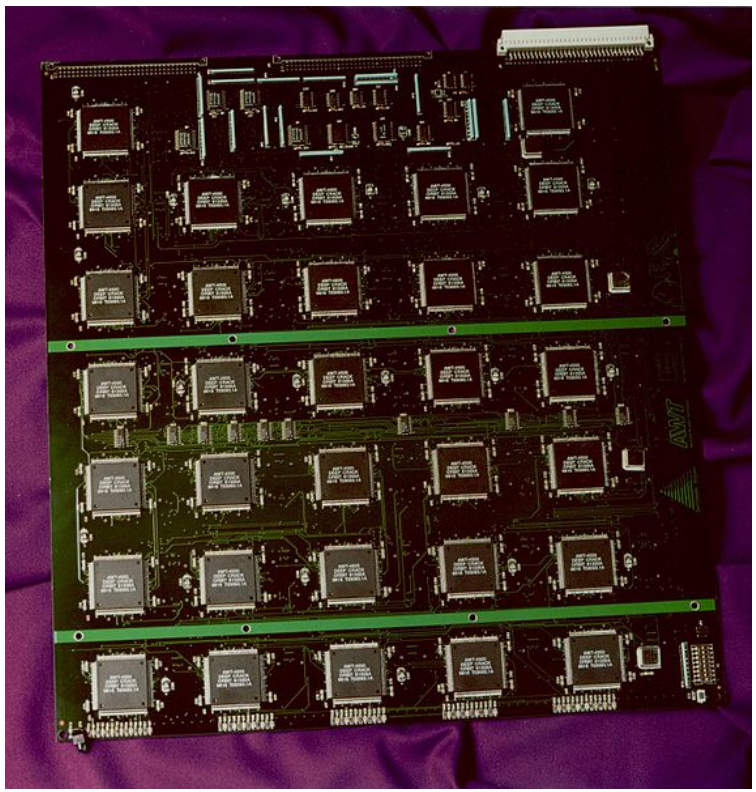
- Chiffrement par bloc
- Peu sûr à cause de la taille de sa clé



Source: commentcamarche.net

DES : Cryptanalyse

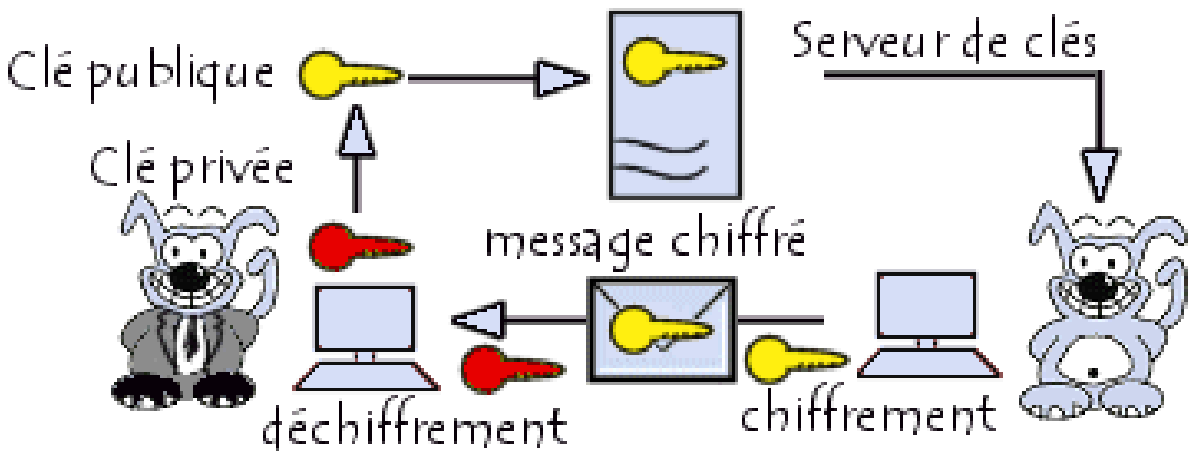
- Nécessité d'une attaque par brute force
- EFF DES cracker: Construite en 1998. Teste l'ensemble des clés en 9 jours.



