Présentation

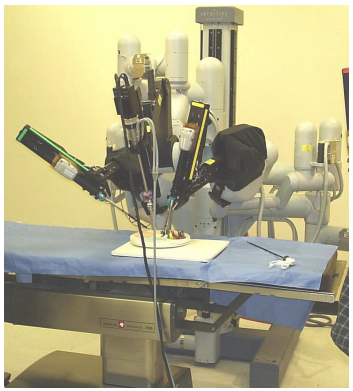
- *Doctorante en informatique* à l'IRISA
- **Doctorat** : entre études et travail, on fait de la **recherche** (apprenti chercheur)
- Mon sujet de recherche : *vérification des systèmes informatiques*

Présentation

- *Doctorante en informatique* à l'IRISA
- **Doctorat** : entre études et travail, on fait de la **recherche** (apprenti chercheur)
- Mon sujet de recherche : *vérification des systèmes informatiques*

- L'informatique est partout de nos jours



- La *moindre erreur* peut être **fatale**
  $\Rightarrow$ Vérification de ces systèmes informatiques pour **garantir leur bon fonctionnement**.

Les protocoles de sécurité

S'authentifier en toute sécurité sur internet

Valérie Murat

Printemps 2011

Plan

1 Introduction

2 La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique

3 Protocole d'authentification sur internet

4 Vers la recherche

Pourquoi les protocoles de sécurité ?

Sur internet (paiement en ligne, envoi de mots de passe, ...), ou encore quand on utilise une carte bancaire, on a besoin de :

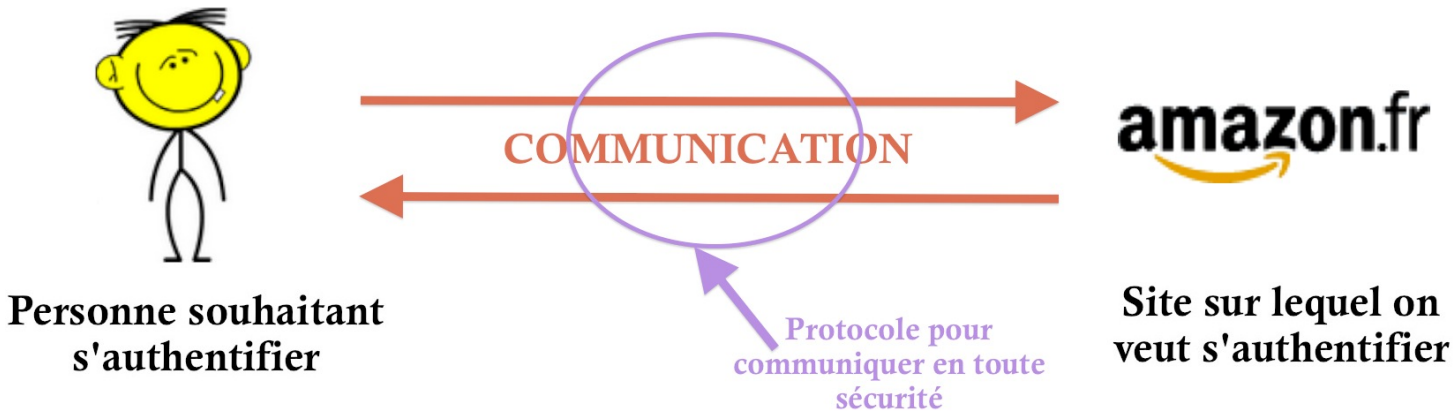
Pourquoi les protocoles de sécurité ?

Sur internet (paiement en ligne, envoi de mots de passe, ...), ou encore quand on utilise une carte bancaire, on a besoin de :

- Établir une communication sécurisée entre 2 individus - **Sécurité**
- Être sûr de communiquer avec la bonne personne, et pas un intrus voulant voler des informations (comme le mot de passe) - **Authentification**
- Être sûr que les données ne sont pas modifiées en cours de route - **Intégrité**

Qu'est-ce qu'un protocole de sécurité ?

Pour cela : **les protocoles de sécurité**
⇒ Ensemble de règles régissant le comportement d'individus pour répondre aux besoins d'une application (paiement en ligne, vote électronique, authentification d'individus, etc)

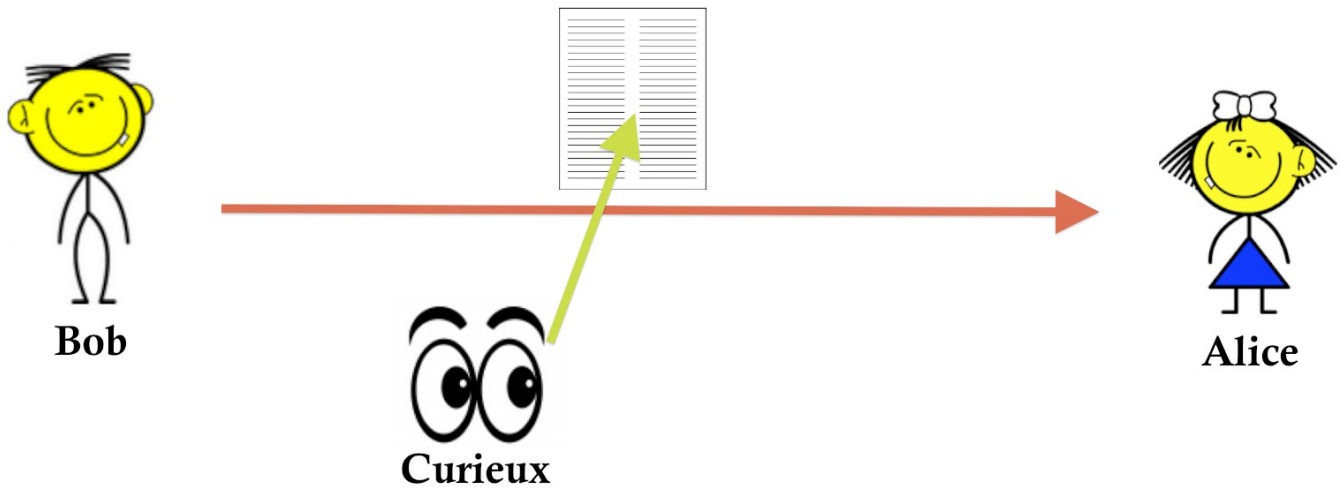


L'utilisation des protocoles est **transparente** pour l'utilisateur.

Sécuriser les messages

Communication entre 2 individus A et B $\rightarrow$ **échange de *messages***
$\Rightarrow$ Besoin que ces messages soient *chiffrés* pour garantir leur confidentialité

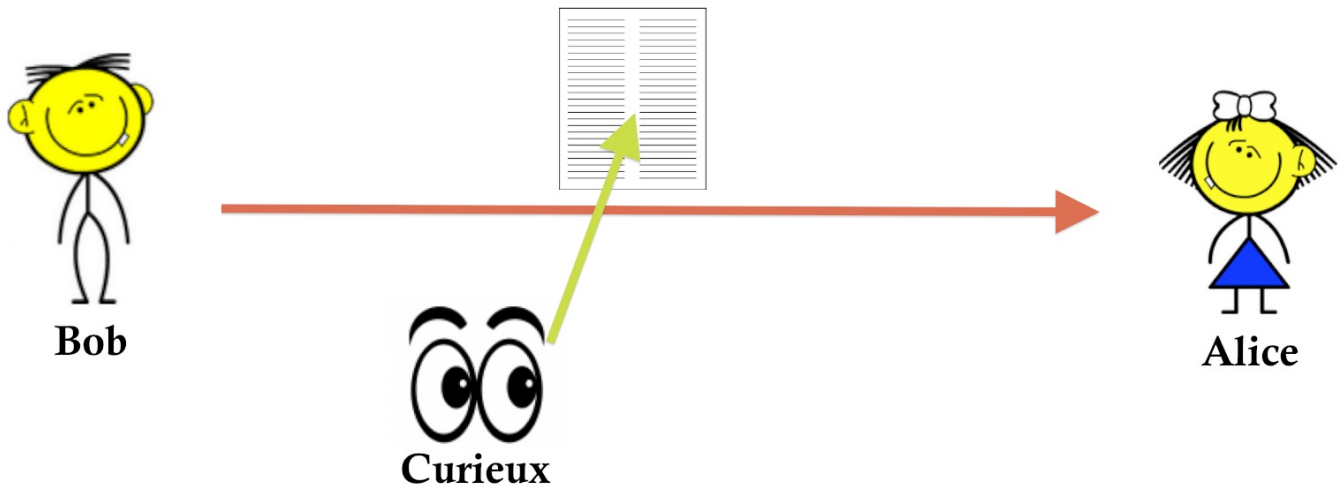
Exemple : Durant leurs cours, Alice et Bob, qui ne sont pas côte à côte dans la classe, communiquent en se faisant passer des petits mots.
Problème : n'importe qui peut lire le mot...



Sécuriser les messages

Communication entre 2 individus A et B $\rightarrow$ **échange de *messages***
$\Rightarrow$ Besoin que ces messages soient *chiffrés* pour garantir leur confidentialité

Exemple : Durant leurs cours, Alice et Bob, qui ne sont pas côte à côte dans la classe, communiquent en se faisant passer des petits mots.
Problème : n'importe qui peut lire le mot...



$\Rightarrow$ Utilisation de la **cryptographie**

Plan

1 Introduction

2 La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique

3 Protocole d'authentification sur internet

4 Vers la recherche

Crypter les messages

Qu'est-ce que la cryptographie ? Un ensemble de méthodes permettant de chiffrer un message *numérique*, grâce à une **clé**.

⇒ Rend le message **incompréhensible** pour quiconque ne possédant pas la clé.

- Chiffrement **symétrique** : une seule clé partagée pour chiffrer et déchiffrer
- Chiffrement **asymétrique** : une clé pour chiffrer, une autre pour déchiffrer

Crypter les messages

Qu'est-ce que la cryptographie ? Un ensemble de méthodes permettant de chiffrer un message *numérique*, grâce à une **clé**.

⇒ Rend le message **incompréhensible** pour quiconque ne possédant pas la clé.

- Chiffrement **symétrique** : une seule clé partagée pour chiffrer et déchiffrer
- Chiffrement **asymétrique** : une clé pour chiffrer, une autre pour déchiffrer

Cryptographie : chiffre des messages **numériques**
Problème : Que faire si on veut chiffrer du *texte* ?
(Exemples : son mot de passe, un message privé, ...)

