Sécurisation des communications

Vocabulaire

- La cryptographie est l'étude des méthodes permet de sécuriser une communication.

Sécurisation des communications

Vocabulaire

- La cryptographie est l'étude des méthodes permet de sécuriser une communication.
- Le chiffrement d'un message est sa transformation en un une suite de caractère incompréhensible (dit *texte chiffré*).

Sécurisation des communications

Vocabulaire

- La cryptographie est l'étude des méthodes permet de sécuriser une communication.
- Le chiffrement d'un message est sa transformation en un une suite de caractère incompréhensible (dit *texte chiffré*).
- Le chiffrement s'effectue via un algorithme nécessitant un paramètre appelé clé de chiffrement. Et de même le déchiffrement nécessite une clé de déchiffrement

Sécurisation des communications

Vocabulaire

- La cryptographie est l'étude des méthodes permet de sécuriser une communication.
- Le chiffrement d'un message est sa transformation en un une suite de caractère incompréhensible (dit *texte chiffré*).
- Le chiffrement s'effectue via un algorithme nécessitant un paramètre appelé clé de chiffrement. Et de même le déchiffrement nécessite une clé de déchiffrement
- Lorsque la connaissance de ces deux clés doit rester secrète on dit qu'il s'agit d'un chiffrement symétrique.

Sécurisation des communications

Vocabulaire

- La cryptographie est l'étude des méthodes permet de sécuriser une communication.
- Le chiffrement d'un message est sa transformation en un une suite de caractère incompréhensible (dit *texte chiffré*).
- Le chiffrement s'effectue via un algorithme nécessitant un paramètre appelé clé de chiffrement. Et de même le déchiffrement nécessite une clé de déchiffrement
- Lorsque la connaissance de ces deux clés doit rester secrète on dit qu'il s'agit d'un chiffrement symétrique.
- Lorsque la clé de chiffrement peut être connu de tous (on parle alors de clé public) et que seul la clé de déchiffrement reste secrète (on parle alors de clé privé), on dit qu'il s'agit d'un chiffrement asymétrique.

Sécurisation des communications

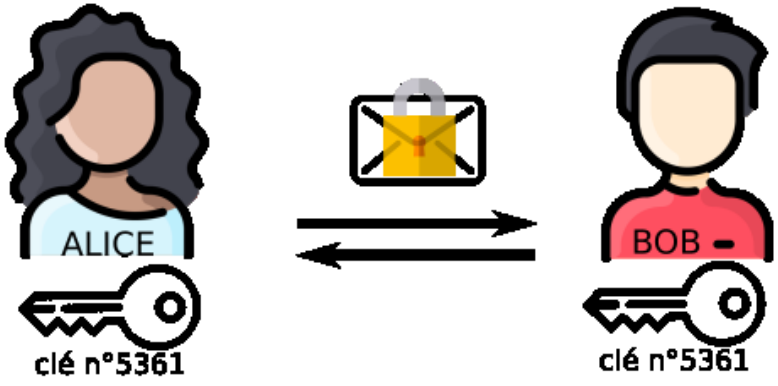
Représentation du chiffrement symétrique

Étape 1

Alice et Bob s'échangent de manière secrète une clé dont ils possèderont chacun un exemplaire.

Étape 2

Alice et Bob chiffrent et déchiffrent leurs messages avec cette clé identique.



Sécurisation des communications

Représentation du chiffrement asymétrique

Sécurisation des communications

Exemples

- Le code de César est l'un des premiers exemples historique :

Sécurisation des communications

Exemples

- Le code de César est l'un des premiers exemples historique :
  - La clé de chiffrement est un entier note C, par exemple 3.

Sécurisation des communications

Exemples

- Le code de César est l'un des premiers exemples historique :
  - La clé de chiffrement est un entier note c, par exemple 3.
  - L'algorithme de chiffrement consiste alors à décaler chaque lettre de c emplacements à droite dans l'alphabet. Avec une clé de 3, le message "NSI", se transforme en "QVL".

Sécurisation des communications

Exemples

- Le code de César est l'un des premiers exemples historique :
  - La clé de chiffrement est un entier note c, par exemple 3.
  - L'algorithme de chiffrement consiste alors à décaler chaque lettre de c emplacements à droite dans l'alphabet. Avec une clé de 3, le message "NSI", se transforme en "QVL".
  - Pour déchiffrer on décale de c emplacements à gauche.

