Philippe Colliard
http://www.mathemagique.com
Décembre 2014

Roulette russe.

Numeri souuerains ne seront éternels
Incomposti troueront leurs loys premieres
Lors seront fleaux onques n'aperceu vn tel,
En quarta perfecti bruslera notre terre

- Mais c'est ridicule ! ... Ridicule ! J'ai passé plus d'une heure, hier, à vous exposer en détail le cœur du système RSA. À vous, l'élite de notre jeunesse, nos informaticiens de demain !

Sous la violence de la voix, les vitraux du vénérable amphithéâtre tremblent. Comme tremblent, plus discrètement peut-être, les 40 étudiants resserrés autour de leur porte-parole, pâle, déterminée mais nerveuse : la vénérable université n'est certes pas un de ces campus modernes au laisser-aller de mauvais goût. On y respecte l'ordre et les formes. On en craint encore les professeurs - ou, plus justement, les Professeurs. Avec un P majuscule qui se décèle même à l'oral.

- … Le cœur du système, les éléments mathématiques sur lesquels il s'appuyait : le petit théorème de Fermat, le théorème d'Euler et naturellement le théorème de Bachet-Bézout !
Et aujourd'hui, vous, jeune femme, vous... Vous me « balancez » - excusez l'expression, mais elle est à la hauteur de mon indignation - vous me balancez un mage de l'Antiquité...

- Du XVIe siècle, Professeur... Et ce n'était pas seulement un mage, il était également le médecin du roi de France...

- Ne m'interrompez pas ! …

Tonne le grand Professeur, celui qui, pour tous, est simplement « Professeur » quand on a l'audace de lui parler. Ou plus rarement « Monsieur », pour les plus téméraires - et oui, le M s'entend majuscule.

… Vous me balancez donc ce... Ce charlatan médical - vous ne nierez pas, je l'espère, que ce qu'on appelait de la « médecine », à cette époque-là, était loin d'être une science - ce charlatan, donc, pour étayer votre thèse subversive. Destructrice... Oui, destructrice ! Si vous n'avez rien de plus sérieux à m'opposer...

- Mais, Professeur, c'est sérieux ! Comment interprétez-vous autrement ces quatre lignes ? Professeur, je vous en prie, je n'ai rien d'une anarchiste. Mes amis non plus, vous nous connaissez bien. Je suis inquiète, c'est tout. Parce que je suis jeune. Et je voudrais pouvoir vivre - excusez-moi, Monsieur - aussi longtemps que vous.

- Fort bien, Mademoiselle. Je vous ai entendu. Et je vous excuse, parce que, justement, vous êtes jeune. Mais vous nous faites perdre notre temps. Eh bien, perdons-le !
Vous mettez en doute la sécurité du système RSA. Croyez-vous vraiment que Messieurs Rivet, Shamir et Adleman, ses concepteurs, aient été des imposteurs ? Ou que les innombrables organismes qui l'utilisent soient dirigés par des incompétents ?

- Non, Professeur non, bien sûr. Je n'ai jamais dit ça. Mais...

- Heureusement que vous ne l'avez pas dit ! Et laissez-moi continuer, je vous prie. Ou plutôt, reprendre : vous ne m'en voudrez pas si je résume, nous y avons passé beaucoup de temps, hier !

Après l'éclat de voix initial, un ton parfaitement contrôlé, lisse et pourtant cinglant.

- RSA repose sur les entier premiers.
Un entier premier est un entier positif qui a exactement deux diviseurs - tout entier supérieur à 1 est soit premier, soit composé, par multiplication, d'entiers premiers.
Ces entiers premiers sont en nombre illimité, et nous en découvrons constamment de nouveaux, mais aucun

algorithme ne permet d'en construire une suite.
En s'appuyant sur ces éléments, les Messieurs que j'ai cité tout à l'heure ont... Concocté, oui, c'est le mot, concocté une méthode de chiffrement inédite et particulièrement efficace : un système à deux clés, l'une privée, l'autre publique. Ce que les cryptographe appellent un système asymétrique.

