Chiffrement RSA

Principe kid RSA : formalisme

Authentification

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification

Protocole https

Chiffrement asymétrique//RSA

Christophe Viroulaud

Terminale NSI

Problématique

Chiffrement R

Principe

kid RSA : formalisme mathématique

> Authentificatior des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

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?

Le chiffrement asymétrique de Diffie-Hellman permet

Chiffrement RSA

Chiffrement asymétrique//RSA

1 Toblematique

Chiffrement RSA

Principe

kid RSA : formalisme mathématique

des participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification

- ▶ 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

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

Chiffrement asymétrique//RSA

Problématique

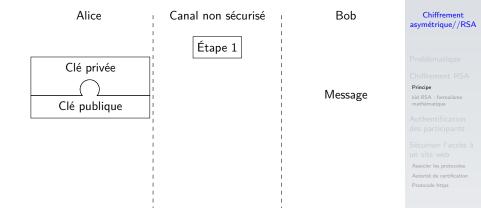
Chiffrement RSA

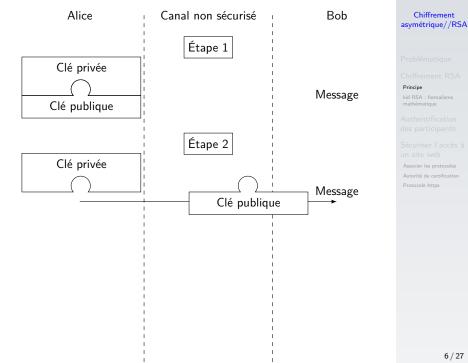
Principe

kid RSA : formalisme mathématique

des participants

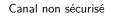
Sécuriser l'accès à un site web





Alice

Clé privée



Étape 3

Bob

CMleé spsuabgleique

Problématique

Chiffrement F

Principe

kid RSA : formalisme mathématique

es participants

Sécuriser l'accès à un site web



CI.: (f...... D)

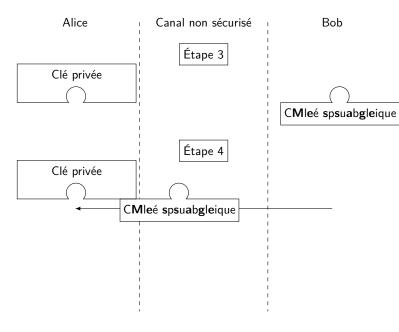
Principe

kid RSA : formalisme mathématique

authentification es participants

Sécuriser l'accès à un site web

Autorité de certificatio



Problématique

hiffrement RS

Principe

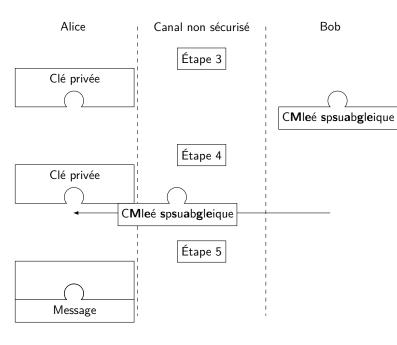
kid RSA : formalisme mathématique

Authentification es participants

Sécuriser l'accès à un site web

Associer les protocoles

Autorité de certification



Problèmatique

Chiffrement F

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.

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

Authentification 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: int) → 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

un site web

Associer les protocoles

Autorité de certification

Autorité de certification Protocole https

$\begin{array}{c} {\sf Chiffrement} \\ {\sf asym\'etrique}//{\sf RSA} \end{array}$

Cliff DC/

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.

Authentification

Chiffrement asymétrique//RSA

Problématique

Chiffrement F

Principe kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à un site web

Authentification

des participants

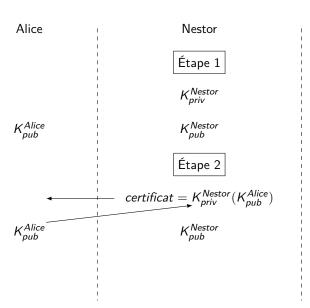
Étape 1

 K_{priv}^{Nestor}

 K_{pub}^{Nestor}

Alice

 K_{pub}^{Alice}



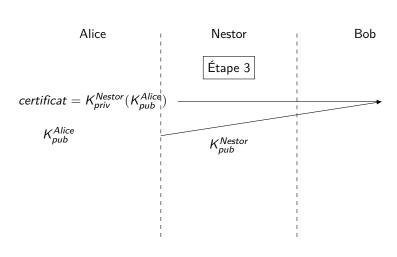
Problématique

Chiffrement F

kid RSA : formalisme

Authentification des participants

Sécuriser l'accès à



i iobiematique

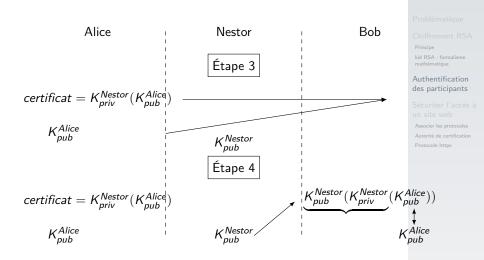
Chiffrement RSA

Principa

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web



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

niffrement RS

Principe kid RSA : formali

mathématique

des participants

Sécuriser l'accès à un site web

Associer les protocoles Autorité de certification

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

Problèmatique

Chiffrement |

kid RSA : formalisme

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'authentif	ication F	Personnes	Serveurs	Autorités	
Vous possédez des	certificats enregistrés id	entifiant ces a	autorités de ce	ertification		
Nom du certificat			Périphérique de sécurité			
✓ AC Camerfirma:	5.A.					
Chambers of Commerce Root - 2008		Buil	ltin Object Tol	ken		
Global Chamb	ersign Root - 2008	Buil	ltin Object Tol	ken		
∨ AC Camerfirma	SA CIF A82743287					
Camerfirma C	hambers of Commerce I	Root Buil	ltin Object Tol	ken		
Camerfirma G	lobal Chambersign Root	: Buil	ltin Object Tol	ken		
<u>V</u> oir <u>M</u>	odifier la confiance	<u>I</u> mporter	Exporter	Supprime	er ou ne plus fa	ire confiance
						OK

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



Problématique

Principe

kid RSA : formalisme mathématique

Authentification des participants

Sécuriser l'accès à un site web

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).

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

Problématique

Chiffrement

Authentification

Sécuriser l'accès à un site web

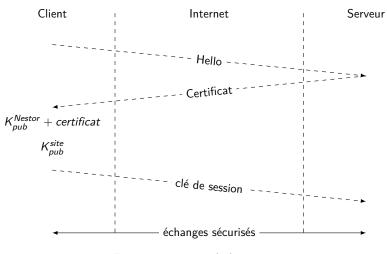


FIGURE – protocole https

Problématique

hiffrement R!

Mathématique

Authentification

Sécuriser l'accès à



FIGURE – Le cadenas atteste des échanges sécurisés

Problématique

niffrement R

kid RSA : formalis

Authentification des participants

Sécuriser l'accès à

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