République Algérienne Démocratique Et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
ECOLE NATIONALE POLYTECHNIQUE D'ORAN MAURICE AUDIN

Département Génie des systèmes
Filière IMSI : 4ème année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

kablifatima47@gmail.com

La cryptographie et ses applications

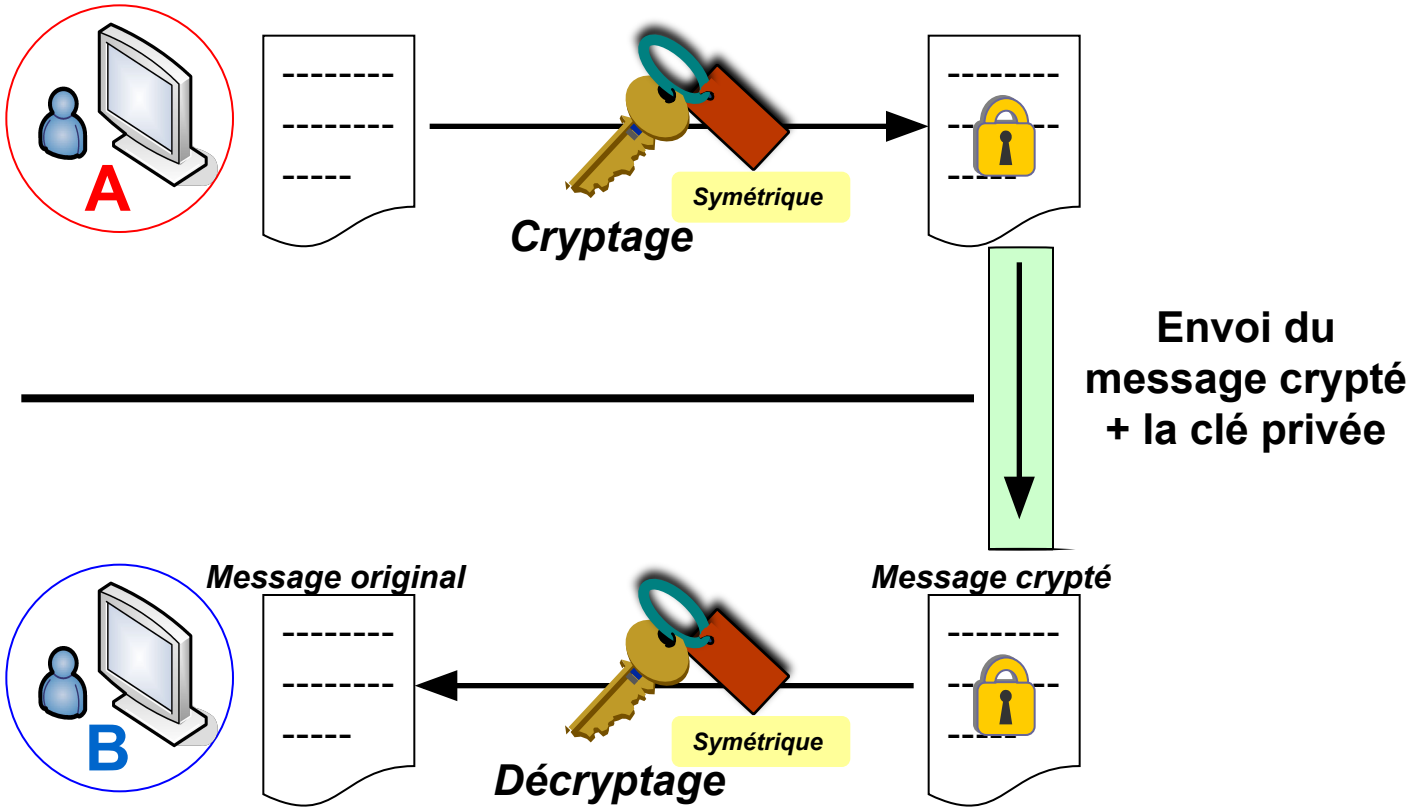
Principales techniques de cryptographie ou de chiffrement de l'information :

- Cryptage par clé symétrique
- Cryptage par clé publique
- Cryptage par clé secrète partagée
- Cryptage par clé de session

La cryptographie et ses applications

Cryptographie à clé symétrique :

