Chapitre 7

Sécurité des réseaux

Services,
attaques
et
mécanismes cryptographiques

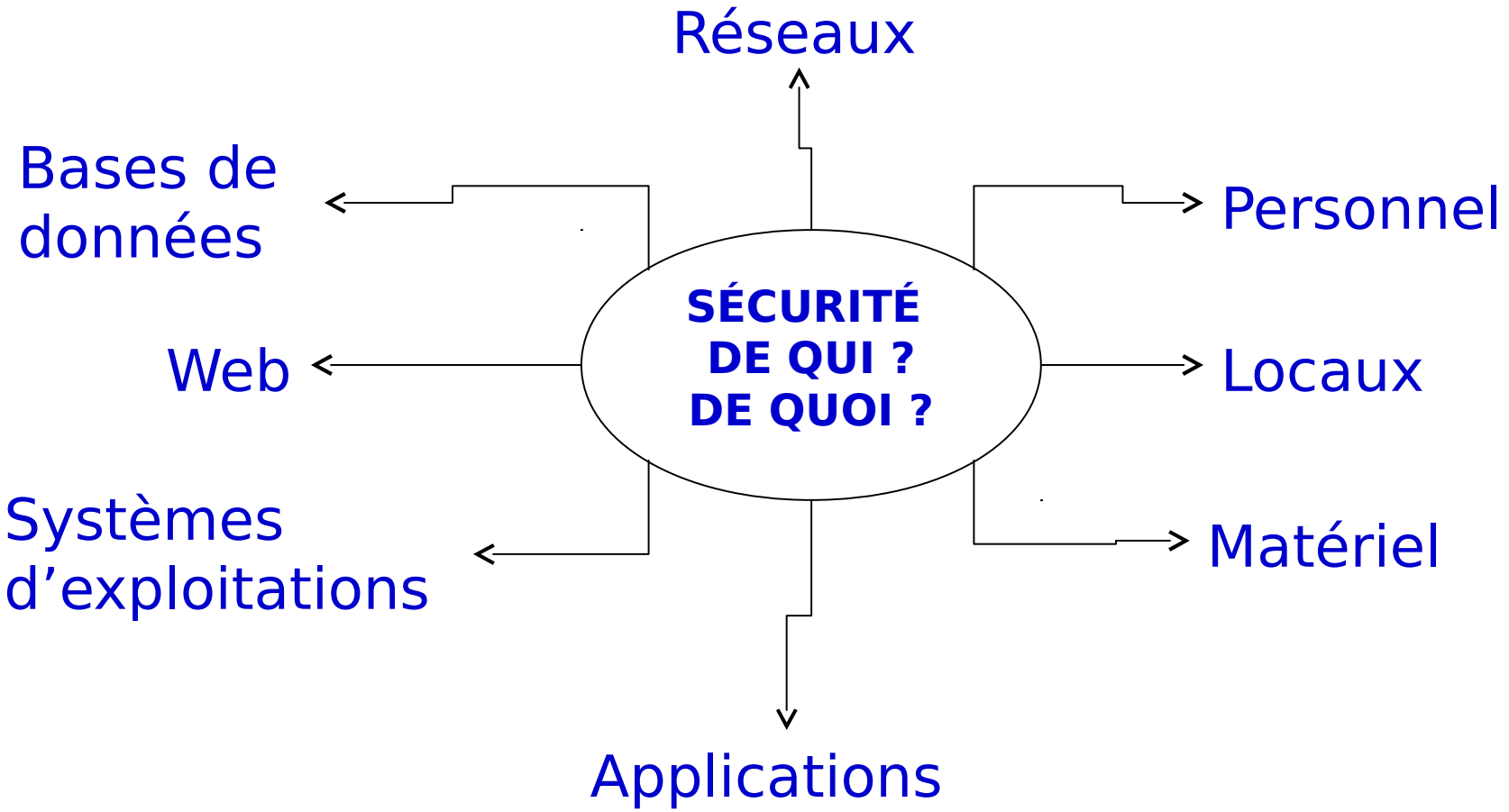
Partie 1:
Introduction à la sécurité des réseaux

Définitions

- Sécurité:
  - Ensemble des techniques qui assurent que les données et les ressources (matérielles ou logicielles) soient utilisées uniquement dans le cadre où il est prévu qu'elles le soient.
  - ➔ Sécurité des systèmes d'informations

- Système d'information:
  - Ensemble d'activités consistant à gérer les informations:
    - acquérir, stocker, transformer, diffuser, exploiter…
  - Fonctionne souvent grâce à un système informatique
  - ➔ Sécurité du système d'information = sécurité du système informatique

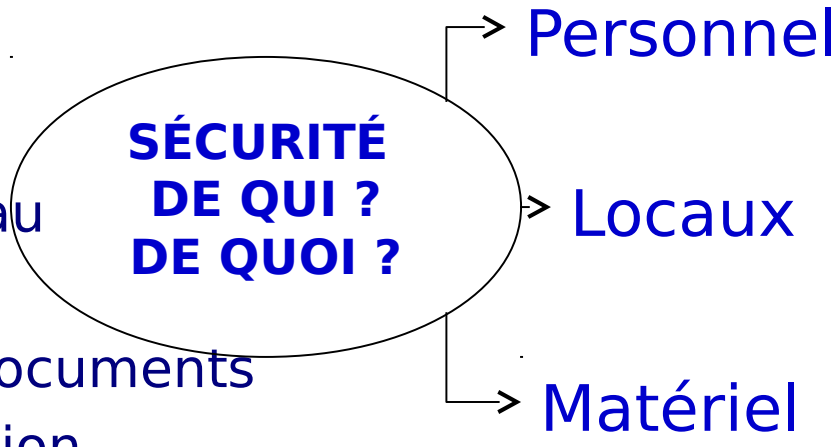
Périmètre de la sécurité (1/3)



Périmètre de la sécurité (1/3)

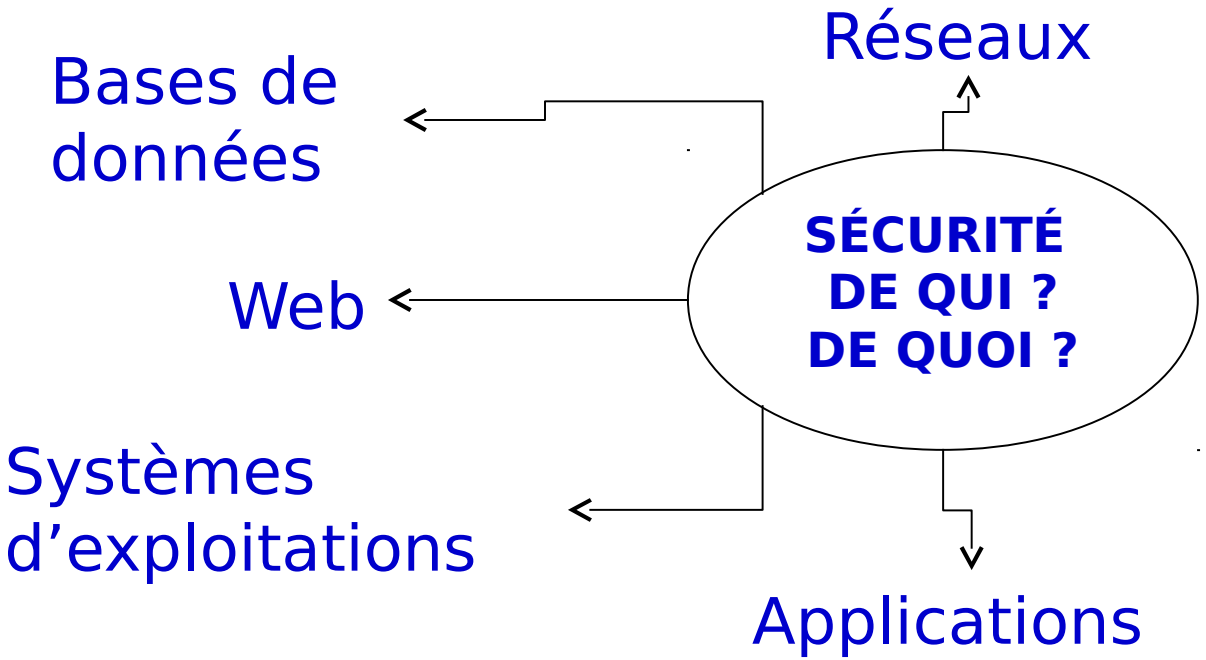
- Périmètre **organisationnel et fonctionnel**:
  - Organisation de la sécurité
    - Répartition des responsabilités
    - Sensibilisations des utilisateurs
    - Contrôle
  - Politique et guides de sécurité
  - Procédure de sécurité

- Sécurité **physique**
  - Lutte anti-incendie, dégâts d'eau
  - Contrôle d'accès physique
  - Sauvegarde et archivage des documents
  - Sécurité du matériel: climatisation…



