



République Algérienne Démocratique Et
Populaire

Ministère De L'enseignement Supérieur Et De
La Recherche Scientifique



Département Génie des systèmes
Filière IMSI : 4^{ème} année ingénieur

Sécurité des systèmes d'information

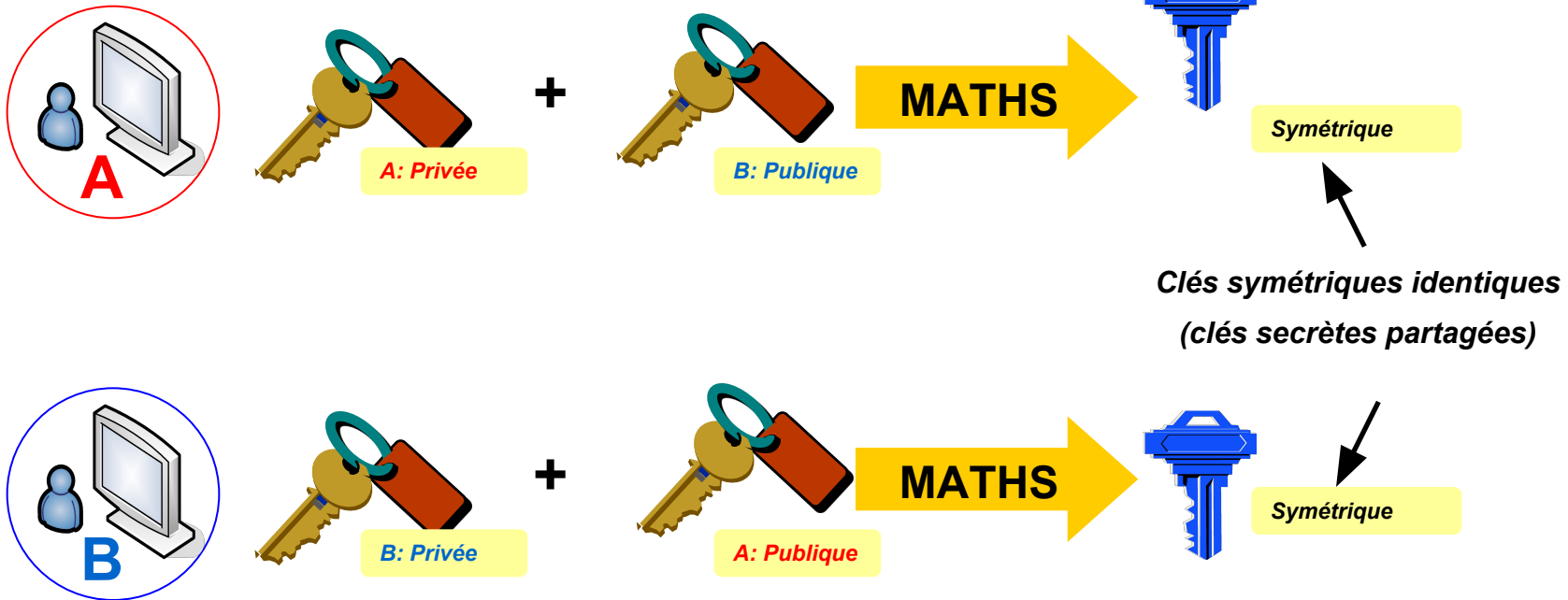
DR F.KABLI

kablifatima47@g
mail.com

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
- Sécurisé : pas de clés inter changées