Un codage RSA est construit à partir de deux entiers premiers, hier je les ai appelés a et b, alors gardons ces noms.
On calcule leur produit - je l'avais appelé p, si vous avez suivi mon exposé.
On calcule ensuite le produit de (a – 1) par (b – 1)... On a décrémenté a et b, n'est-ce pas ? J'avais appelé p1 ce nouveau produit.
Ensuite encore, on choisit un nouvel entier, e, qui n'a pas à être premier, mais qui doit être strictement inférieur à p1 et premier avec lui.
Enfin, on calcule l'inverse modulaire, modulo p1, de e. Ce dernier entier, que j'ai appelé ie dans mon exposé, est donc également strictement inférieur à p1.

Un silence. Un regard hautain, que la jeune étudiante subit vaillamment. La petite foule se resserre autour d'elle, la rassure de sa présence, de sa complicité.

- Et c'est tout, Mademoiselle ! La clé publique est constituée des nombres p et e ; la clé privée, des nombres p et ie… Et personne, je répète, Mademoiselle, personne n'est capable, uniquement à partir de p et de e, de déterminer ie. Tout au moins avec a et b suffisamment grands ! Cela supposerait de savoir reconstituer p1 - et pour cela, de savoir déterminer ce que certains mathématiciens appellent le « spectre » de p : sa décomposition en facteurs premiers.
Oh, bien sûr, avec du temps, ce n'est pas impossible. Mais avec beaucoup de temps, Mademoiselle ! Une tentative récente de « cassage » d'un code RSA a nécessité plus de deux ans de travail à des ordinateurs très puissants. Et vous imaginez bien, Mademoiselle, qu'au bout de deux ans, un peu moins peut-être si des ordinateurs quantiques voient le jour, mais tout de même un certain temps, un message a perdu son importance…

Quant à nous, nous avons, grâce à vous, perdu beaucoup de temps. J'espère au moins vous avoir convaincue ? … Oui… Vous voulez dire quelque chose, monsieur ?

- Professeur, excusez-moi, mais je... Enfin, je... Je crois parler au nom d'un certain nombre d'étudiants, ici. Bon, hier soir, Laure nous a parlé du quatrain et, euh, on s'est pas mal moqué d'elle... Alors, bien sûr, on comprend votre réaction. Mais voilà, on a discuté et... Bon, elle était quand même drôlement convaincante. Alors, euh, alors...

- Alors vous aussi, c'est ça ?

Le Professeur secoue la tête, s'ébroue comme pour dissiper son exaspération.
- Mais c'est une véritable cabale !

- Professeur... On se demande juste...

- Oui, oui. Je sais ! Eh bien, l'heure est perdue, n'est-ce pas ? Alors autant se vautrer jusqu'au bout dans ces inepties. Que raconte-t-il, précisément, votre quatrain ?

- C'est une des dernières prédictions de Nostradamus, Monsieur. Dans ses centuries, vers 1550. Laure, tu peux donner une copie au Professeur ? Vous voyez, Monsieur :

Numeri souuerains ne seront éternels
Incomposti troueront leurs loys premieres
Lors seront fleaux onques n'aperceu vn tel,
En quarta perfecti bruslera notre terre

- Eh bien... Oui, je vois - et quelqu'un peut-il me traduire ce charabia ?

- C'est du vieux français, Monsieur, et un peu de latin. Laure a fait quelques recherches. « *Incomposti* », c'est comme ça qu'on appelait les entiers premiers, à cette époque-là. C'est ça qui l'a fait euh… Flasher sur ce quatrain !

Hier, vous nous avez dit que personne n'était capable de déterminer ie - avec a et b assez grands ! Cela supposerait de savoir reconstituer p1, mais pour y arriver, il faudrait d'abord déterminer le « spectre » de p, et ça, on ne savait pas le faire ! En tout cas, pas rapidement.
Mais Monsieur, si nous avons bien compris, c'est parce qu'il n'existe pas d'algorithme de construction des entiers premiers ? Sinon, ça deviendrait tout à fait possible ?

- Vous avez bien compris, oui. Et non, il n'existe pas d'algorithme de construction des entiers premiers. Et ?

- Mais s'il en existait un, Monsieur, « casser » rapidement p serait envisageable ?