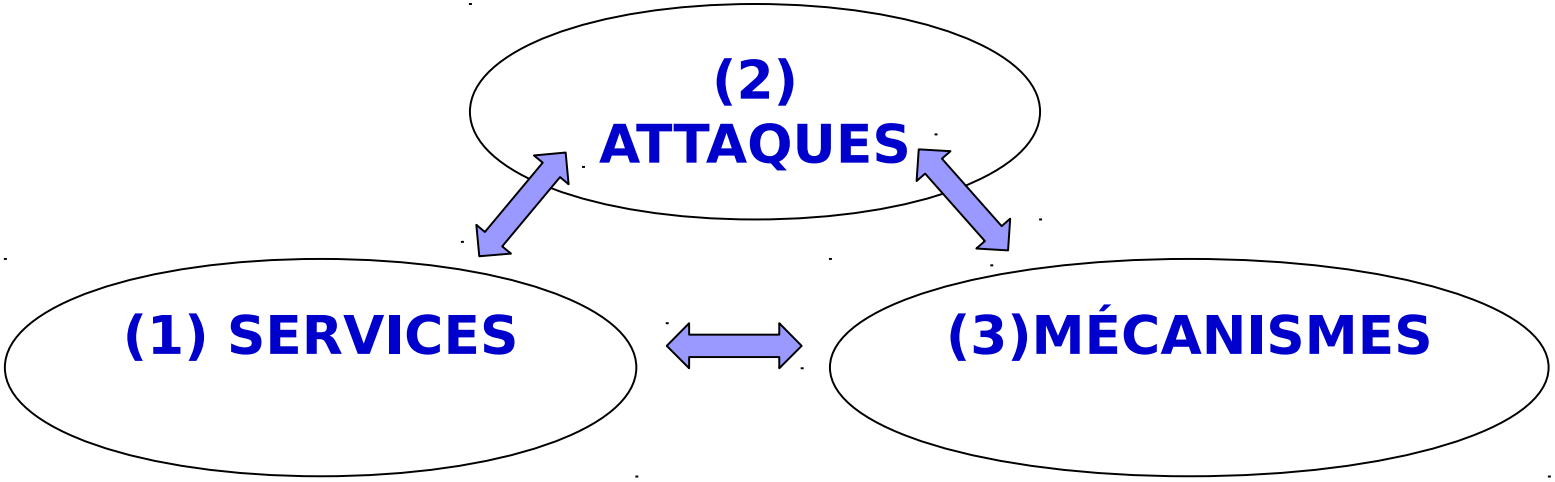
Périmètre de la sécurité (2/2)

- Sécurité **logique**:
  - des données,
  - des applications,
  - des systèmes d'exploitation.
  - Des communications réseaux



Aspects de la sécurité

Méthodes employées pour casser les services de la sécurité en détournant les mécanismes



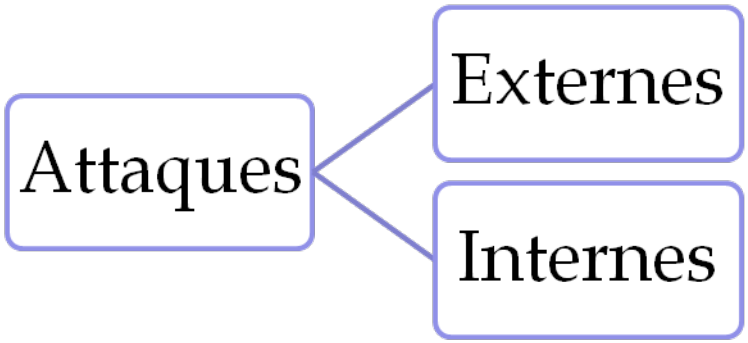
Fonctionnalités requises pour assurer un environnement sécurisé en faisant appel aux mécanismes

Moyens utilisés pour assurer les services de la sécurité en luttant contre les attaques

Aspects de la sécurité: services

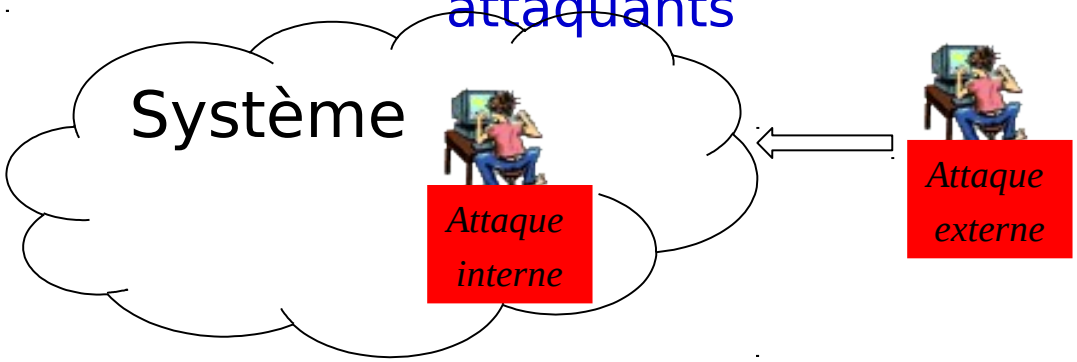
- Authentification
  - Assurance de l'identité d'un objet de tout type qui peut être une personne (identification), un serveur ou une application.
- Intégrité
  - Garantie qu'un objet (document, fichier, message, etc.) ne soit pas modifié par un tiers que son auteur.
- Confidentialité
  - Assurance qu'une information ne soit pas comprise par un tiers qui n'en a pas le droit
- Non répudiation
  - Assurance que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et que son récepteur ne puisse pas nier l'avoir reçu.
- Disponibilité
  - Assurance que les services ou l'information soient utilisable et accessible par les utilisateurs autorisés

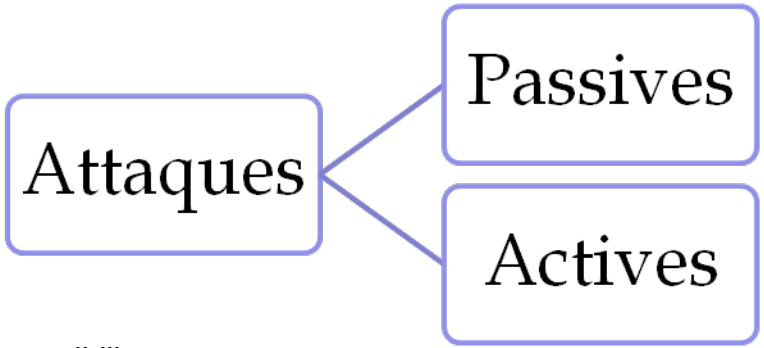
Aspects de la sécurité: attaques



Exécutées par des entités **externes** au système victime

Exécutées par des entités **internes** au système victime parce qu'ils sont malicieux ou détenu par des attaquants

