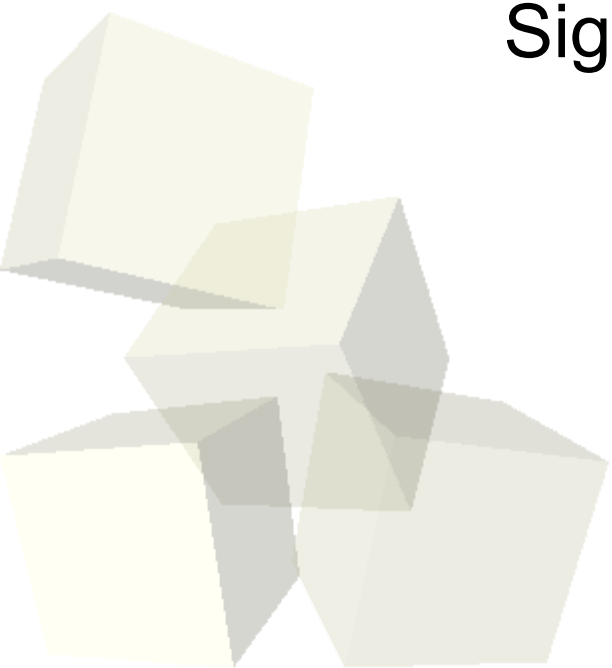


Cryptographie

Cours 4

Signature, Hachage et Scellement

Jérémy Briffaut

Plan

I. Histoire, définition et objectifs de la cryptographie
   - Concepts et algorithmes de permutation et de substitution

II. Chiffrement Symétrique
   - DES, 3DES, AES, IDEA

III. Chiffrement Asymétrique
   - RSA, ElGamal

IV. Signature, Hachage et Scellement

V. Echange de clés
   - Algorithme Deffie-Hellman

VI. Hachage : MD5, SHA-1, SHA-2

VII. Code d'Authentification & MAC

- Service souhaité : pouvoir s'assurer que le message
  - émane bien de l'expéditeur annoncé
    - → **authentification** de l'origine des données
  - n'a pas été modifié pendant le transfert
    - → **intégrité**
- Authentification de l'origine des données et intégrité sont inséparables
- **Authenticité** = authentification + intégrité
- "Authentification" souvent utilisé pour désigner en fait l'authenticité

- Fonctions de hachage, signature et scellement
  - Mécanismes fournissant les services
    - d'**intégrité**
    - d'**authentification de l'origine** des données
    - de **non-répudiation** de la source

Fonctions de hachage

- Fonction de hachage à sens unique
  - Convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe = empreinte ou condensé
  - A sens unique :
    - Facile à calculer mais difficile à inverser
    - Il est difficile de trouver deux messages ayant la même empreinte
- **MD5 (Message Digest 5)**
  - Empreinte de 128 bits
- **SHA (Secure Hash Algorithm)**
  - Norme NIST
  - Empreinte de 160 bits
  - SHA-1 révision publiée en 1994 (corrige une faiblesse non publique)
    - considéré comme plus sûr que MD5
  - SHA-2 (octobre 2000) agrandit la taille de l'empreinte

Plan

I. Histoire, définition et objectifs de la cryptographie
- Concepts et algorithmes de permutation et de substitution

II. Chiffrement Symétrique
- DES, 3DES, AES, IDEA

III. Chiffrement Asymétrique
- RSA, ElGamal

IV. Signature, Hachage et Scellement

V. Echange de clés
- Algorithme Deffie-Hellman

VI. Hachage : MD5, SHA-1, SHA-2

VII. Code d'Authentification & MAC

Signature numérique

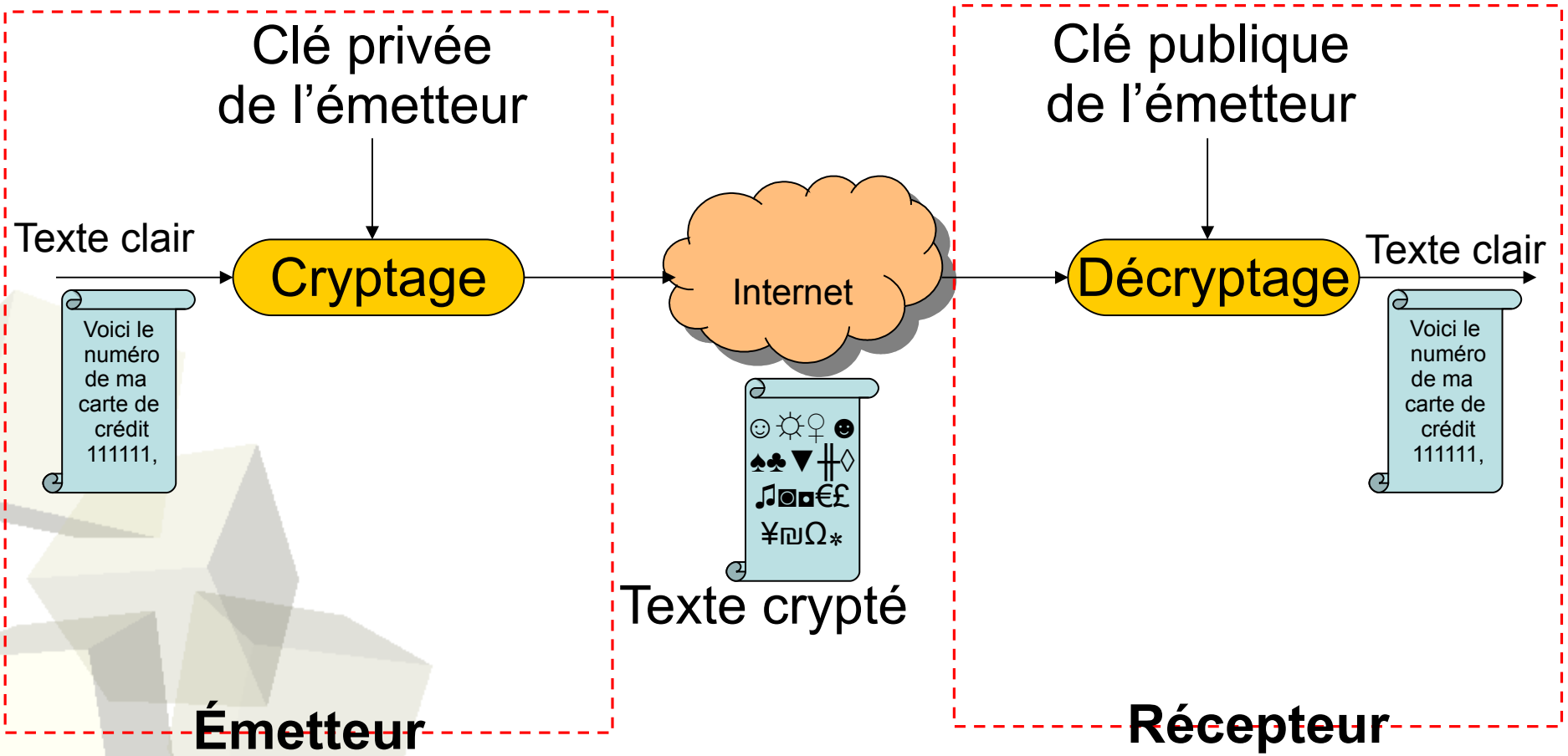
- Mécanisme qui fournit les services suivants :
  - **Authentification** de l'origine des données
  - **Intégrité**
  - **Non-répudiation** de la source
- Algorithmes
  - DSS : standard NIST
  - SHA-1 + El-Gamal
  - RSA : norme de fait
    - MD5 + RSA
    - SHA-1 + RSA

