Chiffrement asymétrique//RSA
Christophe Viroulaud
Terminale NSI

Chiffrement asymétrique//RSA

Christophe Viroulaud

Terminale NSI

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

En s'inspirant de ces travaux, *Ron Rivest, Adi Shamir et Len Adleman* créent une méthode qui lève cette difficulté.

Problématique

Le chiffrement asymétrique de Diffie-Hellman permet d'échanger des clés via un canal non sûr mais ne gère pas les problèmes liés à l'authentification des interlocuteurs.

Comment authentifier avec certitude les participants ?

Problématique

Le chiffrement asymétrique de Diffie-Hellman permet d'échanger des clés via un canal non sûr mais ne gère pas les problèmes liés à l'authentification des interlocuteurs.

Comment authentifier avec certitude les participants ?

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Chiffrement RSA

- 1977 : Ron Rivest, Adi Shamir et Len Adleman.
- breveté en 1983 ; expiration du brevet en 2000.
- *fonctions à sens unique* (comme Diffie-Hellman)
- une paire de clés publique et privée.

Chiffrement RSA

- 1977 : Ron Rivest, Adi Shamir et Len Adleman.
- breveté en 1983 ; expiration du brevet en 2000.
- *fonctions à sens unique* (comme Diffie-Hellman)
- une paire de clés publique et privée.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

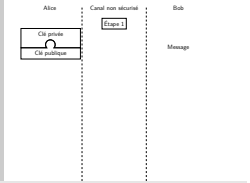
À retenir
$K_{priv}(K_{pub}(m)) = K_{pub}(K_{priv}(m)) = m$

principe de Diffie-Hellman était différent : $f(f(x,y),z) = f(f(x,z),y)$

À retenir

$$K_{priv}(K_{pub}(m)) = K_{pub}(K_{priv}(m)) = m$$

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



Alice | Canal non sécurisé | Bob

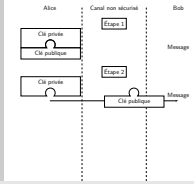
Étape 1

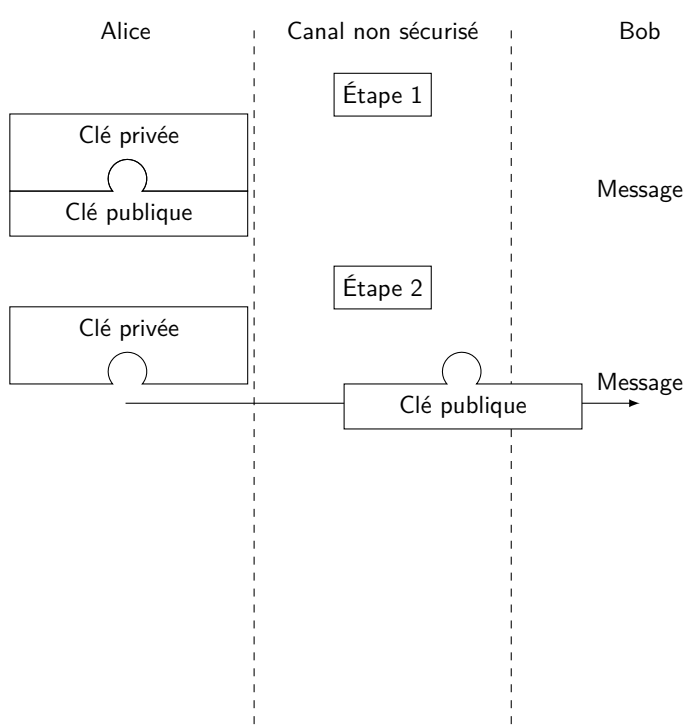
Clé privée

Clé publique

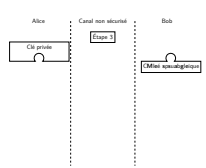
Message

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



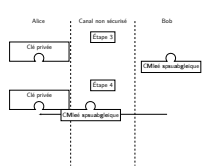


Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



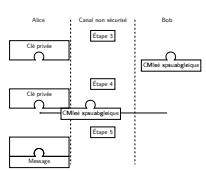
Alice
Canal non sécurisé
Bob
Étape 3
Clé privée
CMleé spsuabgleique