Crypter les messages

Qu'est-ce que la cryptographie ? Un ensemble de méthodes permettant de chiffrer un message *numérique*, grâce à une **clé**.

⇒ Rend le message **incompréhensible** pour quiconque ne possédant pas la clé.

- Chiffrement **symétrique** : une seule clé partagée pour chiffrer et déchiffrer
- Chiffrement **asymétrique** : une clé pour chiffrer, une autre pour déchiffrer

Cryptographie : chiffre des messages **numériques**
Problème : Que faire si on veut chiffrer du *texte* ?
(Exemples : son mot de passe, un message privé, ...)

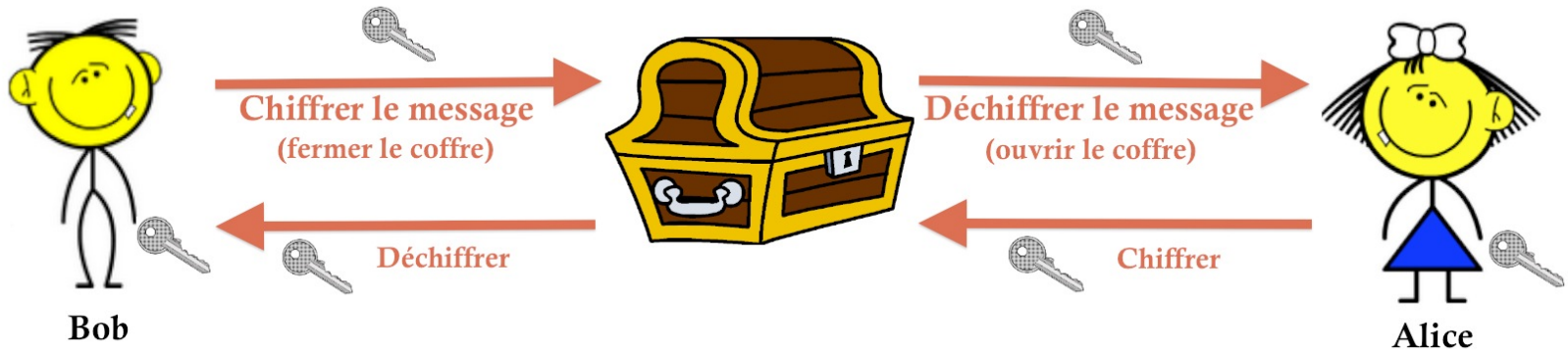
⇒ On fait correspondre chaque lettre de l'alphabet à un nombre :

A	B	C	D	E	F	G	H	I ...
0	1	2	3	4	5	6	7	8 ...

Chiffrement symétrique

Principe :

Les 2 individus voulant communiquer de façon sécurisée (Alice et Bob) se mettent d'accord sur une même clé secrète qui leur permet de chiffrer et déchiffrer leurs messages.

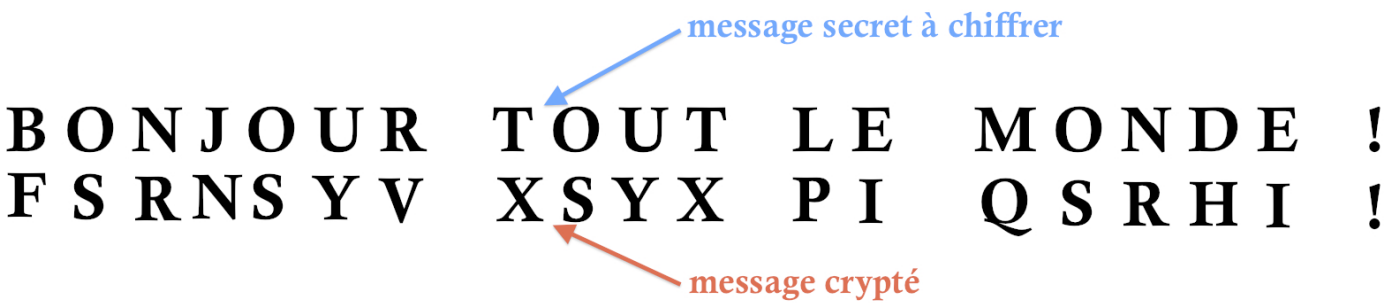


On note K_{AB} la clé partagée par Alice et Bob.
Clé **secrète** connue d'**eux seuls**.

Chiffrement symétrique : exemple

A	B	C	D	E	F	G	H	I ...
0	1	2	3	4	5	6	7	8 ...

Chiffrement par décalage : on décale les lettres du mot à chiffrer.
Exemple : décalage de 4 lettres.



Ici, la clé partagée $K_{AB} = 4$.
On note le message chiffré grâce à la clé K_{AB} : $\{\text{message}\}_{K_{AB}}$
Ici : $\{\textbf{BONJOUR TOUT LE MONDE !}\}_{K_{AB}} = \textbf{FSRNSYV XSYX PI QSRHI !}$

Décalage de 3 : chiffrement de **César**.

Chiffrement symétrique : exemple

Est-ce qu'un curieux  peut casser ce code s'il n'a pas la clé ?
Comment feriez-vous par exemple pour déchiffrer le message « Hutpuax ! » ?

Chiffrement symétrique : exemple

Est-ce qu'un curieux  peut casser ce code s'il n'a pas la clé ?
Comment feriez-vous par exemple pour déchiffrer le message « Hutpuax ! » ?

26 lettres dans l'alphabet $\Rightarrow$ 25 décalages possibles.
On peut **tous les essayer** jusqu'à ce que le message *signifie quelque chose*.

Ici, si on essaie avec $K_{AB} = \mathbf{5}$, on obtient : Cpokpvs !
Avec $K_{AB} = \mathbf{6}$: Bonjour !

Facile à craquer $\Rightarrow$ codes plus robustes en pratique.

Chiffrement symétrique : exemple

Est-ce qu'un curieux  peut casser ce code s'il n'a pas la clé ?
Comment feriez-vous par exemple pour déchiffrer le message « Hutpuax ! » ?

26 lettres dans l'alphabet $\Rightarrow$ 25 décalages possibles.
On peut **tous les essayer** jusqu'à ce que le message *signifie quelque chose*.

Ici, si on essaie avec $K_{AB} = \mathbf{5}$, on obtient : Cpokpvs !
Avec $K_{AB} = \mathbf{6}$: Bonjour !

Facile à craquer $\Rightarrow$ codes plus robustes en pratique.

Problème

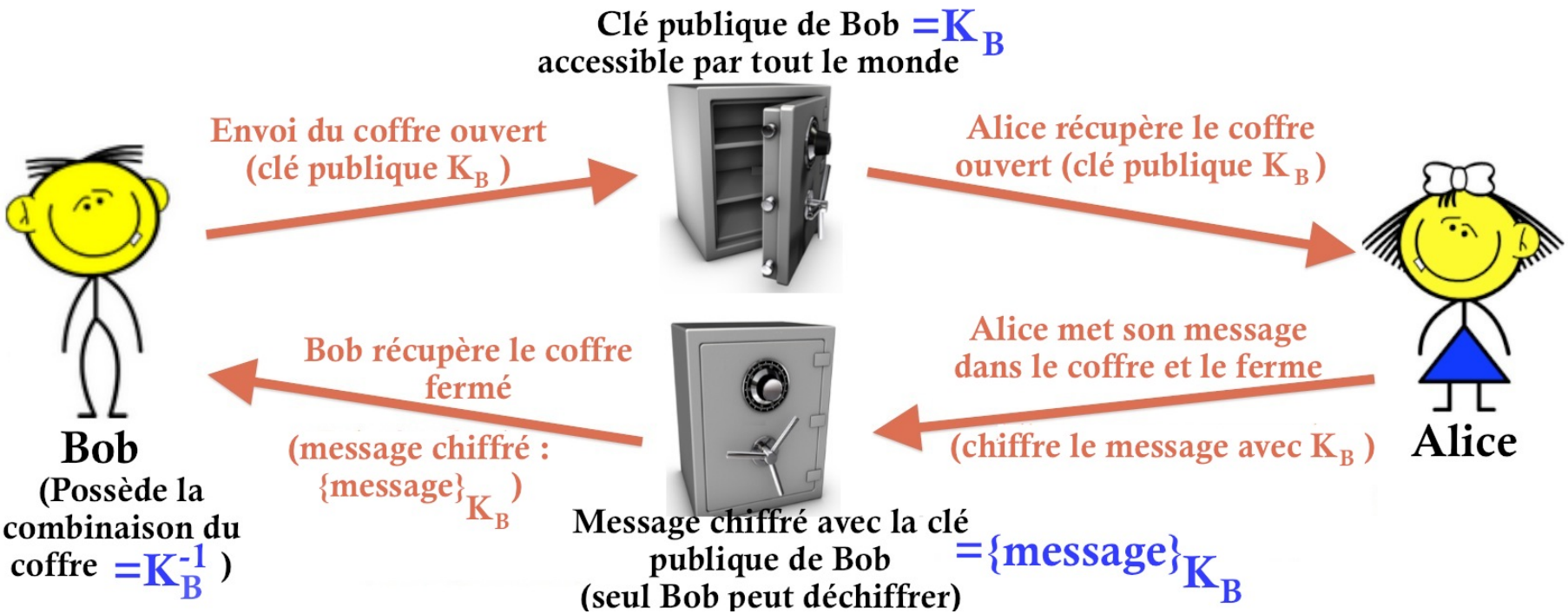
Pour avoir la *même clé*, Alice et Bob ont dû se **rencontrer**, mais ce n'est pas toujours possible !
On ne peut pas "rencontrer" un site internet pour se mettre d'accord sur une clé secrète.
Comment résoudre ce problème ?