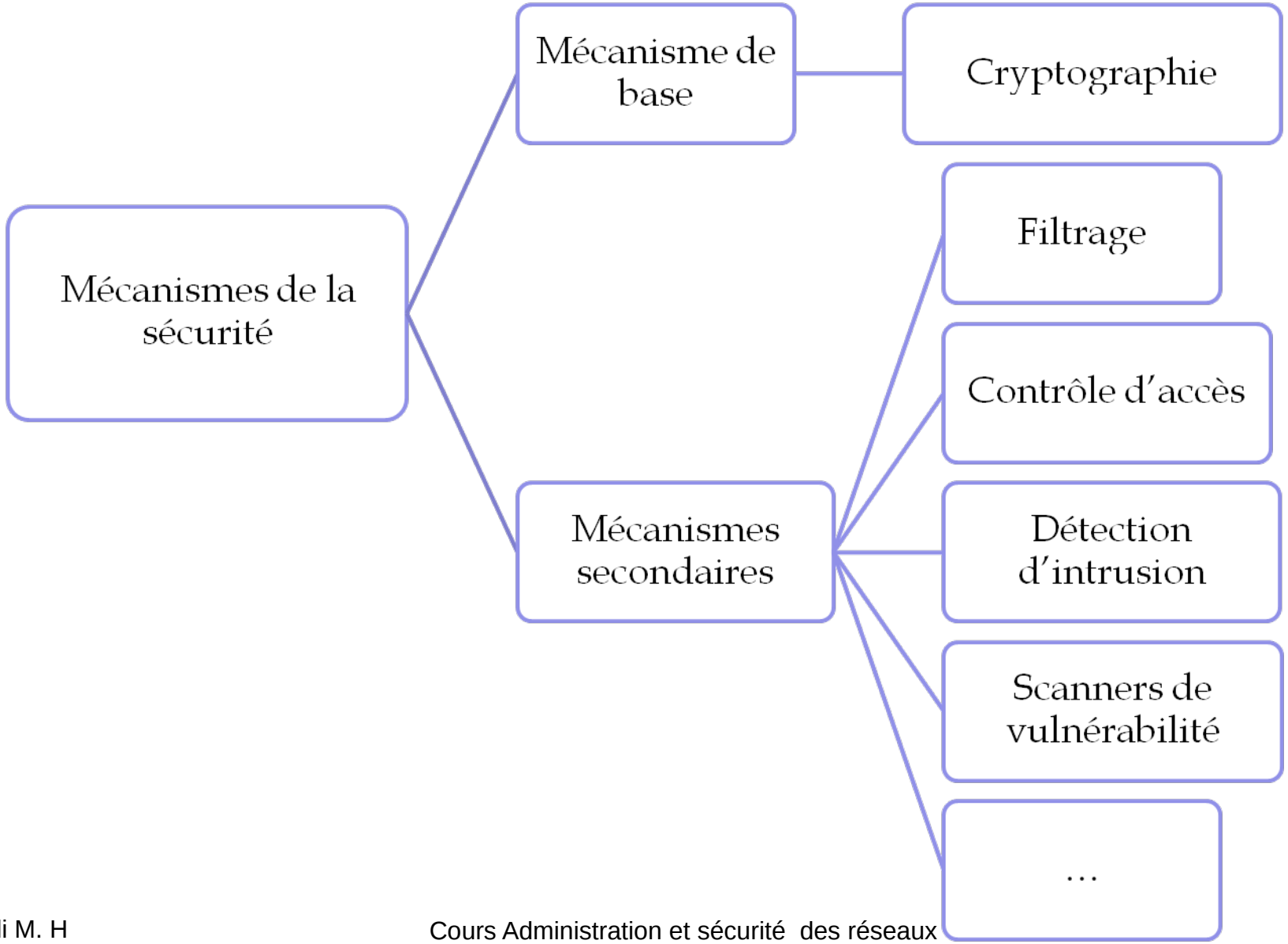




Ecoute du système (réseau) pour l'analyser

Injection, suppression ou modification de données

Aspects de la sécurité: Mécanismes



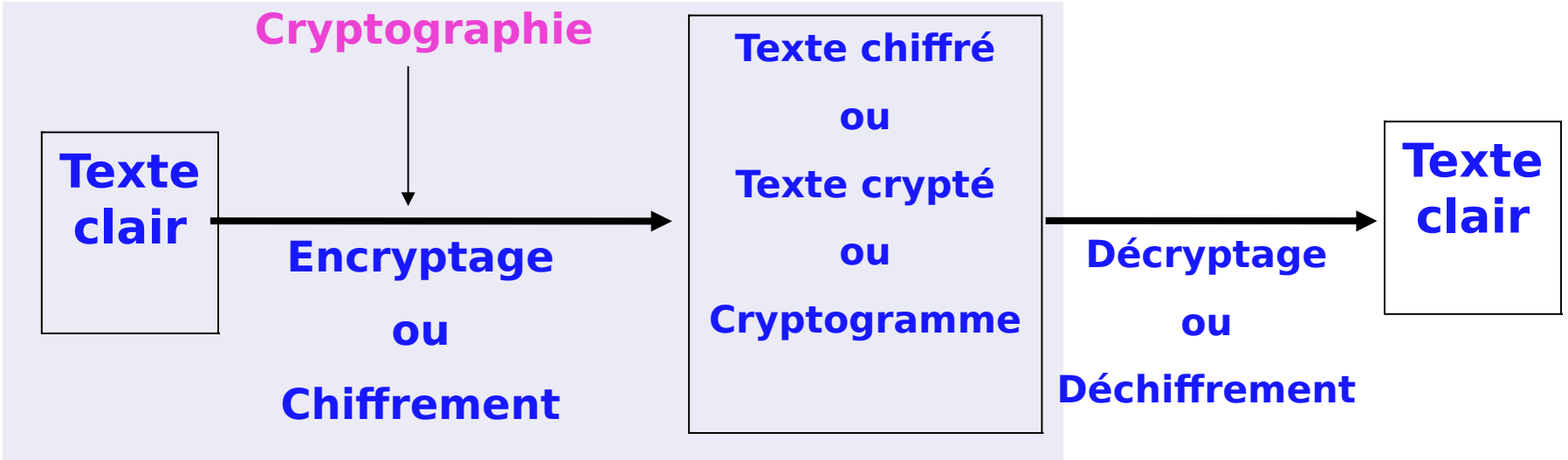
Partie 2:
Mécanismes cryptographique de la sécurité

Définitions

- **Cryptologie (Cryptology) :**
  - Science (branche des mathématiques) des communications secrètes.
  - Composée de deux domaines d'études complémentaires :
    - Cryptographie
    - Cryptanalyse.

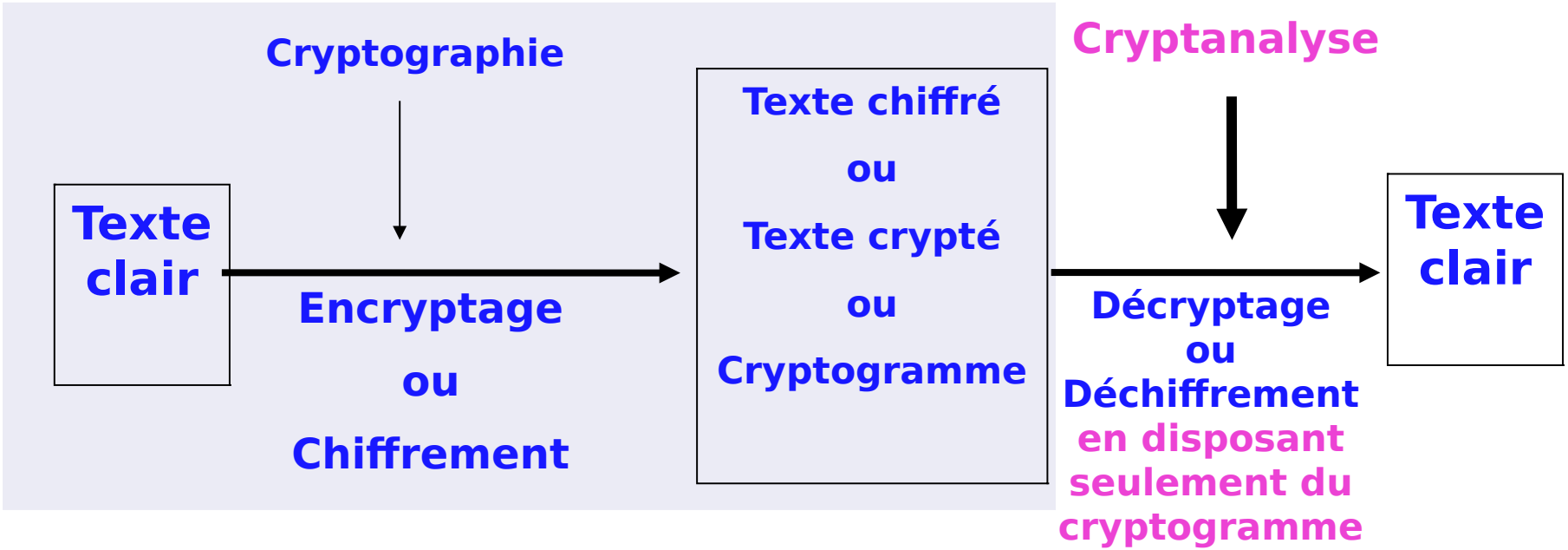
Définitions

- **Cryptographie (cryptography) = Chiffrement=Encryptage**
  - Ensemble des méthodes et techniques qui permettent de transformer un message afin de le rendre incompréhensible pour quiconque n'est pas doté du moyen de le déchiffrer.
    - On parle d'***encrypter*** (***chiffrer***) un message,
    - Le code résultant s'appelle ***cryptogramme***.
    - L'action inverse s'appelle ***décryptage*** (***déchiffrement***).



Définitions

- **Cryptanalyse (cryptanalysis)**
  - **Art de révéler les messages** qui ont fait l'objet d'un encryptage.
  - Lorsqu'on réussie, au moins une fois, à **déchiffrer un cryptogramme**, on dit que l'**algorithme** qui a servi à l'encrypter a été **cassé**.



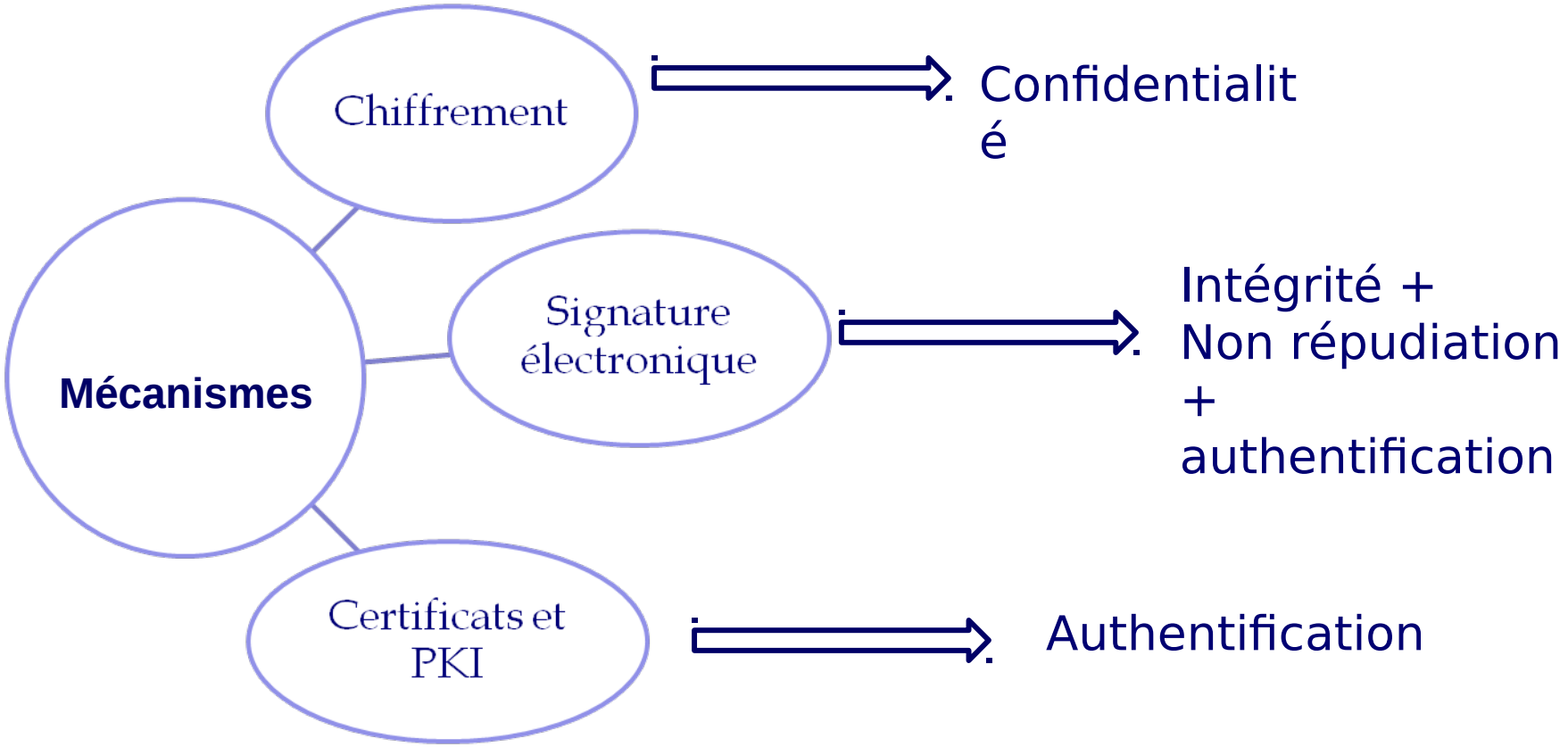
Définitions

- **Clé :**
  - Information qui sera utilisée pour encrypter et / ou décrypter un message.

