

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

Christophe Viroulaud

Terminale NSI

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

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

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

- ▶ 1997 : 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.

À retenir

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

Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

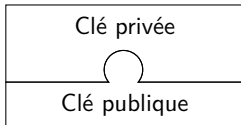
Autorité de certification

Protocole https

Alice

Canal non sécurisé

Bob



Étape 1

Message

Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

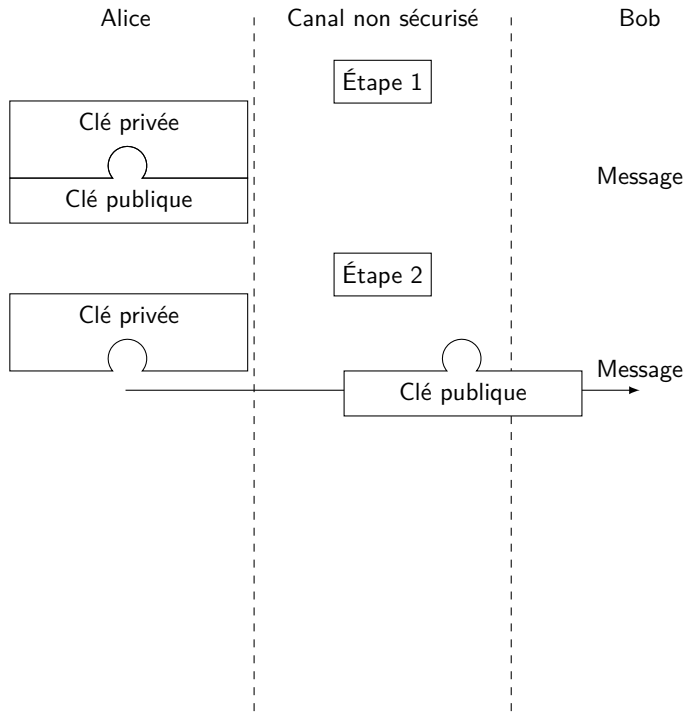
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

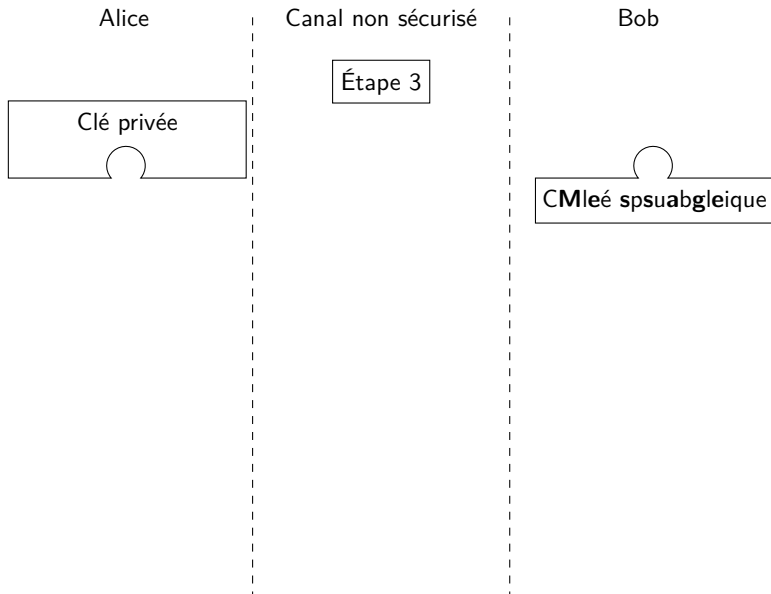
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