- Je vous en prie, ça devient ridicule. Mais continuons : oui ce serait envisageable.

- Monsieur, je vous assure qu'on y a réfléchi. Au début, c'est vrai qu'on n'y croyait pas du tout... Et puis...
Bon, notre lecture du texte, c'est quelque chose comme :

> les nombres souverains ne le seront pas éternellement
> les entiers premiers trouveront une loi qui les régit
> alors viendront des fléaux tels qu'on n'en a jamais vus
> et au quart d'un parfait notre terre brûlera

- Eh bien, jeune homme, je vous accorde que ça ressemble à une traduction plausible de ce quatrain.
Et, si je puis me permettre, vous en déduisez quoi ?

- Que d'après Nostradamus, le règne des nombres va se terminer, parce qu'il existe une loi - un algorithme - de construction des entiers premiers. Et que la conséquence en sera plus ou moins la destruction de la Terre !

- Jeune homme !

- Oui, Monsieur, je sais, ça fait un peu délirant. Mais vous l'avez dit vous-même : si cet algorithme existe, les codes RSA peuvent être hackés. Monsieur ! Ce sont les codes de tout le système bancaire, de tous les gouvernements, de toutes les armées ! Alors ?

- Je vous en prie ! Cet algorithme n'existe pas.

- Mais quelqu'un a-t-il démontré qu'il n'existait pas ? Je n'ai pas vos connaissances, Monsieur... Mais il me semble que non ?

Un temps d'hésitation, le premier, du Maître :

- vous avez raison, personne ne l'a démontré. Mais ça ne prouve évidemment pas qu'il existe !

Une pause :

- ni qu'il n'existe pas, c'est vrai.

- Vous voyez, Monsieur ? Et s'il existe, si quelqu'un, comme le prédit Nostradamus, le trouve. Et si ce quelqu'un est génial, mais cinglé : il pourrait, en quelques jours, détruire toute l'économie de la planète. Et pourquoi pas, s'il découvre les codes, faire péter les charges de toutes les têtes nucléaires du monde...

- S'il vous plaît, un peu de calme. Oui, c'est vrai, il le pourrait. Mais vous ne trouvez pas que ça fait tout de même beaucoup de « si » ?

- Si, nous sommes d'accord, Monsieur. Mais nous avons quand même l'impression que tous ces grands organismes internationaux qui utilisent ces codes, eh bien... Ils jouent tout de même à la roulette russe avec notre monde, non ?

- Dans une certaine mesure, vous n'avez pas absolument tort. Mais il faut aussi avoir un peu confiance en l'adaptabilité de nos procédures : si on découvrait un tel algorithme, il est vraisemblable qu'on prendrait les mesures nécessaires pour que ça ne tourne pas à la catastrophe que vous évoquez, n'est-ce pas.

- Bien sûr, Monsieur... Si on en a le temps. Quand Laure disait tout à l'heure qu'elle aimerait vivre aussi longtemps que vous - sans offense, Monsieur, c'est vrai pour nous tous, ici. Et la dernière ligne, eh bien... Elle nous flanque un peu la frousse, vous voyez.

- La dernière ligne ? Voyons, vous la traduisez comment ?

- Là, c'est Lounès qui a trouvé. Enfin, on croit. Et ça ne nous plaît pas du tout !
« Notre terre brûlera », c'est plutôt clair, hein : si on lâche toutes les bombes sur la planète…
Mais le « quart d'un parfait » ???
Et là, Lounès s'est rappelé le cours sur les nombres parfaits, vous savez bien, Monsieur ?

- Oui, évidemment. Le « *τέλειος ἀριθμός* » des grecs. Un nombre entier dont le double est la somme de tous ses diviseurs. Et ?

- Et les premiers nombres parfaits sont 6, 28, 496 et 8128. Le suivant est 33 550 336.
Monsieur, le quart de 496, c'est passé depuis longtemps. Et si la Terre brûle en l'an 8 387 584, bon, on a le temps de voir venir.

Mais le quart de 8128, c'est 2032, Monsieur. Et franchement, maintenant, on a les jetons !

Philippe Colliard