Sécurisation des communications

J. Boucher

Lycée Pierre-Paul RIQUET, Terminale NSI

19 mars 2025

Plan

Problématique

Si les méthodes de chiffrement symétrique comme l'AES offre des garanties très importantes en terme de sûreté et d'efficacité, il existe cependant un problème majeur :
Comment deux personnes voulant établir un canal de communication sûr peuvent-elles échanger la clé à utiliser ?

Problématique

Si les méthodes de chiffrement symétrique comme l'AES offre des garanties très importantes en terme de sûreté et d'efficacité, il existe cependant un problème majeur :

Comment deux personnes voulant établir un canal de communication sûr peuvent-elles échanger la clé à utiliser ?

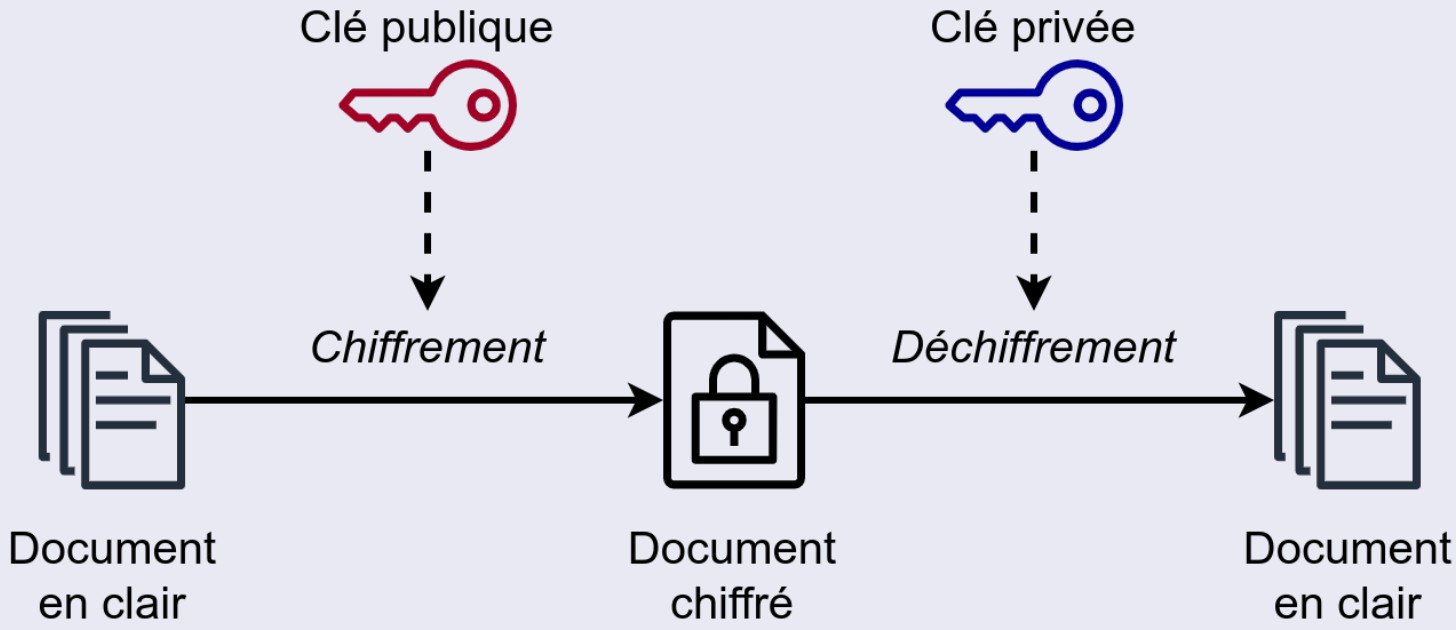
1. soit échanger la clé par un moyen de communication non sûr (courriel, messagerie)
   $\rightarrow$ un intermediaire peut s'emparer de la clé
2. soit s'échanger physiquement un support de stockage contenant la clé
   $\rightarrow$ très contraingnant

Pour résourdre ce problème, des techniques de cryptographie asymétrique, aussi appelée cryptographie à clé publique ont été développé dès les années 1970.