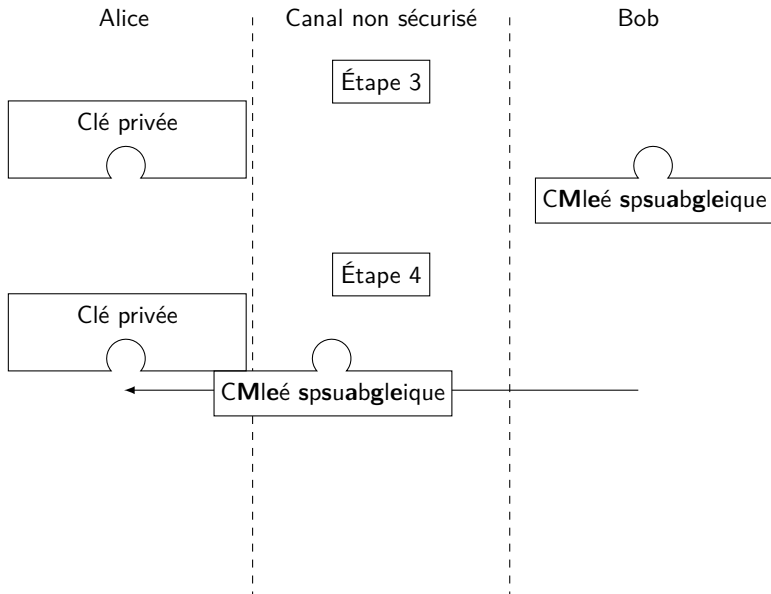
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

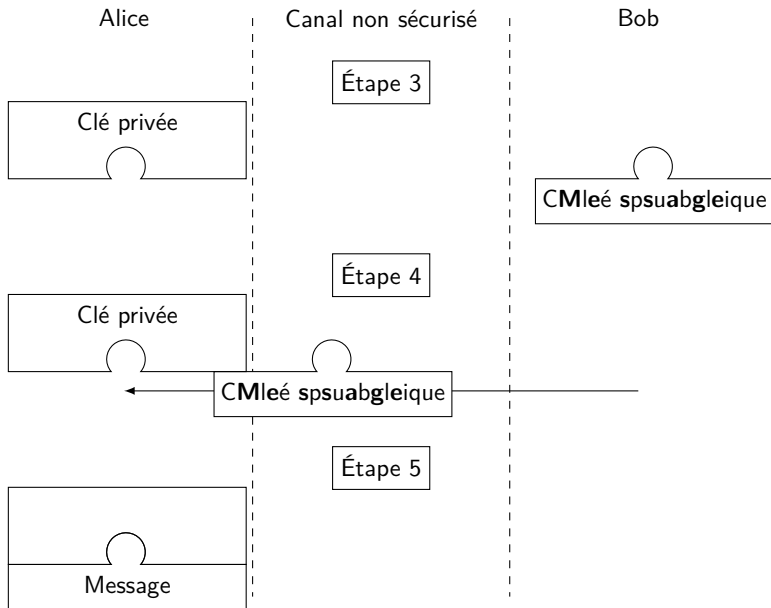
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



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.

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

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.

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: int) → int` qui déchiffre *message_chiffre* avec la clé privée (d, n) .
5. Tester l'algorithme de chiffrage avec un entier (inférieur à n).

Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématiqueAuthentification
des participantsSécuriser 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.

Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

Authentication
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https

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

Alice

K_{pub}^{Alice}

Nestor

Étape 1

K_{priv}^{Nestor}

K_{pub}^{Nestor}

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

Nestor

Étape 1

K_{priv}^{Nestor}

K_{pub}^{Nestor}

Étape 2

K_{pub}^{Alice}

K_{pub}^{Alice}

$certificat = K_{priv}^{Nestor}(K_{pub}^{Alice})$

K_{pub}^{Nestor}

Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

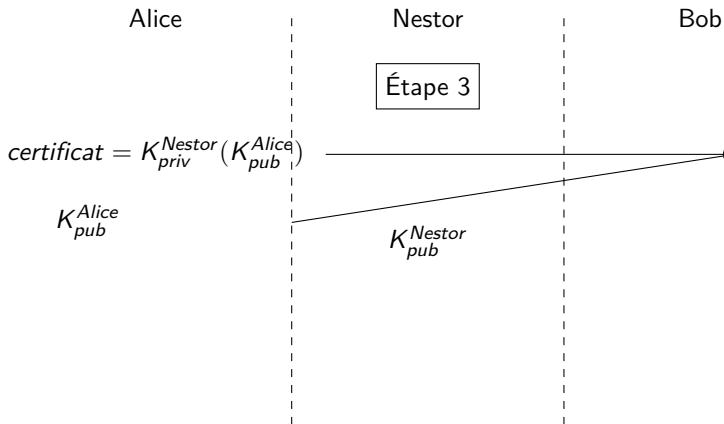
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