La signature numérique

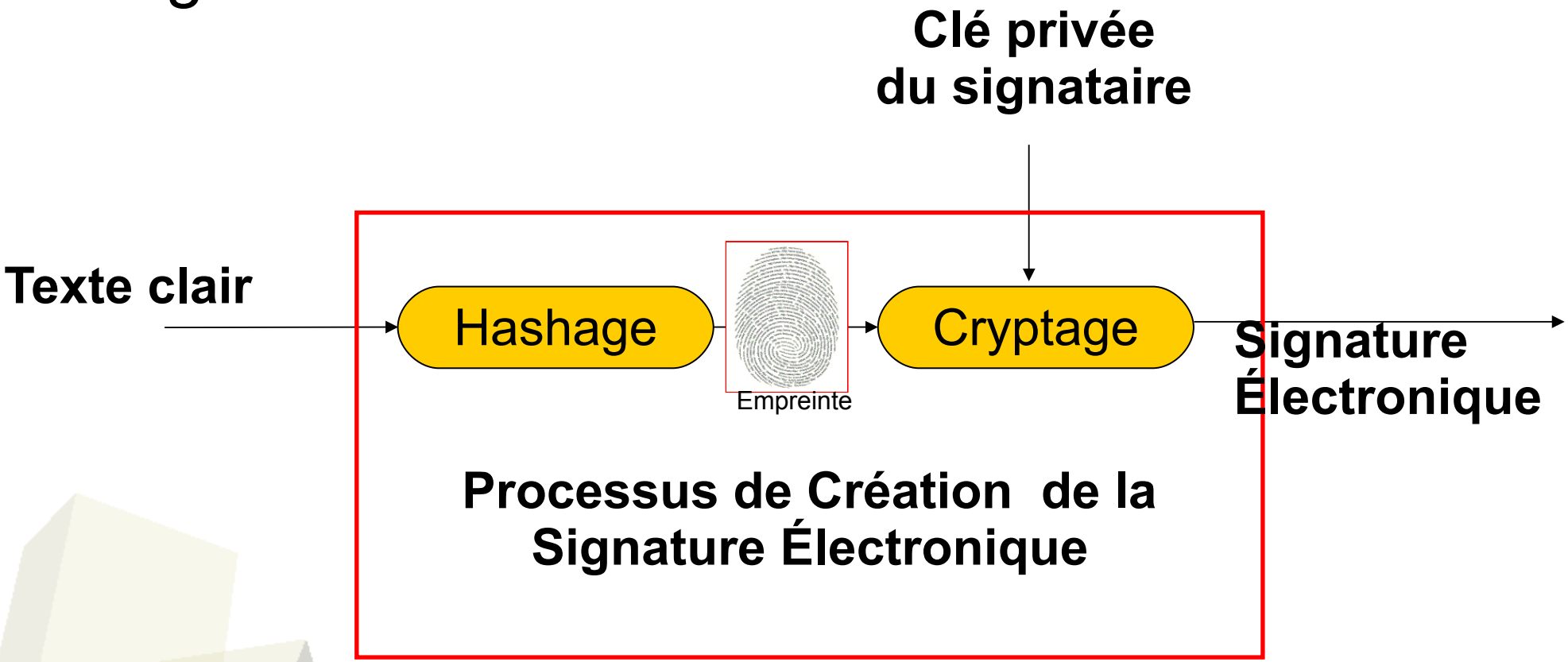
- On peut **signer** un message en **cryptant** la totalité du message avec une clef secrète. Ceci donne des méthodes lentes lors de l'éxecution, il faut traiter tout le message pour la vérification.
- Aussi, comme pour le chiffrement, il existe des méthodes **sysmétriques** et **asymétriques** pour garantir l'intégrité.
  - Ce sont les "codes d'authentification des messages" **MAC (Message Authentification Code)**.
- Les fonctions de hachage sont utilisées dans ce cas.
  - Pour générer un MAC il suffit de hacher le message puis de crypter l'empreinte obtenue avec une clé secrète.
  - La génération d'une empreinte hachée est plus rapide qu'une signature numérique.
- Il existe un type spécial de hachage appelé **HMAC** qui sécurise plus encore la fonction de hachage sur laquelle il repose.
  - On parle de **HMAC-SHA** ou du **HMAC-MD5**

