L'évolution de la cryptologie moderne

Gilles Zémor

Institut de Mathématiques

5 novembre 2015

Un vieux défi

H.W. Jevons, 1873 :

«There are many cases in which we can easily and infallibly do a certain thing but may have much trouble in undoing it...

Given any two numbers, we may by a simple and infallible process obtain their product, but when a large number is given it is quite another matter to determine its factors. Can the reader say what two numbers multiplied together will produce the number

8 616 460 799 ?

I think it is unlikely that anyone but myself will ever know ; for they are two large prime numbers. »

Une constatation lourde de conséquences

Pour certaines fonctions f, il est facile de calculer :

$$x \mapsto f(x)$$

mais pas forcément de faire le chemin inverse :

comment trouver x à partir de $f(x)$? ? ?
Exemple :

$$x \mapsto x^2 \bmod n$$

Comment trouver x tel que $x^2 = 8059 \bmod 10403$?

Une telle fonction f est dite à sens unique (one-way).

La protection des mots de passe

Needham, 196x.

Ne jamais stocker le mot de passe m sur une machine, mais $y = f(m)$!

Connexion : sur l'entrée m la machine calcule $z = f(m)$. Est-ce que $z = y$?

L'idée de Lamport (1981)

Comment ne pas utiliser deux fois le même mot de passe ?

La machine stocke :

$$y = f(f(m)).$$

Première connexion : on soumet

$$z = f(m).$$

La machine calcule $f(z)$. Est-ce que $f(z) = y$?

Puis la machine jette y, et conserve z.

Deuxième connexion : l'utilisateur soumet

$$m.$$

La machine calcule $f(m)$. Est-ce que $f(m) = z$?

A protocol for solving impossible problems, Blum 1982

Comment jouer à pile ou face par téléphone.

A protocol for solving impossible problems, Blum 1982

Comment jouer à pile ou face par téléphone.

L'idée clé : les enveloppes sont remplacées par des fonctions à sens unique.

On voit apparaître la notion cryptographique *d'engagement* (ou de mise en gage).

Années 1970, développement de la théorie de la complexité

De la difficulté de démontrer des formules et des théorèmes.

$$\Big((x+3)(x+4)(x-1)+(x+2)^2\Big)^2 =$$

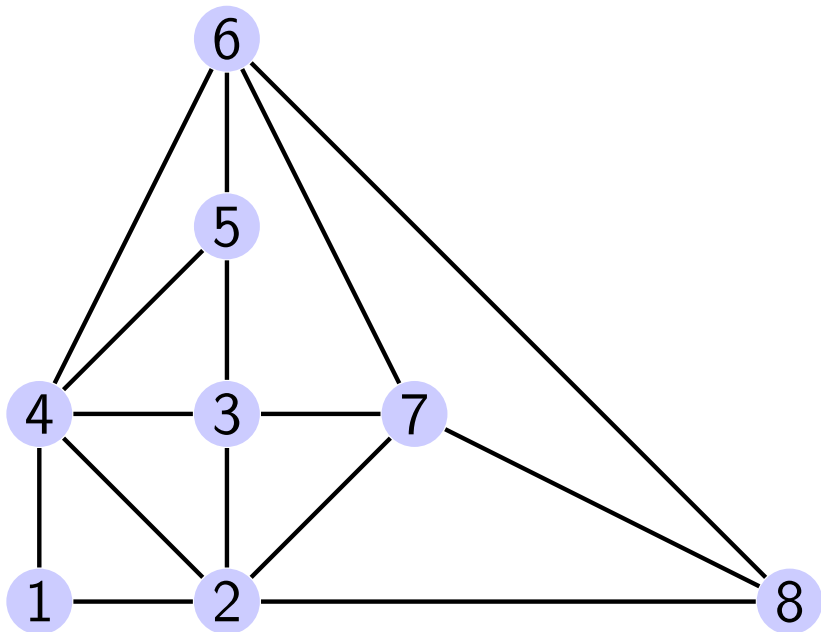
$$x^6+14\,x^5+67\,x^4+110\,x^3-31\,x^2-144\,x+64.$$

Le hasard est un très bon démonstrateur !

Années 1980, les cryptologues contribuent à la théorie de la complexité.

Vers des preuves impossibles à reproduire !

Un ancien problème algorithmique, la coloration des cartes et des graphes avec un nombre minimum de couleurs.



Peut-on colorier $\{1, 2, \ldots, 8\}$ avec trois couleurs ?

Démontrer des affirmations sans tout révéler

Peut-on démontrer que deux solutions $(x_1, \ldots, x_n)$ sont égales ?

Peut-on démontrer qu'on a une solution $(x_1, \ldots, x_n)$ au problème ? Sans la révéler ?

Et si c'était un mirage ?

Les fonctions à sens unique existent-elles vraiment ?

C'est la question P vs NP à \$1 000 000.

`http://www.claymath.org/millennium/P_vs_NP/`

Une préoccupation très actuelle, SHA3

Des fonctions à sens unique f destinées à signer (sceller) des gros fichiers. Les fonctions de condensation ou de hachage. Repèrent les fichiers contenant des virus.

Une *collision* : un couple d'entrées distinctes x et y tels que $f(x) = f(y)$.

MD5

La nouvelle norme de hachage : août 2015, après compétition 2012.