2032(*)

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

J'ai cherché à écrire ce texte sur le modèle des nouvelles courtes d'Isaac Asimov – mais je n'ai malheureusement pas son talent ! Le système RSA est bien de Messieurs Rivet, Shamir et Adleman. Michel de Nostradamus est lui-même, le quatrain est de moi… et les mathématiques sont les mathématiques !

Philippe Colliard

Fin du cours. L'amphithéâtre se vide, le vieux prof rassemble lentement les notes éparpillées sur toute la longueur de son bureau, sourit au couple d'étudiants qui l'attend pour une dernière question, une dernière remarque, un dernier n'importe quoi. Il n'y a aucun calcul dans leur présence rituelle, ni Mathilde ni Lounès ne s'imagine être différent(e) des autres étudiant(e)s. Et pourtant… son sourire s'élargit, une paraphrase d'Orwell dans ses pensées : *tous les étudiants sont égaux mais certains sont plus égaux que d'autres* !

– Oui ?

– Lundi, vous avez mentionné le « système RSA ». Juste mentionné, vous avez dit que ce n'était pas au programme.

– C'est vrai, ça ne l'est pas… et ?

L'étudiante hésite, cherche du regard l'appui de son ami, hausse les épaules :

– on avait rien à faire alors on a un peu cherché. Sur ordi mais aussi dans la bibliothèque de la fac. Vous avez quelques minutes ?

Le sourire du prof s'agrandit encore, ces deux-là sont tellement rafraîchissants dans leur confiance tranquille :

– pour des personnes qui vont à la bibliothèque quand elles n'ont rien à faire, j'ai *toujours* quelques minutes !

– D'accord. Si on a bien compris, RSA est un système de codage qui s'appuie sur les entiers premiers…

– euh, rendez à César, etc. : c'est avant tout les initiales de Messieurs Rivet, Shamir et Adleman, non ? Mais oui, ils ont conçu un système de chiffrement particulièrement efficace : un système à deux clés, l'une privée, l'autre publique. Les cryptographes appellent ça un système asymétrique.

– Mais toujours en partant de deux entiers premiers ?

– Oui, toujours. Écoutez, je ne vais vraiment pas vous faire un cours ? On part de deux entiers premiers, a et b, on calcule leur produit p puis le produit $p1$ de $(a-1)$ par $(b-1)$…

– Oui, tout ça, on l'a compris…

Lounès l'interrompt avec une grimace impatiente, lui montre le bloc-notes de la jeune fille :

– Mathilde a tout résumé… ensuite on choisit un entier e quelconque, sauf qu'il doit être inférieur à $p1$ et premier avec lui et on calcule l'inverse modulaire modulo $p1$ de e.

– C'est ça ! Bravo, vous n'avez pas perdu votre temps…

Maintenant même ses yeux leur sourient :

– et c'est tout, n'est-ce pas ? La clé publique, c'est p et e, la clé privée $p1$ et l'inverse modulaire que vous avez calculé. Et personne n'est capable, uniquement à partir de p et de e, de déterminer cet inverse. Tout au moins avec a et b suffisamment grands ! Génial, non ?

– Mais si on a bien compris en vrai, ce n'est pas qu'on n'en est pas capable, c'est juste que ça obligerait à « casser » *p* en entiers premiers et que ça prendrait beaucoup de temps.

– Effectivement : avec des *a* et *b* suffisamment grands, plusieurs mois, même avec des ordinateurs hyper puissants. C'est pour ça qu'on utilise le chiffrement RSA à peu près partout, enfin, dans les systèmes bancaires, les organes gouvernementaux, militaires etc. ! Parce que le temps qu'un code soit déchiffré… il sera largement obsolète !

– Oui mais…

Une grimace embarrassée de Mathilde, un regard qui bizarrement semble lui demander de les rassurer. Pourquoi de les rassurer ?

– je ne suis pas sûre mais Lounès et moi on a compris que s'il faut beaucoup de temps pour casser *p* c'est juste 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, casser rapidement *p* serait envisageable ?