2. Cryptographie asymétrique

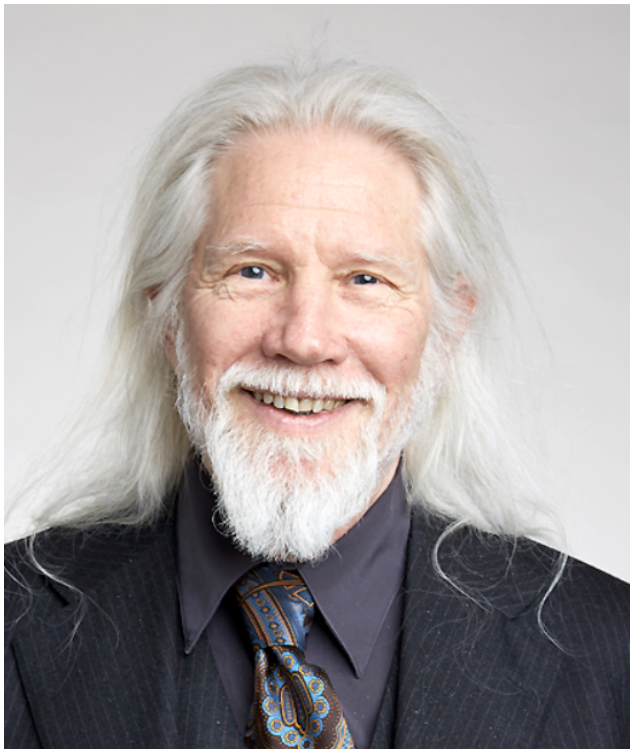
Principe de la cryptographie asymétrique

Les algorithmes de cryptographie asymétrique sont basés sur l'utilisation d'une clé publique, c'est-à-dire connue de tous, associée à une clé privée, qui elle est gardée secrète.

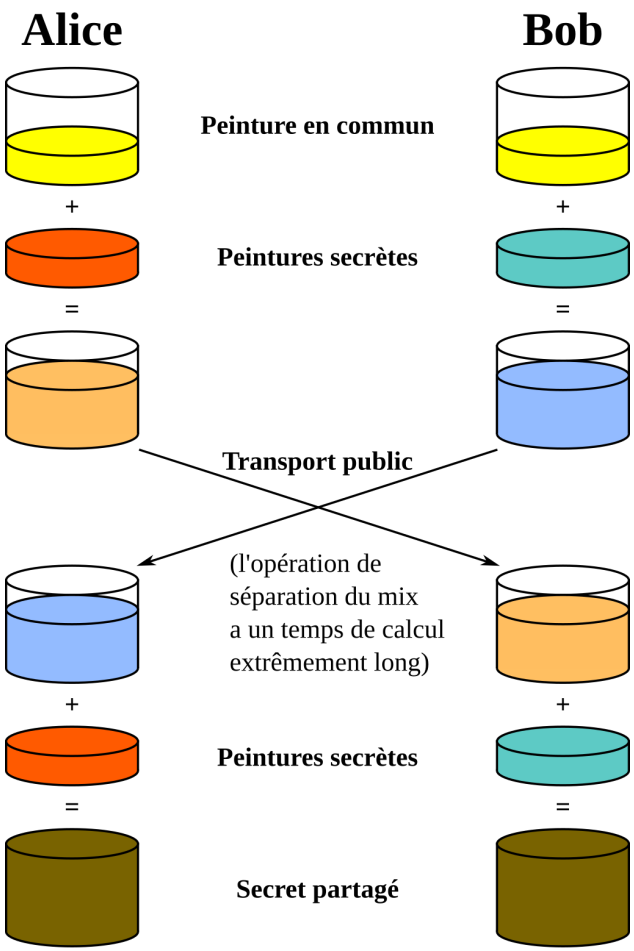


Méthode de Diffie-Hellman

→ Premier protocole de chiffrement asymétrique proposé par *B. W. Diffie* et *M. Hellman* en 1976.



