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

Comment authentifier avec certitude les participants ?

2 Chiffrement RSA

2.1 Principe

Les trois cryptologues décrivent leur algorithme en 1977. Tout comme Diffie et Hellman, ils s'appuient sur des *fonctions à sens unique* et une paire de clés publique et privée.

À retenir

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

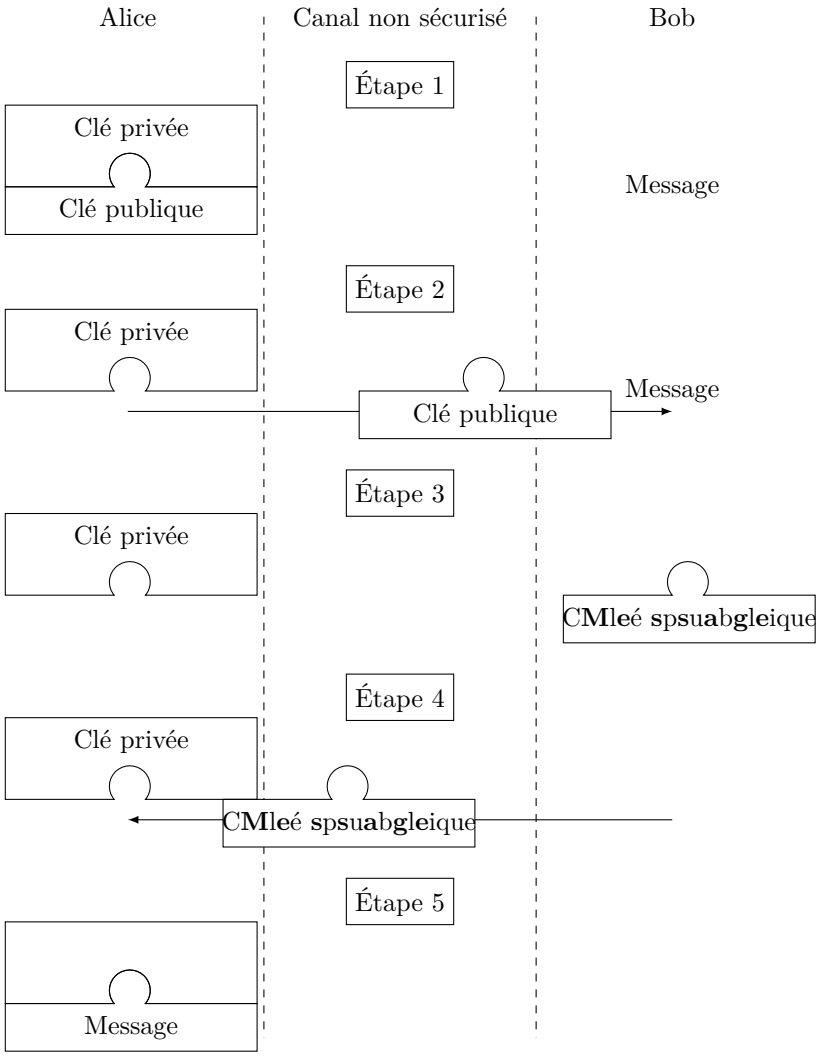


FIGURE 1 – Clé publique / clé privée

Christophe Viroulaud

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.