Chiffrement asymétrique

Principe :

Une clé pour **chiffrer** ⇒ clé publique de Bob (**tout le monde peut chiffrer**)

Une clé pour **déchiffrer** ⇒ clé privée que seul Bob possède (**seul Bob peut déchiffrer** les messages chiffrés avec sa clé publique)



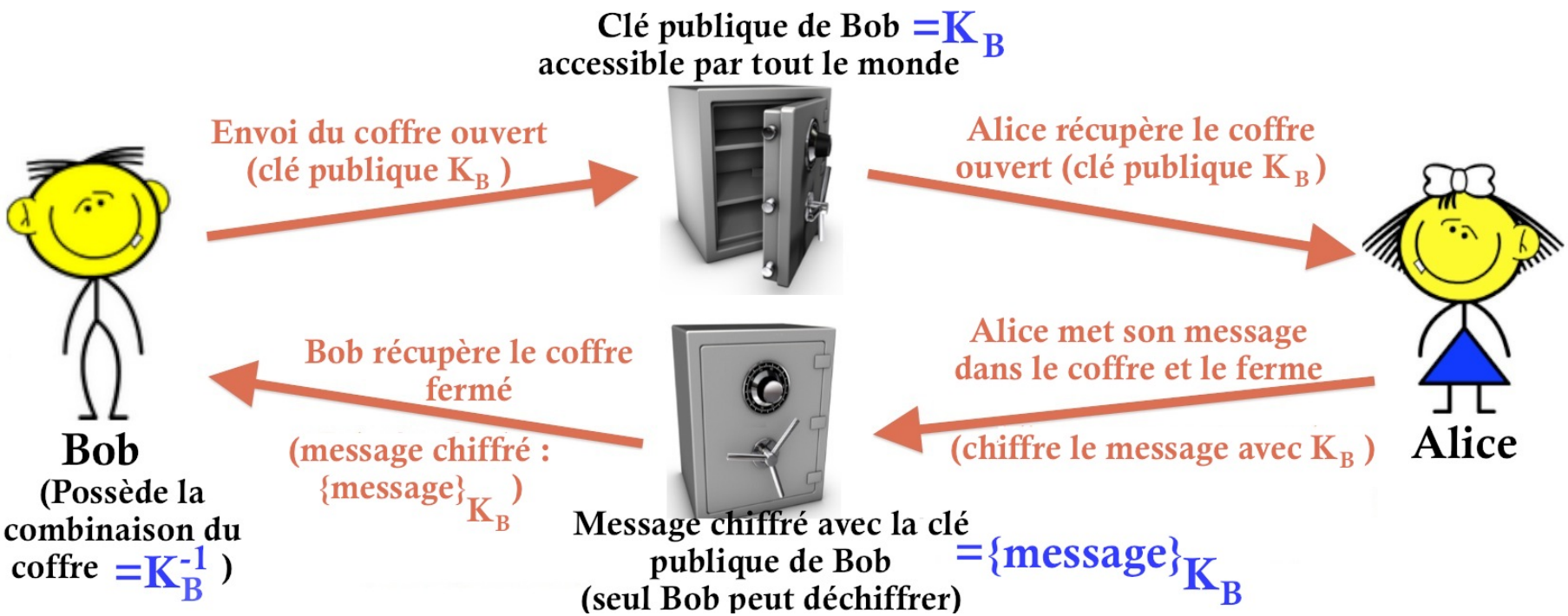
K_B : clé publique de Bob, K_B^{-1} : clé privée de Bob.

Chiffrement asymétrique

Principe :

Une clé pour **chiffrer** ⇒ clé publique de Bob (**tout le monde peut chiffrer**)

Une clé pour **déchiffrer** ⇒ clé privée que seul Bob possède (**seul Bob peut déchiffrer** les messages chiffrés avec sa clé publique)



Si **Alice** veut aussi recevoir des messages, elle utilise le même principe (avec K_A sa clé publique, et K_A^{-1} sa clé privée).

Chiffrement asymétrique : exemple

Soit $e = 7$, $e^{-1} = 3$ et $n = 33$
On a : $K_B = \{e, n\}$, et $K_B^{-1} = \{e^{-1}, n\}$.

Chiffrement asymétrique : exemple

Soit $e = 7$, $e^{-1} = 3$ et $n = 33$
On a : $K_B = \{e, n\}$, et $K_B^{-1} = \{e^{-1}, n\}$.

Chiffrement :

$\{\text{message}\}_{K_B} = \text{reste}(\text{message}^e \div n)$

Si **message** $= 13$, on a :

$$\{13\}_{K_B} = 13^7$$
$$= 62\,748\,517 \mid 33$$
$$1\,901\,470 \quad \text{reste } 7$$

$\Rightarrow \{13\}_{K_B} = 7$

Chiffrement asymétrique : exemple

Soit $e = 7$, $e^{-1} = 3$ et $n = 33$
On a : $K_B = \{e, n\}$, et $K_B^{-1} = \{e^{-1}, n\}$.

Chiffrement :

$\{\text{message}\}_{K_B} = \text{reste}(\text{message}^e \div n)$

Si **message** = 13, on a :

$\{13\}_{K_B} = 13^7$

$= 62\,748\,517 \mid 33$

$1\,901\,470$

reste = 7

$\Rightarrow \{13\}_{K_B} = 7$

Déchiffrement :

$\{\{\text{message}\}_{K_B}\}_{K_B^{-1}}$

$= \text{reste}((\{\text{message}\}_{K_B})^{e^{-1}} \div n)$

$\{7\}_{K_B^{-1}} = 7^3 = 343 \mid 33$

10

reste = 13

$\Rightarrow \{7\}_{K_B^{-1}} = 13 = \textbf{message}\,!$

Chiffrement asymétrique : exemple

Soit $e = 7$, $e^{-1} = 3$ et $n = 33$
On a : $K_B = \{e, n\}$, et $K_B^{-1} = \{e^{-1}, n\}$.

Chiffrement :

$\{\text{message}\}_{K_B} = \text{reste}(\text{message}^e \div n)$

Si **message** = 13, on a :

$$\{13\}_{K_B} = 13^7$$

$$= 62\,748\,517 \;\big|\; 33$$

$$1\,901\,470$$

reste = 7

$\Rightarrow \{13\}_{K_B} = 7$

Déchiffrement :

$\{\{\text{message}\}_{K_B}\}_{K_B^{-1}}$

$= \text{reste}((\{\text{message}\}_{K_B})^{e^{-1}} \div n)$

$$\{7\}_{K_B^{-1}} = 7^3 = 343 \;\big|\; 33$$

$$10$$

reste = 13

$\Rightarrow \{7\}_{K_B^{-1}} = 13 = \textbf{message}\,!$

On a bien : $13 \xrightarrow{K_B} 7 \xrightarrow{K_B^{-1}} 13$

Chiffrement asymétrique : exemple

Soit $e = 7$, $e^{-1} = 3$ et $n = 33$
On a : $K_B = \{e, n\}$, et $K_B^{-1} = \{e^{-1}, n\}$.

Chiffrement :

$\{\text{message}\}_{K_B} = \text{reste}(\text{message}^e \div n)$

Si **message** = 13, on a :

$$\{13\}_{K_B} = 13^7$$

$$= 62\,748\,517 \;\big|\; 33$$

$$1\,901\,470$$

reste = 7

$\Rightarrow \{13\}_{K_B} = 7$

Déchiffrement :

$\{\{\text{message}\}_{K_B}\}_{K_B^{-1}}$

$= \text{reste}((\{\text{message}\}_{K_B})^{e^{-1}} \div n)$

$$\{7\}_{K_B^{-1}} = 7^3 = 343 \;\big|\; 33$$

$$10$$

reste = 13

$\Rightarrow \{7\}_{K_B^{-1}} = 13 = \textbf{message}\,!$

On a bien : $13 \xrightarrow{K_B} 7 \xrightarrow{K_B^{-1}} 13$

Marche aussi dans *l'autre sens* : $13 \xrightarrow{K_B^{-1}} 19 \xrightarrow{K_B} 13$

Comparaison symétrique/asymétrique

- Chiffrement symétrique : chiffrement *plus rapide*, mais nécessite de se "rencontrer" pour pourvoir s'échanger la clé commune
- Chiffrement asymétrique : algorithmes de cryptages *plus complexes*, donc plus lent, mais communication sans échange préalable de clé

Comparaison symétrique/asymétrique

- Chiffrement symétrique : chiffrement *plus rapide*, mais nécessite de se "rencontrer" pour pourvoir s'échanger la clé commune
- Chiffrement asymétrique : algorithmes de cryptages *plus complexes*, donc plus lent, mais communication sans échange préalable de clé

$\Rightarrow$ **En pratique, sur internet, *mélange des 2* :**

1. D'abord le chiffrement *asymétrique* pour s'échanger une **clé commune**
2. Puis chiffrement *symétrique* à l'aide de la clé commune échangée pour communiquer **plus rapidement**

Plan

1 Introduction

2 La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique

3 Protocole d'authentification sur internet

4 Vers la recherche

Pourquoi s'authentifier ?

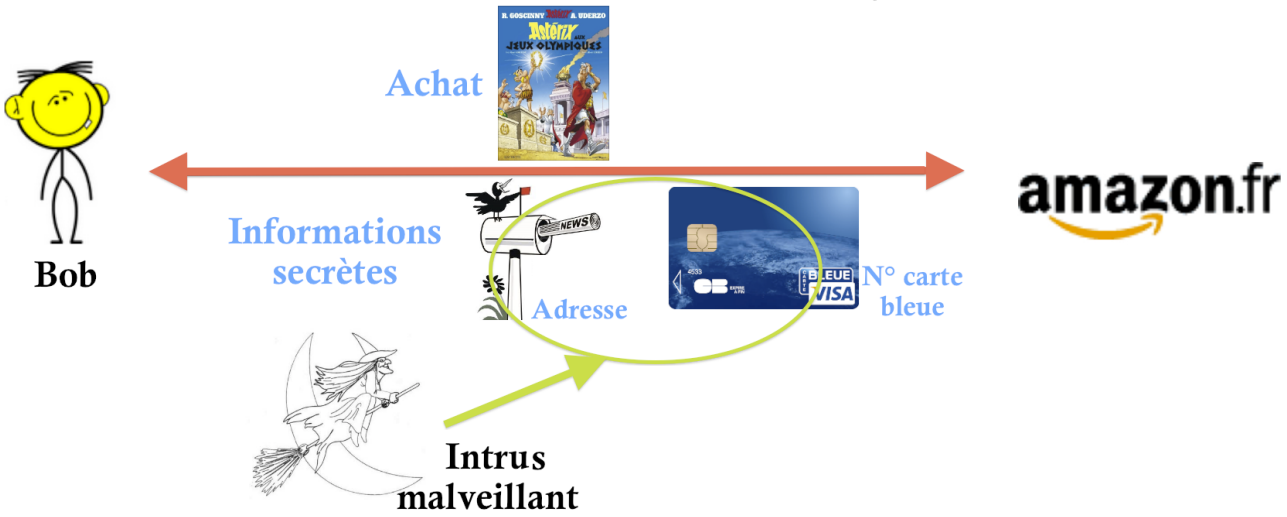
Pour communiquer avec un site internet (ex : Amazon) de manière sécurisée, il faut **s'authentifier**.