Sommaire

Cryptographie asymétrique (dite à clé publique)

- chiffrement sans secret partagé
- utilisation d’une clé privée et une publique
- taille des clés supérieures aux clés symétriques
- tout message chiffré avec une clé est déchiffrable avec l’autre



Source: commentcamarche.net

Chiffrement

Alice veut chiffrer des données pour Bob:

- elle chiffre les données avec la clé publique de Bob
- celui-ci les déchiffre avec sa clé privée

Avantages/Inconvénients

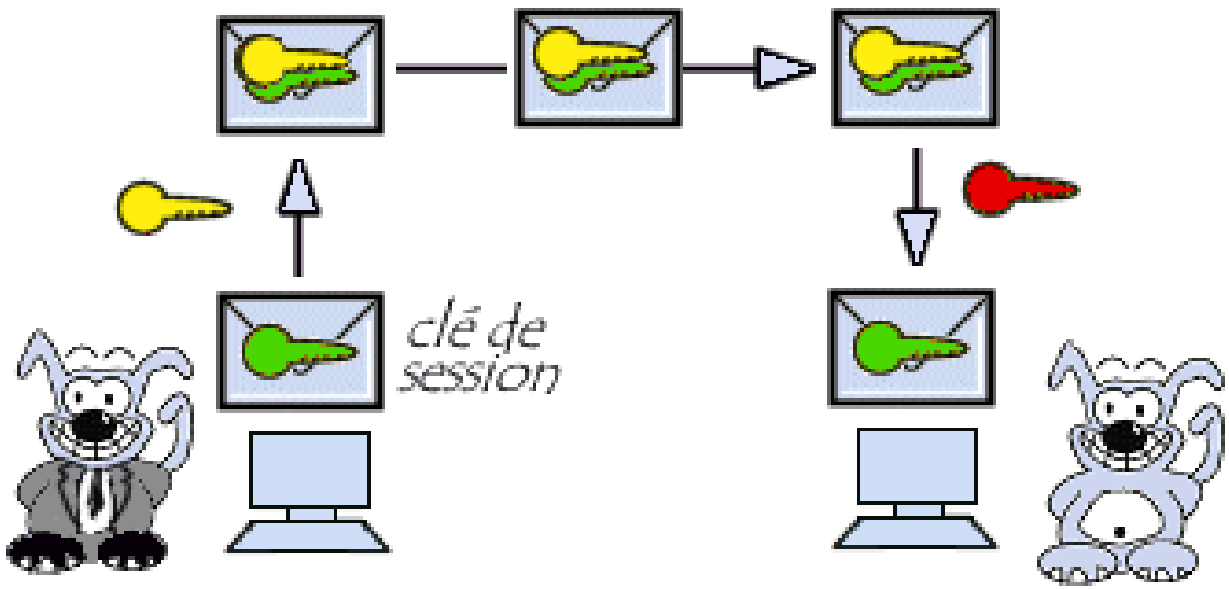
- Avantages: Plus besoin d'un autre canal pour la diffusion d'une clé privée
- Inconvénients: 1000 fois plus lent que la crypto symétrique

Chiffrement hybride: Clé de session

Alice veut chiffrer des données pour Bob:

- Alice chiffre le message avec une clé symétrique aléatoire
- Elle chiffre la clé de de session avec la clé publique de Bob
- Elle transmet le tout à Bob