    *On peut cependant concevoir un algorithme **qui n'utilise pas de clé**, dans ce cas c'est lui-même qui constitue le secret et son principe représente la clé*

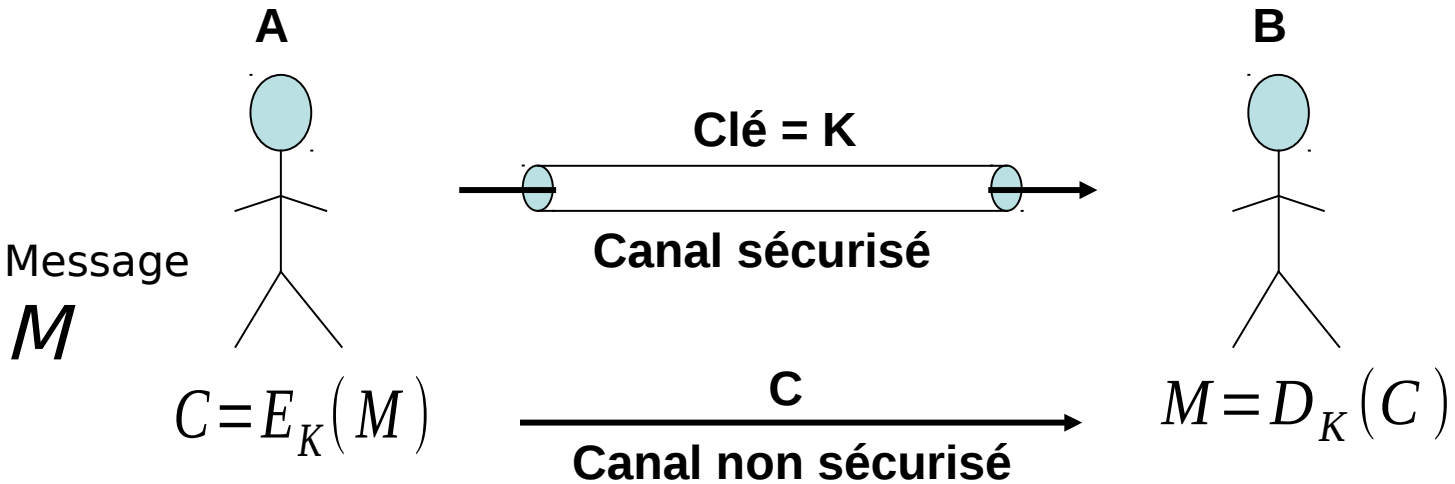
- **Crypto système:**
  - Ensemble composé d'un algorithme, de tous les textes en clair, de tous textes chiffrés et de toutes clés possibles.

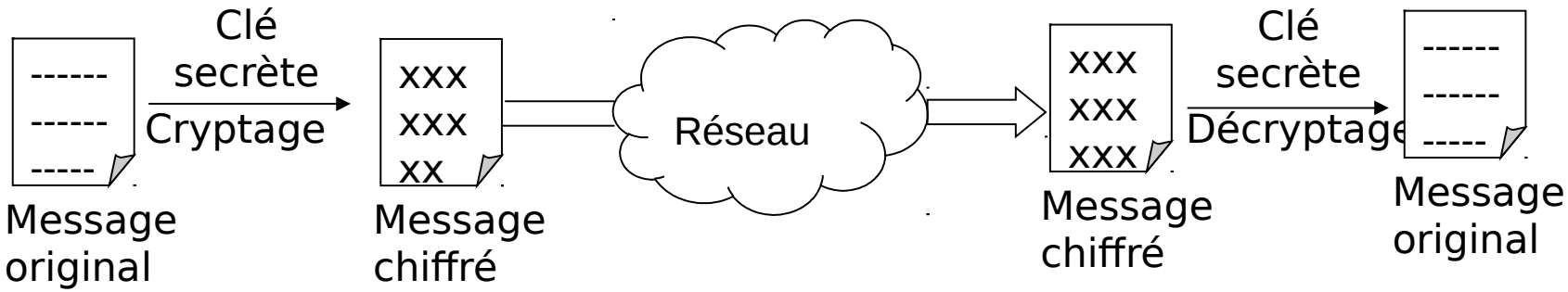
Mécanismes cryptographiques de la sécurité



Chiffrement

- **Chiffrement symétrique**





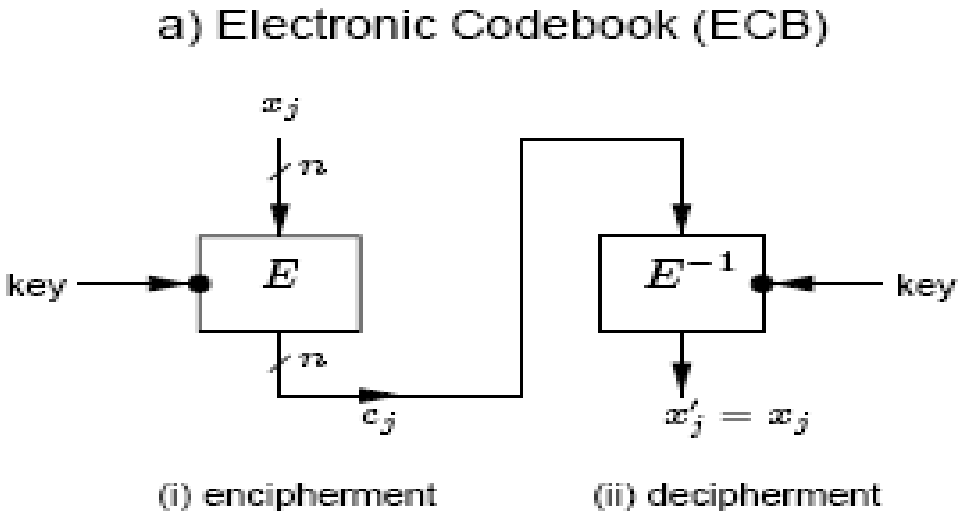
- Exemples: ECB, CBC, DES, AES, IDEA…

Chiffrement

- **Cryptosystèmes symetriques modernes**
  - Deux modes de chiffrement
    - En Stream
    - Par bloc
      - Segmentation du message M à chiffrer
        - M est scindé en un nombre de bloc de taille fixe
      - Cryptage des blocs
      - C est obtenu en concaténant les cryptogrammes des bloc
  - Modes de chiffrement par bloc
    - ECB (Electronic CodeBook)
    - CBC(Cipher bloc Chaining)
    - CBF (Cipher FeedBack)
    - OFB (Output FeedBack)

Chiffrement

- **Mode ECB (Electronic CodeBook)**
  - Un bloc de texte se chiffre indépendamment de tout en un bloc de texte chiffré



7.11 Algorithm ECB mode of operation

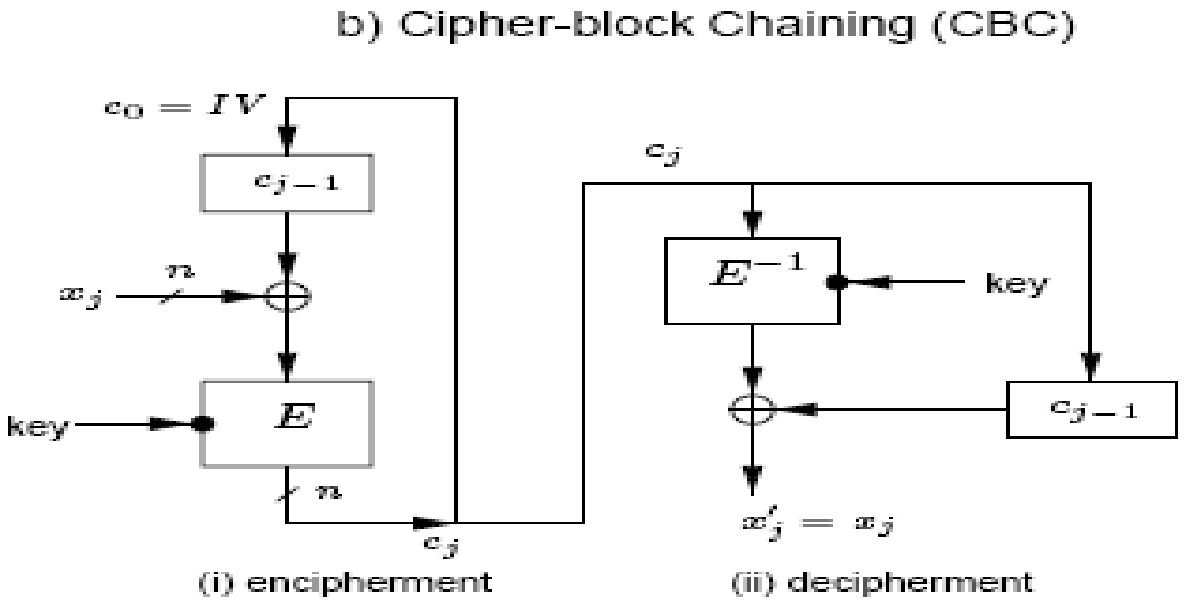
INPUT: k-bit key K; n-bit plaintext blocks $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; decrypt to recover plaintext.