Bob veut acheter une BD sur amazon.fr ⇒ partage d'informations **privées** avec Amazon.

Pourquoi s'authentifier ?

Pour communiquer avec un site internet (ex : Amazon) de manière sécurisée, il faut **s'authentifier**.

Bob veut acheter une BD sur amazon.fr ⇒ partage d'informations **privées** avec Amazon.



Pour que personne n'accède à ces *informations secrètes*, il faut que Bob et Amazon communiquent de manière **sécurisée**.

⇒ Il faut d'abord **s'authentifier** = donner son *identité*, pour être sûr de communiquer avec la **bonne personne** !

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$, avec K_{BA} la **clé partagée** par Bob et amazon.fr .

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$,
  avec K_{BA} la **clé partagée** par Bob et amazon.fr .

- Ils doivent donc d'abord **s'échanger** cette clé partagée.

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$,
  avec K_{BA} la **clé partagée** par Bob et amazon.fr .

- Ils doivent donc d'abord **s'échanger** cette clé partagée.

- Pour cela, on doit commencer par un chiffrement **asymétrique**.
  $\Rightarrow$ Bob doit donc connaître la clé publique d' amazon.fr .

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$,
  avec K_{BA} la **clé partagée** par Bob et amazon.fr .

- Ils doivent donc d'abord **s'échanger** cette clé partagée.

- Pour cela, on doit commencer par un chiffrement **asymétrique**.
  $\Rightarrow$ Bob doit donc connaître la clé publique d' amazon.fr .

- **Problème :** comment obtenir cette clé et être sûr que c'est la bonne ?
  $\Rightarrow$ Bob doit être sûr qu'il communique bien avec amazon.fr .

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$,
  avec K_{BA} la **clé partagée** par Bob et amazon.fr .

- Ils doivent donc d'abord **s'échanger** cette clé partagée.

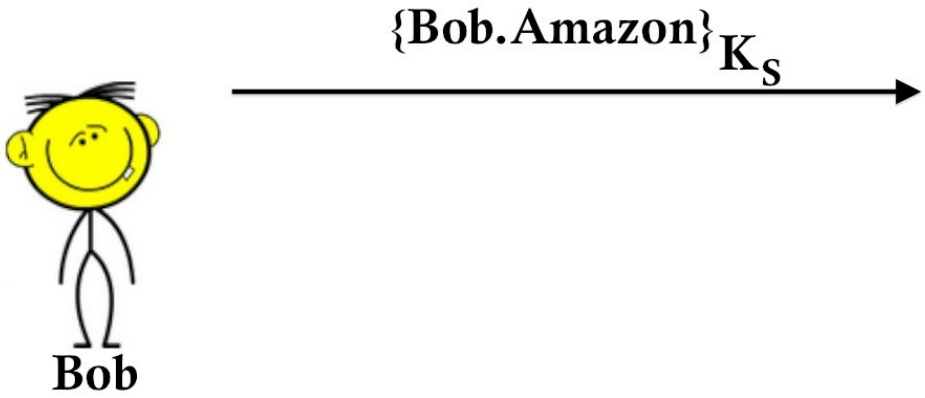
- Pour cela, on doit commencer par un chiffrement **asymétrique**.
  $\Rightarrow$ Bob doit donc connaître la clé publique d' amazon.fr .

- **Problème :** comment obtenir cette clé et être sûr que c'est la bonne ?
  $\Rightarrow$ Bob doit être sûr qu'il communique bien avec amazon.fr .

Pour cela : **serveurs de certificats**.
Serveurs spéciaux dont la **clé publique est intégrée au navigateurs web**, et qui permettent de *garantir l'identité* des 2 individus.

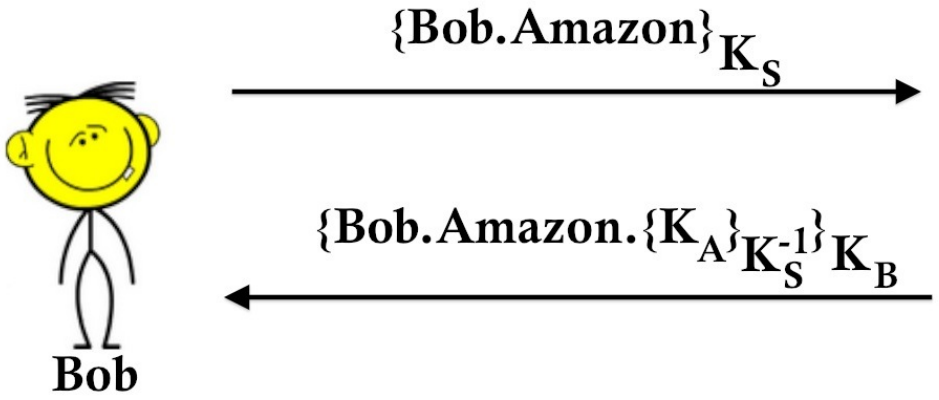
On connait donc la clé publique du serveur de certificat (K_S), et on lui demande de nous donner la clé publique d'Amazon (K_A).

Obtention de la clé publique



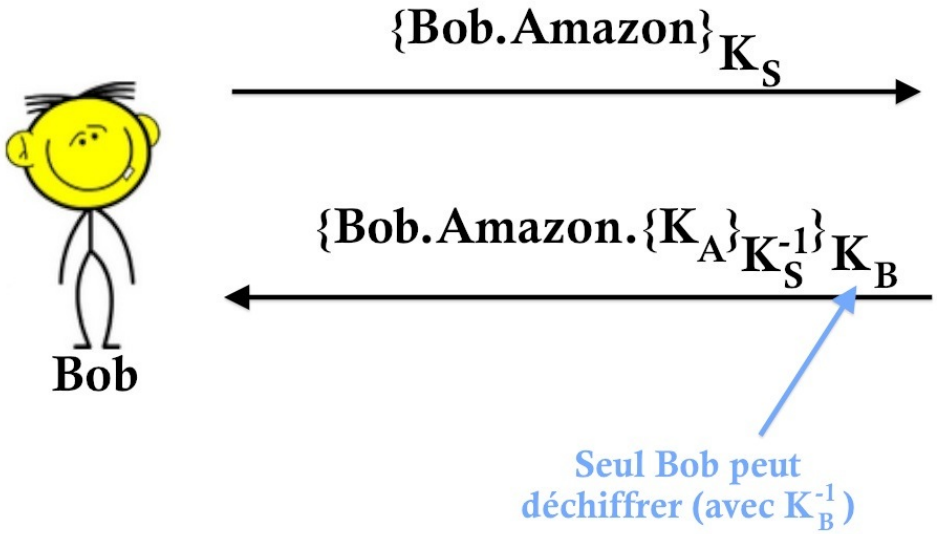
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus

Obtention de la clé publique



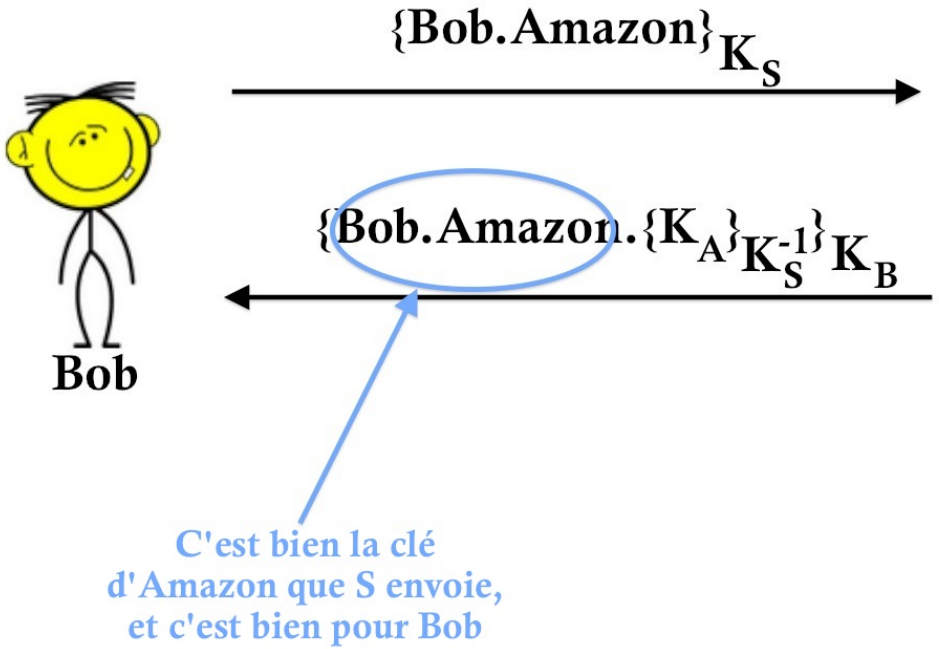
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus