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



Alice
Canal non sécurisé
Bob
Étape 3
Clé privée
CMleé spsuabgleique
Étape 4
Clé privée
CMleé spsuabgleique

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



Alice
Canal non sécurisé
Bob
Étape 3
Clé privée
CMleé spsuabgleique
Étape 4
Clé privée
CMleé spsuabgleique
Étape 5
Message

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Mathématiquement, la fonction respecte les règles suivantes :
- Il est impossible de deviner la clé privée en connaissant la clé publique.
- Il est impossible de deviner le message avec une seule des deux clés.

Mathématiquement, la fonction respecte les règles suivantes :

- Il est impossible de deviner la clé privée en connaissant la clé publique.
- Il est impossible de deviner le message avec une seule des deux clés.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

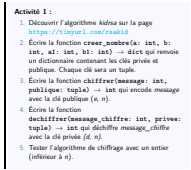
kid RSA

La création des clés suit un algorithme mathématique complexe. L'université de Rhode Island a produit une version simplifiée (à utilisation pédagogique) pour simuler le protocole.

kid RSA

La création des clés suit un algorithme mathématique complexe. L'université de Rhode Island a produit une version simplifiée (à utilisation pédagogique) pour simuler le protocole.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https


Activité 1 :

1. Découvrir l'algorithme *kidrsa* sur la page https://tinyurl.com/rsakid
2. Écrire la fonction `creer_nombre(a: int, b: int, a1: int, b1: int)` → `dict` qui renvoie un dictionnaire contenant les clés privée et publique. Chaque clé sera un tuple.
3. Écrire la fonction `chiffrer(message: int, publique: tuple)` → `int` qui encode *message* avec la clé publique (*e, n*).
4. Écrire la fonction `dechiffrer(message_chiffre: int, privee: tuple)` → `int` qui déchiffre *message_chiffre* avec la clé privée *(d, n)*.
5. Tester l'algorithme de chiffrage avec un entier (inférieur à n).

Activité 1 :

1. Découvrir l'algorithme *kidrsa* sur la page https://tinyurl.com/rsakid
2. Écrire la fonction **`creer_nombre(a: int, b: int, a1: int, b1: int)`** → **`dict`** qui renvoie un dictionnaire contenant les clés privée et publique. Chaque clé sera un tuple.
3. Écrire la fonction **`chiffrer(message: int, publique: tuple)`** → **`int`** qui encode *message* avec la clé publique (*e, n*).
4. Écrire la fonction **`dechiffrer(message_chiffre: int, privee: tuple)`** → **`int`** qui déchiffre *message_chiffre* avec la clé privée *(d, n)*.
5. Tester l'algorithme de chiffrage avec un entier (inférieur à n).

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Correction

Code 1 – Alice crée ses clés

Correction

```
1  def creer_nombre(a: int, b: int, a1: int, b1: int) -> dict
       :
2      """
3      crée un couple clé privée/publique
4      Returns:
5          dict: {"publique" : (e, n), "privee":(d, n)}
6      """
7      M = a*b-1
8      e = a1*M+a
9      d = b1*M+b
10     n = (e*d)//M
11     return {"publique": (e, n), "privee": (d, n)}
```

Code 1 – Alice crée ses clés

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Correction

```
def chiffrer(message: int, publique: tuple) -> int:
    """
    Args:
        message (int)
        publique (tuple): (e, n)

    Returns:
        int: message chiffré
    """
    return (publique[0]*message) % publique[1]
```

Code 2 – Bob chiffre son message avec la clé publiqe d'Alice

Correction

```
def chiffrer(message: int, publique: tuple) -> int:
    """
    Args:
        message (int)
        publique (tuple): (e, n)

    Returns:
        int: message chiffré
    """
    return (publique[0]*message) % publique[1]
```

Code 2 – Bob chiffre son message avec la clé publiqe d'Alice

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Correction

Code 3 – Alice déchiffre le message de Bob avec sa clé privée

Correction

```
1  def dechiffrer(message_secret: int, privee: tuple)
       -> int:
2      """
3      Args:
4          message_secret (int)
5          privee (tuple): (d, n)
6
7      Returns:
8          int: message déchiffré
9      """
10     return (privee[0]*message_secret) % privee[1]
```

Code 3 – Alice déchiffre le message de Bob avec sa clé privée

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

Pour l'instant, l'algorithme RSA ne fait rien de plus que celui de Diffie-Hellman. Nous n'avons toujours pas réglé le problème de l'authentification.

