Chiffrement asymétrique RSA

Christophe Viroulaud

Terminale - NSI

Archi 23

Chiffrement RSA

Principe

kid RSA : formalism

Authentification des participants

Sécuriser l'accès à un site web

Chiffrement RSA

Description
kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification

Protocole https

Informations techniques

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.

Chiffrement RSA

Description
kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles
Autorité de certification
Protocole https
Informations techniques

Comment authentifier avec certitude les participants?

Sommaire

Chiffrement asymétrique RSA

Chiffrement RSA

1. Chiffrement RSA

- 1.3 kid RSA : formalisme mathématique

Chiffrement RSA - Principe

Chiffrement asymétrique RSA

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

À retenir

Une fonction à sens unique est une fonction mathématique facile à calculer mais pour laquelle il est très compliqué de retrouver l'antécédent d'une image.

Chiffrement RSA

Principe

Description

Authentification les participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification Protocole https Informations techniques

Chiffrement RSA

Principe

kid RSA : formalisme

Authentification les participants

Sécuriser l'accès à un site web

Autorité de certification
Protocole https

À retenir

Le principe du protocole RSA s'inspire de la méthode de Diffie-Hellman :

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

Sommaire

Chiffrement asymétrique RSA

Description

1. Chiffrement RSA

- 1.2 Description
- 1.3 kid RSA : formalisme mathématique

Description

Alice

Canal non sécurisé

Bob

Clé privée

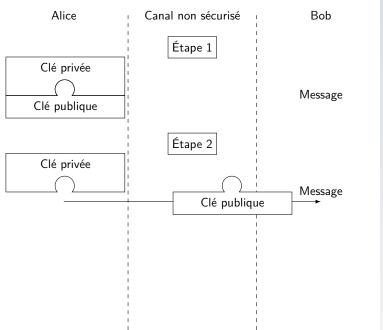
Clé publique

Étape 1

Message

Chiffrement asymétrique **RSA**

Description



Chiffrement RSA

Principe

Description

kid RSA : formalisme

uthentification

Sécuriser l'accès à

Alice

Clé privée

Canal non sécurisé

Étape 3

Bob

CMleé spsuabgleique

, D

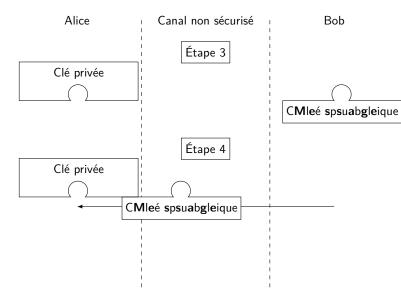
Principe

Description

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web



Chiffrement RSA

Principe

Description

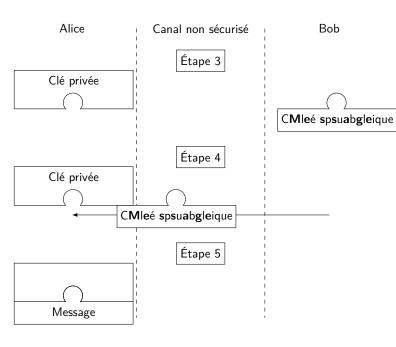
kid RSA : formalisme

Authentification les participants

Sécuriser l'accès à un site web



Description



Description

À retenir

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.

Sommaire

Chiffrement asymétrique RSA

kid RSA · formalisme mathématique

- 1. Chiffrement RSA

- 1.3 kid RSA : formalisme mathématique

kid RSA

Chiffrement asymétrique RSA

Chiffrement RSA

Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles

Protocole https

ormations techniq

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 : formalisme

mathématique

RSA

1. Découvrir l'algorithme *kidrsa* sur la page https://tinyurl.com/rsakid

Activité 1:

- 2. Écrire la fonction creer nombre(a: int, b: int, a1: int, b1: int) \rightarrow 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) \rightarrow int qui encode message avec la clé publique (e, n).
- 4. Écrire la fonction dechiffrer(message_chiffre: int, privee: tuple) \rightarrow int qui déchiffre message chiffre avec la clé privée (d, n).
- 5. Tester l'algorithme de chiffrage avec un entier (inférieur à n). Le message à chiffrer sera l'entier 538.