Obtention de la clé publique



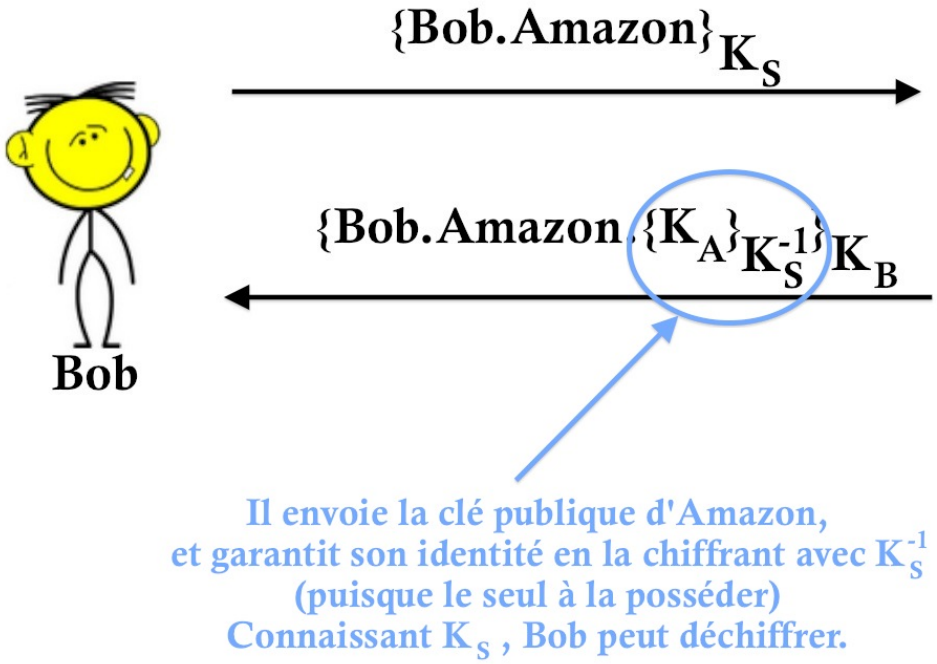
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus

Obtention de la clé publique



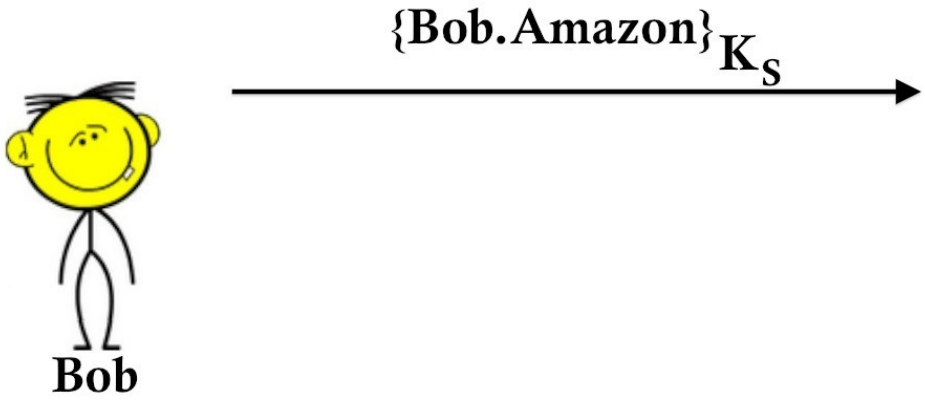
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus

Obtention de la clé publique

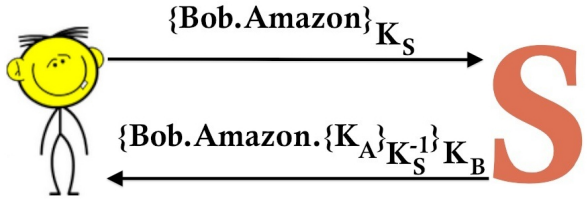


K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus

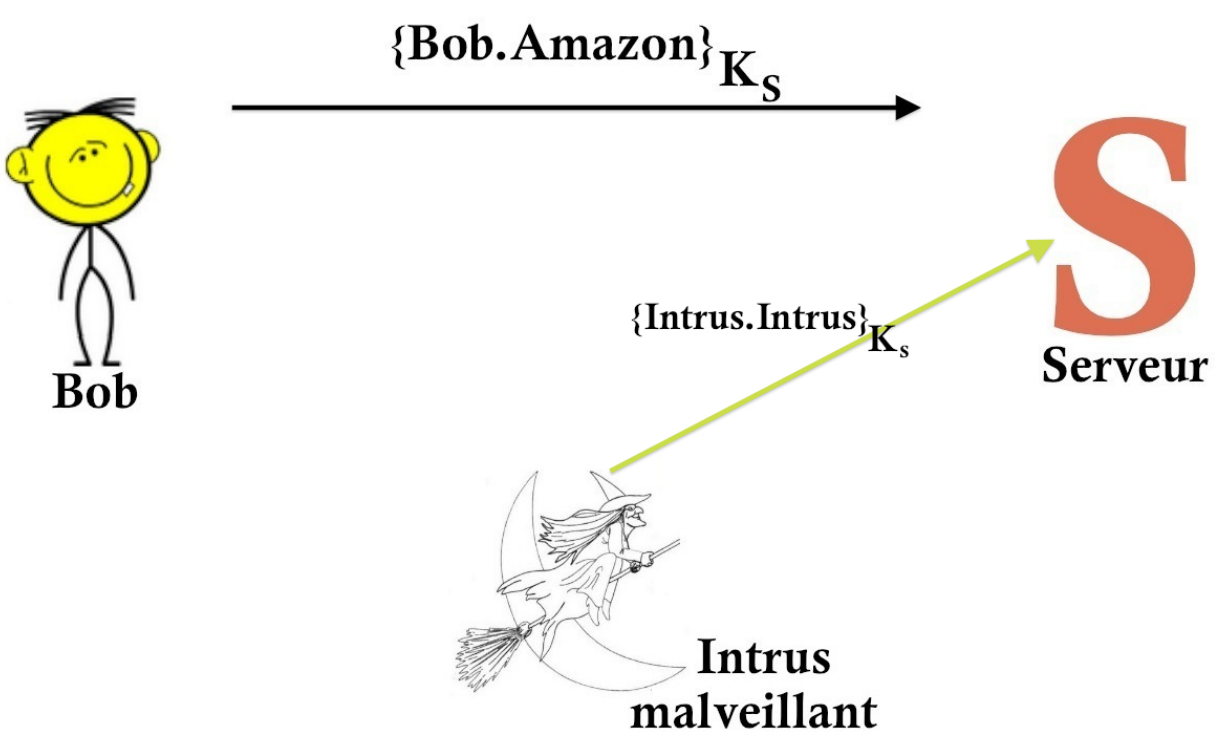
Obtention de la clé publique



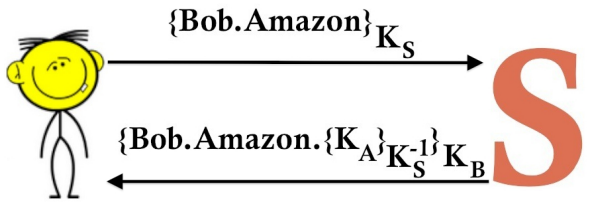
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



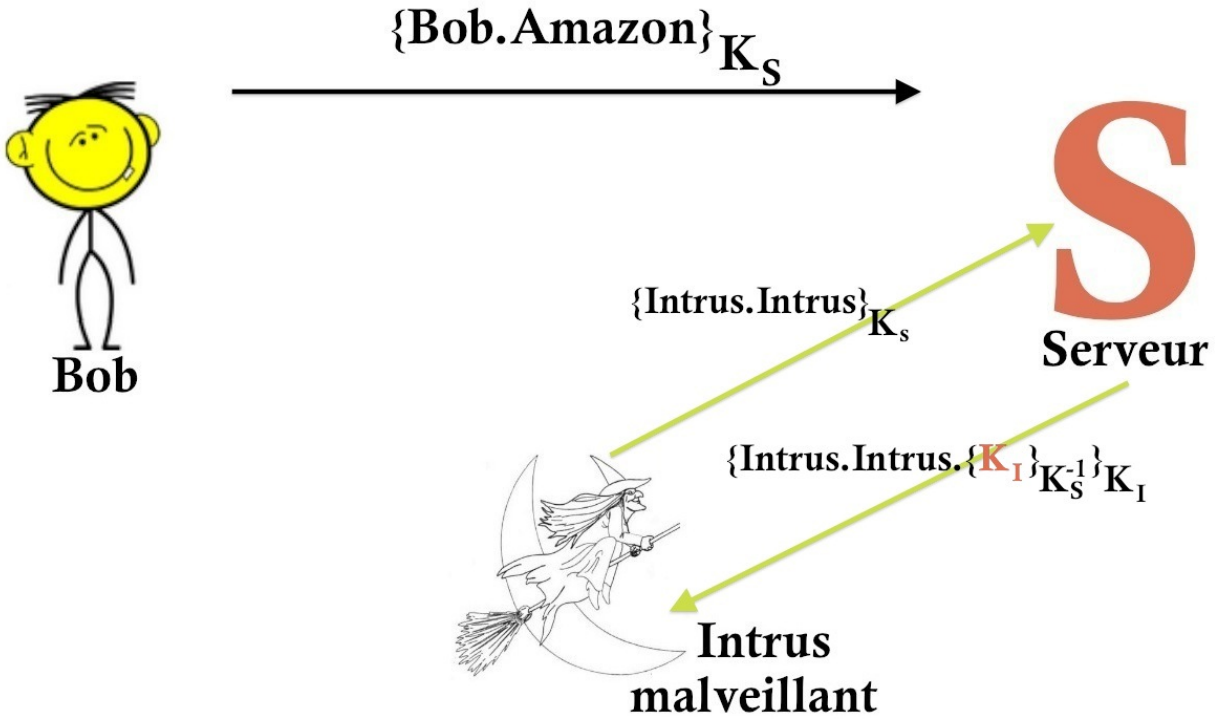
Obtention de la clé publique



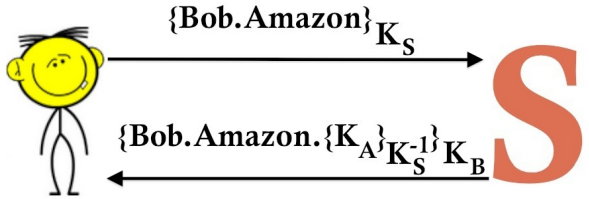
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