- Utilisation de la même clé pour crypter et décrypter



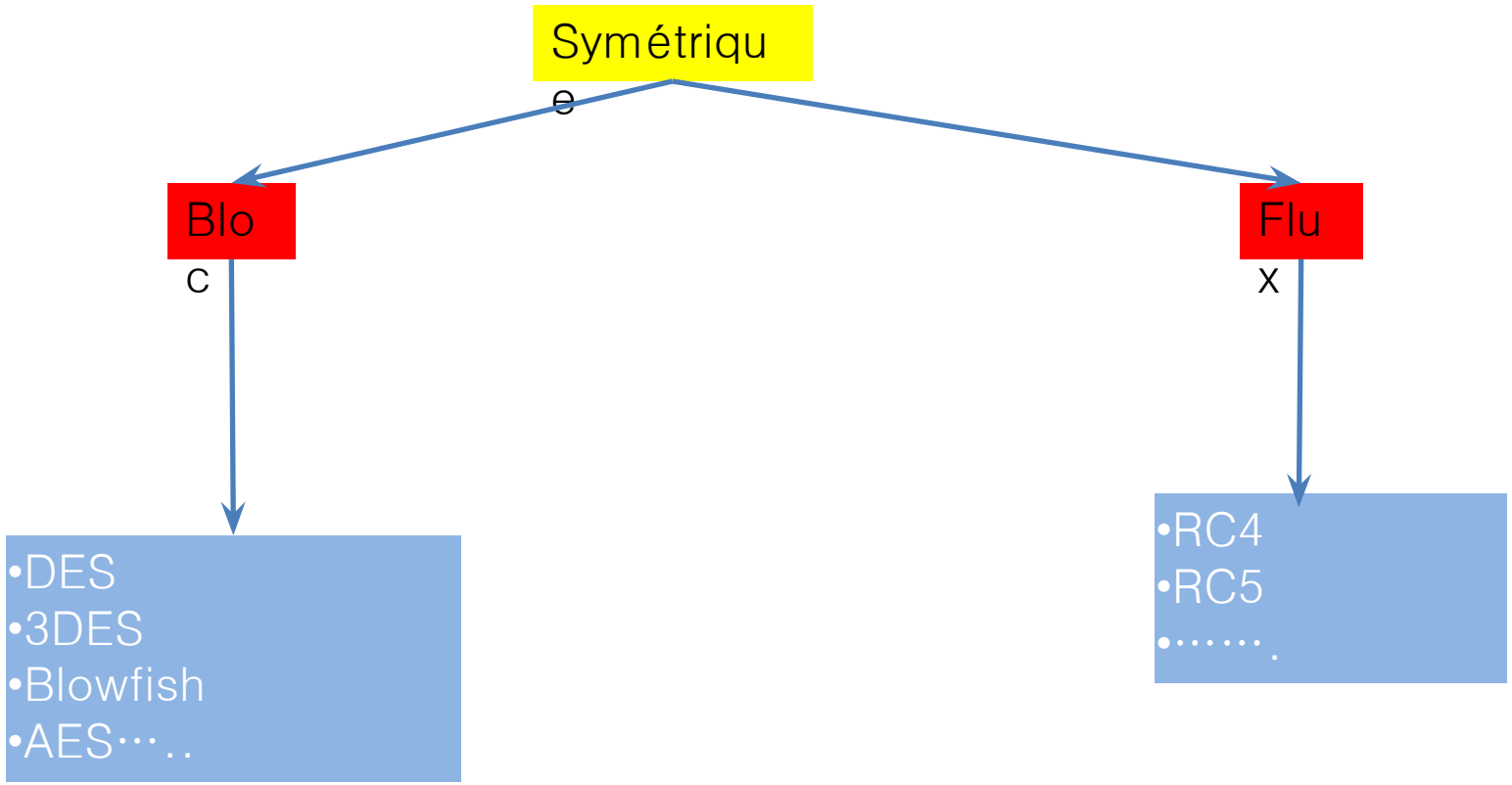
La cryptographie et ses applications

Cryptographie à clé symétrique (ii)

- **Avantage**
  - Mécanisme très rapide
- **Inconvénients**
  - Nécessite la distribution de la clé
  - Si une personne arrive à lire le message et la clé, peut déchiffrer le message
- **Exemples d'algorithmes à clé symétrique**
  - DES (Data Encryption Standard)
  - 3DES (Triple DES)
  - RC2, RC4, RC5
  - AES (Advanced Encription Standard)

La cryptographie et ses applications

- Il y a deux catégories de systèmes à clé privée: les chiffrements **par blocs** et les chiffrements **de flux**.