1. Encryption: for $1 \leq j \leq t$, $c_j \leftarrow E_K(x_j)$.
2. Decryption: for $1 \leq j \leq t$, $x_j \leftarrow E_K^{-1}(c_j)$.

Chiffrement

Mode CBC (Cipher Block Chaining)

- Chaque bloc du cryptogramme dépend du bloc de texte en clair et de tous les blocs précédents



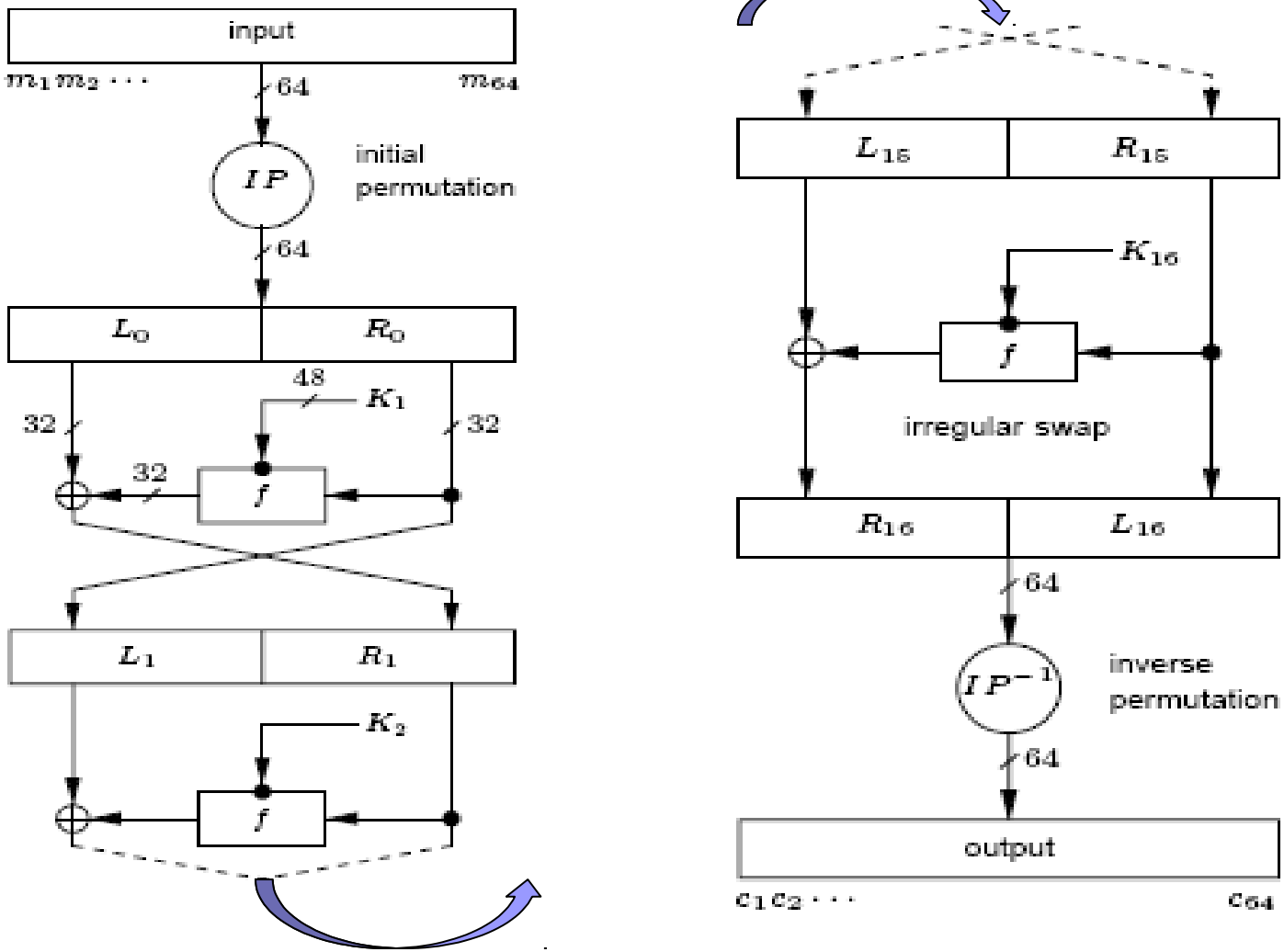
7.13 Algorithm CBC mode of operation

INPUT: k-bit key K; n-bit IV; n-bit plaintext blocks $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; decrypt to recover plaintext.

1. Encryption: $c_0 \leftarrow IV$. For $1 \leq j \leq t$, $c_j \leftarrow E_K(c_{j-1} \oplus x_j)$.
2. Decryption: $c_0 \leftarrow IV$. For $1 \leq j \leq t$, $x_j \leftarrow c_{j-1} \oplus E_K^{-1}(c_j)$.

Chiffrement

Chiffrement symétrique : DES

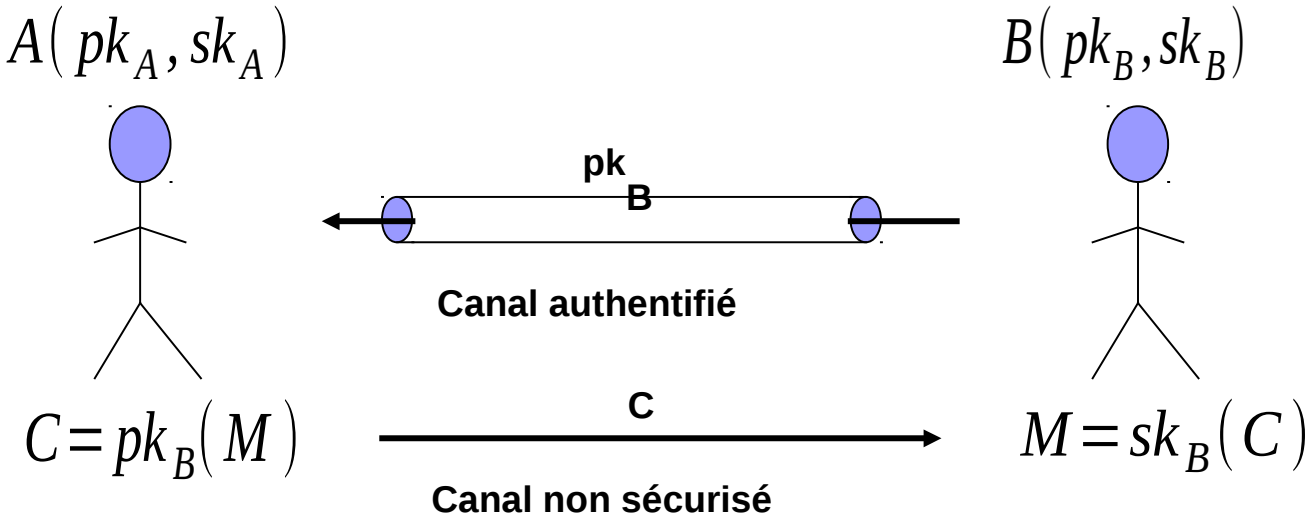


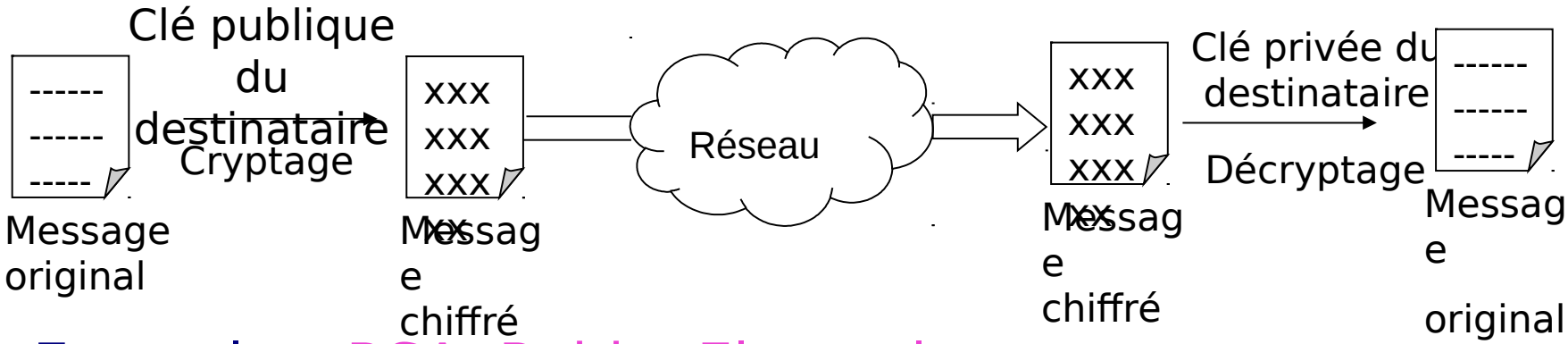
$$L_i = R_{i-1};$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \quad \text{where } f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

Chiffrement

- **Chiffrement asymétrique**





- Exemples: RSA, Rabin, Elgamal…

Cryptosystèmes asymétriques

public-key encryption scheme	computational problem
RSA	integer factorization problem (§3.2) RSA problem (§3.3)
Rabin	integer factorization problem (§3.2) square roots modulo composite n (§3.5.2)
ElGamal	discrete logarithm problem (§3.6) Diffie-Hellman problem (§3.7)
generalized ElGamal	generalized discrete logarithm problem (§3.6) generalized Diffie-Hellman problem (§3.7)
McEliece	linear code decoding problem
Merkle-Hellman knapsack	subset sum problem (§3.10)
Chor-Rivest knapsack	subset sum problem (§3.10)
Goldwasser-Micali probabilistic	quadratic residuosity problem (§3.4)
Blum-Goldwasser probabilistic	integer factorization problem (§3.2) Rabin problem (§3.9.3)

Chiffrement

- **Chiffrement asymétrique: RSA**

8.1 Algorithm Key generation for RSA public-key encryption

SUMMARY: each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$. (See Note 8.5.)
3. Select a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e); A's private key is d.

