Chiffrement asymétrique//RSA

Christophe Viroulaud

Terminale NSI

Chiffrement RSA

Principe

mathématique

des participants

Sécuriser l'accès à un site web

Problématique

Chiffrement R

Principe

kid RSA : formalisme mathématique

Authentification les participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

Comment authentifier avec certitude les participants?

d'échanger des clés via un canal non sûr mais ne gère pas les

Le chiffrement asymétrique de Diffie-Hellman permet

problèmes liés à l'authentification des interlocuteurs.

Chiffrement RSA

Chiffrement asymétrique//RSA

Principe

- 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.

À retenir

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

Chiffrement asymétrique//RSA

Problèmatique

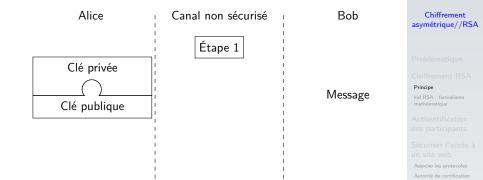
Chiffrement RSA

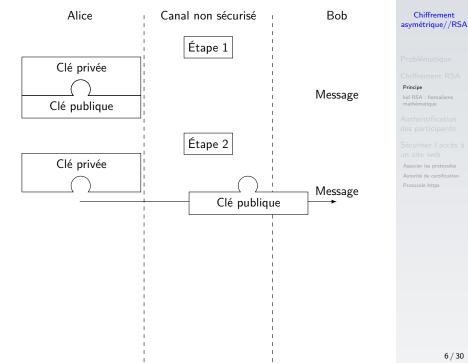
Principe

kid RSA : formalisme mathématique

des participants

Sécuriser l'accès à un site web





Problématique

Chiffrement I

Principe

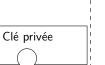
kid RSA : formalisme mathématique

des participants

Associer les protocoles

Autorité de certification

Étape 3



Alice

Bob



Chimana D

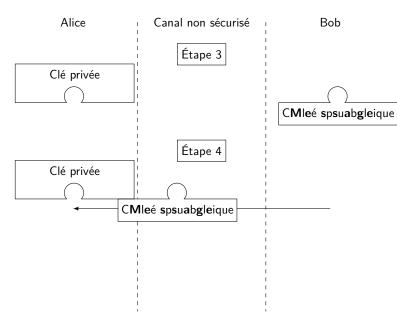
Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles
Autorité de certification





21.16..... DC

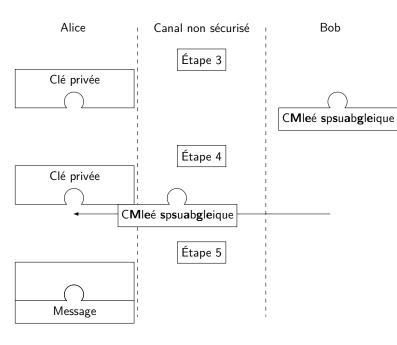
Principe

kid RSA : formalisme mathématique

uthentification es participants

Sécuriser l'accès à

Autorité de certification
Protocole https



Problematique

Chiffrement F

Principe

kid RSA : formalisme mathématique

Authentification des participant

Sécuriser l'accès à un site web

Associer les protocoles
Autorité de certification

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.

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.

Problematique

Principe

kid RSA : formalisme mathématique

des participants

Sécuriser l'accès à un site web

Activité 1:

- 1. Découvrir l'algorithme kidrsa sur la page https://tinyurl.com/rsakid
- 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) \rightarrow 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).
- Tester l'algorithme de chiffrage avec un entier (inférieur à n).

Problématique

Principe

kid RSA : formalisme mathématique

des participants

kid RSA : formalisme mathématique

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

Code 1 – Alice crée ses clés

kid RSA : formalisme mathématique

```
def chiffrer(message: int, publique: tuple) -> int:
1
 2
3
        Args:
           message (int)
4
           publique (tuple): (e, n)
5
6
        Returns:
 7
           int: message chiffré
8
        77 77 77
9
        return (publique[0]*message) % publique[1]
10
```

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

```
def dechiffrer(message_secret: int, privee: tuple) -> int:
1
 2
3
       Args:
           message secret (int)
4
           privee (tuple): (d, n)
5
6
        Returns:
 7
           int: message déchiffré
8
        77 77 77
9
        return (privee[0]*message_secret) % privee[1]
10
```

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

Principe kid RSA : formalisme mathématique

Authentification

Sécuriser l'accès à un site web

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. Problematique

Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

Authentification

Chiffrement asymétrique//RSA

Problématique

Chiffrement

Principe kid RSA : formalisme

Authentification 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.