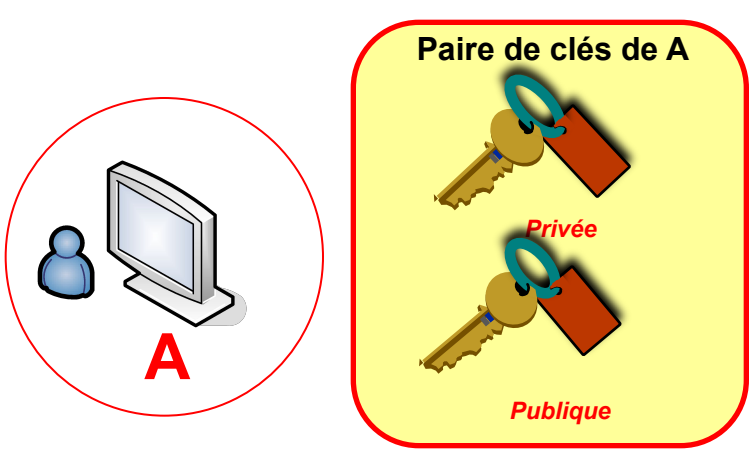


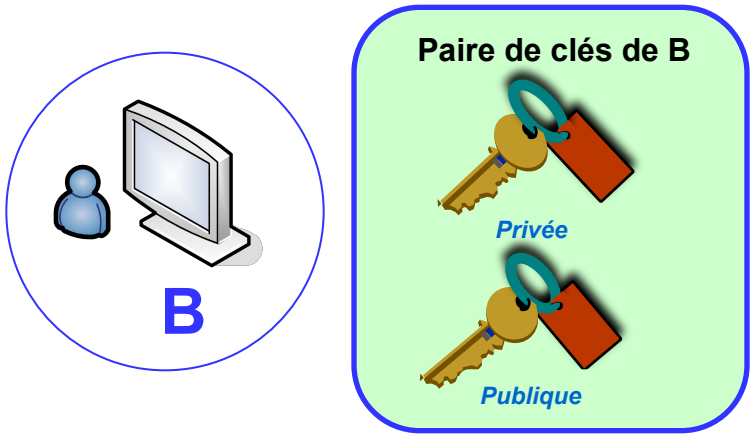
La cryptographie et ses applications

Cryptographie à clé asymétrique ou publique :

Chaque utilisateur du système possède une paire de clés:

- ✔ **Une clé privée**: est connue seulement par son propriétaire
- ✔ **Une clé publique**: est connue par tous les utilisateurs





La cryptographie et ses applications

La paire de clés est **complémentaire :**

- Message chiffré avec la **CLE PRIVEE**

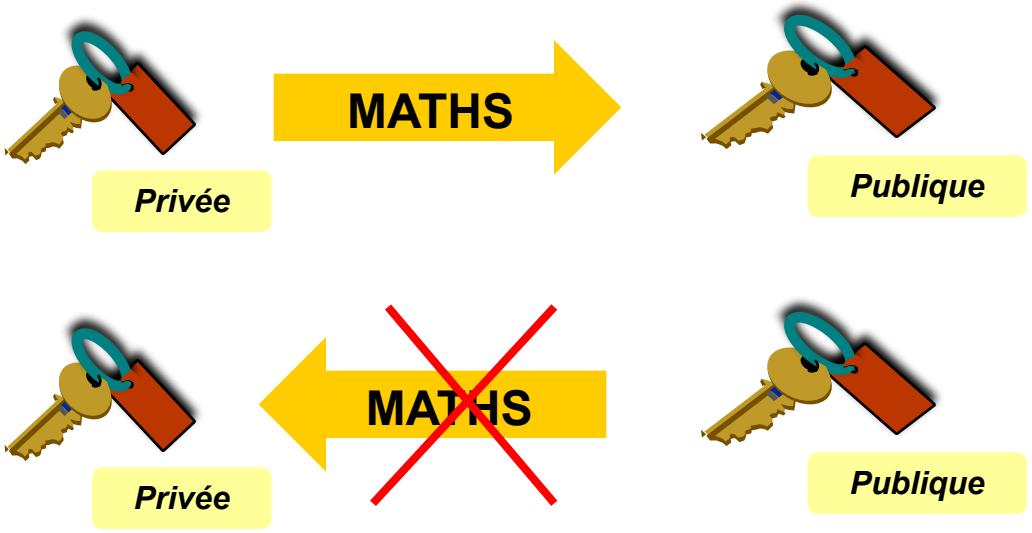
 Seule la clé publique est utilisée pour le déchiffrer