– oui, ce serait envisageable. Et si c'est ça que vous voulez dire, ça ficherait une super pagaille. Mais il n'en existe pas… et heureusement, le monde est déjà assez dangereux comme ça.

Est-ce qu'il se trompe ? Il lui semble voir un vrai début d'angoisse dans les yeux des deux étudiants, qu'est-ce qui leur arrive ? Il fronce les sourcils :

– bon, si vous me disiez ce qui ne va pas ?

– Vous n'allez pas vous moquer de nous ? À la bibliothèque, on faisait une recherche sur les entiers premiers et on est tombés sur un très vieil article qui citait une prédiction des centuries de Nostradamus, vers 1550…

– De… Nostradamus ?

– Oui je sais, vous allez nous prendre pour des cinglés. Mais d'après l'article Nostradamus n'était pas seulement un mage, il était également le médecin du roi de France alors c'était peut-être quelqu'un de sérieux quand même ?

– Euh… oui, bon, qu'est-ce qu'elle disait cette prédiction ?

– C'est un mélange de vieux français de latin, On l'a notée, là :

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

– Vous savez, moi le latin… votre article, il en donnait une traduction ?

– Non, mais nous on a essayé. « *Incomposti* », c'est comme ça qu'on appelait les entiers premiers, au XVIe siècle. C'est à cause de ça qu'on est tombé sur ce quatrain ! On pense que 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

– Bon je n'y connais vraiment pas grand-chose, d'accord ? Mais ça ressemble à une traduction plausible. Et 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 !

– Mathilde !

– Oui, je sais, ça fait un peu délirant. Mais vous l'avez dit vous-même : si cet algorithme existe, les codes RSA peuvent être hackés ! Et vous l'avez dit, ce sont les codes de toutes les banques, tous les gouvernements, toutes les armées ! Est-ce que quelqu'un a ***démontré*** qu'il n'existait pas ? Nous on n'en sait rien, mais vous, vous le savez sûrement ?

Un temps d'hésitation du prof, leur angoisse est contagieuse, c'est idiot :

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

Tout de même un nouveau froncement de sourcils, discret :

– ni qu'il n'existe pas, c'est vrai.

– Vous voyez ? 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 !

– 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. Mais nous avons quand même l'impression que tous ces grands organismes internationaux qui utilisent ces codes, eh bien, ils jouent un peu à la roulette russe avec notre monde, non ?

– Bon ce n'est pas complètement faux. Mais il faut aussi avoir confiance en l'adaptabilité de nos procédures : si on découvrait un tel algorithme, on peut supposer qu'on prendrait les mesures nécessaires pour que ça ne tourne pas à la catastrophe que vous évoquez, n'est-ce pas.

– Bien sûr... si on en a le temps. Mais c'est la dernière ligne, là. Elle nous flanque la frousse, vous voyez.

– La dernière ligne ? Pourquoi ?

– C'est Lounès qui a trouvé. Enfin, on croit. Et ça ne nous plaît pas du tout ! Lounès, tu expliques ?

Un oui inquiet de l'étudiant, une grimace de dérision contredite par l'agitation de sa voix :

– « Notre terre brûlera », c'est plutôt clair, hein : si on lâche toutes les bombes sur la planète !
Et « au quart d'un parfait »… vous vous rappelez votre cours sur les nombres parfaits, vous savez, le mois dernier ?

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

– Vous nous les avez fait calculer. Les premiers sont 6, 28, 496 et 8128. Le suivant est 33 550 336.
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…

Comme un début de panique dans ses yeux :

– mais le quart de 8128, c'est 2032. Vous comprenez ?

Et le cœur du vieux prof se serre, oui, il comprend. Il tente un sourire rassurant, voudrait leur raconter que ce n'est jamais que du Nostradamus. Seulement ça tient debout. Une pensée le ravage :

moi ça n'aurait plus beaucoup d'importance, j'ai eu le temps de vivre… mais eux ?

(*) *J'ai publié ce texte en 2014 sous le titre « roulette russe », mais dans le contexte actuel ce serait d'un goût plus que douteux !*