Sécurisation des communications

Exemples

- Le code de César est l'un des premiers exemples historique :
  - La clé de chiffrement est un entier note c, par exemple 3.
  - L'algorithme de chiffrement consiste alors à décaler chaque lettre de c emplacements à droite dans l'alphabet. Avec une clé de 3, le message "NSI", se transforme en "QVL".
  - Pour déchiffrer on décale de c emplacements à gauche.
  - La connaissance des deux clés doit rester secrète, c'est donc un chiffrement symétrique.

Sécurisation des communications

Exemples

1. Le code de César est l'un des premiers exemples historique :
   - La clé de chiffrement est un entier note c, par exemple 3.
   - L'algorithme de chiffrement consiste alors à décaler chaque lettre de c emplacements à droite dans l'alphabet. Avec une clé de 3, le message "NSI", se transforme en "QVL".
   - Pour déchiffrer on décale de c emplacements à gauche.
   - La connaissance des deux clés doit rester secrète, c'est donc un chiffrement symétrique.
2. Parmi les méthodes modernes (et bien plus robustes) de chiffrement symétrique, on peut citer : AES (Advanced Encryption Standard) ou encore Chacha20.

Sécurisation des communications

Exemples

1. Le code de César est l'un des premiers exemples historique :
   - La clé de chiffrement est un entier note c, par exemple 3.
   - L'algorithme de chiffrement consiste alors à décaler chaque lettre de c emplacements à droite dans l'alphabet. Avec une clé de 3, le message "NSI", se transforme en "QVL".
   - Pour déchiffrer on décale de c emplacements à gauche.
   - La connaissance des deux clés doit rester secrète, c'est donc un chiffrement symétrique.
2. Parmi les méthodes modernes (et bien plus robustes) de chiffrement symétrique, on peut citer : AES (Advanced Encryption Standard) ou encore Chacha20.
3. L'exemple classique de chiffrement asymétrique est RSA (voir activité.)

Sécurisation des communications

Avantages et inconvénients des deux méthodes

- Un chiffrement symétrique est souvent rapide et donc adapté au transfert d'un volume important d'informations.

Sécurisation des communications

Avantages et inconvénients des deux méthodes

- Un chiffrement symétrique est souvent rapide et donc adapté au transfert d'un volume important d'informations.
- Un chiffrement symétrique peut-être très sûr (voire inviolable).

Sécurisation des communications

Avantages et inconvénients des deux méthodes

- Un chiffrement symétrique est souvent rapide et donc adapté au transfert d'un volume important d'informations.
- Un chiffrement symétrique peut-être très sûr (voire inviolable).
  Par exemple, un chiffrement `xor` utilisant un masque aussi long que le message est inviolable
- L'inconvénient est que puisque le canal de transmission n'est pas sûr, les deux interlocuteurs doivent convenir au préalable d'une clé de chiffrement.

Sécurisation des communications

Avantages et inconvénients des deux méthodes

- Un chiffrement symétrique est souvent rapide et donc adapté au transfert d'un volume important d'informations.
- Un chiffrement symétrique peut-être très sûr (voire inviolable).
  Par exemple, un chiffrement `xor` utilisant un masque aussi long que le message est inviolable
- L'inconvénient est que puisque le canal de transmission n'est pas sûr, les deux interlocuteurs doivent convenir au préalable d'une clé de chiffrement.
- Dans un chiffrement asymétrique par contre, la clé de chiffrement peut être connue de tous car elle ne permet pas de déchiffrer. Elle peut donc être rendue publique sans mettre en danger la sécurité de la communication.

