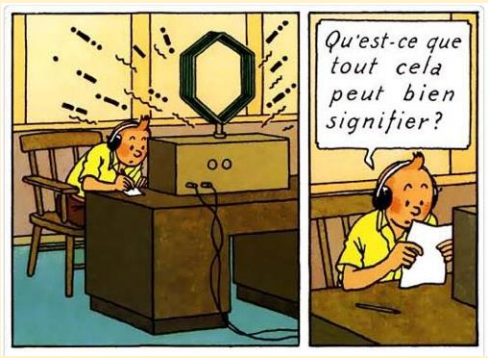
Sujet Lycée – Codage et décodage de messages secrets



Longtemps, la cryptographie était l'apanage des militaires. Désormais, l'usage civil (banque, commerce électronique, téléphonie mobile…) est très nettement prédominant. En effet, si la cryptographie doit encore assurer la confidentialité des échanges, ce n'est plus son seul usage. Elle est aujourd'hui garante :

- de l'authenticité des expéditeurs (la signature électronique)
- de l'identification des personnes (courriers électroniques, relevés de compte, paiements par carte bleue…)
- de la validité des votes électroniques
- de la sécurité du commerce électronique (confidentialité des informations relatives au compte de l'acheteur).

Une méthode de codage et décodage de messages secrets inventée en 1976

Bob veut qu'Alice lui fasse parvenir un nombre secret (numéro de téléphone, numéro d'un compte bancaire…). Il ne faut surtout pas que des malotrus découvrent ce nombre secret.

Ce nombre secret doit donc lui être envoyé sous une forme codée.

Alice et Bob ont choisi ensemble un nombre premier p et un entier g de $[\![0; p-1]\!]$. Ce couple de nombres (p, g) est rendu public, on l'appelle la clé publique.

Alice choisit un entier confidentiel a et envoie à Bob le reste de la division euclidienne de g^a par p.
Bob fait de même : il choisit discrètement un entier confidentiel b et envoie à Alice le reste de la division euclidienne de g^b par p.

1/ Expliquez comment Alice et Bob vont calculer, chacun de leur côté, le reste de la puissance $g^{a\times b}$ par p. Ce reste est appelée la clé privée. On le notera s.

Autrement dit, cette méthode permet à Bob et Alice de se mettre d'accord sur une clé privée (ou secrète) sans qu'un troisième agent appelé Eve ne puisse la découvrir, même en ayant écouté Bob et Alice. Elle propose ainsi un protocole d'échange de clés totalement sécurisé. Le problème est le suivant :

2/ Bob veut transmettre le nombre secret M à Alice. On suppose que $M \in [\![0; p]\!]$.

Pour cela, Bob va coder le message (qui est ici le nombre M) en calculant le reste de la division euclidienne de $M \times s$ par p. Il enverra à Alice ce reste.

3/ Donnez un moyen à Alice de retrouver le message initial M.

4/ Ecrivez un algorithme permettant à partir de p, g, a et b de calculer :

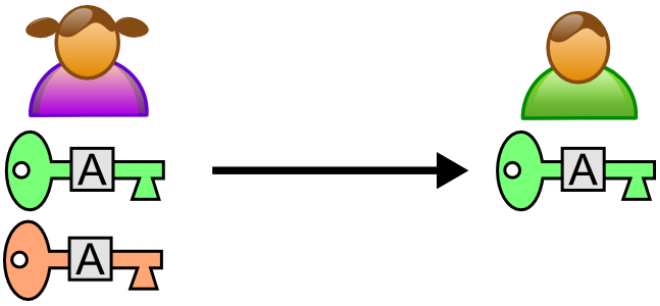
- la clé privée
- les codages et décodages de messages secrets.

5/ Que pensez-vous de cette méthode ? Alice et Bob peuvent-ils être rassurés quant à la confidentialité de leurs échanges ?

Ce protocole a un défaut : il exige la simultanéité des actions d'Alice et de Bob. Si Alice veut envoyer un e-mail à Bob alors que celui dort ou n'est simplement pas connecté, elle ne pourra pas le faire immédiatement (expliquez cela). Même s'il est encore utilisé pour les problèmes d'appariement de deux objets dans la technologie Bluetooth, il fut en réalité très vite supplanté.

Une méthode de codage et décodage de messages secrets inventée en 1977

Bob veut toujours qu'Alice lui fasse parvenir un nombre secret (numéro de téléphone, numéro d'un compte bancaire…).



On considère $n = pq$ le produit de deux nombres premiers distincts.

Bob prend pour clé publique (n,e) et pour clé privée (n,d). Le code secret qu'Alice veut transmettre est M ($M \in [\![0; n]\!]$). Alice code le message en l'élevant à la puissance e, puis envoie le message codé obtenu en considérant le reste de la division euclidienne de M^e par n.

Bob décodera le message en élevant le message codé à la puissance d. Il obtient le message décodé en considérant le reste de la division euclidienne de $(M^e)^d$ par n.

1/ Soit a un entier naturel. Montrez[1] que $a^p \equiv a(\mathrm{mod}\ p)$, c'est-à-dire que $a^p - a$ est un multiple de p.

Déduisez-en que si a est un entier naturel non divisible par p et q, alors on a :

$$a^{(p-1)(q-1)} \equiv 1(\mathrm{mod}\ n).$$

2/ Considérez un entier naturel e premier[2] avec $(p-1)(q-1)$ et inférieur strictement à ce produit. L'entier e est appelé l'exposant de codage. Comment construire alors la clé privée (n, d) ?

3/ Ecrivez les algorithmes calculant :

- une clé privée pour une clé publique donnée
- le décodage d'un message secret à partir des clés publique et privée.

4/ Pour décoder les messages secrets, les malotrus doivent être capables de trouver la clé privée à partir de la clé publique. Pensez-vous que cette recherche sera facile ?

Les quatre problèmes arithmétiques mobilisés

Ces deux méthodes font appel à des problèmes arithmétiques très difficiles :

- reconnaître un nombre premier (c'est-à-dire élaborer des tests de primalité)
- trouver de très grands nombres premiers
- décomposer en facteurs premiers
- résoudre le problème du logarithme discret, autrement dit trouver x tel que $g^x \equiv s[\mathrm{mod}\ p]$ si s, g et p sont connus, p étant un nombre premier.

Faites des recherches sur internet au sujet de ces quatre problèmes.

---

[1] On dit que les entiers u et v sont congrus modulo n lorsque u-v est un multiple de n. On note alors : $u \equiv v[\mathrm{mod}\ n]$.

[2] Deux entiers a et b sont premiers entre eux lorsque leur PGCD est 1.