- Message chiffré avec la **CLE PUBLIQUE**

  Seule la clé privé est utilisée pour le déchiffrer

Relation mathématique entre les clés :

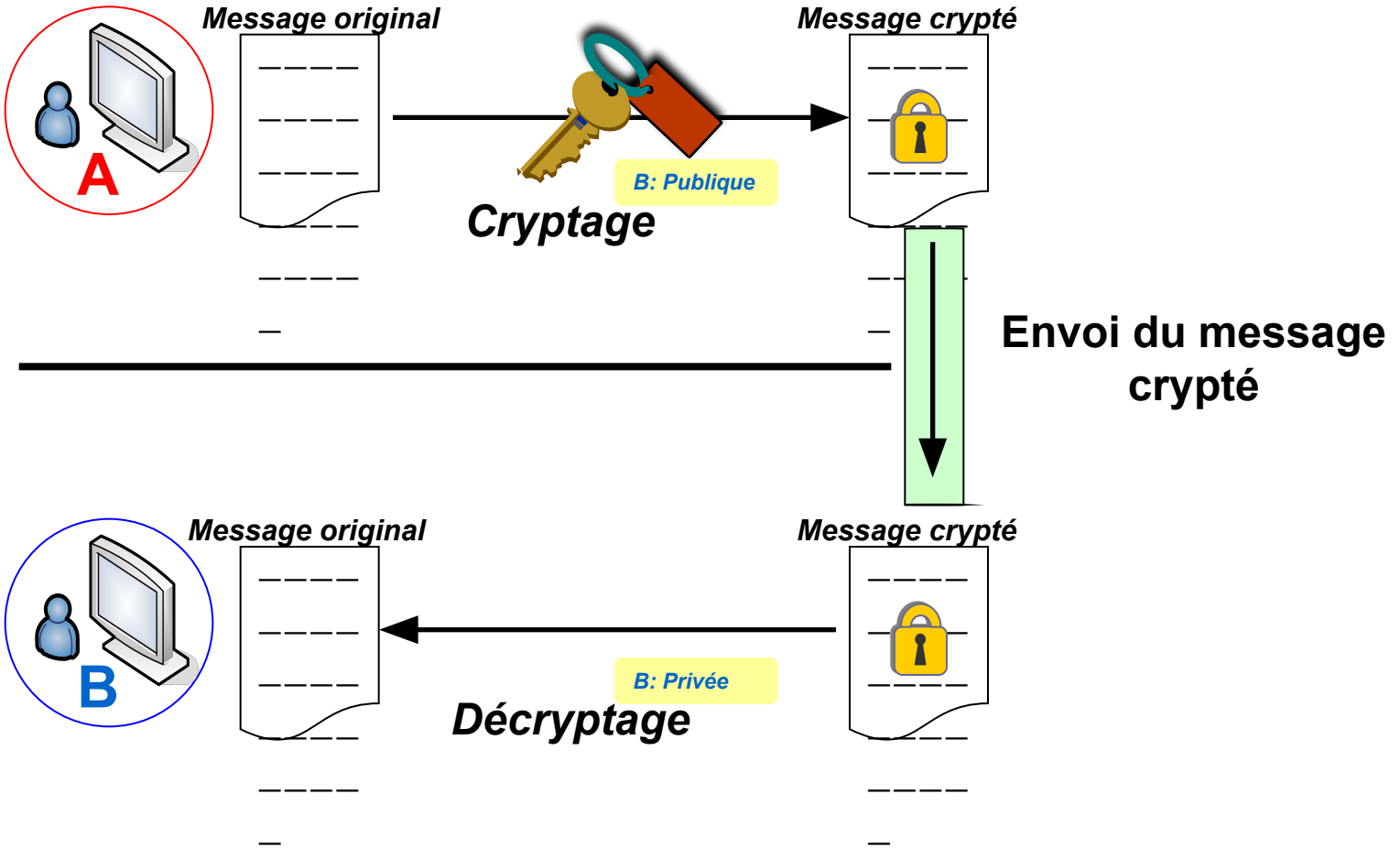
- La clé publique est générée mathématiquement à partir de la clé privé
- Par contre, obtenir la clé privé à partir de la clé publique est mathématiquement impossible