Pour l'instant, l'algorithme RSA ne fait rien de plus que celui de Diffie-Hellman. Nous n'avons toujours pas réglé le problème de l'authentification.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

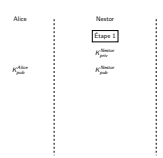
Authentification

Il faut qu'un **tiers de confiance** (Nestor) intervienne.

Authentification

Il faut qu'un **tiers de confiance** (Nestor) intervienne.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



Le tiers de confiance crée un couple privé/publique ; On ne s'intéresse qu'à la clé publique de Alice = celle qui va être transmise.

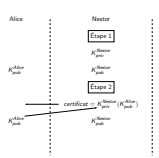
Alice
Nestor
Étape 1

K_{priv}^{Nestor}

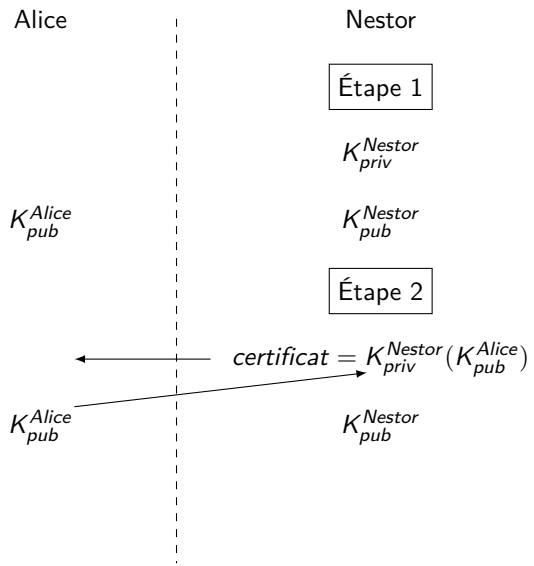
K_{pub}^{Alice}

K_{pub}^{Nestor}

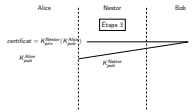
Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



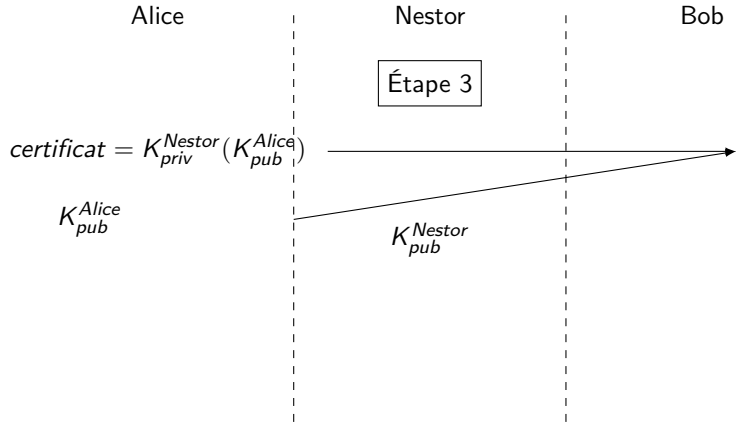
Nestor chiffre la clé publique d'Alice avec sa clé privée → certificat.