Chiffrement

- **Chiffrement asymétrique: RSA**

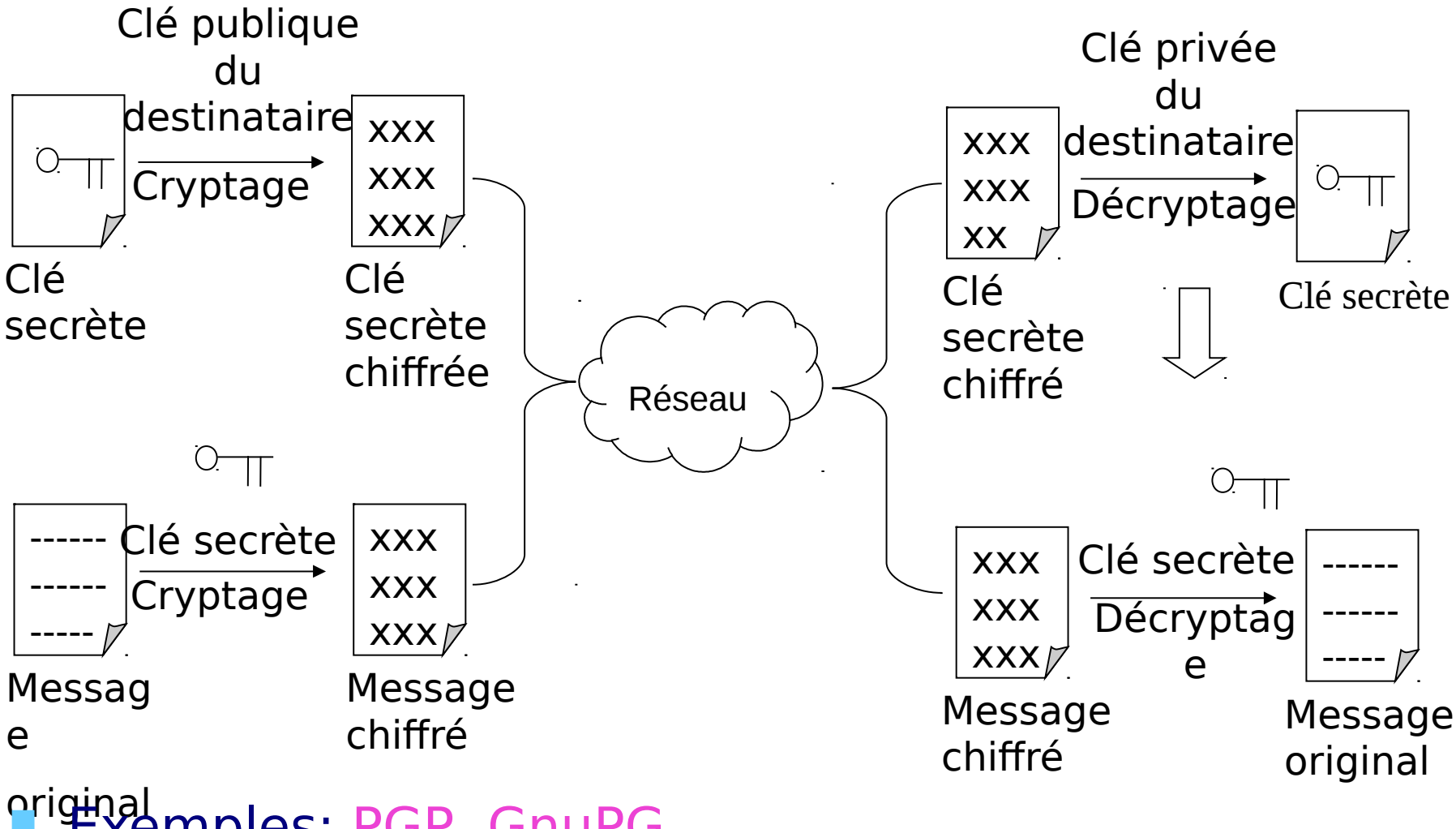
8.3 Algorithm RSA public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:
   (a) Obtain A's authentic public key (n, e).
   (b) Represent the message as an integer m in the interval $[0, n-1]$.
   (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).
   (d) Send the ciphertext c to A.
2. *Decryption.* To recover plaintext m from c, A should do the following:
   (a) Use the private key d to recover $m = c^d \bmod n$.

Chiffrement

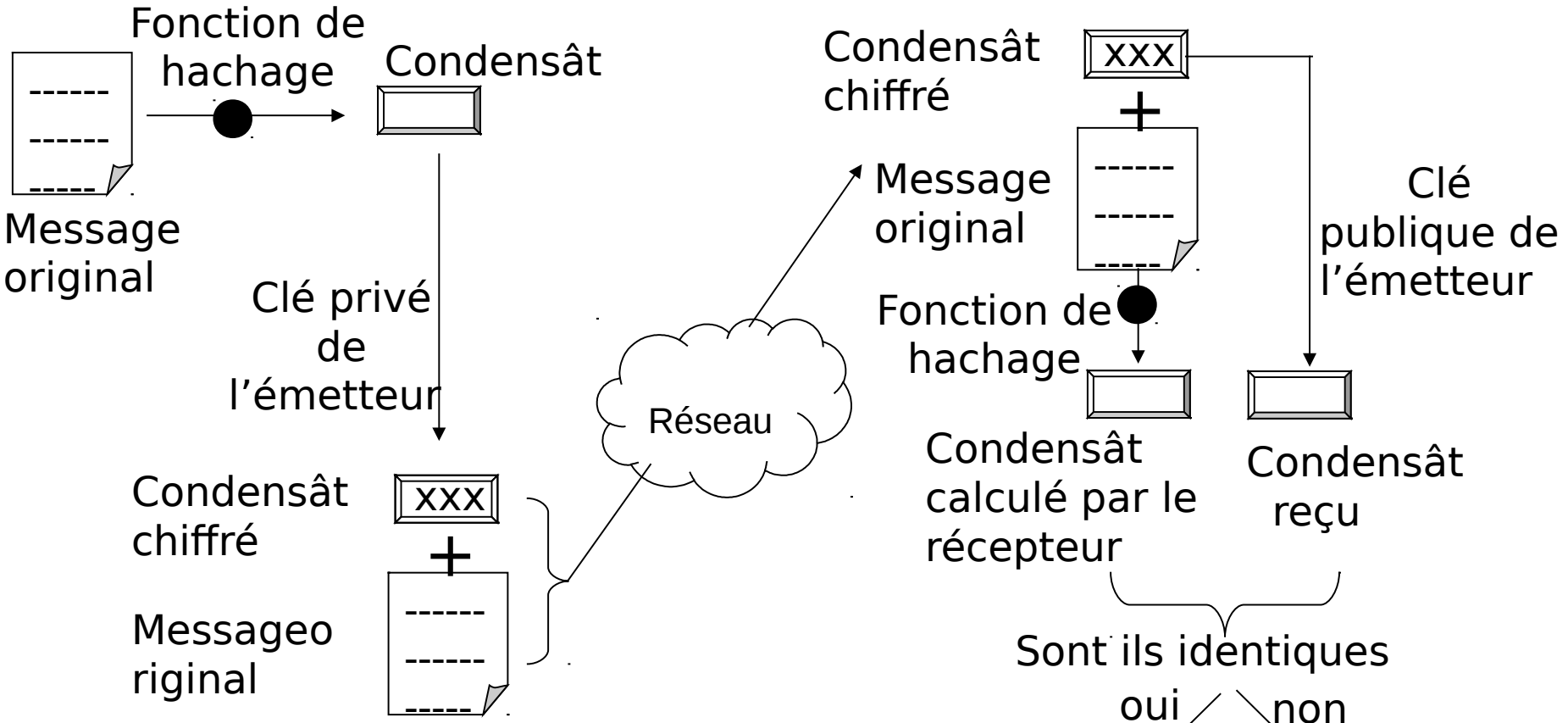
- **Chiffrement hybride**



- Exemples: PGP, GnuPG

Signature électronique

- **Permet l'authentification, l'intégrité et la non répudiation**



- Exemples: signatures RSA, Elgamal, Rabin, Schnorr, ESIGN…

Signature électronique

Signature RSA

11.19 Algorithm RSA signature generation and verification

SUMMARY: entity A signs a message $m \in \mathcal{M}$. Any entity B can verify A's signature and recover the message m from the signature.

1. *Signature generation.* Entity A should do the following:
   (a) Compute $\bar{m} = R(m)$, an integer in the range $[0, n-1]$.
   (b) Compute $s = \bar{m}^d \bmod n$.
   (c) A's signature for m is s.
2. *Verification.* To verify A's signature s and recover the message m, B should:
   (a) Obtain A's authentic public key (n, e).
   (b) Compute $\bar{m} = s^e \bmod n$.
   (c) Verify that $\bar{m} \in \mathcal{M}_R$; if not, reject the signature.
   (d) Recover $m = R^{-1}(\bar{m})$.