La cryptographie et ses applications

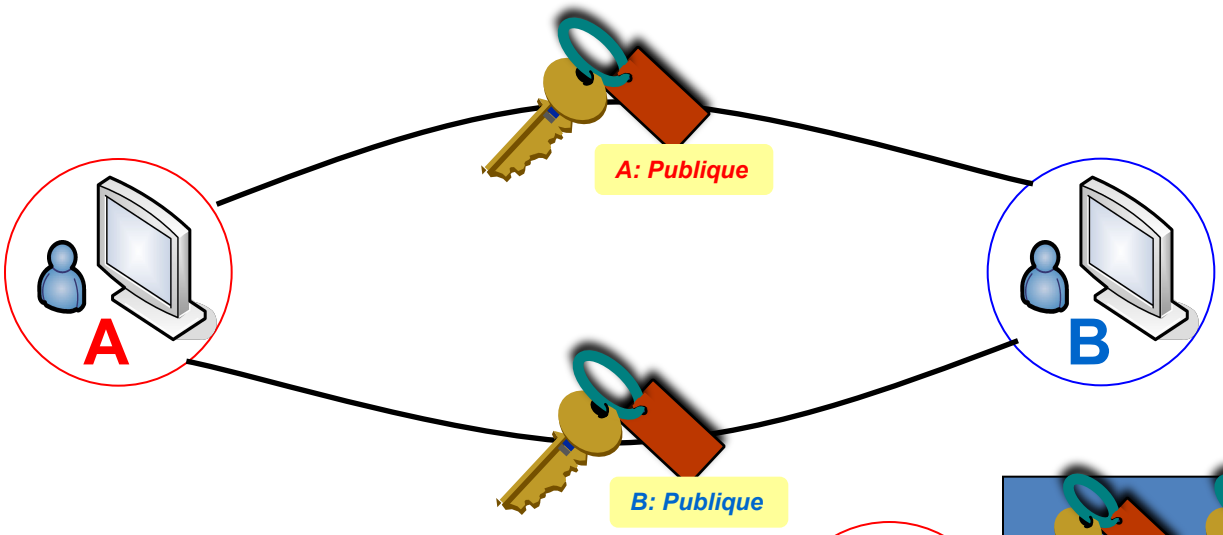
Cryptographie à clé asymétrique ou publique (iii)