Problématique

Chiffrement RSA

Principe

kid RSA : formalisme
mathématique

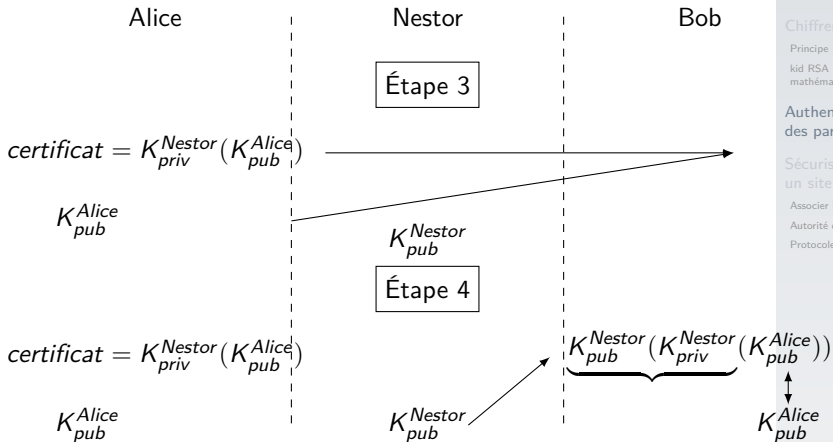
Authentification
des participants

Sécuriser l'accès à
un site web

Associer les protocoles

Autorité de certification

Protocole https



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

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

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.

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.

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

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

Une autorité de certification peut être :

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

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

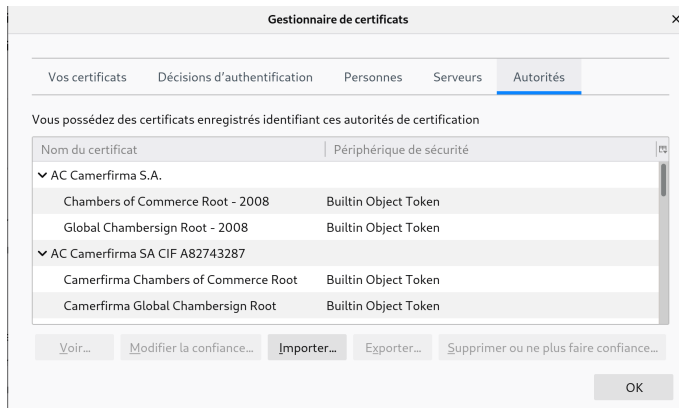


FIGURE – Firefox/préférences/vie privée et sécurité/certificats

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).

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

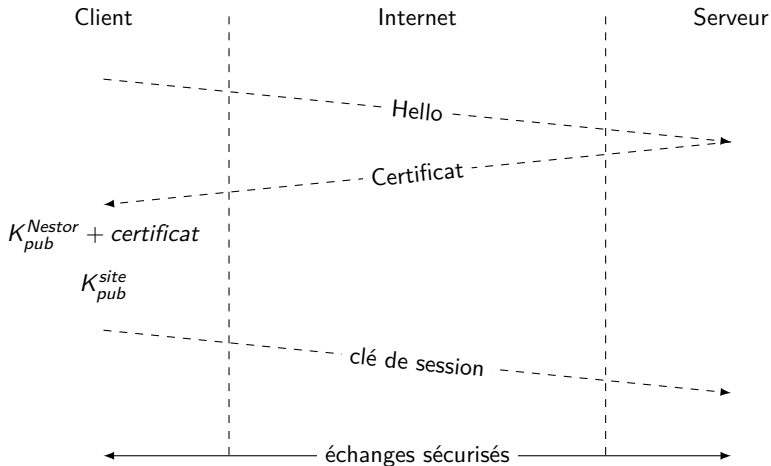


FIGURE – protocole https

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

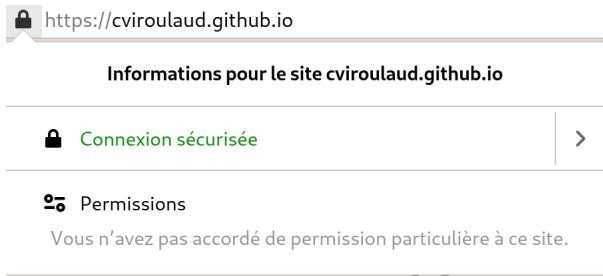


FIGURE – Le cadenas atteste des échanges sécurisés

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

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)