- **Inconvénients**

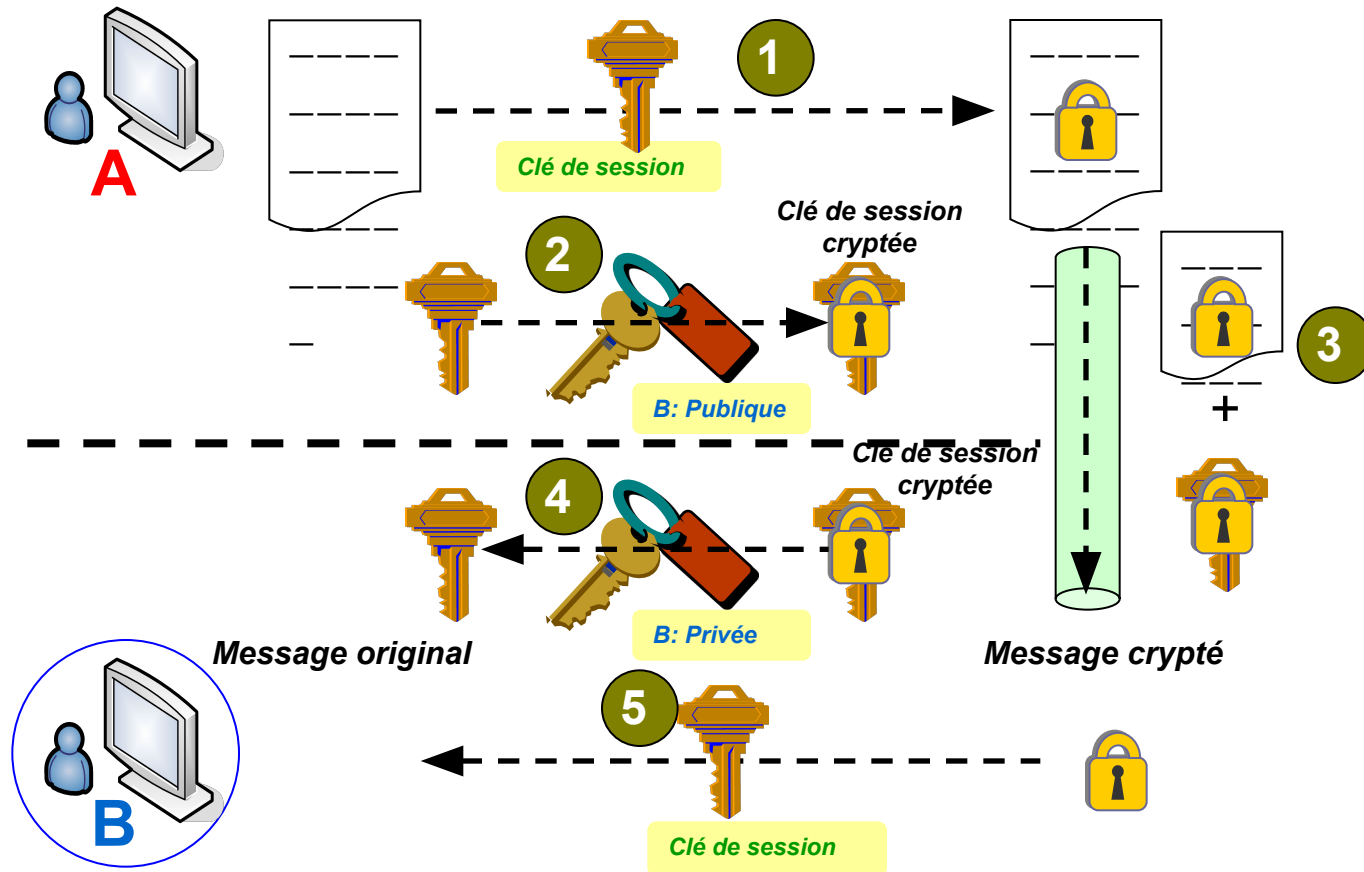
- Utilisation de la même clé
 - risque de reconnaître cette clé

- **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
- Sécurisé :
 - 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.