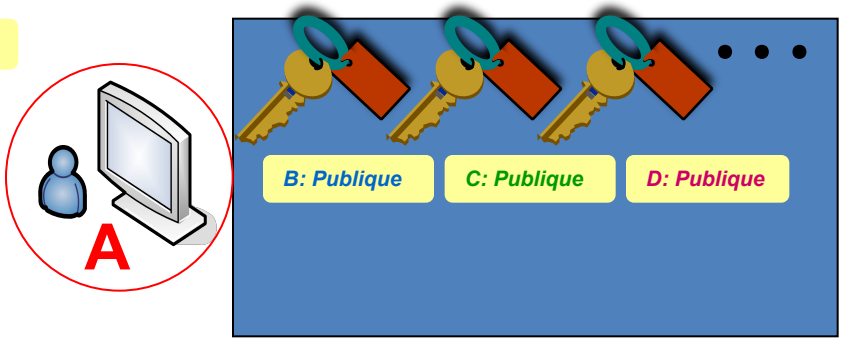
- Fonctionnement



La cryptographie et ses applications

Nécessité d'inter changer les clés publiques





- Collection des clés publiques des autres utilisateurs

La cryptographie et ses applications

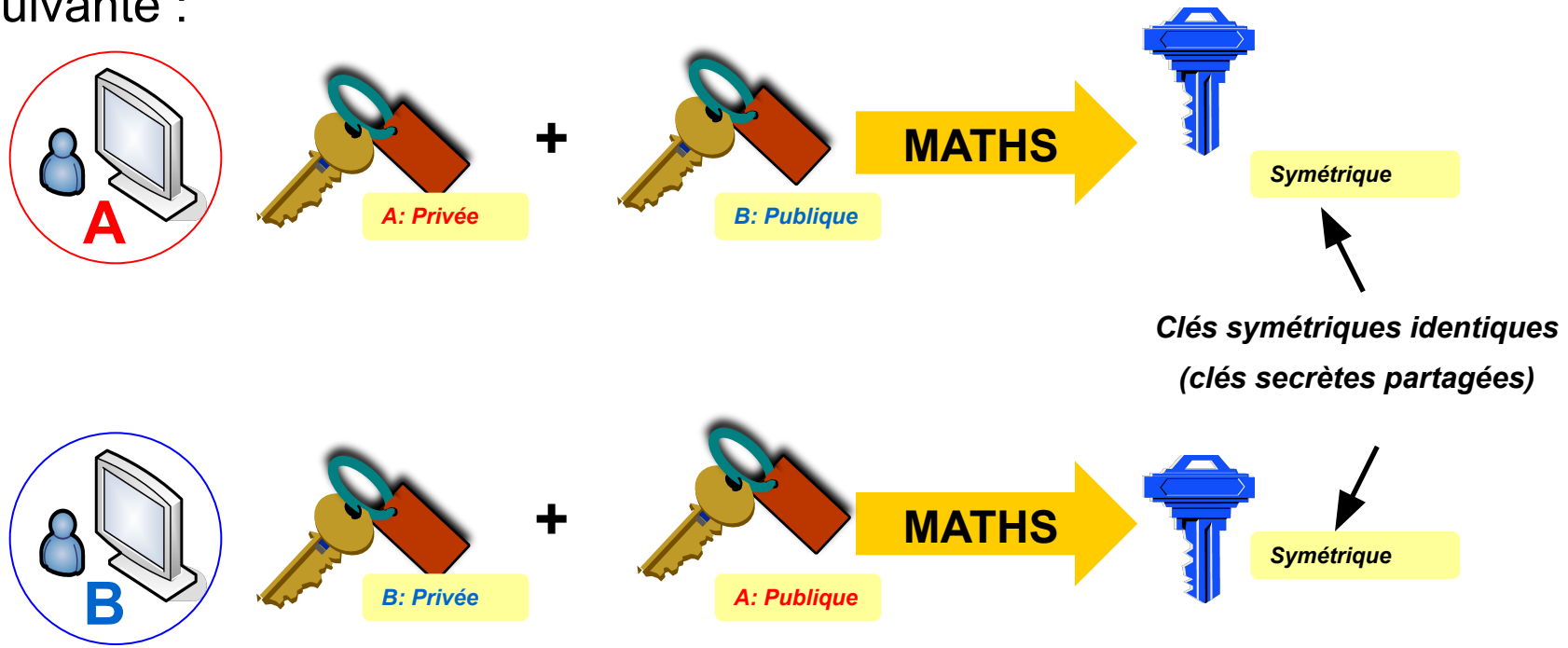
Cryptographie à clé asymétrique ou publique

- **Avantage**
  - Plus sécurisée
- **Inconvénients**
  - Processus de chiffrement lent
  - Peu recommandée pour les messages très longs
- **Exemples d'algorithmes à clé asymétrique**
  - RSA (Rivest, Shamir y Adleman)
- **Solution :** combiner le mécanisme à clé symétrique avec le mécanisme à clé asymétrique

La cryptographie et ses applications

Cryptographie à clé secrète partagée (i)

- Basée sur la clé symétrique
  - La clé privée ne s'inter change pas
  - Elle est générée par chacun des utilisateurs d'extrémité de la manière suivante :