1

6

.0

Chiffrement RSA

```
def creer_nombre(a: int, b: int, a1: int, b1: int) -> dict:
                                                                  formalisme
    11 11 11
    crée un couple clé privée/publique
    Returns:
        dict: {"publique": (e, n), "privee":(d, n)}
    11 11 11
    M = a*b-1
    e = a1*M+a
    d = b1*M+b
    n = (e*d)//M
    return {"publique": (e, n), "privee": (d, n)}
```

Code 1 – Alice crée ses clés

```
def chiffrer(message: int, publique: tuple) -> int:
       11 11 11
       Args:
           message (int)
            publique (tuple): (e, n)
6
       Returns:
            int: message chiffré
       11 11 11
       return (publique[0]*message) % publique[1]
0
```

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

Chiffrement RSA

kid RSA : formalisme mathématique

Authentification les participants

Sécuriser l'accès à un site web

Associer les protocoles
Autorité de certification
Protocole https
Informations techniques

11 11 11

6

.0

```
def dechiffrer(message_secret: int, privee: tuple)

-> int:
    """

Args:
    message_secret (int)
    privee (tuple): (d, n)

Returns:
    int: message déchiffré
```

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

return (privee[0]*message secret) % privee[1]

```
kid RSA · formalisme
mathématique
```

```
>>> cles = creer_nombre(9, 11, 5, 8)
  >>> cles
   {'publique': (499, 4048), 'privee': (795, 4048)}
4
  >>> s = chiffrer(538, cles["publique"])
5
  >>> s
   1294
   >>> e = dechiffrer(s, cles["privee"])
9
  >>> e
0
  538
1
```

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. Le problème de l'authentification n'est toujours pas résolu.

Sommaire

Chiffrement asymétrique **RSA**

Authentification des participants

- 2. Authentification des participants

Authentification des participants

Chiffrement asymétrique RSA

Chiffrement RSA

Description kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification

Protocole https

À retenir

Pour certifier l'identité des individus, il faut qu'un **tiers de confiance** (Nestor) intervienne.

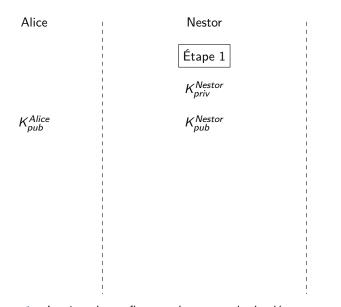


FIGURE 1 – Le tiers de confiance crée un couple de clés privée/publique.

Chiffrement RSA

Principe
Description
kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à

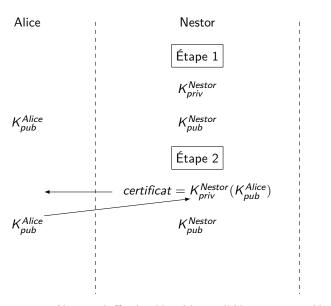


FIGURE 2 – Nestor chiffre la clé publique d'Alice avec sa clé privée : il crée un **certificat**.

Chiffrement RSA

rincipe Description

Authentification des participants

Sécuriser l'accès à un site web

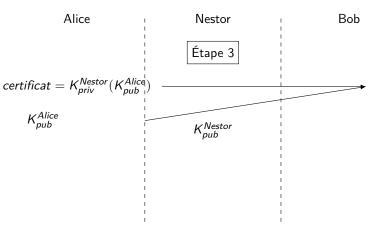


FIGURE 3 – Alice envoie le certificat et sa clé publique en clair.