La cryptographie et ses applications

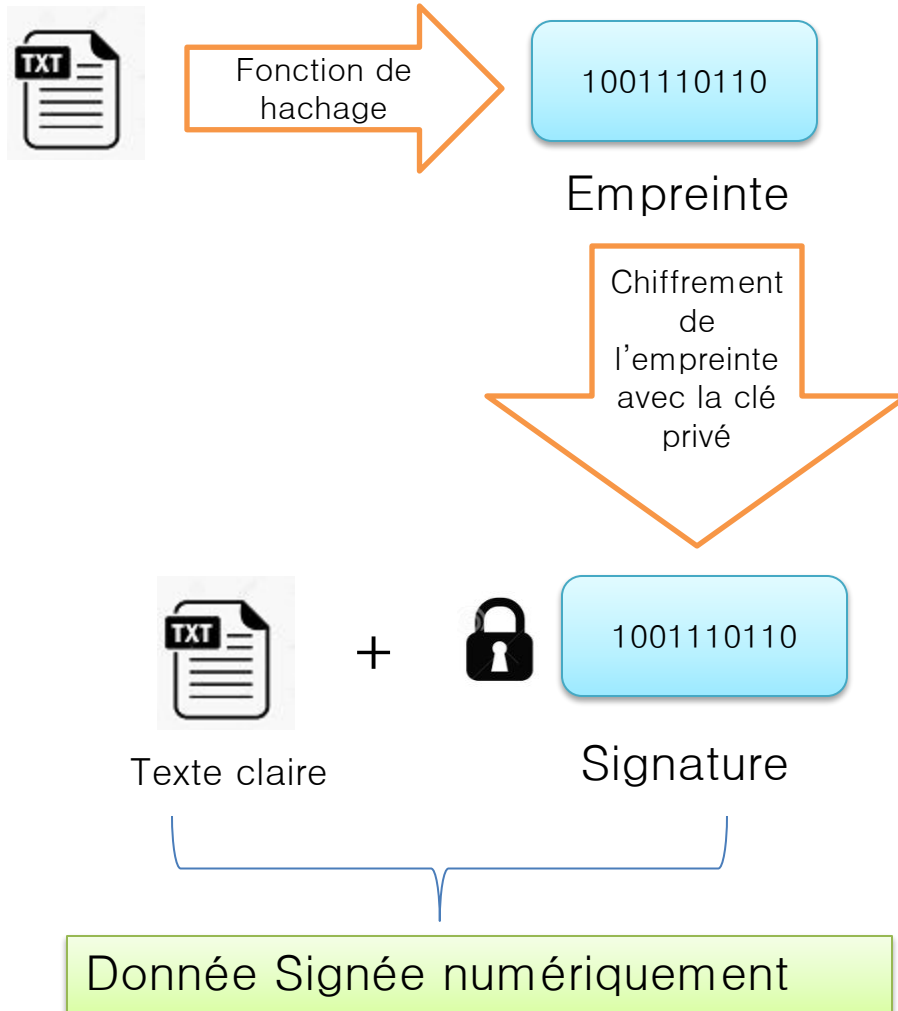
Fonction de hachage et Signature numérique :

A quoi ça sert une signature digitale ?

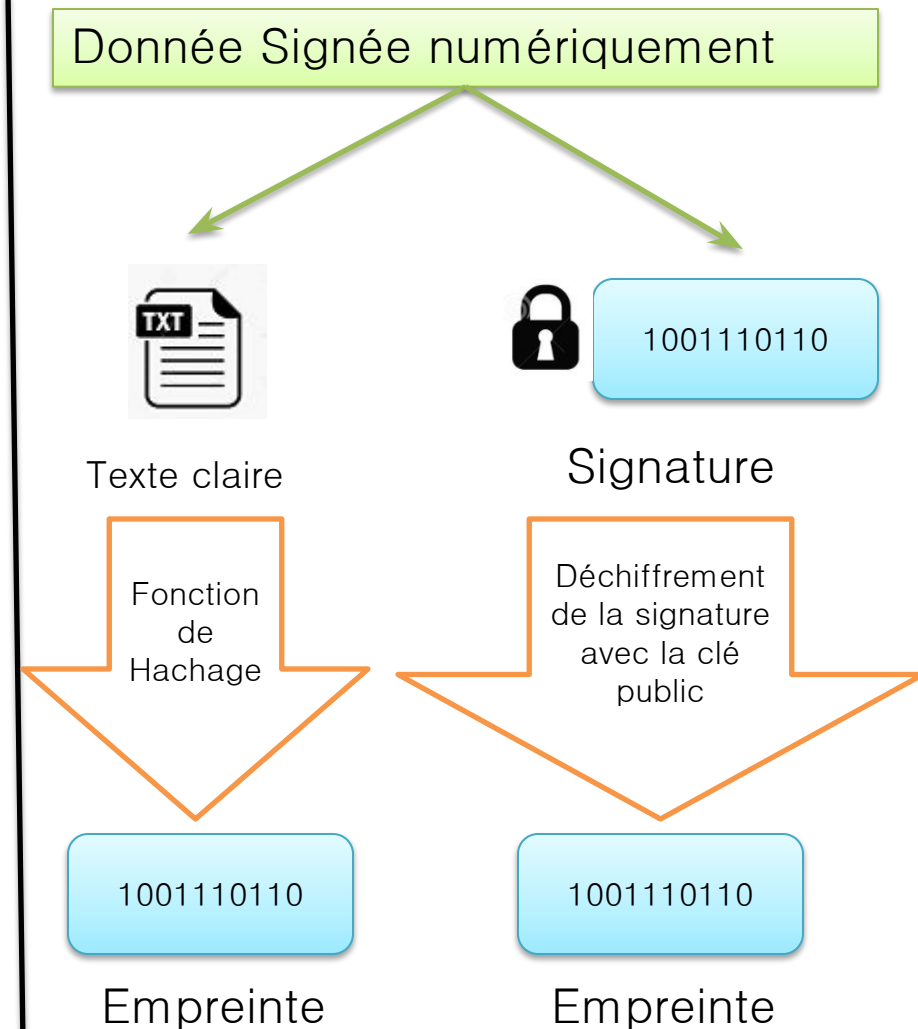
- Permet au récepteur de vérifier l'identité de l'expéditeur
 - **l'authentification**
- Permet au récepteur de vérifier que l'information n'a pas été modifiée pendant son acheminement
 - **l'intégrité**
- La signature est générée à partir de:
 - **La clé privée de l'expéditeur**
 - L'expéditeur doit disposer d'une paire de clés privée et publique
 - La clé privée est employée pour générer la signature digitale
 - Ceci garantit **l'authentification**
 - **Le message original**
 - Au message original, s'applique une fonction de hachage (hash)
 - Le message haché est crypté avec la clé privée formant la signature digitale de l'expéditeur
 - Ceci garantit **l'intégrité**