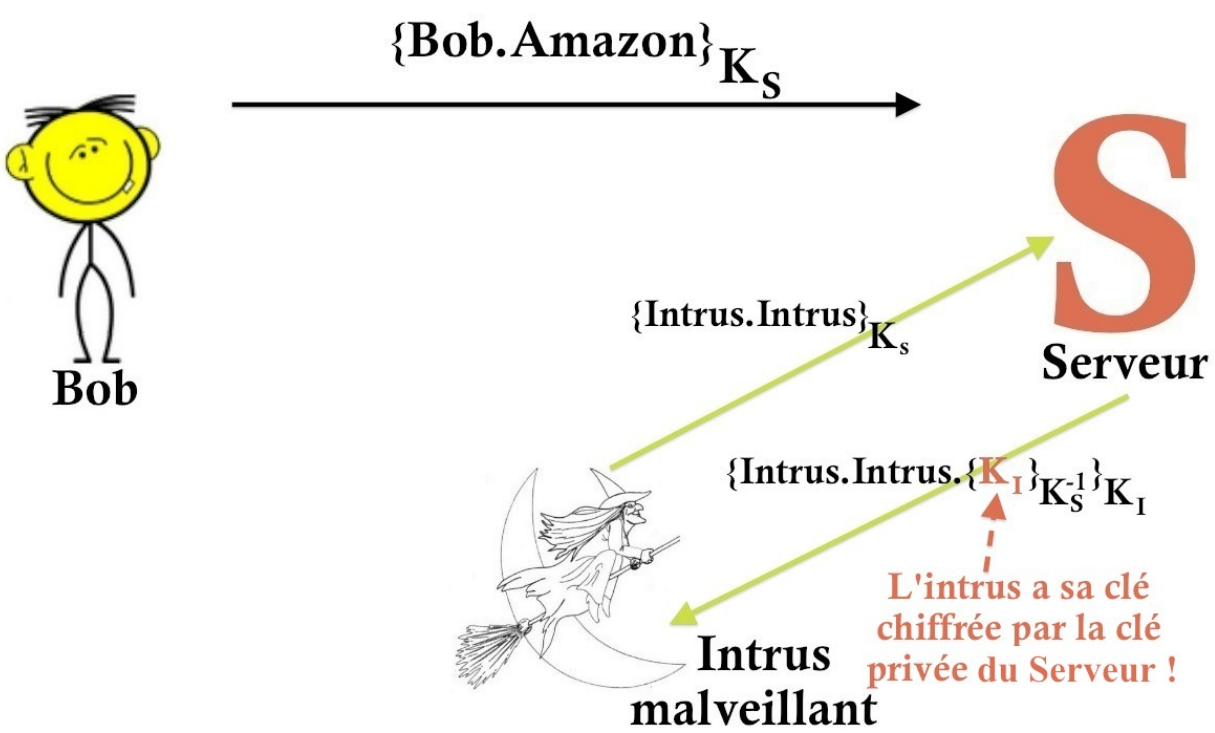
Obtention de la clé publique



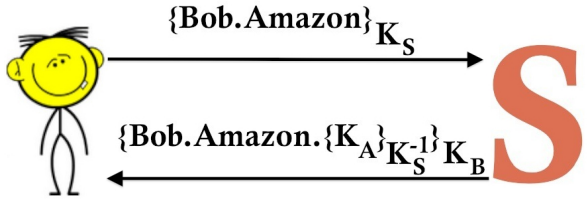
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



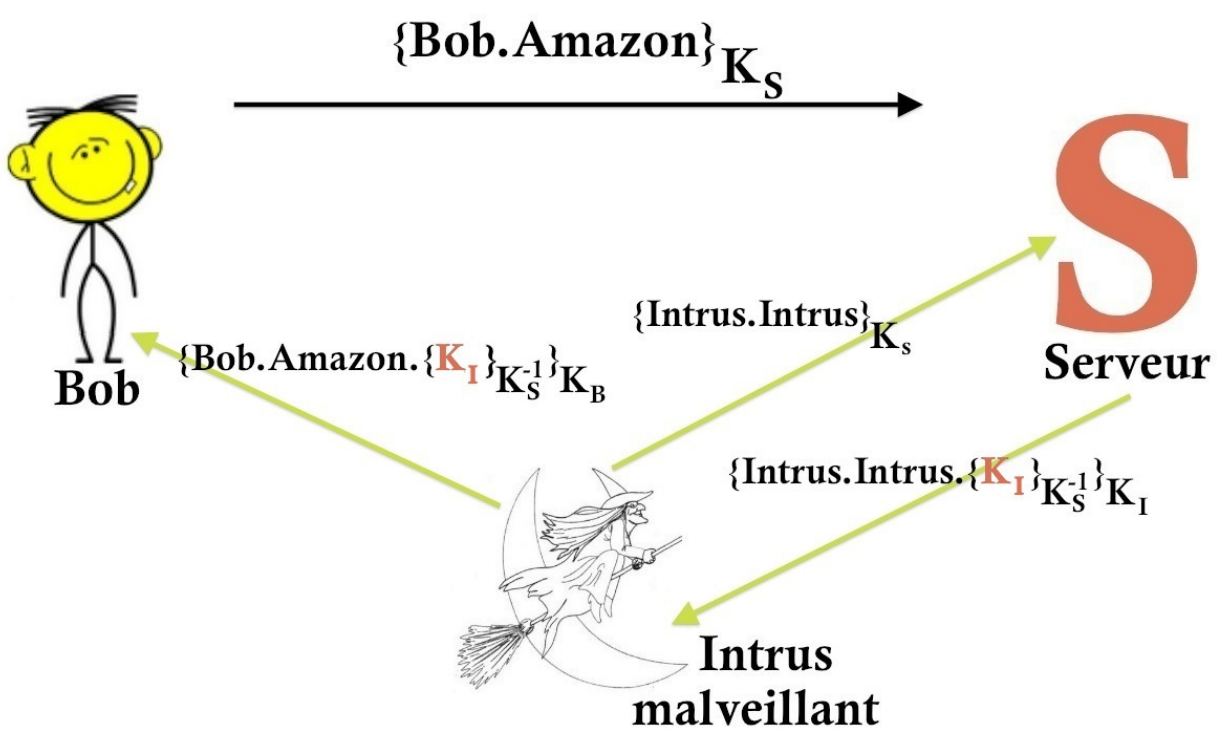
Obtention de la clé publique



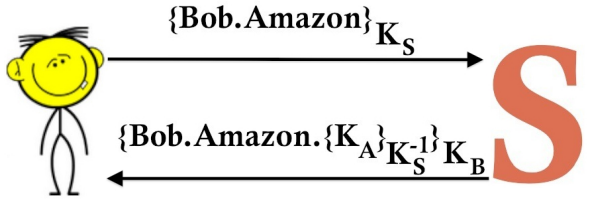
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



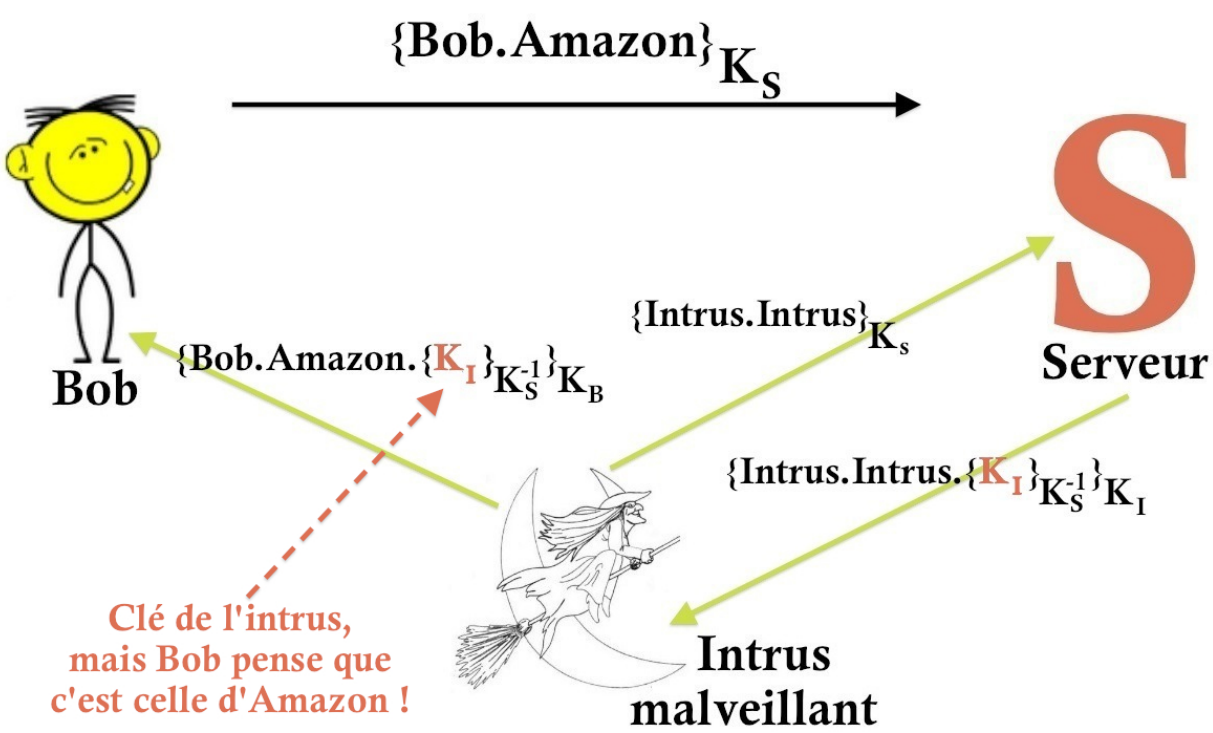
Obtention de la clé publique



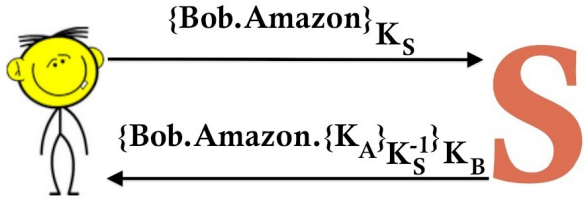
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