Chiffrement RSA

Principe

Description kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Autorité de certification Protocole https

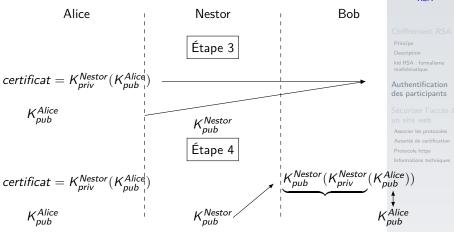


FIGURE 4 – À l'aide de la clé publique de Nestor, Bob déchiffre la clé publique d'Alice (le certificat) et la compare à la clé publique fournie en clair.

Sommaire

- Chiffrement asymétrique RSA

- Sécuriser l'accès à un site web

- 3. Sécuriser l'accès à un site web

- 3.4 Informations techniques

Sécuriser l'accès à un site web

Chiffrement asymétrique RSA

Chiffrement RSA

Description
kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à

Associer les protocoles
Autorité de certification
Protocole https

L'algorithme RSA:

avantage : permet de sécuriser les données

Sécuriser l'accès à un site web

Chiffrement asymétrique RSA

Chiffrement RSA

Description
kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à

Associer les protocoles

Associer les protocoles

Autorité de certification

Protocole https

L'algorithme RSA:

avantage : permet de sécuriser les données

avantage : permet d'authentifier les participants.

Sécuriser l'accès à un site web

Chiffrement asymétrique RSA

Chiffrement RSA

Description
kid RSA : formalisme

des participants

Sécuriser l'accès à

Associer les protocoles Autorité de certification

Protocole https

L'algorithme RSA :

- avantage : permet de sécuriser les données
- **avantage**: permet d'authentifier les participants.
- inconvénient : 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 chiffrer les données avec une clé de chiffrement symétrique.
- ► Le chiffrement asymétrique, permettant d'authentifier les participants, sera utilisé pour transmettre la clé de chiffrement symétrique.

Chiffrement RSA

Principe

Description

mathématique

des participants

Sécuriser l'accès à

Associer les protocoles

Autorité de certification Protocole https

Sommaire

- Chiffrement asymétrique RSA
- Chiffrement RSA
- Description

 kid RSA : formalisme
- Authentification des participants
- Sécuriser l'accès à
- Associer les protocoles
- Autorité de certification
- Protocole https Informations techniques

- 1. Chiffrement RSA
- 2. Authentification des participants
- 3. Sécuriser l'accès à un site web
- 3.1 Associer les protocoles
- 3.2 Autorité de certification
- 3.3 Protocole http:
- 3.4 Informations techniques

Autorité de certification

Chiffrement asymétrique RSA

Chiffrement RSA

Description
kid RSA : formalisme

des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

rotocole https

rotocole https

nformations techniques

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.

Gestionnaire de certificats					
Vos certificats	Décisions d'authentification	Personnes	Serveurs	Autorités	
Vous possédez des	certificats enregistrés identifia	nt ces autorités de c	ertification		
Nom du certificat		Périphérique de sécurité			
✓ AC Camerfirma	5.A.				
Chambers of Commerce Root - 2008		Builtin Object Token			
Global Chambersign Root - 2008		Builtin Object Token			
✓ AC Camerfirma	5A CIF A82743287				
Camerfirma C	hambers of Commerce Root	Builtin Object To	ken		
Camerfirma G	lobal Chambersign Root	Builtin Object To	ken		
<u>V</u> oir <u>M</u>	odifier la confiance <u>I</u> mpor	rter Exporter.	<u>S</u> upprim	er ou ne plus faire c	onfiance
					ОК

FIGURE 5 – Firefox/préférences/vie privée et sécurité/certificats

Chiffrement asymétrique RSA



Autorité de certification

Hors programme

En pratique, l'autorité de certification 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).

