Dis maman (ou papa), comment on cache des secrets dans le monde numérique ?

Aurélien Alvarez, Thierry Viéville

17 janvier 2014 **1 commentaire — commenter cet article**

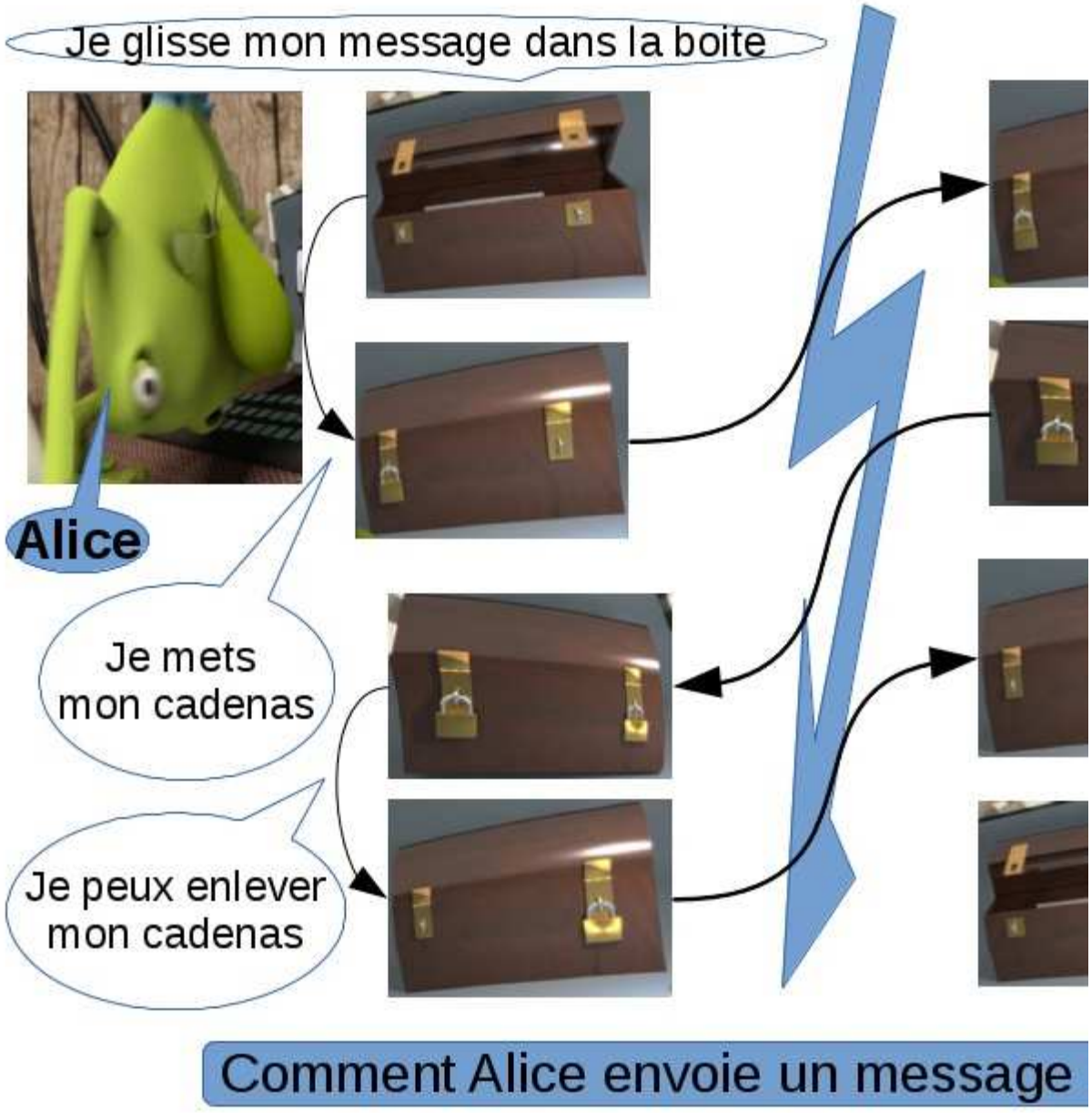
Objet du mois

Dis maman (ou papa), comment on cache des secrets dans le monde numérique ?