2.2 kid RSA : formalisme mathématique

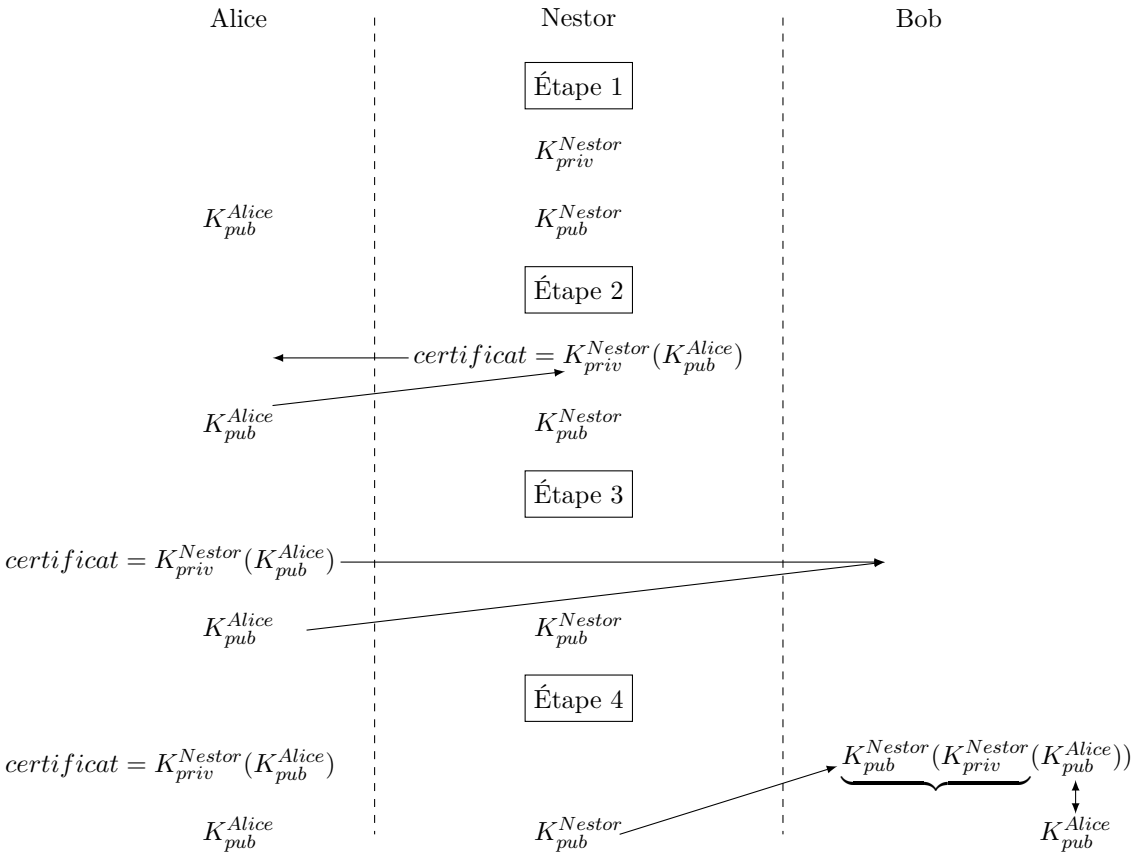
La création des clés suit un algorithme mathématique complexe. L'université de Rhode Island a produit une version simplifiée (à utilisation pédagogique) pour simuler le protocole.

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).

3 Authentification des participants

Contrairement à la méthode de Diffie-Hellman, le protocole RSA peut être utilisé pour authentifier les participants. Il faut pour cela qu'un **tiers de confiance** (Nestor) intervienne.



Christophe Viroulaud

FIGURE 2 – Authentification

4 Sécuriser l'accès à un site web

4.1 Associer les protocoles

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.

4.2 Autorité de certification

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.

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

4.3 Protocole https

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

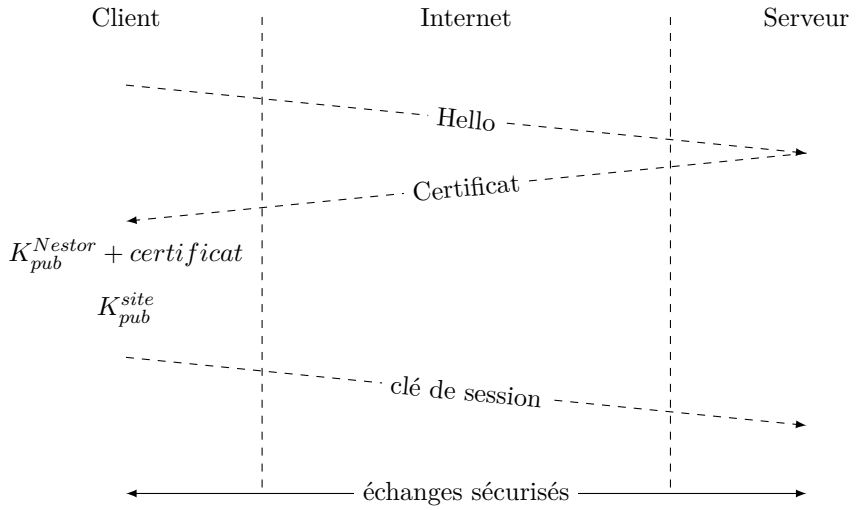


FIGURE 3 – protocole https

Christophe Viroulaud