C'est le principe de base de PGP: Pretty Good Privacy



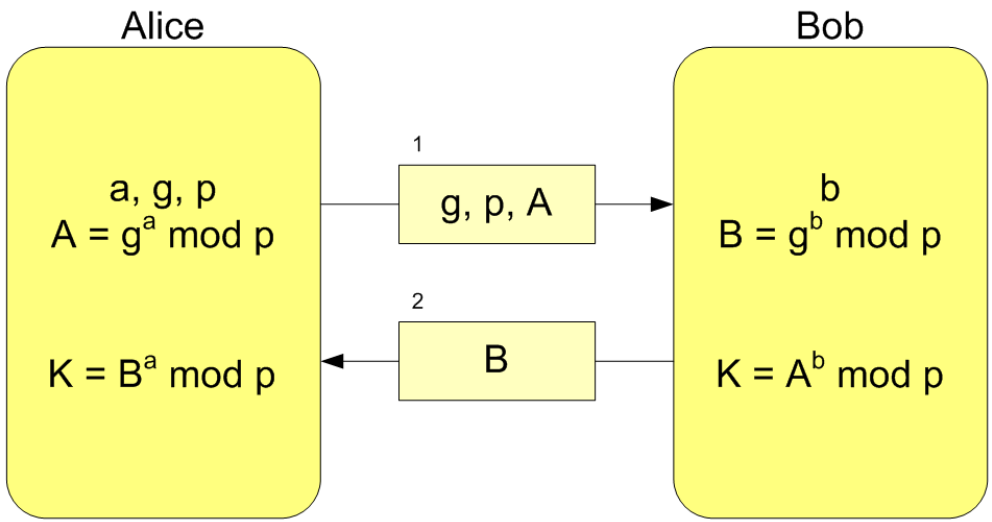
Source: commentcamarche.net

Génération de clé de session

Comment générer un secret partagé sur un canal de communication non sûr?

- On ne peut pas le générer d'un coté et le transmettre
- Il doit être généré des 2 cotés en parallèle

C'est l'algorithme de Diffie-Hellman.



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Signature

Alice veut prouver qu'elle est l'auteur d'un texte:

- elle chiffre les données avec sa clé privée
- Bob déchiffre les données avec la clé publique d'Alice

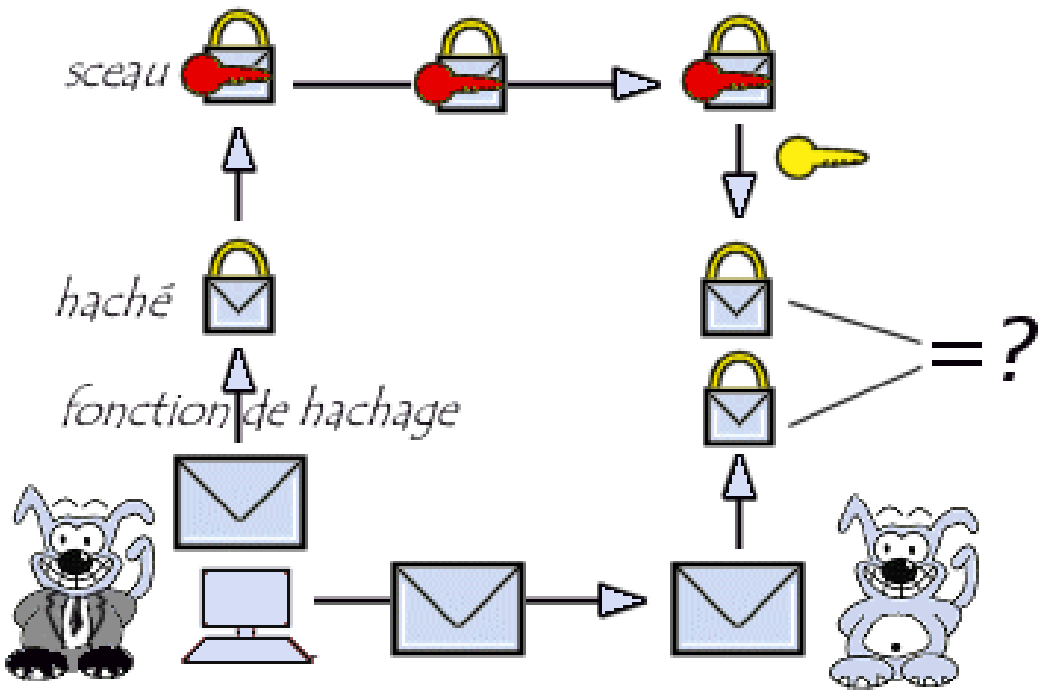
Problèmes

- Le texte n'est pas disponible en clair
- Le chiffrement peut prendre beaucoup de temps