Signature numérique et chiffrement asymétrique

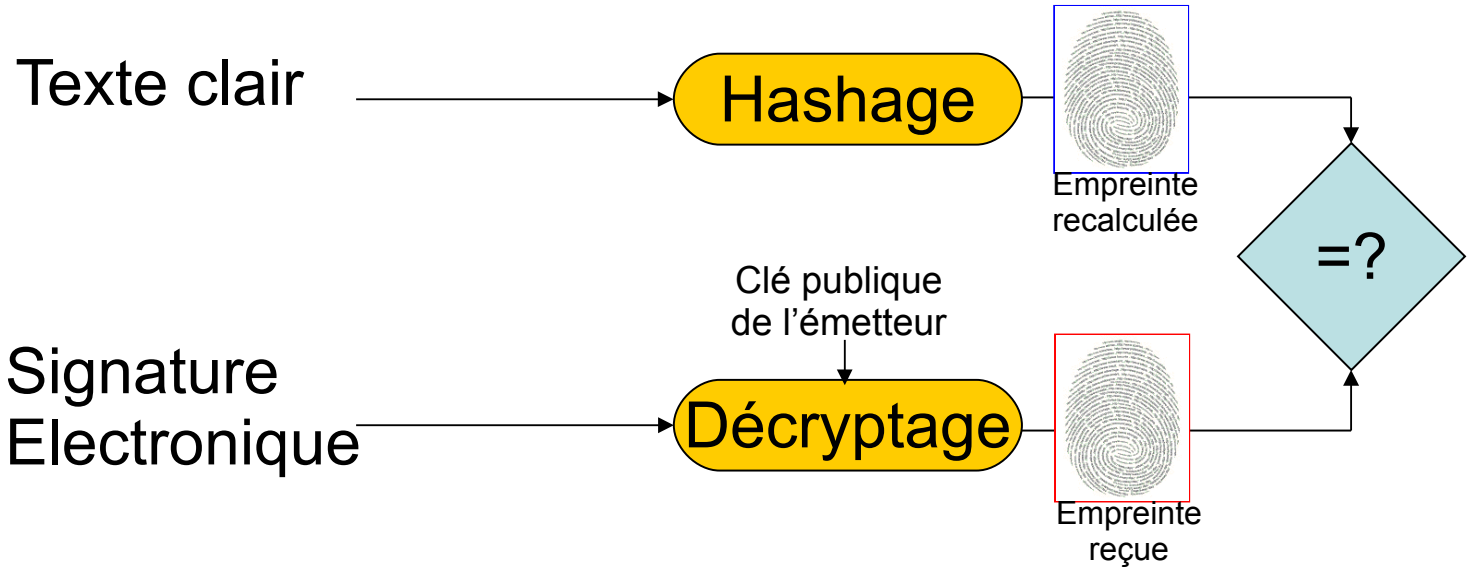
- **Signature** par clef asymétrique
  - Clef **privée** utilisée pour le **chiffrement**
    - seul son détenteur peut chiffrer
    - mais tout le monde peut **déchiffrer** avec la clef **publique**
      - et donc vérifier la "signature"



- Signature


Clé privée
du signataire
Texte clair
Hashage
Empreinte
Cryptage
Signature
Électronique
Processus de Création de la
Signature Électronique

Vérification



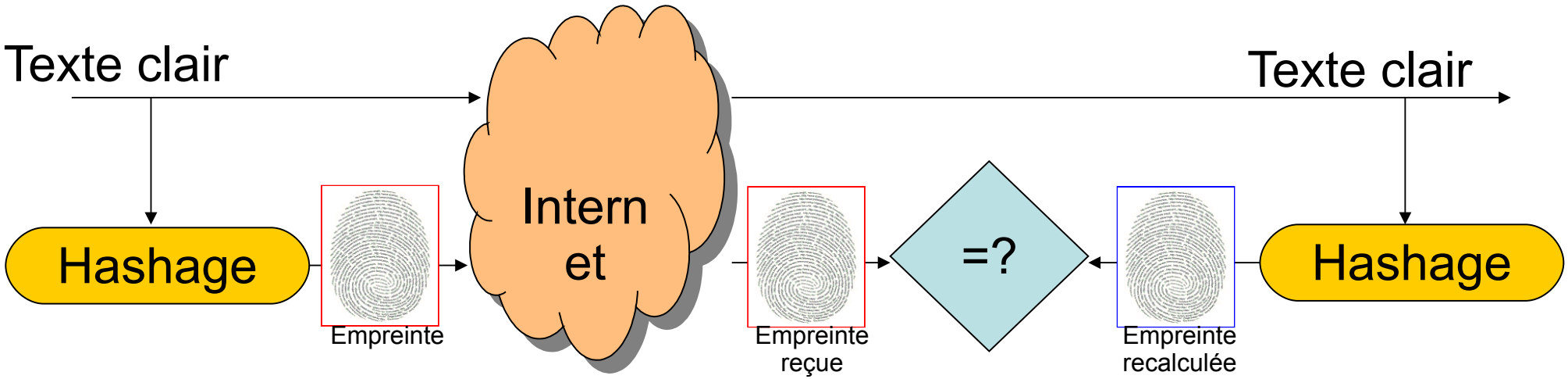
1)  =  **La signature reçue est correcte**