Sécurisation des communications

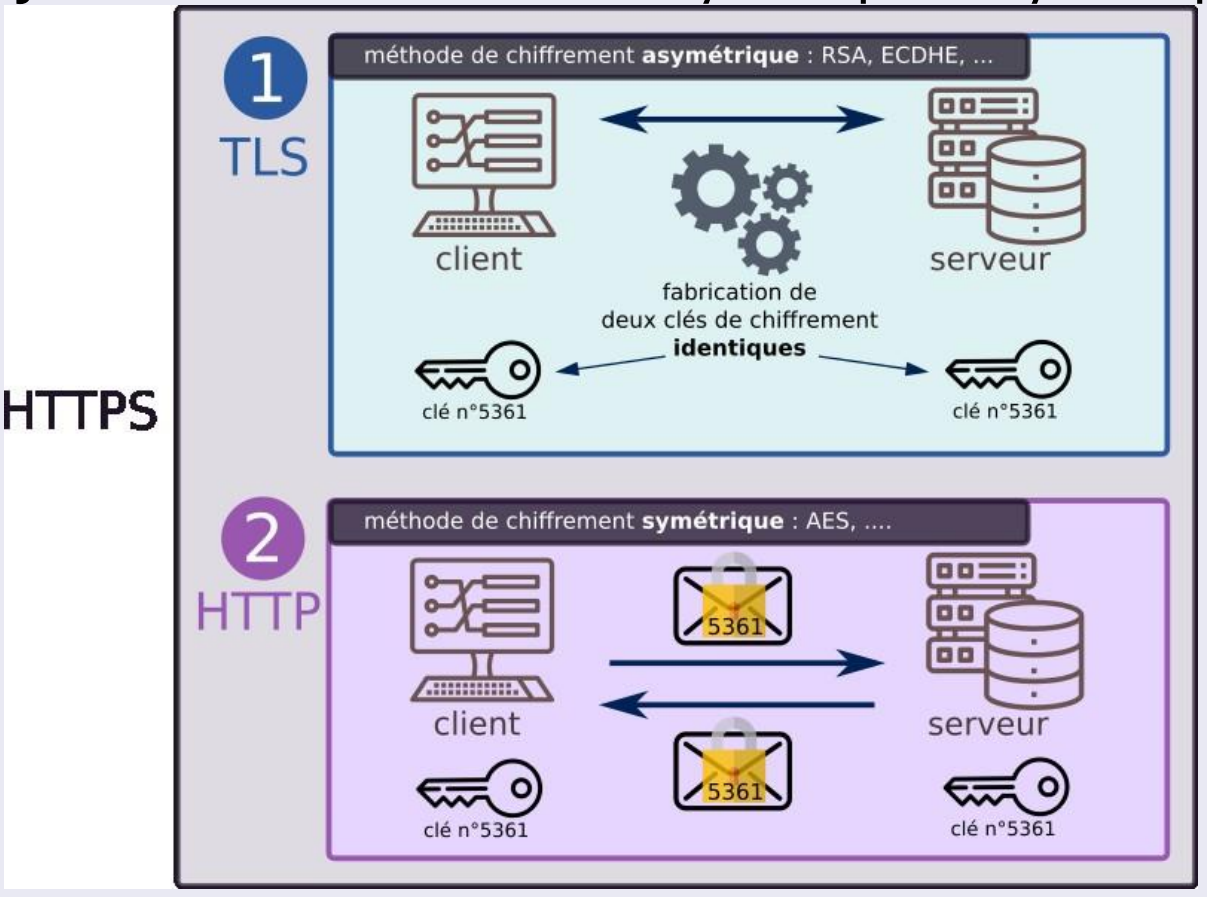
Avantages et inconvénients des deux méthodes

- Un chiffrement symétrique est souvent rapide et donc adapté au transfert d'un volume important d'informations.
- Un chiffrement symétrique peut-être très sûr (voire inviolable).
  Par exemple, un chiffrement `xor` utilisant un masque aussi long que le message est inviolable
- L'inconvénient est que puisque le canal de transmission n'est pas sûr, les deux interlocuteurs doivent convenir au préalable d'une clé de chiffrement.
- Dans un chiffrement asymétrique par contre, la clé de chiffrement peut être connue de tous car elle ne permet pas de déchiffrer. Elle peut donc être rendue publique sans mettre en danger la sécurité de la communication.
- Par contre, un chiffrement asymétrique peut être gourmand en ressource et donc non adapté à un volume important d'informations.

Sécurisation des communications

Protocole `https`

Le protocole `https` qui permet de sécuriser les transmissions est un exemple d'utilisation conjointe des deux méthodes : asymétrique et symétrique.



Sécurisation des communications

Autorité de certification

D'autre part, afin d'éviter une attaque du type *homme du milieu* une autorité extérieure garanti l'identité du serveur.