Comment les nombres premiers protègent vos données

En janvier dernier, le plus grand nombre premier connu à ce jour a été découvert. Celui-ci comporte plus de 22 millions de chiffres ! Au-delà du simple aspect « record », on peut légitimement s'interroger sur l'intérêt de cette découverte. En fait, les nombres premiers ne sont pas une simple curiosité mathématique : ils sont utilisés tous les jours dans notre vie quotidienne car ils permettent de « crypter » nos messages…

La *cryptographie* est l'art de chiffrer un message ou des données pour assurer leur protection. Autrement dit, la cryptographie cherche à assurer la confidentialité de données en les transformant en un message incompréhensible pour toute personne autre que leur destinataire.

La cryptographie est devenue au fil du temps un outil indispensable à plusieurs égards : protection de données privées, sécurisation de messages hautement confidentiels, protection des transactions bancaires par Internet, etc. D'une personne à un gouvernement, en passant par les entreprises ou l'armée, tout le monde est donc concerné.

Toutefois, l'avènement de l'informatique et d'Internet a considérablement augmenté les ressources disponibles pour déchiffrer un message crypté, ce qui impose des techniques de cryptage de plus en plus pointues. C'est là que les nombres premiers interviennent. Mais faisons un petit retour en arrière...

Mxohv Fhvdu vh vhuydlw gh od fubswrjudsklh

Historiquement, la cryptographie était déjà employée dans l'Antiquité. L'exemple le plus connu est sans conteste le *chiffrement de Jules César*. Celui-ci est relativement simple : il consiste à **décaler de trois rangs vers la droite les lettres de l'alphabet**. Ainsi, par exemple, un « a » est transformé en un « d », un « b » en un « e » et un « c » en un « f ». Mais « x » devient « a », « y » devient « b » et « z » devient « c » !

Lettres de départ	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
Lettres cryptées	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

VeNI VIDI VICI. JC.

Imaginons que nous souhaitons crypter le mot « gladiateur ». En respectant la technique du célèbre Romain, nous devons remplacer « g » par « j », « l » par « o », « a » par « d » et ainsi de suite. Cela nous donne alors « jodgldwhxu »…

Pour décoder, il suffit de faire de même, mais en décalant cette fois les lettres de trois crans vers la *gauche* de l'alphabet. Le titre de cette section peut ainsi être déchiffré[1] !

À l'époque, ce procédé était relativement sûr, mais ce n'est plus le cas aujourd'hui. En effet, on sait par exemple que le « e » est la lettre la plus utilisée de la langue française. Dès lors, une personne voyant un message chiffré, comme le titre de cette section, pourra remarquer rapidement un emploi plus important de la lettre « h ». Comme « h » correspond effectivement à « e » dans le chiffrement de César, elle aura vite compris que chaque lettre du message de départ a été décalée de trois crans vers la droite…

C'est ici que réside toute la difficulté de la cryptographie : fournir un moyen suffisamment sûr de protéger nos données, tout en veillant à ce que nos destinataires puissent encore les lire !

Quand les machines sont avec ou (surtout) contre nous

Avec le temps, la cryptographie est donc devenue plus complexe, notamment en incorporant des techniques mathématiques. Hélas, des chercheurs sont souvent parvenus à mettre au point des méthodes pour les déchiffrer, elles aussi basées sur les maths les plus pointues.

Ainsi, une étape marquante dans l'évolution de la cryptographie est assurément la Seconde Guerre mondiale avec l'emploi de la machine *Enigma* par les Allemands, qui fut vaincue par des mathématiciens polonais et britanniques (dont Alan Turing[2]), aidés de gros calculateurs. Poursuivant sur leur lancée, les Britanniques mirent au point le *Colossus,* premier ordinateur de l'Histoire, pour déchiffrer les échanges entre Hitler et ses généraux (ceux-ci se servaient alors d'une autre machine de cryptage, la machine *Lorentz*).

À partir de ce moment, la cryptographie prit une autre dimension car ces supercalculateurs ont la capacité d'accomplir une quantité invraisemblable d'opérations en comparaison avec l'Homme. À l'heure actuelle, suivant les modèles, **le nombre de calculs qu'un ordinateur peut réaliser en une seconde se compte en milliards (voire en dizaines de milliards)**.

Prenons un exemple : le code PIN d'un téléphone mobile ou d'une carte bancaire, constitué de 4 chiffres. Comme pour chacun de ces chiffres, il y a 10 possibilités (0, 1, 2, 3 et ainsi de suite jusque 9), il existe 10 x 10 x 10 x 10 = 10 000 codes PIN différents. Si un être humain tente de trouver le bon code en testant toutes les possibilités et prend 2 secondes pour chaque test, il lui faudra jusqu'à 20 000 secondes pour atteindre son objectif. Cela représente un peu plus de **5 heures et demie de travail, sans le moindre arrêt et surtout sans commettre la moindre erreur** ! Par contre, un ordinateur qui peut faire un million de tests par seconde (ce qui est très peu) **aura tout passé en revue en un centième de seconde** ! Seule parade : **limiter le nombre de tentatives à 3**. Dès lors,

[1] Il s'agit de « Jules Cesar se servait de la cryptographie ».

[2] Alan Turing (1912-1954) est un mathématicien britannique considéré comme l'un des pères fondateurs de l'informatique. Il a en outre fait l'objet d'un film de 2014, intitulé « *The Imitation Game* ».

ordinateur ou pas, il n'y a que 0.03 % de chances de trouver le code au cours de ces 3 tentatives : ce n'est pas impossible – avec un peu de (mal)chance – mais c'est très peu vraisemblable.