Signature sans chiffrement du texte

Alice veut prouver qu'elle est l'auteur d'un texte sans le chiffrer:

- Alice effectue une empreinte numérique de son fichier (hash)
- elle chiffre ce hash avec sa clé privée
- Bob peut ainsi vérifier l'authenticité et l'intégrité



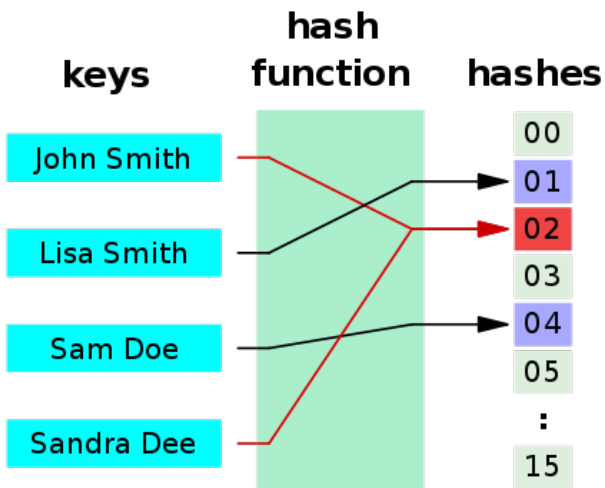
Source: commentcamarche.net

Fonction de hachage

Pour être sûre cryptographiquement, une fonction de hash doit être résistante aux collisions:

- On ne doit pas pouvoir retrouver le message d'origine à partir du hash
- Difficulté de trouver 2 messages aléatoires générant le même hash

MD5 n'est plus considéré comme sûr! Utilisez la famille SHA-1.



Liste d’algorithmes de chiffrement asymétrique

- RSA: clés de 1024 bits. Basé sur le problème du logarithme discret
- ECC: clés de 160 bits. Basé sur le problème des courbes elliptiques