Empreinte reçue — Empreinte recalculée

2)  ≠  **La signature reçue est incorrecte**

Empreinte reçue — Empreinte recalculée

Fonctions de hachage, scellement et signature



1)  = **Le texte reçu est intègre**

Empreinte reçue — Empreinte recalculée

2)  ≠ **Le texte reçu est altéré**

Empreinte reçue — Empreinte recalculée

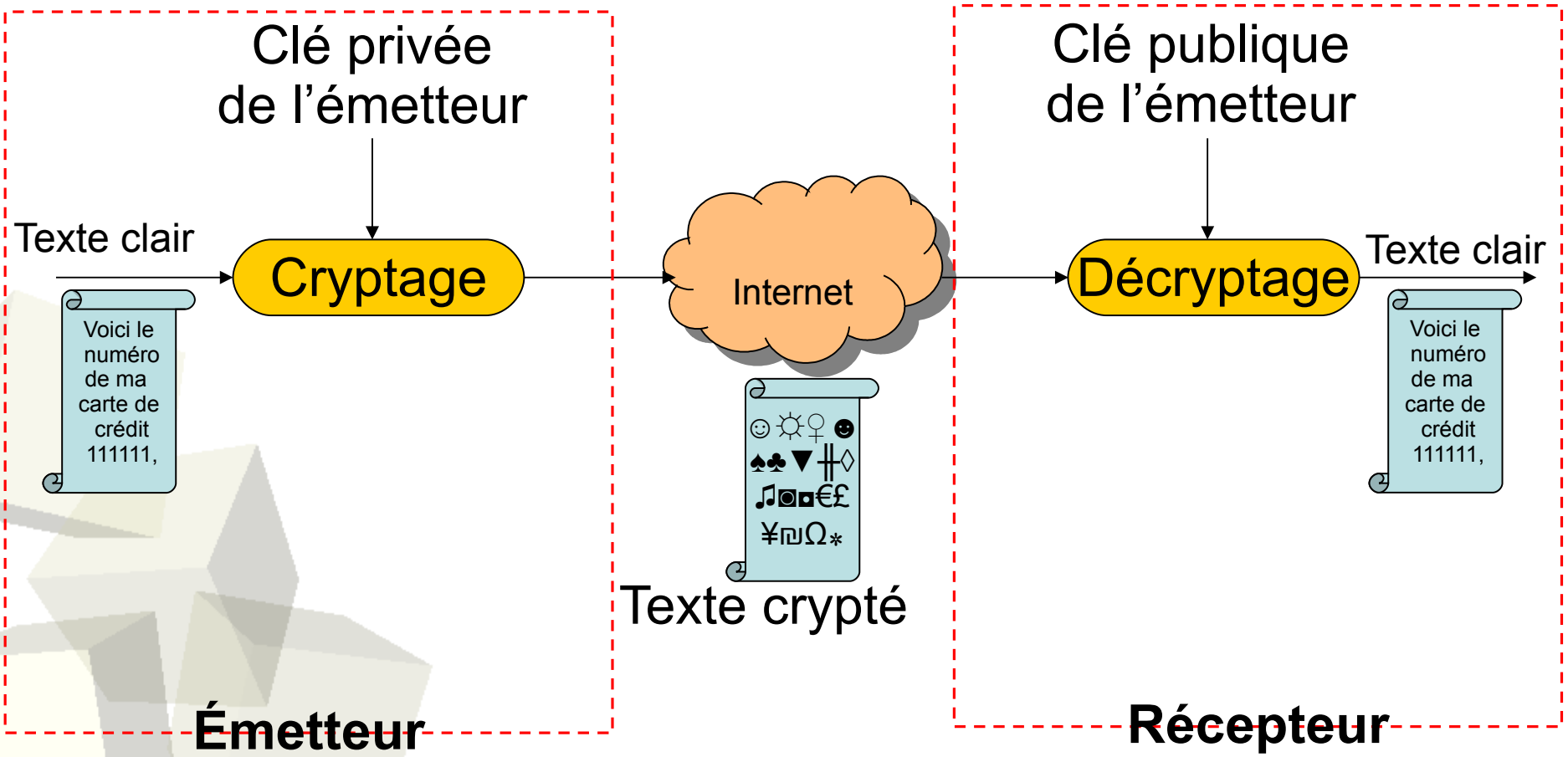
- Signature numérique
  - Mécanisme qui fournit les services suivants :
    - **Authentification** de l'origine des données
    - **Intégrité**
    - **Non-répudiation** de la source
  - Algorithmes
    - DSS : standard NIST
    - SHA-1 + El-Gamal
    - RSA : norme de fait
      - MD5 + RSA
      - SHA-1 + RSA

La signature numérique

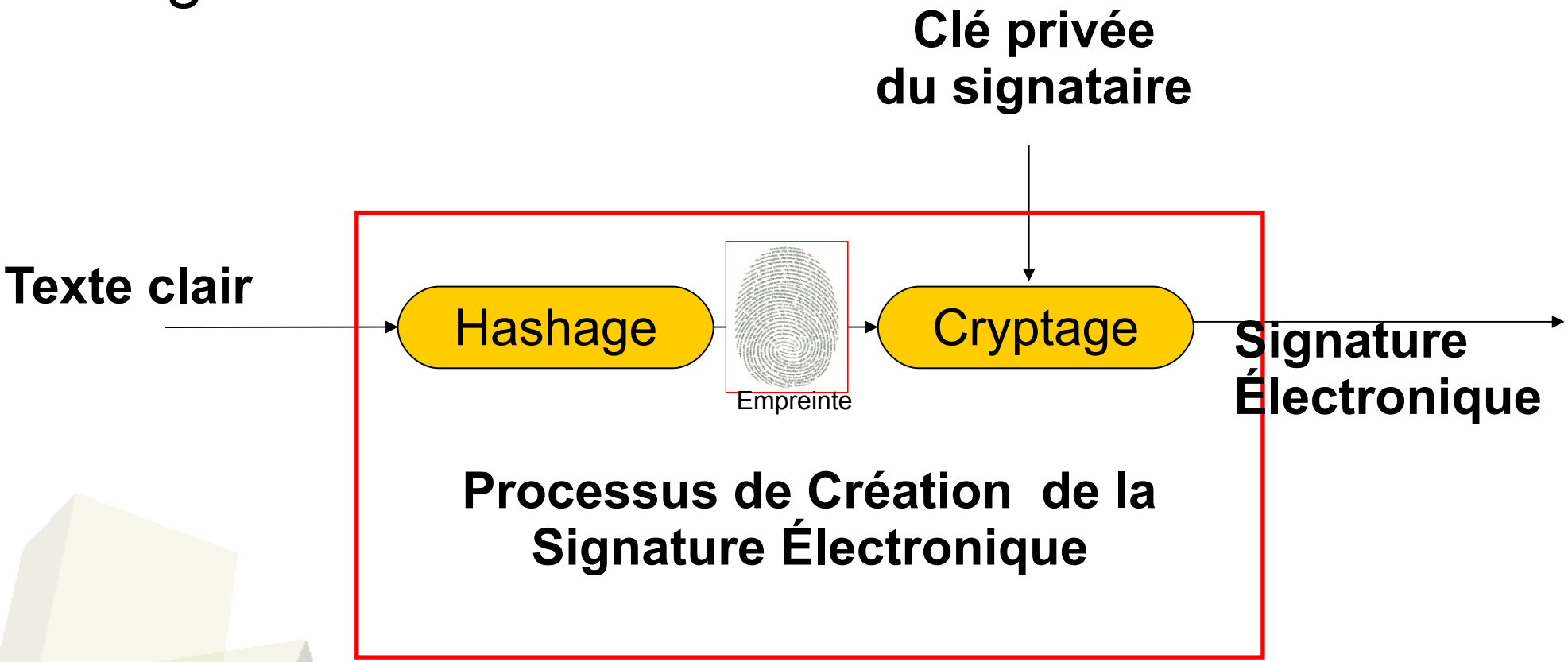
- On peut **signer** un message en **cryptant** la totalité du message avec une clef secrète. Ceci donne des méthodes lentes lors de l'éxecution, il faut traiter tout le message pour la vérification.
- Aussi, comme pour le chiffrement, il existe des méthodes **sysmétriques** et **asymétriques** pour garantir l'intégrité.
  - Ce sont les "codes d'authentification des messages" **MAC (Message Authentification Code)**.
- Les fonctions de hachage sont utilisées dans ce cas.
  - Pour générer un MAC il suffit de hacher le message puis de crypter l'empreinte obtenue avec une clé secrète.
  - La génération d'une empreinte hachée est plus rapide qu'une signature numérique.
- Il existe un type spécial de hachage appelé **HMAC** qui sécurise plus encore la fonction de hachage sur laquelle il repose.
  - On parle de **HMAC-SHA** ou du **HMAC-MD5**