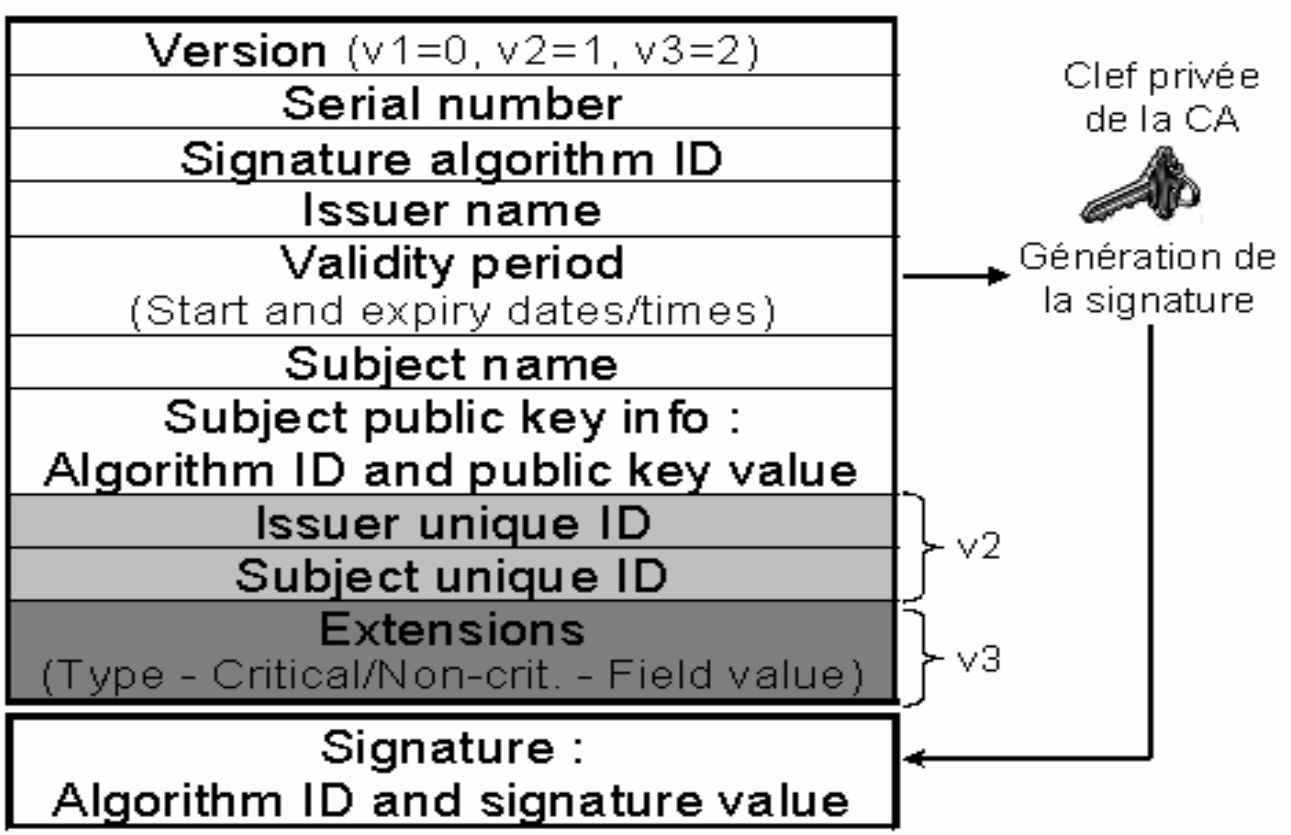
Fonctions de hashage

- **Fonction de hashage**
  - H (M) = C
    - M est de taille quelconque
    - C est de taille fixe (16 ou 20 octets)
      - appelé condensât, ou empreinte, ou fingerprint, ou message digest
  - Fonction à sens unique
  - Si H (M_1) = C_1 ,
    - il est très difficile de trouver :
      M_2 différent de M_1 tel que H (M_2) = C_1
  - Usage : checksums, « intégrité »

- **Exemples**
  - MD5, SHA-1

Certificat numérique

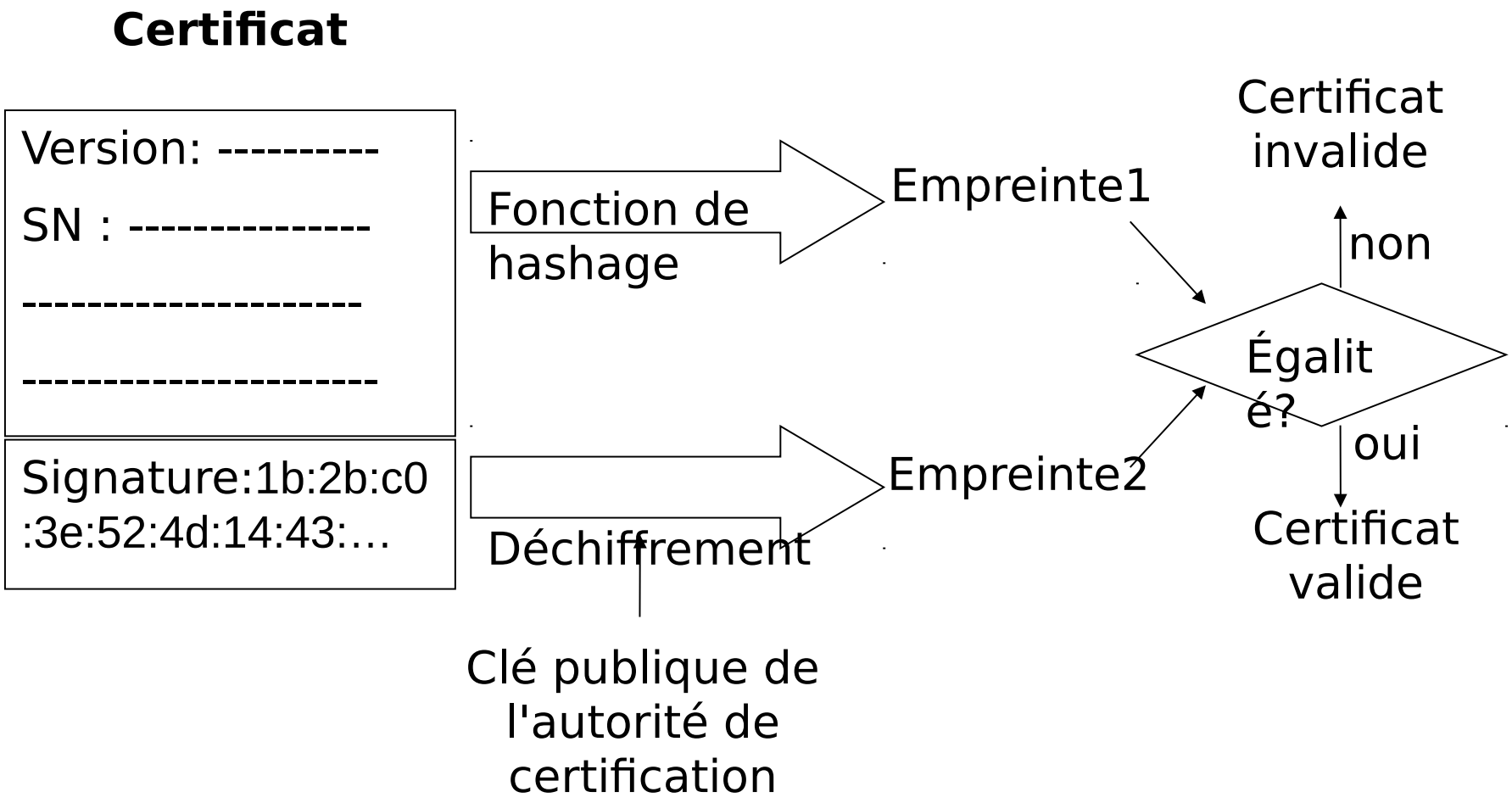
- **Permet l'authentification**
  - Garantit l'appartenance d'une clé publique à une entité
- **Principal format: certificats X.509**



Certificat numérique

- *Serial number* :
  - Numéro de série du certificat (propre à chaque CA).
- *Signature Algorithm ID :*
  - Identifiant du type de signature utilisée.
- *Issuer Name :*
  - *Distinguished Name (DN)* de CA qui a émis ce certificat.
- *Subject Name :*
  - *Distinguished Name (DN)* du détenteur de la clé publique.
- *Subject public key info :*
  - Informations sur la clé publique du certificat.
- *Signature :*
  - Signature numérique du CA sur l'ensemble des champs