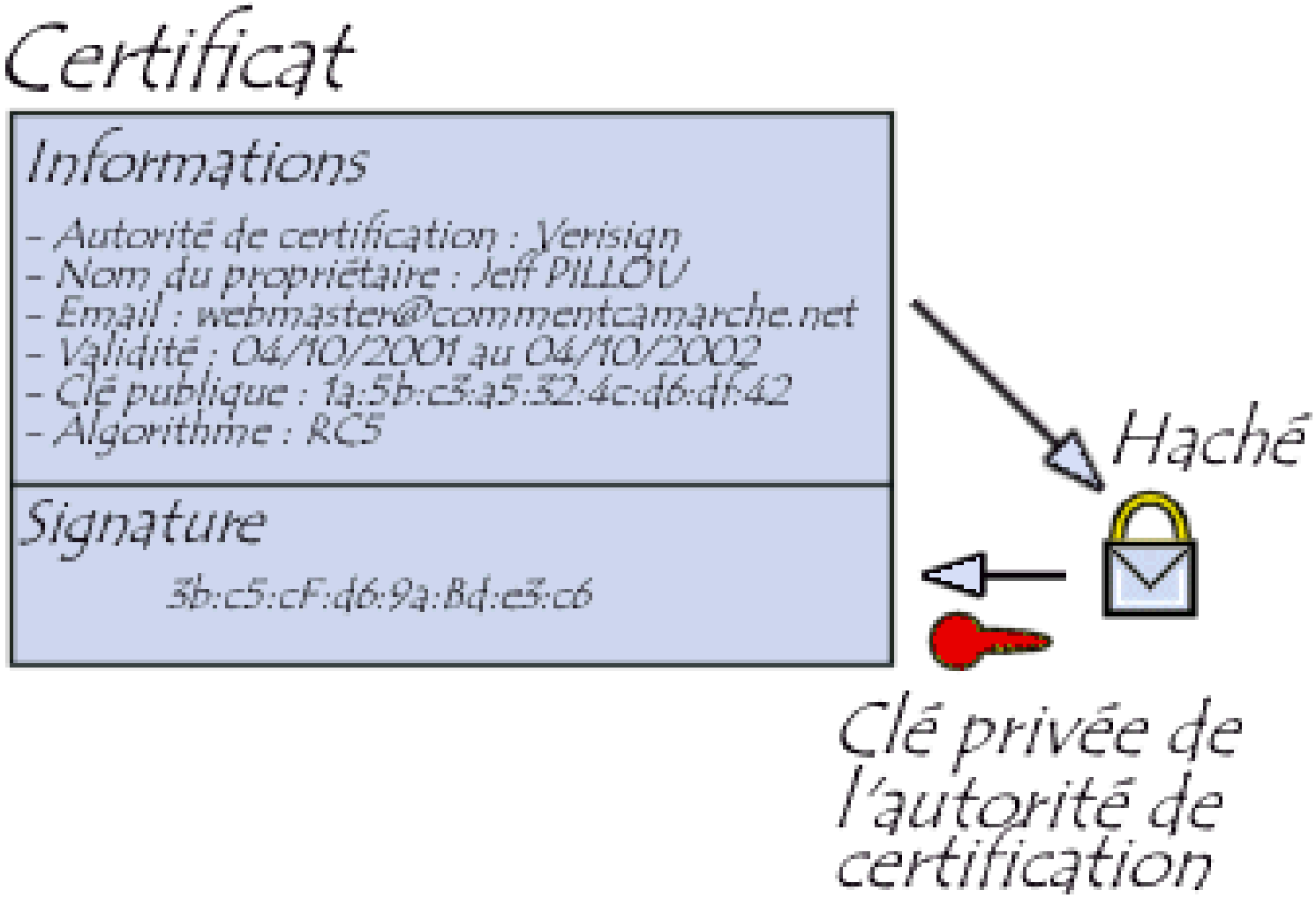
Sommaire

Problèmes de sécurités avec les clés publiques

Quand Alice veut vérifier l'identité de Bob, elle va chercher la clé publique dans un annuaire. Si l'annuaire est corrompu par un pirate, il peut se faire passer pour Bob en remplaçant sa clé publique

Besoin d'une autorité de certification

Besoin de certification d'authenticité d'une clé publique. C'est ce que l'on appelle un certificat.



Source: commentcamarche.net

Certificats X.509

- Le numéro de série du certificat
- L'algo de chiffrement utilisé pour signer
- Le nom (DN) de l'autorité de certification
- La date de début et de fin de validité du certificat
- L'objet de l'utilisation de la clé publique
- La clé publique du propriétaire du certificat
- La signature de l'émetteur du certificat (thumbprint)