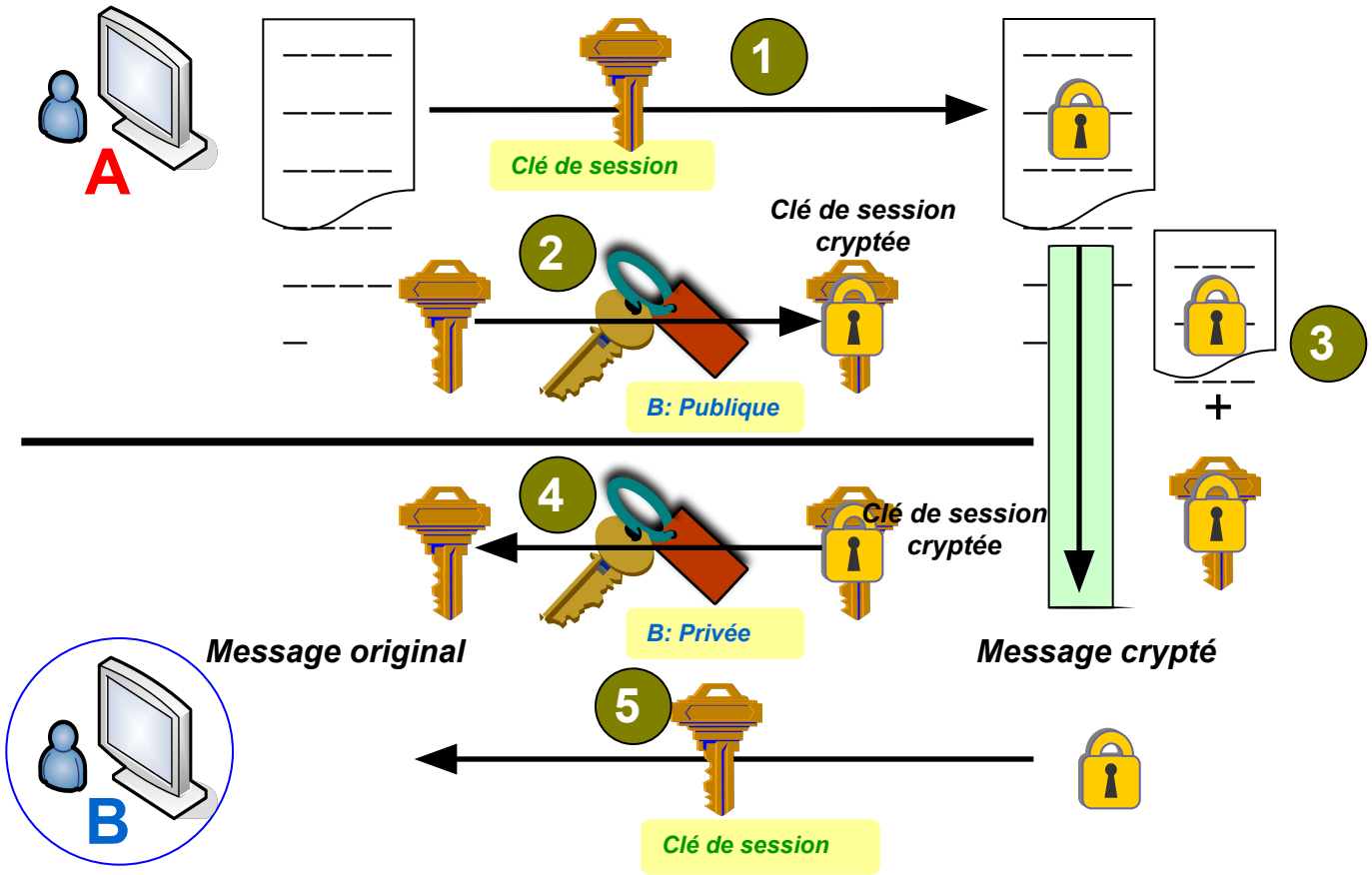
La cryptographie et ses applications

Cryptographie à clé secrète partagée (ii)

- **Avantage**
  - Rapide
  - Sécurisée : pas de clés inter changées
- **Inconvénients**
  - Utilisation de la même clé (toujours)
    - risque de reconnaître cette clé
- **Exemples d'algorithmes**
  - Diffie-Hellman

La cryptographie et ses applications

Cryptographie par clé de session (i)



La cryptographie et ses applications

Cryptographie par clé de session (ii)

- **Avantages**
  - Rapide
  - Sécurisée :
    - La clé de session est envoyée cryptée
    - Pour chaque session, on utilise une clé de session distincte
- **Exemples d'algorithmes**
  - SSL (*Secure Socket Layer*) : utilisé dans les serveurs Web sécurisés (https) ou dans les applications de e-commerce.