Confidentialité et algorithmes de chiffrement

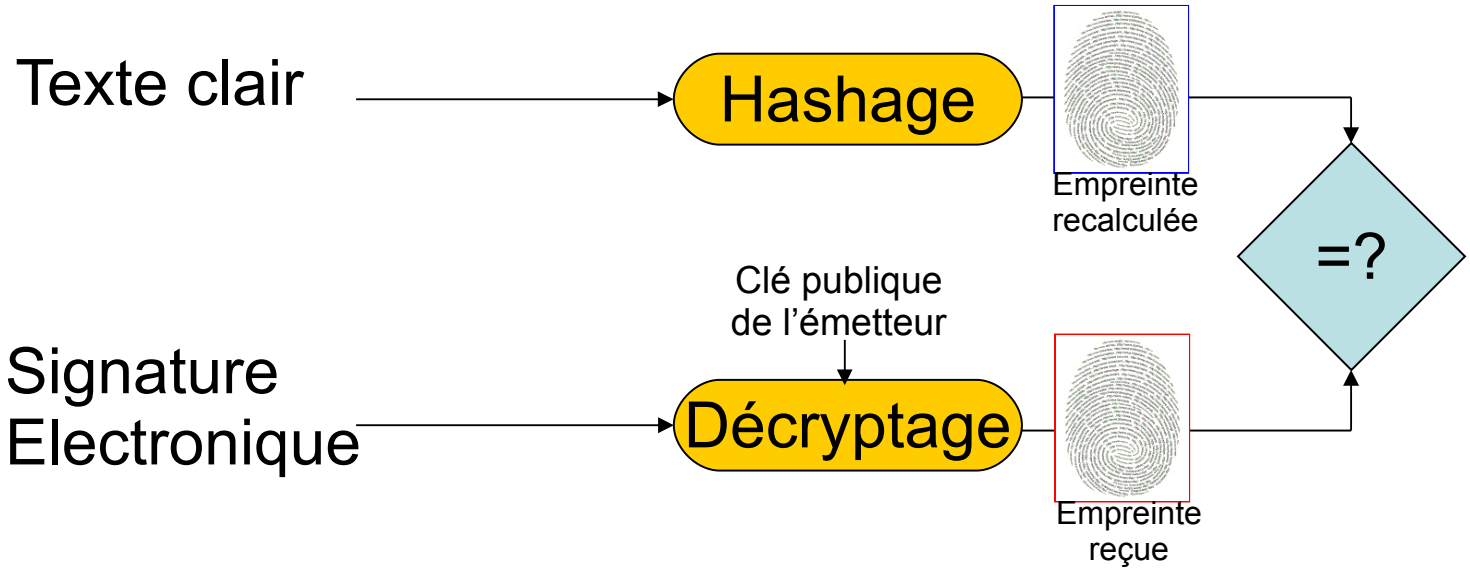
- **Signature** par clef asymétrique
  - Clef **privée** utilisée pour le **chiffrement**
    - seul son détenteur peut chiffrer
    - mais tout le monde peut **déchiffrer** avec la clef **publique**
      - et donc vérifier la "signature"



- Signature


Clé privée
du signataire
Texte clair
Hashage
Empreinte
Cryptage
Signature
Électronique
Processus de Création de la
Signature Électronique