Type de signatures

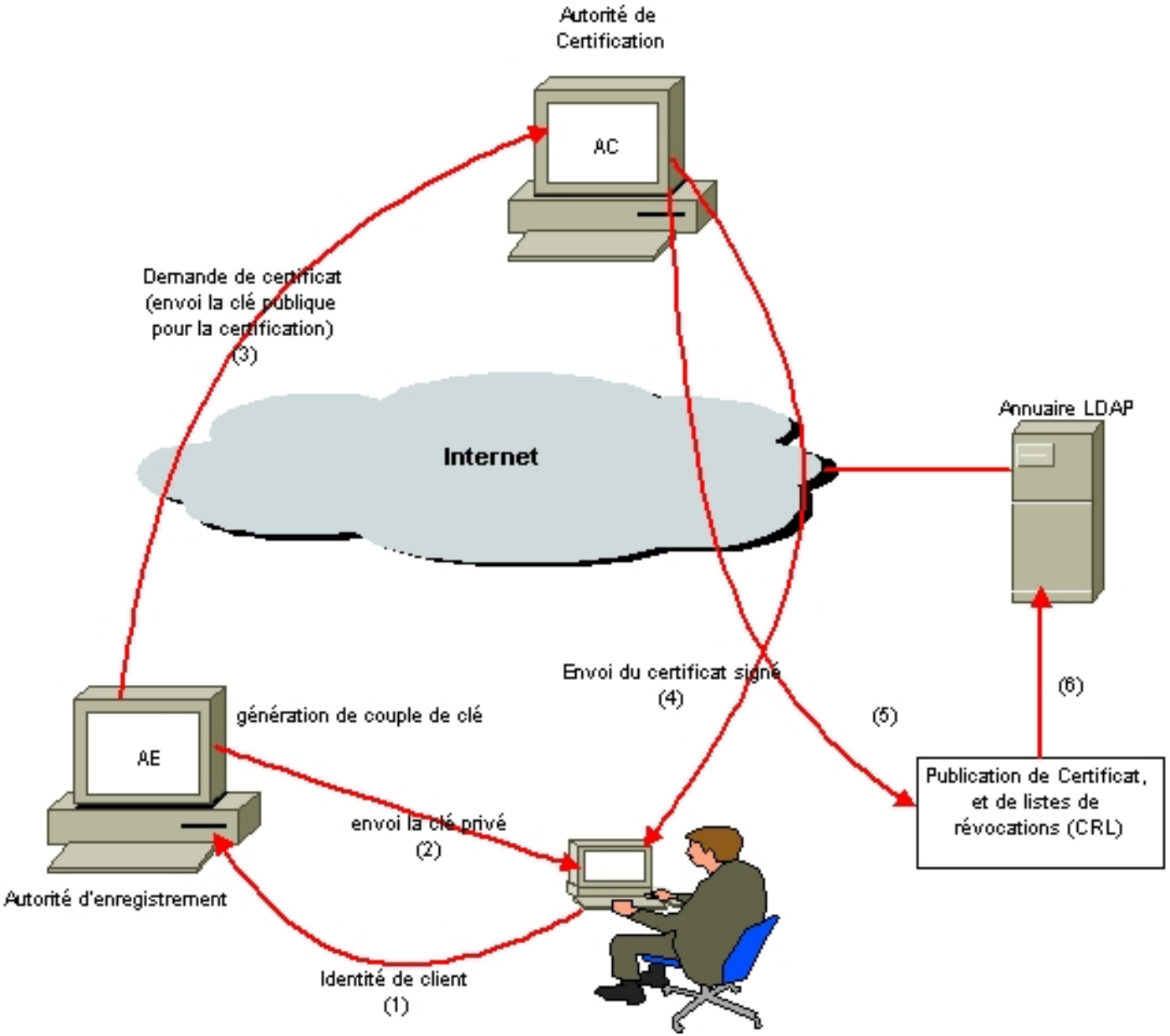
- Auto-signé: Certificat au plus haut de la chaîne de certificat
- Signé par une autorité de certification

Public Key Infractructure

Une PKI est constituée de

- Une autorité d'enregistrement
- Une autorité de certification (le coffre fort)
- Une liste de révocation
- Un annuaire

PKI


Autorité de Certification
AC
Demande de certificat (envoi la clé publique pour la certification) (3)
Internet
Annuaire LDAP
Envoi du certificat signé (4)
(5)
(6)
AE
génération de couple de clé
Publication de Certificat, et de listes de révocations (CRL)
envoi la clé privé (2)
Autorité d'enregistrement
Identité de client (1)