La cryptographie et ses applications

Signature

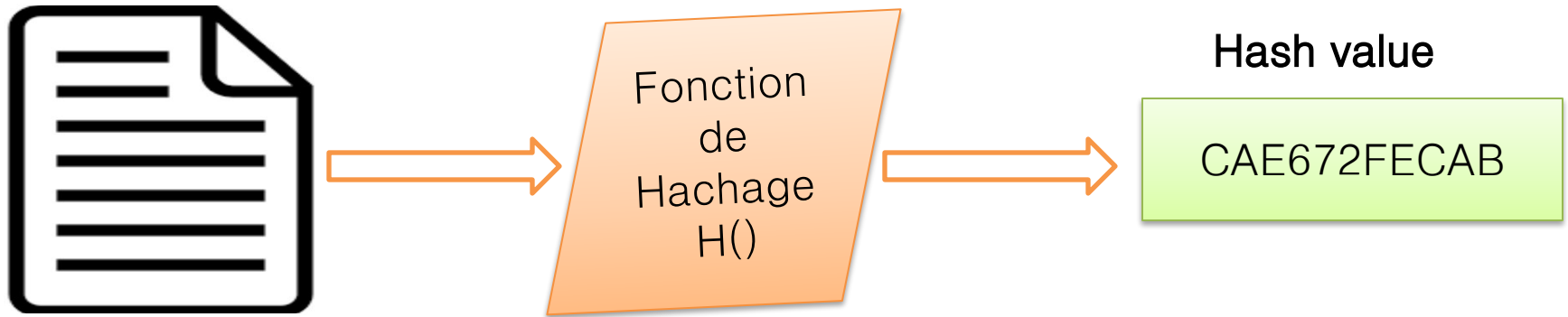


Vérification



La cryptographie et ses applications

Message



Conditions de base d'une fonction de hachage :

1. L'entrée peut être de dimension variable.
2. La sortie doit être fixe.
3. $H(m)$ doit être relativement facile à calculer.
4. $H(m)$ doit être une **fonction à sens unique**.
5. $H(m)$ doit être **sans collision**.

La cryptographie et ses applications

Exemples : Algorithmes de hachage

- MD5 (Message Digest 5).
- SHA1 (Secure Hash Algorithm 1)
- SHA 256–512
- SHA3 256–512
- Tiger
- Whirlpool

La cryptographie et ses applications

Préparation du message signé :

Un Emetteur (A) prépare le message signé, pour cela :

Il produit un résultat de hachage du message par la fonction de hachage choisie $H(M)$;

Il chiffre ce résultat grâce à la fonction de chiffrement C en utilisant sa clé privée K_{pr} . Le résultat obtenu est la signature du message : $S_M = C(K_{pr}, H(M))$

Il prépare le message signé en plaçant le message en clair M et la signature S_M dans un conteneur quelconque : $M_{signé} = (S_M, M)$.

(A) transmet $M_{signé}$, le message signé, à (B) par un canal non sécurisé

La cryptographie et ses applications

Réception du message signé :

(B) réceptionne le message signé, pour vérifier l'authenticité du message :

il produit un résultat de hachage du texte clair en utilisant la fonction de hachage : $H(M)$;

il déchiffre la signature en utilisant la fonction de déchiffrement D avec la clé publique K_{pb} soit : $D_{sm} = D(K_{pb}, S_M)$;

il compare D_{sm} avec $H(M)$.

Si D_{sm} et $H(M)$ sont égaux alors la signature est valide

$D_{sm} = D(K_{pb}, S_M) = D(K_{pb}, C(K_{pr}, H(M))) = H(M)$.