Authentification des participants

Étape 1

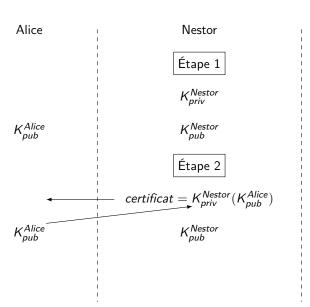
 K_{priv}^{Nestor}

 K_{pub}^{Nestor}

 K_{pub}^{Alice}

Alice

18/30



Problématique

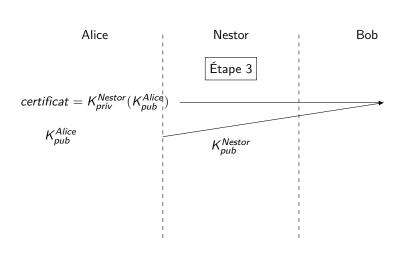
hiffrement P

p . .

kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à



Froblematique

Chiffrement RSA

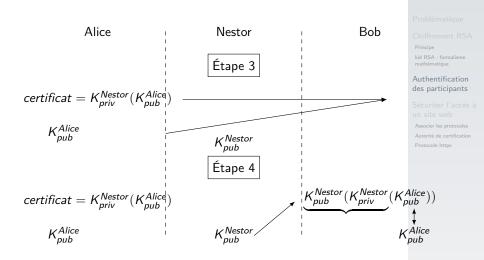
Princip

kid RSA : formalisme mathématique

Authentification des participants

Securiser l'accès à un site web

Autorité de certification Protocole https



Sécuriser l'accès à un site web

Chiffrement asymétrique//RSA

Problématique

Chiffrement R

Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à

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

hiffrement RS

Principe

mathématique

des participants

Sécuriser l'accès à

Associer les protocoles

Autorité de certification Protocole https

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

Principe

mathématique

Authentification des participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification Protocole https

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

Gestionnaire de certificats						
Vos certificats	Décisions d'authentifi	cation F	Personnes	Serveurs	Autorités	
ous possédez des d	ertificats enregistrés ide	ntifiant ces a	autorités de c	ertification		
Nom du certificat			Périphérique de sécurité			
✓ AC Camerfirma S	5.A.					
Chambers of Commerce Root - 2008		Buil	Builtin Object Token			
Global Chambersign Root - 2008			Builtin Object Token			
✓ AC Camerfirma S	5A CIF A82743287					
Camerfirma Cl	hambers of Commerce R	oot Buil	ltin Object To	ken		
Camerfirma Global Chambersign Root			Builtin Object Token			
<u>V</u> oir <u>M</u> o	odifier la confiance	Importer	Exporter	Supprime	er ou ne plus faire	confiance
						ОК

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



Autorité de certification

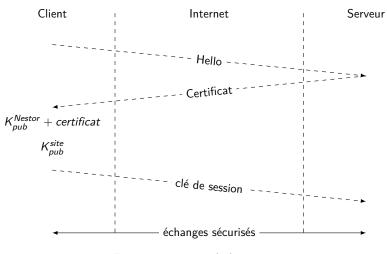
En pratique, elle ne signe pas la clé publique entière du site (2048 ou 4096 bits) mais sa somme de contrôle calculée (256 bits) par une fonction de hachage (souvent sha256).

Au

Sécuriser l'accès à

Associer les protocoles
Autorité de certification
Protocole https

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



 $\label{eq:figure} Figure - \text{protocole https}$

Problématique

hiffrement RS

Principe

Authentification

Sécuriser l'accès à



FIGURE – Le cadenas atteste des échanges sécurisés

Problématique

hiffrement R

Principe kid RSA : formalism

Authentification les participants

Sécuriser l'accès à un site web

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)

Protocole https