Conférence 07/03/2025

Paco AVEZEDO, laboratoire de maths de Versailles

« L'algèbre appliquée : cryptographie moderne », à partir de l'exemple RSA.

Thèse CIFFRE avec l'entreprise Thalès.

Algèbre appliquée : chiffrement des sites WEB, sécurisation des paiements, ...

Trois domaines mathématiques sont concernés :

① la cryptographie = la cryptologie, « science du secret ».

Un des thèmes : la génération de nombres aléatoires.

② le calcul formel

On y recherche des solutions exactes d'équations polynomiales $f(x_1, x_2, \dots, x_n) = 0$.

③ l'algèbre effective, où l'on manipule des objets algébriques avec des ordinateurs. Par exemple :

- programmer efficacement la diagonalisation d'une matrice
- quand on a un théorème d'existence, peut-on avoir une méthode constructive ? (ex) il existe une infinité de nombres premiers, mais peut-on écrire un algorithme qui en calcule ?)

Algorithme RSA

clé publique ⇝ encryptage message ⇝ clé secrète décriffrement

p et q 2 grands nombres premiers.
$n = pq$
On choisit e entier tel que $1 < e < (p-1)(q-1)$ et $e \wedge (p-1)(q-1) = 1$.

La clé publique est (n, e).
La clé secrète est (p, q, d) où d est l'inverse de e dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ (s'obtient avec le théo de Bezout).
L'encryptage du message m est :
$$c = m^e \ [n]$$
Le décryptage est $m = c^d \ [n]$

- Trouver la clé secrète, c'est trouver p et q ; c'est donc réussir à factoriser $n = pq$.
  À l'heure actuelle, on estime que c'est infaisable pour $n \geq 2^{1900}$ (avec le meilleur algorithme : General Number Field Sieve) et une puissance de calcul "terrestre" sur 1 million d'années : 2^{128}.

- L'attaquant du système peut essayer de non pas tout déchiffrer (c'est-à-dire obtenir la clé secrète) mais seulement quelques messages !
  Le domaine d'étude concerne des idéaux et des

racines de polynômes sur des corps finis.

- <u>Au sujet de l'envoi du message</u> $m = c^d\ [n]$
  On rappelle que $n \geq 2^{1900}$.
  On procède non pas avec l'envoi de $\underbrace{c \times c \times \dots \times c}_{d \text{ fois}}$,
  mais avec :
  * la méthode des restes chinois
    $$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$
    méthode de type « diviser pour mieux régner »
    On calcule $c^d\ [p]$ et $c^d\ [q]$, et ça permet d'obtenir plus efficacement $c^d\ [n]$.
  * De plus, on effectue le calcul des puissances par exponentiation rapide (pas par $c \times c \times \dots \times c$).

- <u>Remarque :</u>
  Comme trouver des nombres premiers est très couteux, la banque pourrait être tentée de prendre toujours les mêmes p et q, et changer seulement l'exposant e dans le calcul d'envoi $m^e\ [n]$.
  Ce serait attaquable si $e_A \wedge e_B = 1$.
  Par Bezout, $\exists (u,v)$ / $ue_A + ve_B = 1$.
  On connaîtrait l'envoi $\begin{cases} c_A = m^{e_A}\ [n] \\ c_B = m^{e_B}\ [n] \end{cases}$
  On pourrait alors trouver $c_A^u\, c_B^v = m^{ue_A + ve_B} = m$

- <u>L'avenir ... ?</u>
  - les ordinateurs quantiques, quand ils arriveront, pourront attaquer le RSA. D'autres algorithmes sont en préparation / prêts.
  Pour plus de sécurité, il peut être conseillé

d'utiliser deux systèmes :

→ un algorithme "ancien" de cryptage (*)

→ un algorithme "récent" résistant aux ordinateurs quantiques dans le cryptage.

(*) les attaques ont déjà été très étudiées du fait de l'ancienneté.

- Des attaques possibles existent depuis les années 2000 en mesurant la consommation d'énergie, très précisément, lors des transferts de données.