▸ Lien

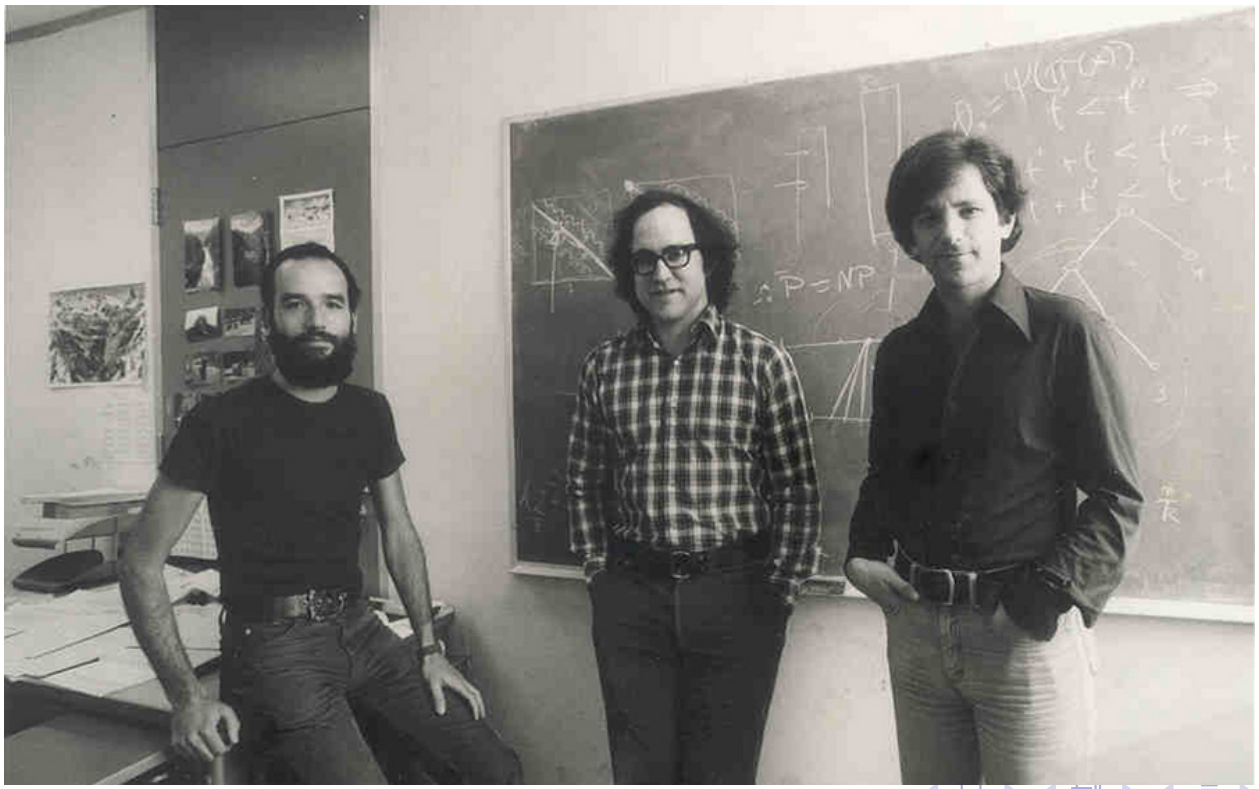


- la méthode de Diffie-Hellman permet à deux participants de construire une clé secrète partagée de manière sûre, à partir d'une clé publique connue de tous.
- La sécurité de la méthode repose sur la difficulté d'extraire les clés secrètes (couleurs rouge et cyan) à partir des données échangées (couleurs orange et bleue) même en connaissant la clé commune de départ (couleur jaune).
- Cette méthode ne permet pas d'authentifier les participants, l'exposant à une attaque du type *attaque de l'homme au milieu* (ou man in the middle en anglais).

Le système RSA

Le système RSA est un système de chiffrement asymétrique basé sur l'utilisation de paires de clés publiques et privées. Il a été présenté en 1977 par les mathématiciens :

Ron **R**ivest, Adi **S**hamir et Len **A**dleman



Propriétés du protocole RSA

On notera respectivement C^{pub} et C^{priv} les clés publiques et privées. L'une permet de chiffrer le message m et l'autre permet de le déchiffrer.

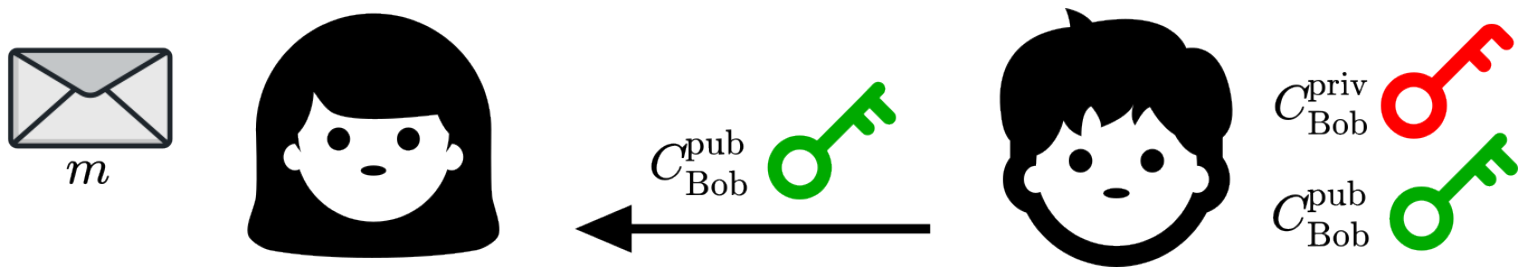
La façon dont sont générées les clés est complexe et repose sur des théorèmes d'arithmétique bien connus (théorème de Bezout et petit théorème de Fermat), non présentés ici.