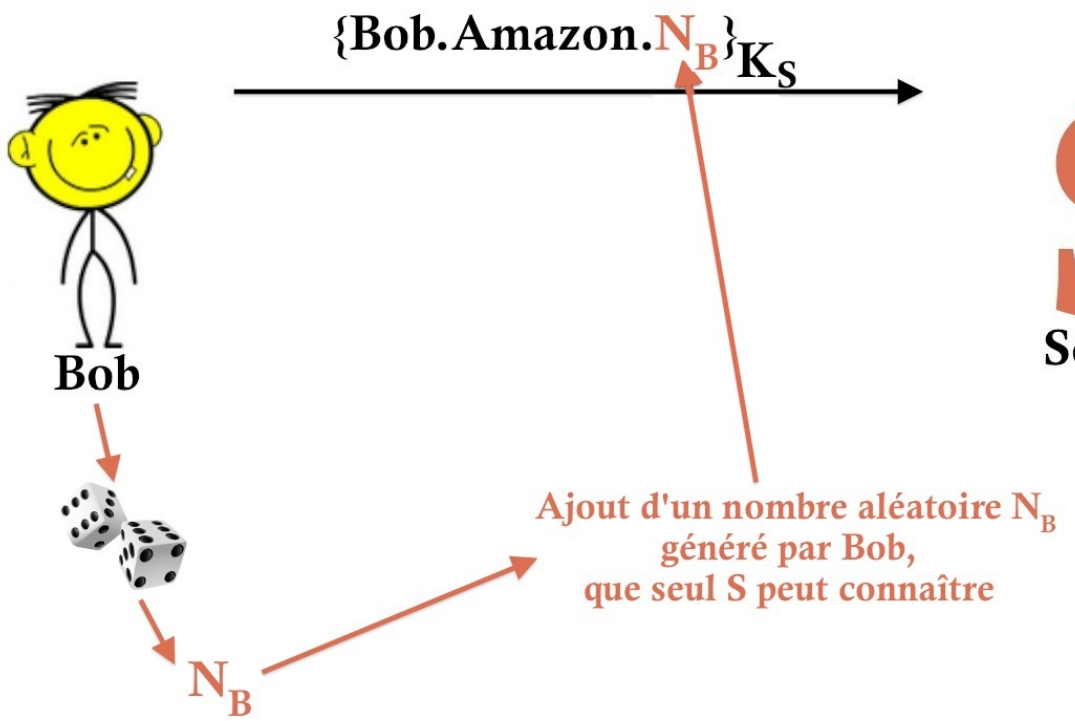
Obtention de la clé publique



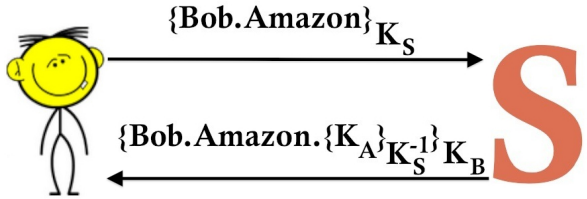
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



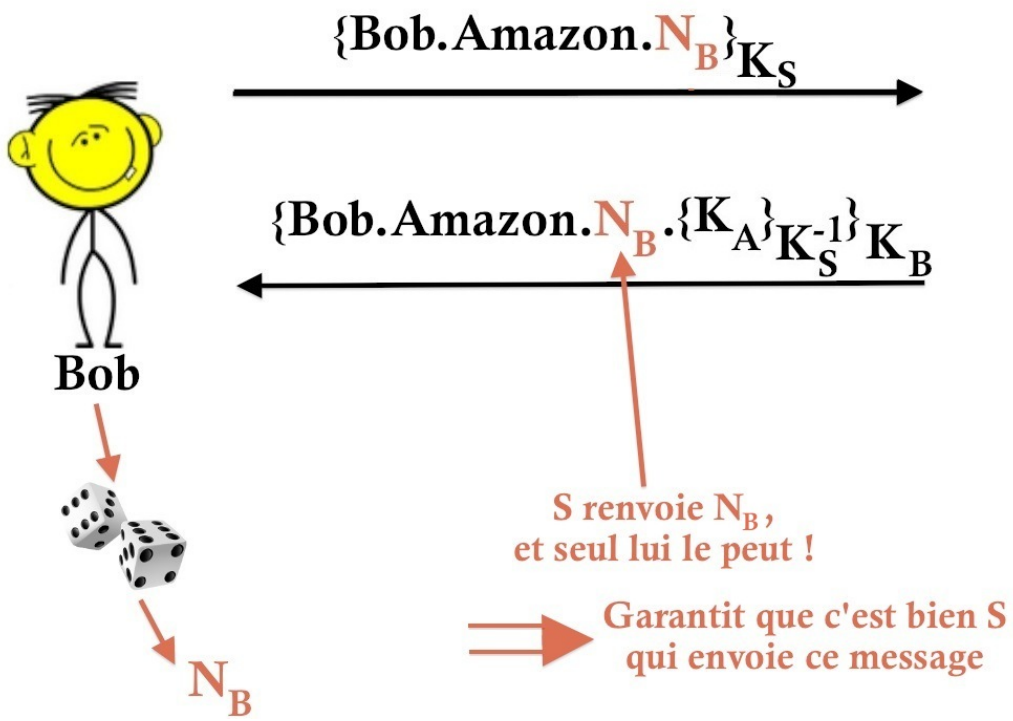
Obtention de la clé publique



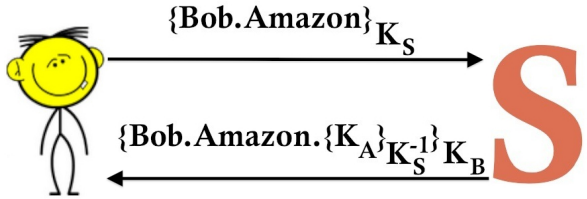
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



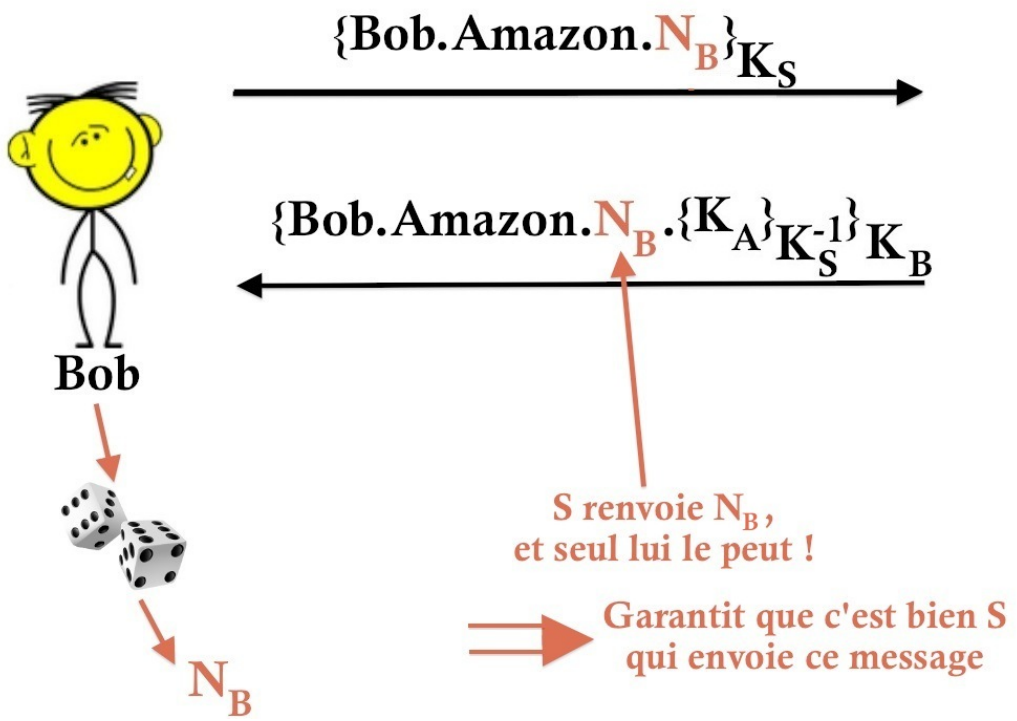
Obtention de la clé publique



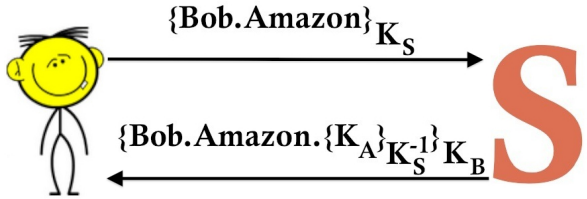
K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



Obtention de la clé publique



K_B : clé publique de Bob
K_B^{-1} : clé privée de Bob
K_S : clé publique du serveur de certificats
K_S^{-1} : clé privée du serveur de certificats
K_A : clé publique d'Amazon
K_I : clé publique de l'intrus



⇒ L'identité d'Amazon est **certifiée**, Bob peut s'authentifier en toute sécurité
⇒ **certificat** créé, K_A enregistré, pour ne pas avoir à recommencer la procédure lors de la prochaine authentification.

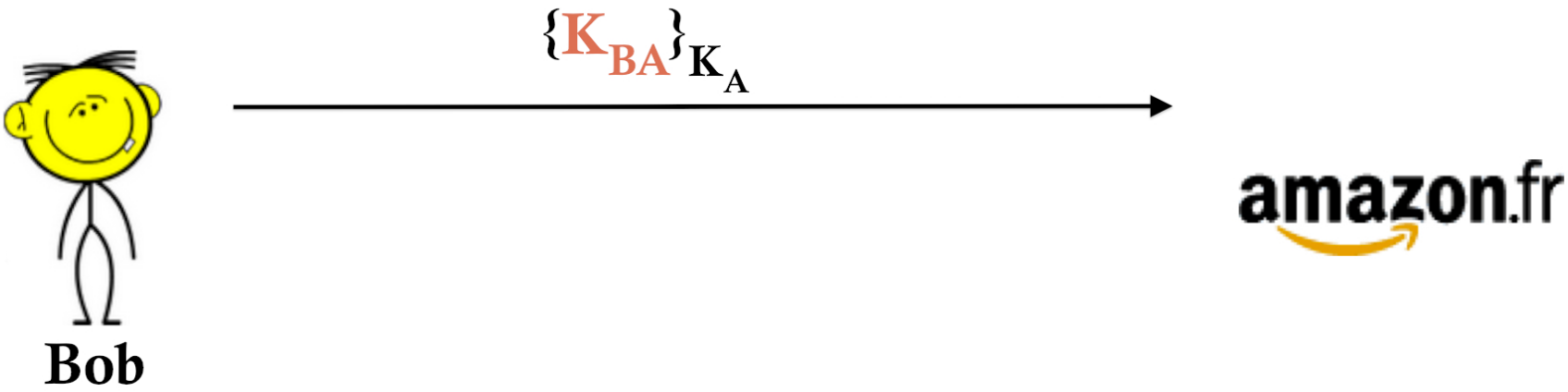
Authentification sur internet

Maintenant que Bob est sûr d'avoir la clé publique d' amazon.fr (K_A), il peut :