Aurélien Alvarez et **Thierry Viéville**

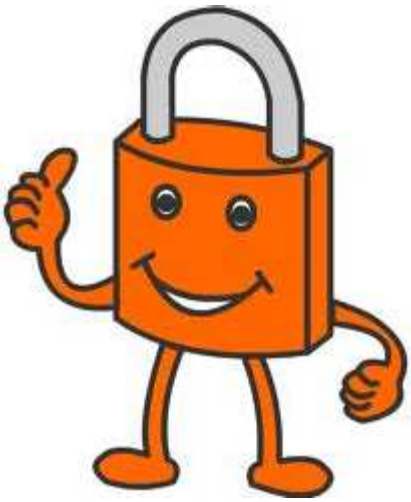
Échanger des informations secrètes sur Internet pose un problème très particulier : il faut que deux personnes, qui ne se connaissent peut-être pas, qui ne peuvent communiquer que publiquement devant tout le monde, donc sans s'envoyer aucune information privée, puissent tout de même s'envoyer un message secret qu'elles seules pourront lire. En étant sûres que personne n'ait volé leur identité.

Une telle solution existe. C'est le cryptage à double clé. Il est très important de comprendre **comment cela marche**, sinon ces mécanismes resteront mystérieux, magiques, au lieu de pouvoir être vus comme des actes du quotidien. Voici très simplement comment il fonctionne :

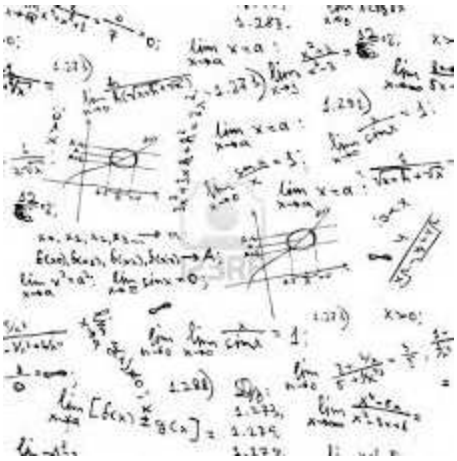


On glisse le message dans une boite, avec un cadenas pour l'émetteur, et un pour le récepteur. L'émetteur s'appelle souvent Alice et le récepteur Bob, **Alice et Bob** quoi ! Grâce au mouvement de va-et-vient, la boite va toujours circuler fermée pour que personne ne puisse y regarder. Chacun garde précieusement la clé du cadenas et les cadenas restent toujours fermés lors du transport, pour que personne ne puisse voler son contenu.

Il est facile de voir que cette solution marche bien. Il est moins facile, mais c'est bien le cas, de réaliser que c'est la solution la plus simple pour faire circuler de l'information entre deux personnes qui restent à distance et ne disposent que d'un cadenas chacune.



Bien entendu, dans le monde numérique, ce qui tient lieu de « cadenas », c'est un calcul qui va prendre le *message initial* et le mélanger avec une formule mathématique pour en faire un *message crypté*. De ce calcul, seul l'émetteur du message a la clé (c'est-à-dire le code pour réaliser le calcul à l'envers afin de retrouver le message initial). Ici on voit que chacun applique son calcul de mélange, puis de démêlage. On note aussi que, pour que ça marche, il faut pouvoir intervertir les deux calculs puisque le démêlage par l'émetteur se fait sur le message mélangé par le récepteur. [1]



Le message est crypté par une certaine formule... pas magique mais quasiment impossible à deviner si on ne la connaît pas !

On note aussi qu'il faut que les personnes soient bien identifiées. Car si un personnage malveillant se fait passer pour Bob au début de l'échange, alors il volera le message d'Alice, de manière tout à fait sécurisée ! Mais commençons par jouer, nous reparlons de cela plus tard même si **Le Chat**, fin mathématicien, a depuis bien longtemps réfléchi à ce dernier petit problème...

Mais comment expliquer cela à nos enfants ?

Il est évidemment très facile de monter cette activité avec une boite quelconque et de vrais cadenas, ou des post-it avec les cadenas dessinés dessus et d'autres post-it qui symbolisent les clés qui ouvrent les cadenas (on pourra symboliser le cadenas par un demi-dessin d'un symbole et la clé par l'autre moitié du dessin).

Selon la pédagogie et le niveau de participation des enfants on pourra, soit mettre en place le jeu de manière complètement dirigée, soit leur faire construire eux-mêmes le jeu à partir du dessin ci-dessus (le premier de l'article, pas celui du Chat !). Le levier pourra être : « As-tu compris ? Oui ? Alors réexplique à quelqu'un de plus petit que toi en le faisant jouer ». Dès 6 à 8 ans, l'enfant est un « grand » qui sait expliquer aux tout petits. Et puis dès qu'on a compris, on a toutes et tous envie de le réexpliquer !