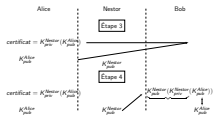
Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



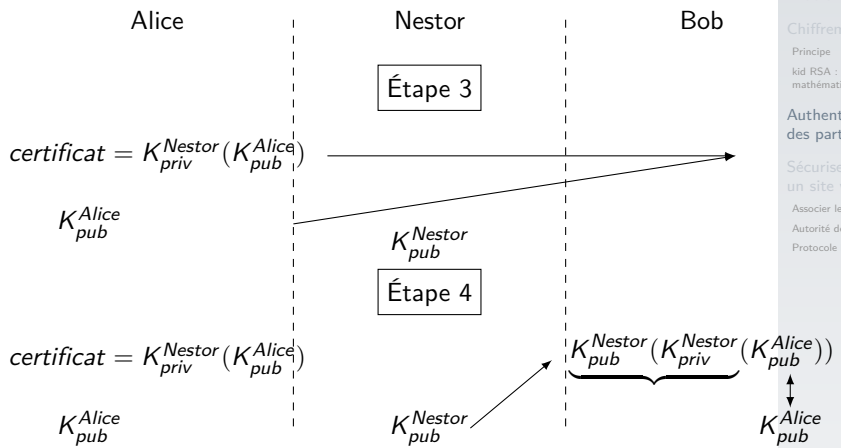
Alice envoie le certificat et sa clé publique en clair



Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



1. À l'aide de la clé publique de Nestor, Bob déchiffre la clé publique d'Alice (le certificat) et la compare à la clé publique fournie en clair.
2. pas possible avec Diffie car $f(f(x,y),z) = f(f(x,z),y)$ ← non réversibilité des pots de peinture



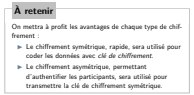
Sécuriser l'accès à un site web

L'algorithme RSA permet de sécuriser les données mais également d'authentifier les participants. Il semble être le candidat idéal pour effectuer toutes ces tâches. Cependant, il est très coûteux en temps de calcul.

Sécuriser l'accès à un site web

L'algorithme RSA permet de sécuriser les données mais également d'authentifier les participants. Il semble être le candidat idéal pour effectuer toutes ces tâches. Cependant, il est très coûteux en temps de calcul.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https



RSA = authentification ; symétrique ou Diffie-Hellman pour chiffrement

À retenir

On mettra à profit les avantages de chaque type de chiffrement :

- Le chiffrement symétrique, rapide, sera utilisé pour coder les données avec *clé de chiffrement*.
- Le chiffrement asymétrique, permettant d'authentifier les participants, sera utilisé pour transmettre la clé de chiffrement symétrique.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

règles très strictes, audités régulièrement

Autorité de certification

Une autorité de certification peut être :
- un état,
- une entreprise spécialisée,
- une association à but non lucratif (Let's Encrypt).

Autorité de certification

Une autorité de certification peut être :

- un état,
- une entreprise spécialisée,
- une association à but non lucratif (Let's Encrypt).

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

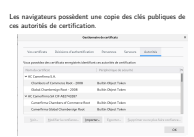


FIGURE – Firefox/préférences/vie privée et sécurité/certificats

Les navigateurs possèdent une copie des clés publiques de ces autorités de certification.

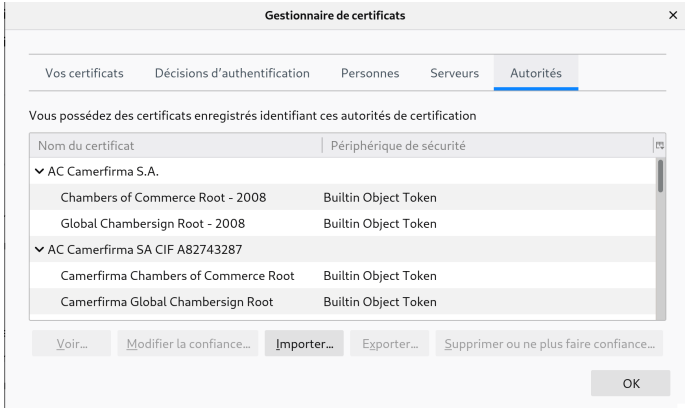


FIGURE – Firefox/préférences/vie privée et sécurité/certificats

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

En pratique, elle ne signe pas la clé publique entière du site (2048 ou 4096 bits) mais sa somme de contrôle calculée (256 bits) par une fonction de hachage (souvent sha256).