Authentification sur internet

Maintenant que Bob est sûr d'avoir la clé publique d' amazon.fr (K_A), il peut :

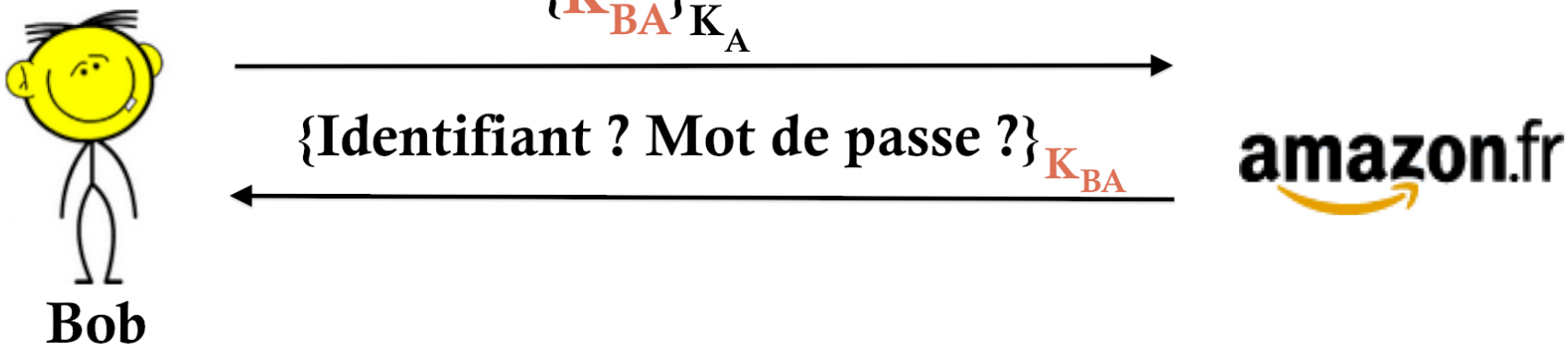
1. Lui envoyer une *clé partagée* K_{BA} qui sera connue d'**eux seuls**.



Authentification sur internet

Maintenant que Bob est sûr d'avoir la clé publique d' amazon.fr (K_A), il peut :

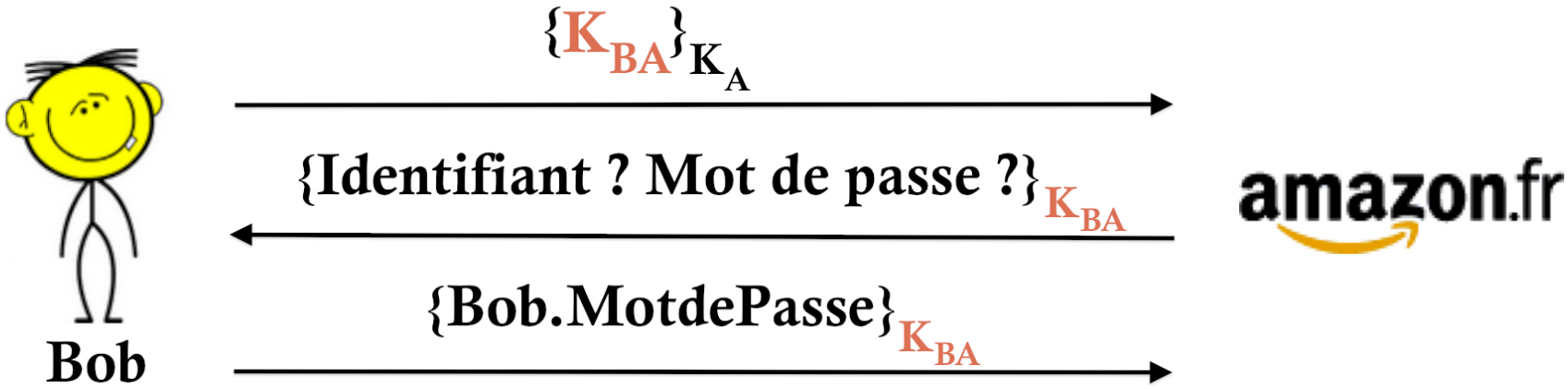
1. Lui envoyer une *clé partagée* K_{BA} qui sera connue d'**eux seuls**.
2. S'authentifier en toute sécurité, après demande d' amazon.fr .



Authentification sur internet

Maintenant que Bob est sûr d'avoir la clé publique d' amazon.fr (K_A), il peut :

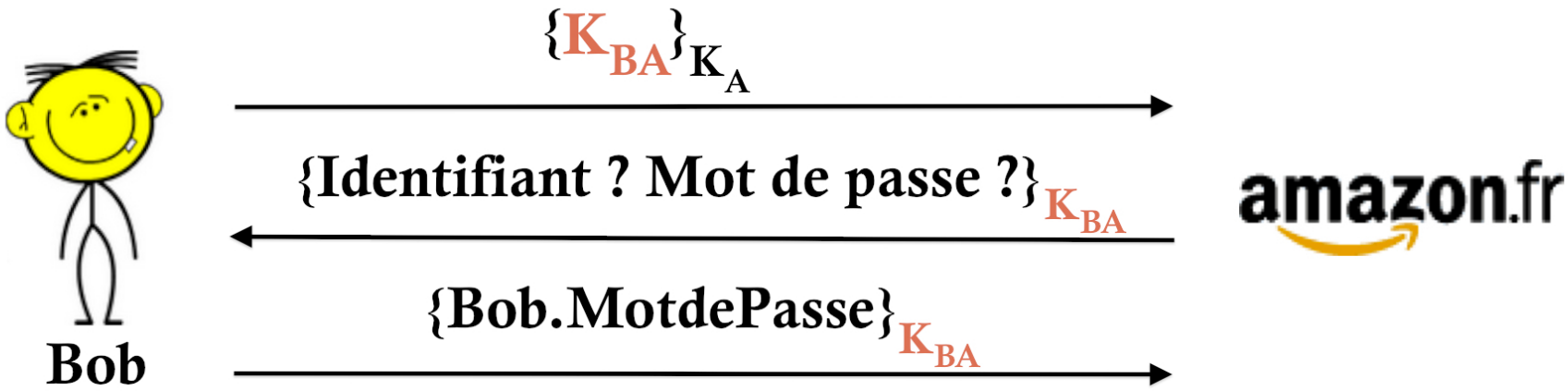
1. Lui envoyer une *clé partagée* K_{BA} qui sera connue d'**eux seuls**.
2. S'authentifier en toute sécurité, après demande d' amazon.fr .



Authentification sur internet

Maintenant que Bob est sûr d'avoir la clé publique d'amazon.fr (K_A), il peut :

1. Lui envoyer une *clé partagée* K_{BA} qui sera connue d'**eux seuls**.
2. S'authentifier en toute sécurité, après demande d'amazon.fr .



Maintenant qu'amazon.fr a bien authentifié Bob, ils peuvent **communiquer en toute sécurité**, en utilisant leur *clé partagée* K_{BA}, pour acheter une BD par exemple !

Pour résumer

1. On commence avec un chiffrement **asymétrique** pour permettre une *première* communication

Pour résumer

1. On commence avec un chiffrement **asymétrique** pour permettre une *première* communication
2. Le *serveur de certificat* **garantit** à Bob qu'il communique avec la bonne personne
   $\Rightarrow$ qu'on a la bonne clé publique (K_A pour Amazon), en la **signant** avec sa clé privée K_S^{-1}

Pour résumer

1. On commence avec un chiffrement **asymétrique** pour permettre une *première* communication
2. Le *serveur de certificat* **garantit** à Bob qu'il communique avec la bonne personne
   $\Rightarrow$ qu'on a la bonne clé publique (K_A pour Amazon), en la **signant** avec sa clé privée K_S^{-1}
3. Bob envoie une *clé partagée secrète* (K_{BA}) à Amazon pour pouvoir s'**authentifier** et **communiquer en toute sécurité**, et de manière efficace.

Pour résumer

1. On commence avec un chiffrement **asymétrique** pour permettre une *première* communication
2. Le *serveur de certificat* **garantit** à Bob qu'il communique avec la bonne personne
   $\Rightarrow$ qu'on a la bonne clé publique (K_A pour Amazon), en la **signant** avec sa clé privée K_S^{-1}
3. Bob envoie une *clé partagée secrète* (K_{BA}) à Amazon pour pouvoir s'**authentifier** et **communiquer en toute sécurité**, et de manière efficace.

Fonctionnement du protocole **SSL** (Secure Sockets Layers), maintenant appelé **TLS** (Transport Layer Security)
$\longrightarrow$ Protocole de sécurité le *plus utilisé* sur internet.

Pour résumer

1. On commence avec un chiffrement **asymétrique** pour permettre une *première* communication
2. Le *serveur de certificat* **garantit** à Bob qu'il communique avec la bonne personne
   $\Rightarrow$ qu'on a la bonne clé publique (K_A pour Amazon), en la **signant** avec sa clé privée K_S^{-1}
3. Bob envoie une *clé partagée secrète* (K_{BA}) à Amazon pour pouvoir s'**authentifier** et **communiquer en toute sécurité**, et de manière efficace.

Fonctionnement du protocole **SSL** (Secure Sockets Layers), maintenant appelé **TLS** (Transport Layer Security)
$\longrightarrow$ Protocole de sécurité le *plus utilisé* sur internet.

Un site sécurisé par SSL possède une adresse URL commençant par **https ://**
("s" pour "sécurisé")

Plan

1 Introduction

2 La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique

3 Protocole d'authentification sur internet

4 Vers la recherche

Et la recherche là-dedans ?

- Les protocoles peuvent être **attaqués**
  $\Rightarrow$ Trouver des outils efficaces permettant de vérifier la **fiabilité** des protocoles et trouver leurs failles.

  Faille du protocole **NSPK** (**N**eeedham-**S**hroëder **P**ublic **K**ey : protocole important d'authentification entre 2 membres d'un même réseau) découverte *en 1995* par *Gavin Lowe*.

- Trouver de nouveaux protocoles *plus sûrs*
  Attention ! Cryptographie parfaite $\not\Rightarrow$ protocole infaillible

- L'algorithme de cryptage du message peut aussi être cassé
  $\Rightarrow$ Trouver de nouvelles méthodes cryptographiques plus sûres (plus longues à casser).

Questions

Merci de votre attention.