Il est possible de faire l'activité avec des chiffres, après avoir utilisé les cadenas. On pourra proposer de jouer avec

des chiffres dans un monde où personne ne sait faire de division : la clé secrète sera **2** et la clé publique sera **5**. Alice publiera sa clé publique **5** et demandera à Bob de crypter [**2**] un chiffre secret entre 2 et 9 (disons 3) en le multipliant par **5** (donc 3 x **5** = 15). Il renvoie le mélange à Alice qui multiplie le nombre par la clé secrète (donc **2** x 15 = 30) et là hop ! le 3 redevient visible à côté du 0. Mais personne dans ce monde ne peut deviner qu'il y avait 3 caché dans 15 puisque personne ne sait faire de division. L'astuce arithmétique est simplissime mais tant mieux, cela permettra à l'enfant de tout comprendre.

Nous allons ensuite jouer à ce jeu « à l'envers » pour non plus crypter un message mais authentifier une personne de manière sûre. Un des joueurs sera « l'autorité » une personne en qui nous avons, toutes et tous, toute confiance. Par exemple, la **NSA**. Humour ;-).

Chaque joueur a un cadenas qu'il va remettre à l'autorité. Celle-ci va bien noter à qui tous les cadenas appartiennent. Ensuite les joueurs vont se cacher sous un masque. Quand, disons Alice, voudra savoir qui est vraiment Bob, alors elle va demander à l'autorité un cadenas qui appartient à Bob, elle va mettre un code dans une boite, qu'elle va fermer par ce cadenas. Seul le vrai Bob, celui qui a la clé, pourra ouvrir le cadenas, donc prouver son identité : *s'authentifier*.

Selon la pédagogie et le niveau de participation des enfants, on pourra pour ce deuxième jeu, soit imposer la règle du jeu avec des petites récompenses à chaque étape passée avec succès, soit poser le problème et laisser le groupe d'enfants chercher une solution qui semble correcte. Au niveau du vocabulaire, on prendra soin de bien expliquer que « codage » et « cryptage » ne sont pas les mêmes mots.

On pourra aussi expliquer que le cadenas est une « clé publique » tandis que la combinaison du cadenas (ou la clé du cadenas) est la « clé privée ». On pourra aussi aller beaucoup plus loin et parler de l'**algorithme RSA**, algorithme que l'on retrouve expliqué sur cette vidéo à des étudiants de première année d'université. Attention il y un piège... Bob s'appelle Bruno !

Mais... [stop] ! Il est sûrement l'heure du goûter :-) [**3**].

Passer du jeu à la séance de cinéma

Allez, il est temps de se reposer et de regarder (en cliquant par exemple sur l'image ci-dessous) un petit **film** de trois minutes [**4**] :

On retiendra que c'est un américain appelé **Whitfield Diffie** qui a inventé ce type de système de code secret de systèmes numériques.

Vous venez de partager la première leçon de sécurité informatique avec votre enfant de 6-12 ans. Et votre troisième leçon d'informatique théorique avec lui... et nous ! Pour la deuxième autour du codage informatique et la première autour des algorithmes, c'est par **ici** et par **là**.

Que venons-nous d'apprendre ensemble ici ?

Faire comprendre le principe du cryptage à clé publique ou cryptage asymétrique permet de susciter la réflexion sur plusieurs choses :

- le fait qu'un algorithme puisse servir à quelque chose de précieux comme protéger ses secrets et que cet algorithme ne s'applique pas que sur des calculs numériques ;
- le fait que « comprendre comment ça marche » permet de gagner et ne pas se « faire avoir par les autres », et qu'utiliser un mécanisme sans bien le comprendre peut nous rendre bien fragile.

On entre aussi dans le domaine des usages du numérique, car c'est lié à la sécurité de nos données et de notre identité. On découvre comment marche l'authentification, cette procédure qui consiste à vérifier l'identité d'une entité (personne ou mécanisme numérique). Cela permet d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, application, etc.). Elle se base [**5**] sur deux procédés :

- 1- Une opération que seule la personne peut effectuer (en lui envoyant un message sur son téléphone portable -supposant qu'il est bien en sa possession- qu'il doit retourner, ou en lui demandant une information qu'il est le seul à détenir -un mot de passe-).