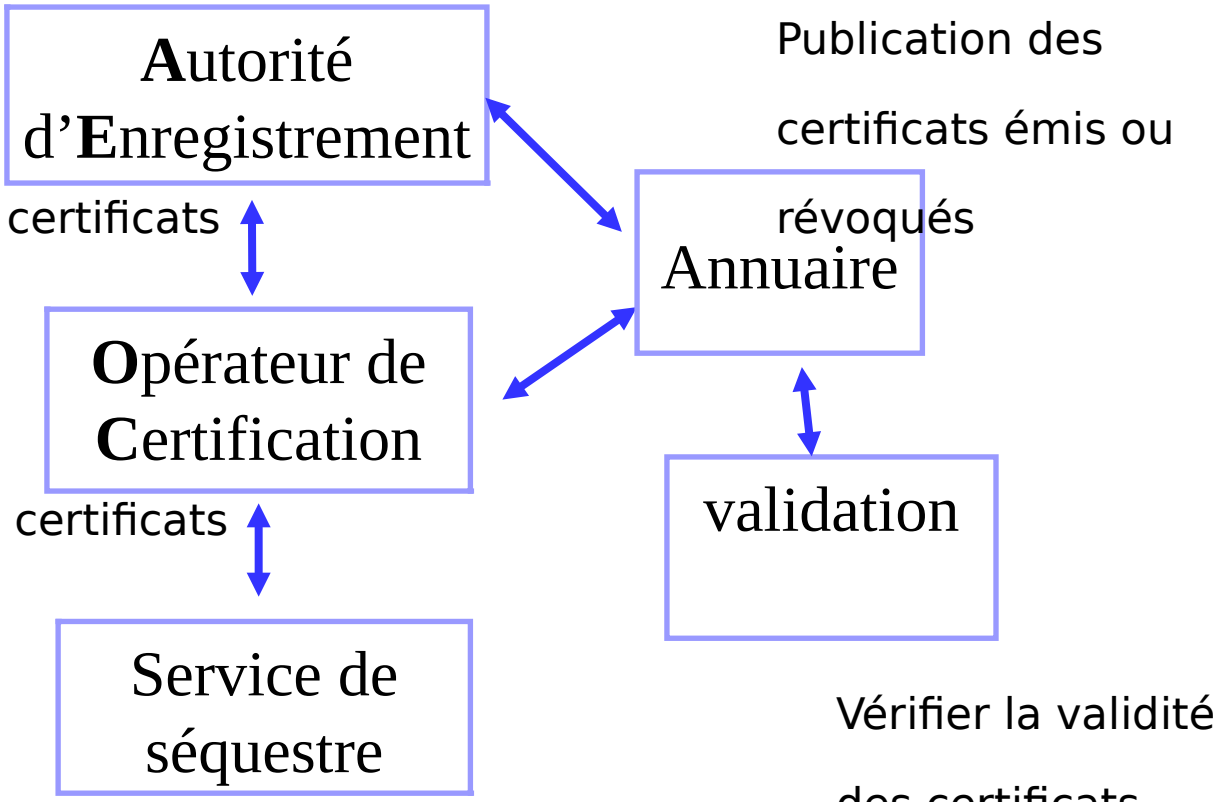
Vérification d’un certificat



PKI: Public Key Infrastructure

Traitement des demande de:

- Création
- Révocation
- Renouvellement de certificats



- Création
- Révocation
- Renouvellement de certificats

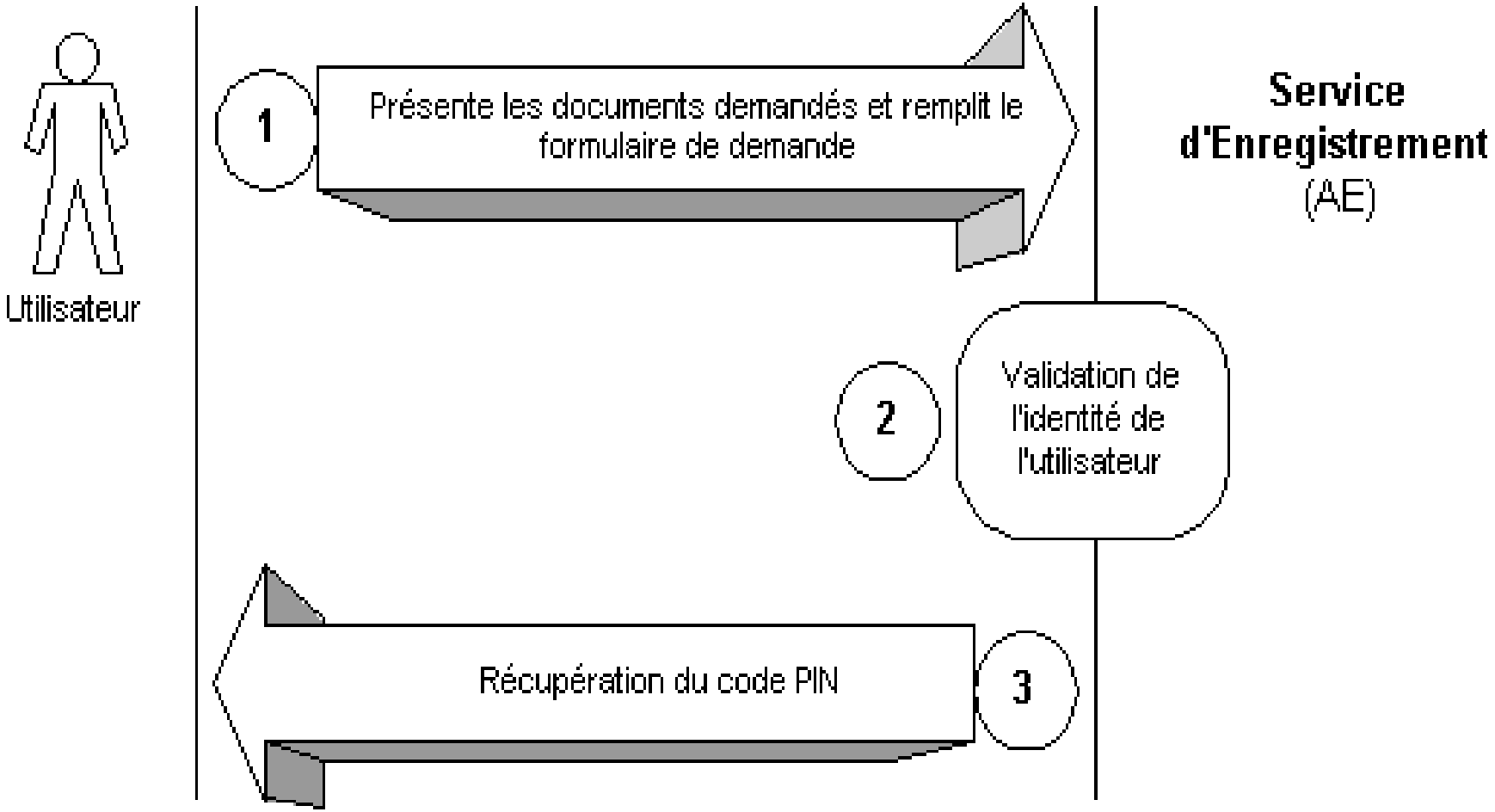
Publication des certificats émis ou révoqués

Vérifier la validité des certificats

Archiver les clés privées/publiques

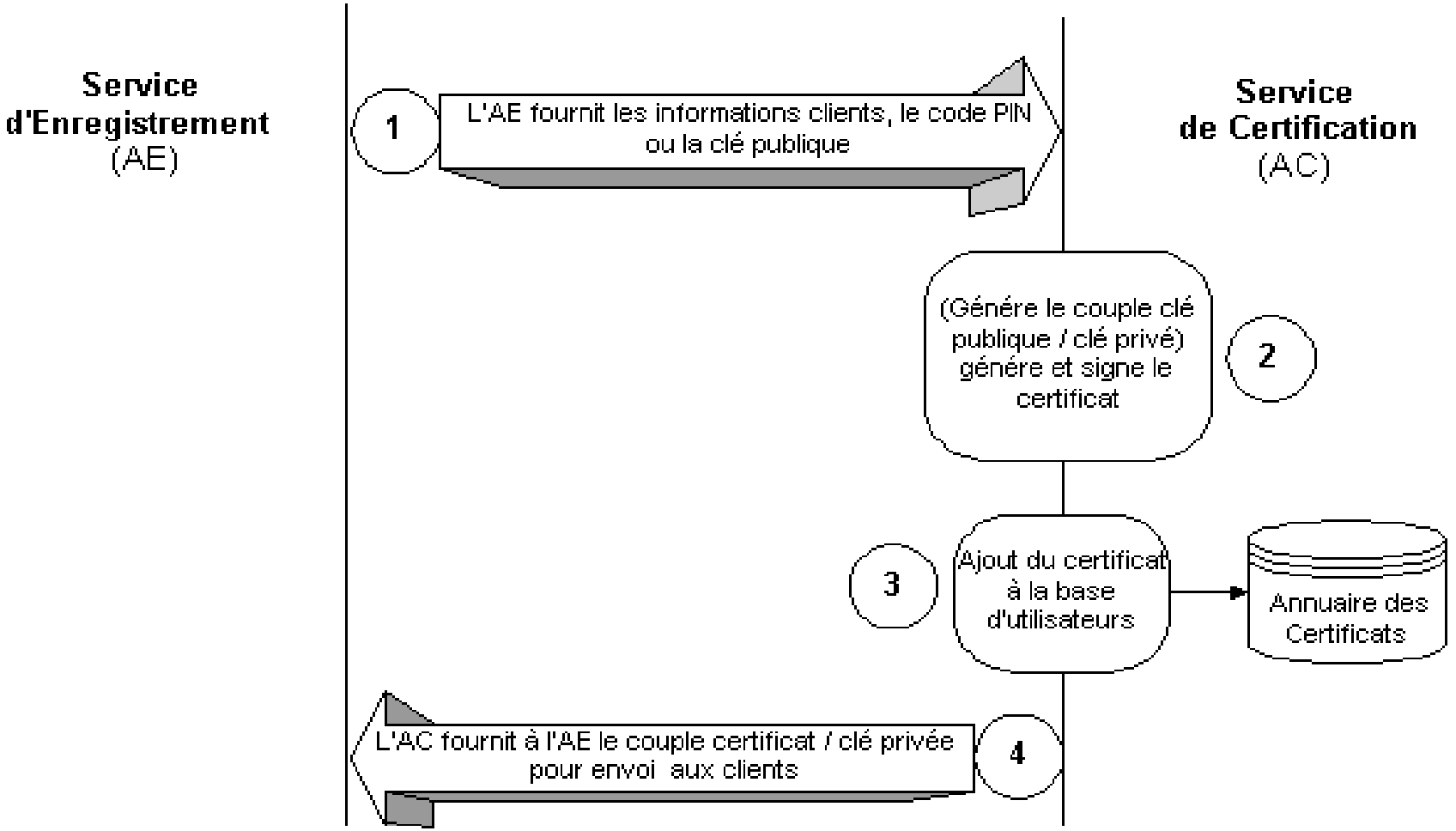
PKI: Exemple de fonctionnement

- **Enregistrement**



PKI: Exemple de fonctionnement

- **Création de certificats**



PKI: Fonctionnement