Sommaire

- Chiffrement asymétrique RSA

- - Protocole https

- 3.3 Protocole https
- 3.4 Informations techniques

3. Sécuriser l'accès à un site web

Protocole https

Chiffrement asymétrique RSA

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

nformations techniques

36 / 44

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

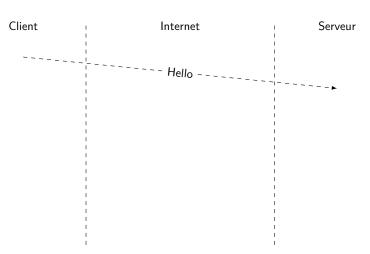


FIGURE 6 – **Hello**: Le navigateur envoie son intention de se connecter et diverses informations techniques.

Chiffrement RSA

Principe

kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

Protocole https

Informations t

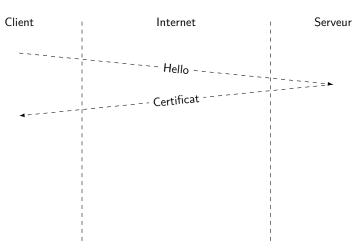


FIGURE 7 – **Certificat :** Le serveur envoie son certificat (sa clé publique signée par la clé privée d'une autorité).

Chiffrement RSA

Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

Autorité de certification

Protocole https

Informations to

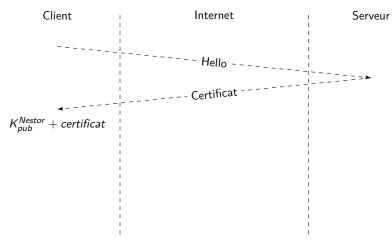


FIGURE 8 – **Authentification :** Le client utilise la clé publique de l'autorité pour déchiffrer le certificat et compare le résultat avec la clé publique du site.

Principe

Description

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

Protocole https

nformations techniqu

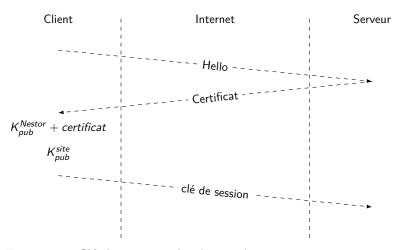


FIGURE 9 – **Clé de session :** Le client et le serveur se mettent d'accord sur un protocole d'échange (symétrique, Diffie-Hellman) : le client peut communiquer sa clé de manière sécurisée grâce à la clé publique authentifiée du site.

Chiffrement RSA

Description
kid RSA : formalisme
mathématique

Authentification les participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification

Protocole https

Informations techniq

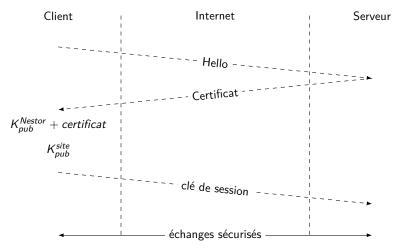


FIGURE 10 – **Échanges :** Le client et le serveur échangent de manière sécurisée.

Chiffrement RSA

Principe

kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

Protocole https

Informations technique

Sommaire

- Chiffrement asymétrique RSA

- Informations techniques

- 3. Sécuriser l'accès à un site web

- 3.4 Informations techniques

Informations techniques



FIGURE 11 – Le cadenas atteste des échanges sécurisés

Chiffrement asymétrique RSA

Chiffrement RSA

Principe

kid RSA : formalisme

Authentification les participants

Sécuriser l'accès à un site web

Associer les protocoles
Autorité de certification
Protocole https

Informations techniques

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.

TLS ECDHE RSA WITH AES 256 GCM SHA384. 256bits, TLS 1.2

- Protocole TLS (Transport Layer Security)
- Algorithme d'échange de clés : ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)
- Algorithme d'authentification : RSA
- Algorithme de chiffrement (symétrique) par bloc : AES 256bits (Advanced Encryption Standard) en mode GCM (Galois/Counter Mode)
- Algorithme de code d'authentification de message : SHA384 (création de la somme de contrôle de la clé)

Informations techniques