Il faut retenir que les deux clés sont liées de la façon suivante :

- $C^{pub}(C^{priv}(m)) = C^{priv}(C^{pub}(m)) = m$
- connaissant C^{pub} il est impossible de trouver C^{priv} et réciproquement
- il est impossible de trouver m en connaissant $C^{pub}(m)$ ou $C^{priv}(m)$

Cas d'usage où Alice veut envoyer un message à Bob

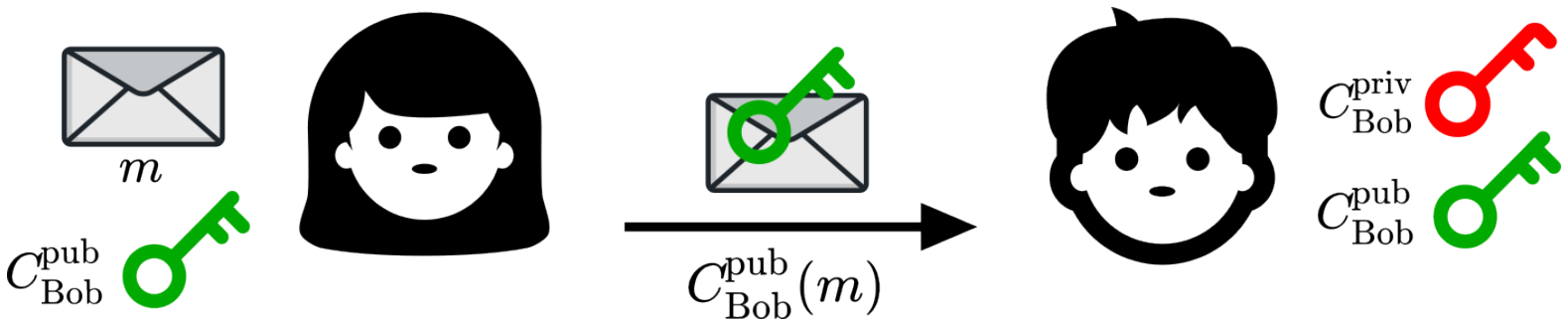
Étape 1



Bob fabrique deux clés :

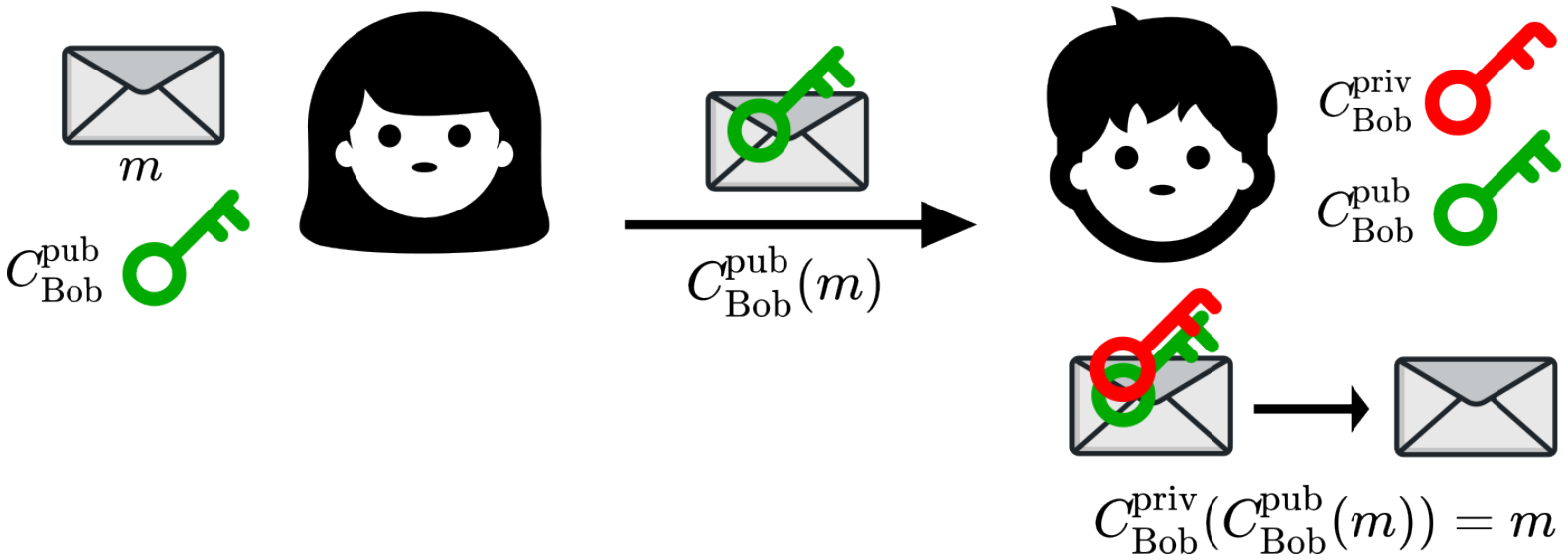
- sa clé publique C^{pub}_{Bob}, qu'il envoie à Alice,
- et sa clé privée C^{priv}_{Bob}, qu'il ne divulgue à personne.