Vérification



1)  =  **La signature reçue est correcte**

Empreinte reçue — Empreinte recalculée

2)  ≠  **La signature reçue est incorrecte**

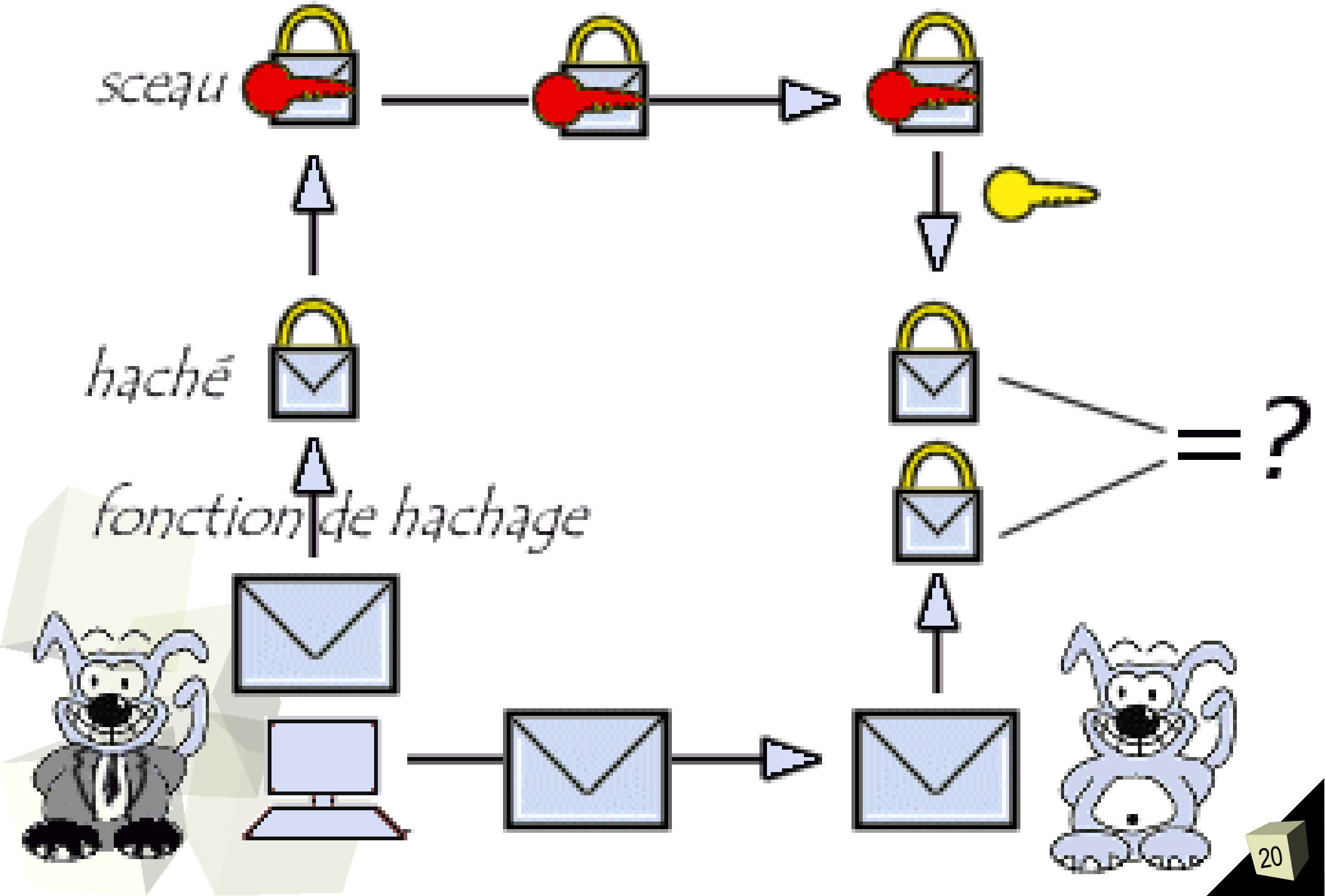
Empreinte reçue — Empreinte recalculée

Code d'authentification des messages

- Une variante de la signature,le **scellement** :
  - ➔ Fournit les services
    - d'**authentification** de l'origine des données
    - d'**intégrité** des données, mais pas la non répudiation
- On utilise dans ce cas la cryptographie à clefs secrètes, donc les deux parties possédent la clef.

- **Scellement**
  - Vocabulaire
    - **Sceau** ou **code d'authentification** de message
    - **Message Authentication Code, MAC**
  - 2 constructions possibles
    - Dernier bloc du cryptogramme obtenu avec un algorithme de chiffrement en mode CBC
    - DES-MAC

Fonctions de hachage, scellement et signature



Comparaison cryptographie symétrique/asymétrique

- Cryptographie symétrique :
  - Rapide mais nécessité de partager un secret.
- Cryptographie asymétrique :
  - Lent mais pas de partage de secret et signature digitale

Combinaison cryptographie symétrique/asymétrique

- Cryptographie asymétrique :
  - Génération de clés de session.
  - Signature digitale (utilisation d'une fonction hash).
- Cryptographie symétrique :
  - Chiffrement à l'aide de la clé de session.

Plan

I. Histoire, définition et objectifs de la cryptographie
   - Concepts et algorithmes de permutation et de substitution

II. Chiffrement Symétrique
   - DES, 3DES, AES, IDEA

III. Chiffrement Asymétrique
   - RSA, ElGamal

IV. Signature, Hachage et Scellement

V. Echange de clés
   - Algorithme Deffie-Hellman

VI. Hachage : MD5, SHA-1, SHA-2

VII. Code d'Authentification & MAC

Résumé cryptographique d'un message

Définition :

Une fonction de hachage, H(M), opère sur un message M de longueur quelconque, et fournit une valeur de hachage (le résumé) de longueur fixe n.

$$H : \{0,1\}^* \rightarrow \{0,1\}n$$

Résumé cryptographique d'un texte
Propriétés.

- A partir du résumé, il est impossible de remonter au texte
- Une modification minime du texte donne un résumé complètement différent
- Il est impossible de trouver deux textes de même résumé

Résumé cryptographique d'un message
Longueur du résumé

- Paradoxe des anniversaires :
  - Si le résumé est de taille n, l'attaquant peut trouver, avec une probabilité de 0,5, deux messages ayant le même résumé en parcourant 2n/2 messages.

- Conséquence :
  - La taille du résumé doit être au moins de 128 bits.

Fonction de Hashage

Résumé cryptographique d'un texte
Exemples

- Message Digest 5 - MD5 : 128 bits
  – RFC 1321, R. Rivest MIT et RSA Data Security Inc.), avril 1992.

- SHA (Secure Hash Algorithm) ou SHS (Secure Hash Standard - NIST) : 160 bits

Informations techniques

- En entrée : 16 blocs de 32 bits (soit 512 bits).
- En sortie : 4 blocs de 32 bits (soit 128 bits).
- Structure globale :
  - Prétraitemant du message : taille multiple de 512 bits.
  - 4 registres d'état ou variables de chaînage
  - 4 fonctions non-linéaires.

Prétraitement du message

- 1ère étape :
  - Compléter le message tel que la taille + 64 bits soit multiple de 512 bits.
  - Pour cela, rajouter 1 suivi d'autant de 0 que nécessaire.
- 2ème étape :
  - Codé la taille du message initial sur 64 bits, et concaténer ces 64 bits au résultat précédent.