En pratique, elle ne signe pas la clé publique entière du site (2048 ou 4096 bits) mais sa somme de contrôle calculée (256 bits) par une fonction de hachage (souvent sha256).

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

1. SSL (Secure Sockets Layer) = ancêtre TLS (sécurité de la couche de transport)

https
Le protocole *https* ajoute une couche *TLS (Transport Layer Security)* au protocole *http* existant.

https

Le protocole *https* ajoute une couche *TLS (Transport Layer Security)* au protocole *http* existant.

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

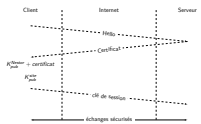


FIGURE – protocole https

1. Hello : navigateur envoie intention de se connecter et infos techniques (algo de chiffrement qu'il peut utiliser)
2. serveur envoie certificat (sa clé publique signée par la clé privée d'une autorité)
3. client utilise la clé publique de l'autorité pour déchiffrer le certificat et compare le résultat avec la clé publique du site
4. le client et le serveur se mette d'accord sur protocole d'échange (symétrique, Diffie-Hellman) : le client peut communiquer sa clé de manière sécurisée grâce à la clé publique du site → clé de session

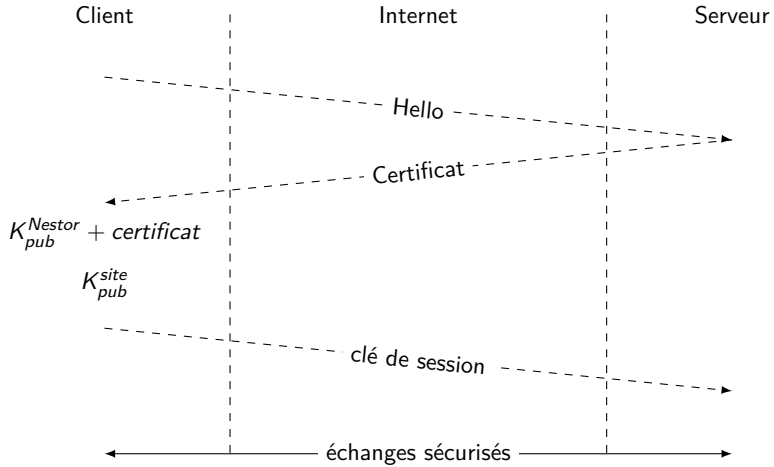


FIGURE – protocole https

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

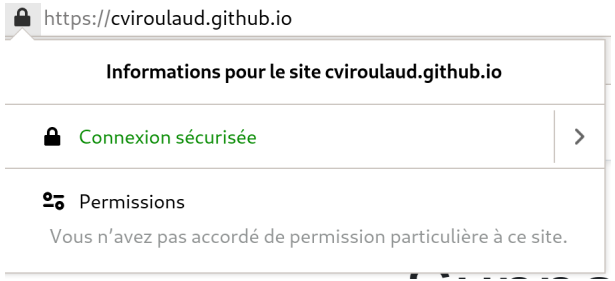


FIGURE – Le cadenas atteste des échanges sécurisés

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
kid RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https

1. plutôt que SSL Secure Sockets Layer
2. Diffie-Hellman pour échanger clé de session

Détails techniques
Connexion chiffrée (clés TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bits, TLS 1.2)
La page actuellement affichée a été chiffrée avant d'avoir été envoyée sur Internet.

Figure – Exemple

- Protocole TLS (Transport Layer Security)
- ECDHE : Elliptic Curve Diffie-Hellman Ephemeral pour l'échange de clé de session
- RSA pour l'authentification
- Le chiffrement symétrique est assuré par AES128 (Advanced Encryption Standard 128 bits)

Chiffrement asymétrique//RSA
Problématique
Chiffrement RSA
Principe
Clé RSA : formalisme mathématique
Authentification des participants
Sécuriser l'accès à un site web
Associer les protocoles
Autorité de certification
Protocole https