Étape 2

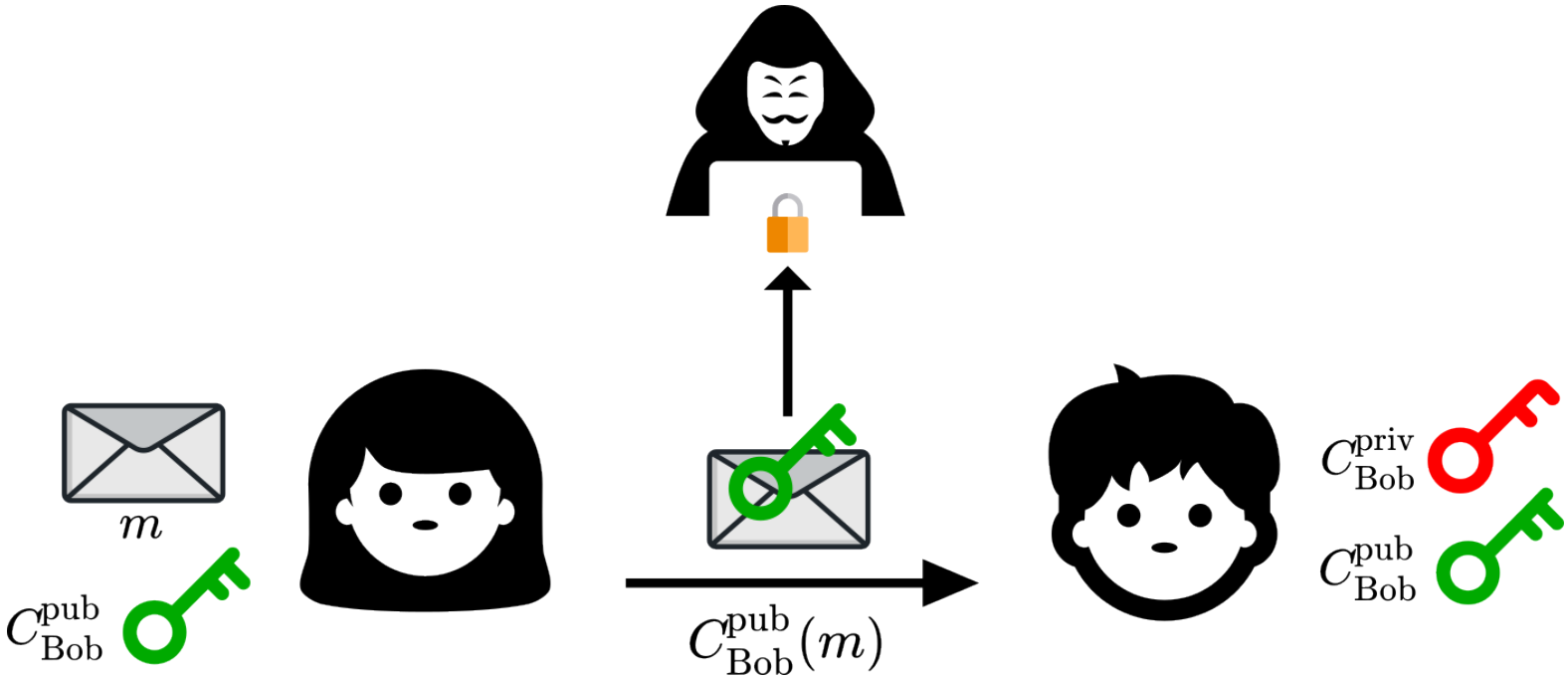


Alice utilise la clé publique de Bob pour chiffrer son message m puis envoie ce message $C^{pub}_{Bob}(m)$ à Bob.