> Dans notre cas, on demande à la personne de lancer un calcul qui a besoin d'une clé

Whitfield Diffie (1944-), l'un des pionniers de la cryptographie asymétrique

publique (que tout le monde connait) et une clé privée (qu'il est le seul à détenir et n'aura jamais communiquée à personne) et le résultat du calcul ne sera correct que si les deux clés sont correctes. Une clé est tout simplement une suite de chiffres avec laquelle se fera ce calcul. On peut donc l'authentifier sans jamais avoir eu besoin qu'il diffuse la clé privée, donc sans risque qu'un tiers ait pu s'en emparer.

- 2- Une autorité de certification (organisme indépendant) auprès de laquelle on dépose la clé publique et qui va vérifier par des moyens solides que le déposant n'usurpe pas une identité. Cette opération lourde se fait une seule fois et reste valide tant que la clé privée n'est pas ventilée. Ensuite c'est auprès de cette autorité que l'on récupère la clé publique pour demander de manière sûre à une personne le calcul d'authentification avec une clé privée. [**6**]

Pour aller plus loin voici quelques sources qui ont permis de proposer cette activité :

- la **cryptographie asymétrique** expliquée sur le site du zéro ;
- la **cryptographie asymétrique** expliquée sur Wikipédia ;
- en savoir plus sur la **crypto** sur **)i(nterstices**.
- en savoir plus sur l'**authentification** sur Wikipédia.

Au moment où nous écrivons ces lignes, l'affaire « **Snowden** » n'en finit pas de révéler que des puissants et des états ont très sereinement bafoué leurs propres lois pour espionner les humaines et les humains qu'ils craignaient. Ils ont pu le faire d'une manière simple à expliquer. Ils ont obtenu de plateformes numériques à qui nous avons accordé notre confiance (Google, Facebook...), et sur lesquelles nous avions déposé un mot de passe, des informations qui n'auraient pas dû être diffusées. C'est donc la notion d'« autorité de confiance » dont nous parlions qui a changé. Les organismes qui ont commis cet acte de *haute trahison* (c'est le terme consacré) n'en font plus partie.

P.S. :

La rédaction d'Images des maths et les auteurs remercient pour leur relecture attentive, les relecteurs Christophe et Reynald Thelliez.

Notes

[**1**] La description du chiffrement asymétrique numérique par analogie est effectivement bien connue et une description des deux analogies est disponible **ici**. Ainsi puisque le cadenas est numérique, on peut le reproduire indéfiniment (contrairement à notre cadenas physique) et distribuer des cadenas ouverts dont on garde la clé, à qui veut nous envoyer un message. Il suffit alors pour crypter le message de fermer le coffre avec ce cadenas, que seul celui qui a distribué les cadenas ouverts, a la clé.

[**2**] On devrait dire chiffrer, ici et dans la suite, si on se refusait tout anglicisme. Ce que nous ne ferons pas !

[**3**] Ceux qui n'ont pas faim pourront toujours aller jeter un oeil à cet **article** ou lire le volume **Codage et cryptographie** de la collection *Le monde est mathématique*.

[**4**] Grâce à **Tralalère**, **Xprod**, **Inria**, avec **Universcience** et la plume d'**Audrey Mikaëlian**, une 20taine de pépites de science attachées à une personne qui a fait avancer la connaissance est racontée aux enfants : ce sont les **Sépas**. Contenu scientifique réalisé grâce à l'aide de **Anne Canteau**, **Sylvie Boldo**, et **Joanna Jongwane**

[**5**] Un grand merci à Pascale Garreau de **Tralalère** avec qui a été co-écrite cette présentation de l'authentification.

[**6**] Le modèle de l'« autorité de certification » n'est pas le seul moyen de s'assurer que l'on dispose de la bonne clé publique, il existe aussi des modèles de **toile de confiance**, non centralisée.

Affiliation des auteurs

Thierry Viéville : Chercheur Inria, équipe mnemosyne. , **Aurélien Alvarez** : Université d'Orléans

---

Pour citer cet article : **Aurélien Alvarez** et **Thierry Viéville**, **« Dis maman (ou papa), comment on cache des secrets dans le monde numérique ? »** — *Images des Mathématiques*, CNRS, 2014.

En ligne, URL : **http://images.math.cnrs.fr/Dis-maman-ou-papa-comment-on-cache.html**

Si vous avez aimé cet article, voici quelques suggestions automatiques qui pourraient vous intéresser :

- **Dis papa (ou maman), comment arrivent les bugs dans le monde numérique ?**, par **Aurélien Alvarez** et **Thierry Viéville**
- **Dis maman (ou papa), c'est quoi un algorithme dans ce monde numérique ?**, par **Aurélien Alvarez** et **Thierry Viéville**
- **Codage et cryptographie**, par **Joan Gómez**