Variables de chaînage

- Définition de 4 registres de 32 bits A, B, C, D :
  - Les calculs seront effectués sur ces registres.
  - A la fin, le résumé est donné en concaténant ces 4 registres.

- Initialisation des registres :

A = 01 23 45 67 B = 89 ab cd ef,
C = fe dc ba 98 D = 76 54 32 10.

Fonctions non-linéaires

- Définition de 4 fonctions F, G, H, I :
  F(X,Y,Z) = X.Y + not(X).Z G(X,Y,Z) = X.Z + Y.not(Z)
  H(X,Y,Z) = X xor Y xor Z I(X,Y,Z) = Y xor (X + not(Z))

- Propriété des fonctions non-linéaires :

  – Permet de faire évoluer les registres d'état de manière non-linéaire, et d'assurer les propriétés de sens unique.

Définition d'une macro M(f,a,b,c,d,M,s,t)

a = b + ((a + f(b,c,d) + M[i] + t) << s).

- Notation :
  - a, b, c et d dénotent l'un des registres A, B, C ou D. f dénote l'une des fonctions non-linéaires. M[i] dénote le bloc (32 bits) courant du message en clair. t et s sont des valeurs entières.

Résumé d'un bloc de 512 bits

1ère étape

M(F,A,B,C,D,M[0],7,0xd76aa478)
M(F,D,A,B,C,M[1],12,0xe8c7b756)
M(F,C,D,A,B,M[2],17,0x242070db)
M(F,B,C,D,A,M[3],22,0xc1bdceee)
M(F,A,B,C,D,M[4],7,0xf57c0faf)
M(F,D,A,B,C,M[5],12,0x4787c62a)
M(F,C,D,A,B,M[6],17,0xa8304613)
M(F,B,C,D,A,M[7],22,0xfd469501)
...
M(F,B,C,D,A,M[15],22,0x49b40821)

Résumé d'un bloc de 512 bits

2ème étape

M(G,A,B,C,D,M[1],5,0xf61e2562)
M(G,D,A,B,C,M[6],9,0xc040b340)
M(G,C,D,A,B,M[11],14,0x265e5a61)
M(G,B,C,D,A,M[0],20,0xe9b6c7aa)
M(G,A,B,C,D,M[5],5,0xd62f105d)
M(G,D,A,B,C,M[10],9,0x02441453)
M(G,C,D,A,B,M[15],14,0xd8a1e681)
M(G,B,C,D,A,M[4],20,0xe7d3fbc8)
...
M(G,B,C,D,A,M[12],22,0x8d2a4c8a)

Résumé d'un bloc de 512 bits

3ème et 4ème étapes

M(H,A,B,C,D,M[5],4,0xfffa3942)
M(H,D,A,B,C,M[8],11,0x8771f681)
M(H,C,D,A,B,M[11],16,0x6d9d6122)
M(H,B,C,D,A,M[14],23,0xfde5380c)
...
M(I,A,B,C,D,M[4],6,0xf7537e82)
M(I,D,A,B,C,M[11],10,0xbd3af335)
M(I,C,D,A,B,M[2],15,0x2ad7d2bb)
M(I,B,C,D,A,M[9],21,0xeb86d391)

Résumé des blocs de 512 bits

- Sauvegarde des registres :
  AA = A, BB = B, CC = C et DD = D.

- Calcul du résumé du premier bloc :
  – Résultat dans A, B, C et D.

- Mise à jour des registres :
  A = A + AA, B = B + BB, C = C + CC et D = D + DD.

- Sauvegarde des registres et calcul du résumé du bloc suivant ...