Étape 3



Bob utilise sa clé privée pour déchiffrer le message d'Alice : $C^{priv}_{Bob}(C^{pub}_{Bob}(m)) = m$.



Ainsi, si un tiers intercepte le message d'Alice à l'étape 2, il ne pourra rien en faire car elle ne connaît pas la clé privée de Bob : la communication est donc sécurisée.

Bilan

- Le système RSA permet de chiffrer des messages sans s'être mis d'accord sur une clé de chiffrement symétrique commune.
- Le coût des calculs de chiffrement et déchiffrement est très élevé.
  $\rightarrow$ il n'est pas possible d'utiliser RSA pour chiffrer à la volée des gros volumes de données ou des flux de communication.
- On peut utiliser RSA comme un moyen sûr pour échanger une clé de chiffrement symétrique, qui permettra alors d'utiliser un protocole comme AES.

Authentification des participants

Scénario d'une attaque de l'homme du milieu

Ève, l'agent malvaillant 😈, veut dérober les informations bancaire d'Alice, cliente de la BobBanque.

1. Alice reçoit un courriel au format HTML de sa banque, lui demandant de se connecter d'urgence sur le site de la banque.

> Veuillez vous connecter d'urgence au site BobBanque.com

```
<html>
...
  <body>
    Veuillez vous connecter d'urgence au site
    <a href=''http://Eve.com''>BobBanque.com</a>.
  </body>
</html>
```

2. Ève reproduit excatement la page d'accueil du site `BobBanque.com` $\rightarrow$ Ève peut recevoir tous les messages envoyés par Alice (dont les informations d'identification au site).
3. Ève peut alors retransmettre passivement les requêtes d'Alice à BobBanque ou les modifier avant de les retransmettre.

Ève se trouve donc dans une position intermédiaire entre Alice et Basile ; on parle d'attaque de l'homme du milieu (ou *man in the middle* en anglais).

La faille fondamentale est l'absence d'authentification ; le serveur d'Ève n'a pas eu à prouver qu'il était bien une machine appartenant à BobBanque.

Certificats et tiers de confiance

- Pour prouver son identité, un participant présente ce qu'on appelle un certificat qui est délivré par un tiers de confiance.
- Ces certificats numériques sont créés à partir des clés RSA publiques et privées des participants.

Bilan : Le protocole RSA permet donc d'authentifier les participants, via des certificats fournis par un tiers de confiance.

Étape 1

Bob va voir une autorité de certification AC (le tiers de confiance) qui :

1. vérifie que Bob est bien propriétaire de `BobBanque.com` ;
2. utilise sa clé privée pour chiffrer celle de Bob : $s = C_{AC}^{priv}(C_{Bob}^{pub})$.

Un tel fichier s s'appelle un certificat.

Étape 2

Alice veut se connecter à `BobBanque.com`.

1. Le site lui fournit la clé publique de Bob, C_{Bob}^{pub} ;
2. le certificat s.

Bilan : Le protocole RSA permet donc d'authentifier les participants, via des certificats fournis par un tiers de confiance.

Étape 3

Alice récupère alors la clé publique de Théo, en qui elle a confiance, et l'applique au certificat :

$$C_{AC}^{pub}(s) = \underbrace{C_{AC}^{pub}(C_{AC}^{priv}}_{s'\,annulent}(C_{Bob}^{pub})) = C_{Bob}^{pub}$$

Si le résultat du calcul précédent correspond à la clé publique que `BobBanque.com` lui a transmise, alors Alice est certaine que `BobBanque.com` est bien le site de Bob.

Étape 4

Alice peut initier avec `BobBanque.com` une communication sécurisée en utilisant la clé publique pour chiffrer une clé symétrique ou en utilisant le protocole de Diffie-Hellman pour se mettre d'accord sur une clé partagée.

Bilan : Le protocole RSA permet donc d'authentifier les participants, via des certificats fournis par un tiers de confiance.