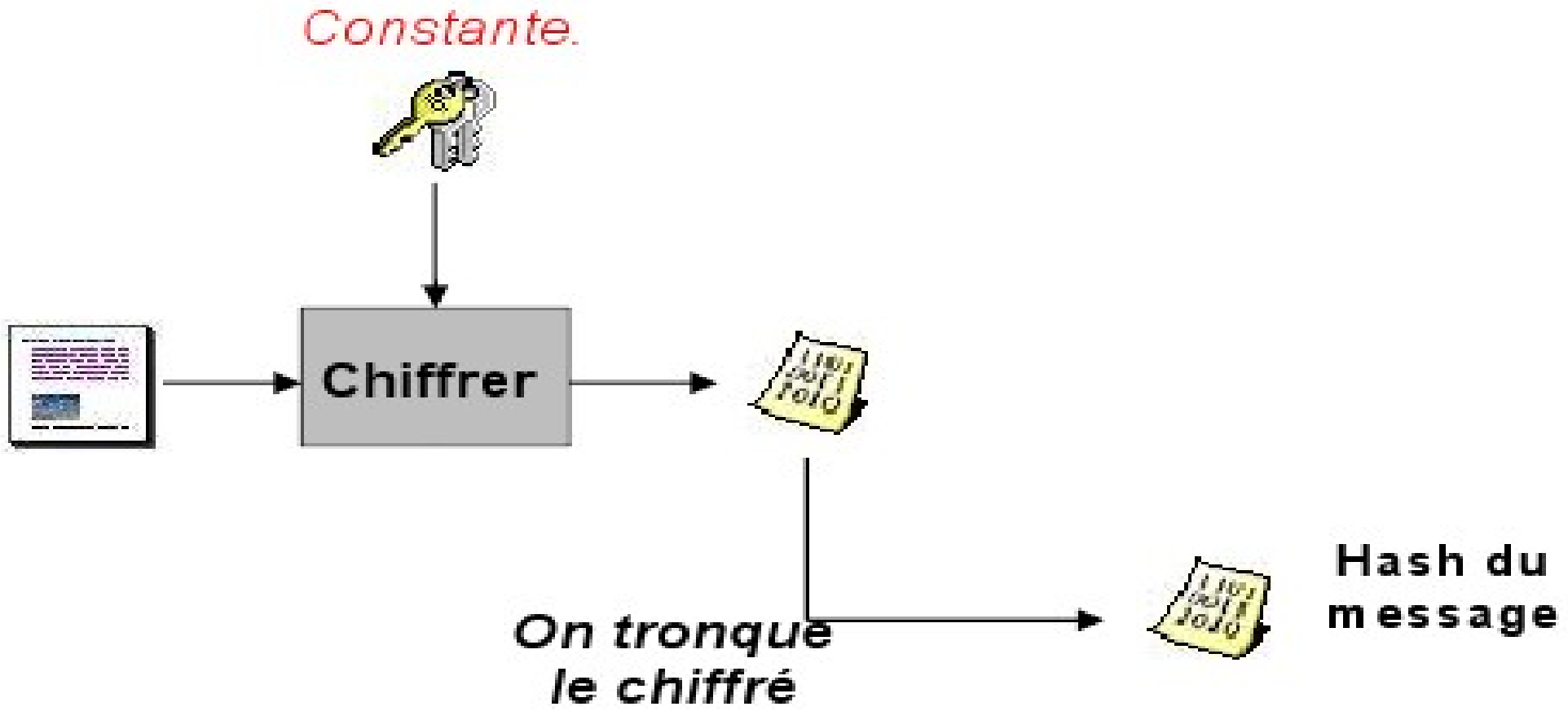
Analyse du MD5

- Performance :
  - Très (trop ?) bonne.
  - Peut-être considéré comme un générateur pseudo-aléatoire.
- Sécurité :
  - Taille du résumé trop court (paradoxe des anniversaires).

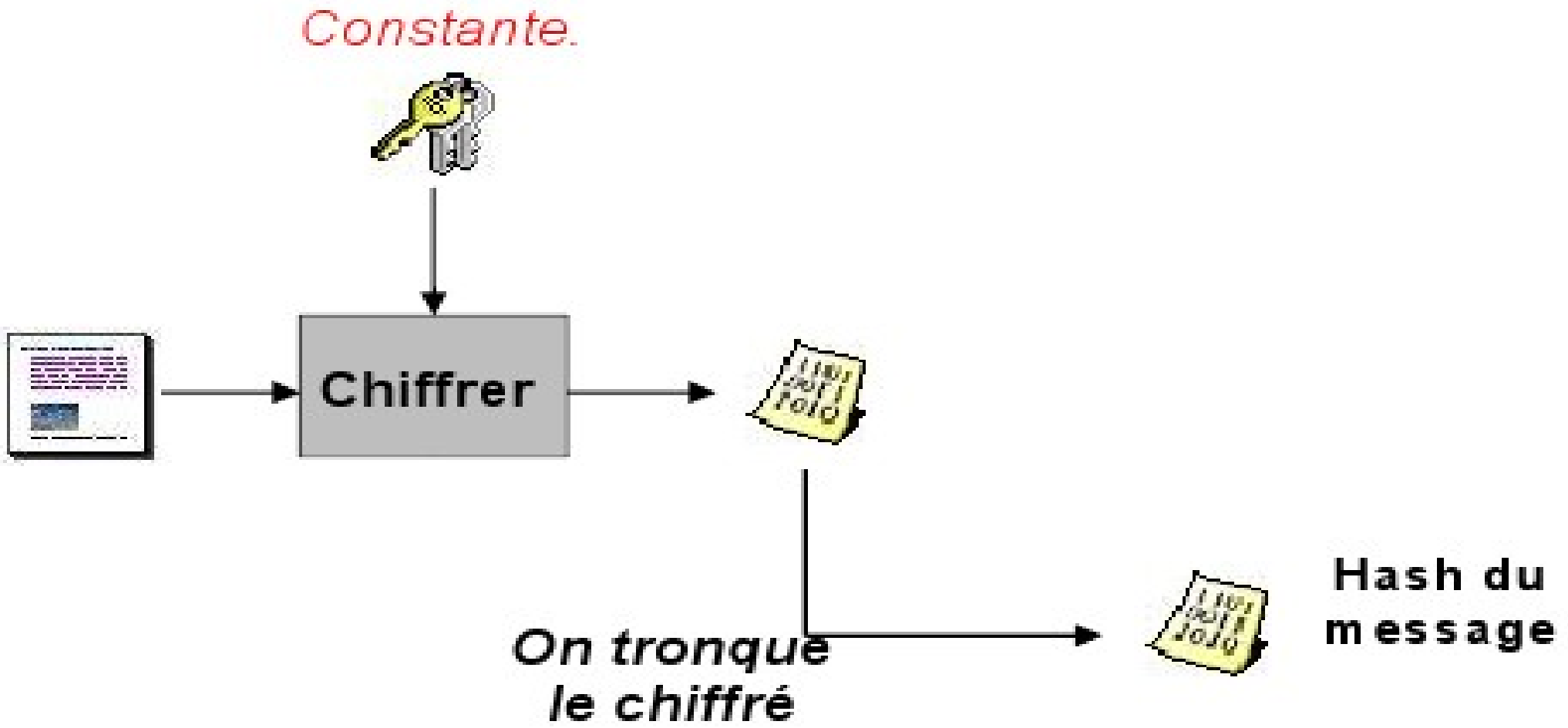
Confusion et Diffusion ?

- Confusion totale :
  - MD5 de « aaaaaaaaaaaaaaaaaaaa » :
    4fce 5e6c c40c 3a60 04d5 246f 830d 5651
- Diffusion totale :
  - MD5 de « eaaaaaaaaaaaaaaaaaaa » :
    7ba4 eed3 bc47 446d 7998 15bc b27f b9dc

A l'aide d'un chiffrement symétrique par bloc



Fonctions de hachage
Message Authentication Code



Exemple du DES

Confusion et Diffusion ?

- Confusion totale :
  - Hash-DES de « aaaaaaaaaaaaaaaaaaaa » :
    46d3 dad6 5f55 dbe0

- Diffusion totale en mode CBC :
  - Hash-DES de « eaaaaaaaaaaaaaaaaaaa » :
    2899 c113 88be c89d

Message Authentication Code
A partir d'une fonction de hachage.

- Paramètres :
  - H : fonction de hachage à sens unique.
  - M : message à authentifier.
  - K : clé secrète partagée.

- Code d'authentification du message :

$$H(K,M) = H(K \mid H(K \mid M))$$