Face au développement de ces machines, la cryptographie a dû se réinventer. Désormais, elle doit employer des techniques dont le déchiffrement nécessite un nombre de calculs tellement grand qu'il en devient insurmontable, y compris pour les ordinateurs.

Nos nombres premiers, ces héros

C'est dans ce contexte que Ron Rivest, Adi Shamir et Leonard Adleman ont introduit le *chiffrement **RSA*** en 1977. Ce système de cryptage est très utilisé dans la protection d'échanges de données. Il se base sur toutes sortes de calculs arithmétiques (exposants, divisions avec reste, etc.). Mais la clé de sa sécurité se base sur une notion mathématique essentielle : celle des **nombres premiers**.

Rappelons la définition d'un nombre premier :

*Un nombre premier est un entier positif possédant **exactement deux diviseurs**.*

En particulier, les deux seuls diviseurs d'un tel nombre sont nécessairement 1 et lui-même. Par exemple, 2, 3, 29 et 71 sont des nombres premiers. Par contre, 4 n'est pas premier, puisqu'il est divisible par 2. Et 1 n'est pas premier non plus car il ne possède qu'un seul diviseur : lui-même !

Et quel est l'intérêt de ces fameux nombres, me direz-vous ? C'est ce qu'on a coutume d'appeler le « Théorème fondamental de l'Arithmétique » :

*Tout nombre entier strictement plus grand que 1 s'écrit comme **un produit de nombres premiers**.*

Ainsi, les nombres premiers permettent de reconstruire les autres nombres, d'où l'appellation « premiers ». Par exemple, 6 n'est pas un nombre premier, mais il est égal à 2 x 3, où 2 et 3 sont des nombres premiers. De même, 9 = 3 x 3, 42 = 2 x 3 x 7, etc.

Et on peut continuer l'exercice avec des nombres plus grands, comme 221. Il faut alors un peu plus de temps pour voir que 221 = 13 x 17. Et si maintenant vous deviez trouver la décomposition en nombres premiers de

3 574 406 403 731 ?

Si vous parvenez à le faire de tête, de grâce, appelez immédiatement la NSA, elle aura sans aucun doute un super job pour vous ! Ce nombre, dépassant les 3 500 milliards, est en fait le produit des nombres premiers 1 299 709 et 2 750 159. Si on veut trouver cette décomposition, il faut a priori vérifier si l'énorme nombre ci-dessus est divisible par 2, puis par 3 et ainsi de suite jusque tomber sur son plus petit diviseur, à savoir 1 299 709. On aura de la sorte dû effectuer **bien plus d'un million de divisions** pour obtenir une réponse ! Si on prend l'exemple d'un homme capable de faire une division toutes les 2 secondes, il lui faudra **environ un mois de travail en continu**. Pour un ordinateur réalisant un million de divisions par seconde, il lui faudra environ **1.3 seconde**.

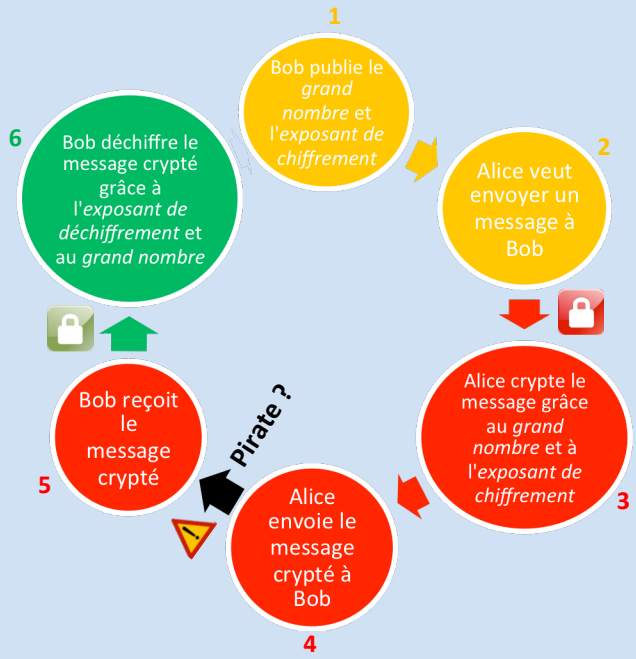
Par contre, si on considère un nombre de **300 chiffres** (celui donné ci-dessus n'en avait que 13…), trouver un éventuel diviseur peut demander un nombre de calculs comportant lui-même 150 chiffres ! Pour le superordinateur annoncé par le décret présidentiel américain du 29 juillet 2015[3], qui devrait être capable de réaliser environ **un milliard de milliards de calculs par seconde**, **le nombre d'années qu'il lui faudrait pour trouver le diviseur tant recherché pourrait comporter jusqu'à 125 chiffres !** Pour avoir un ordre de grandeur, **l'âge de la Terre est estimé à 4 milliards et demi d'années**, un nombre de seulement… **10 chiffres** !

Cryptons avec le RSA…

Imaginons qu'Alice veut envoyer un message confidentiel à Bob en utilisant le RSA.

Pour ce faire, l'ordinateur de Bob choisit un très grand nombre (**300 à 600 chiffres**) ayant la particularité **d'être le produit de deux nombres premiers (150 à 300 chiffres chacun)**. À partir de ces nombres premiers, il calcule deux nombres entiers appelés respectivement *exposant de chiffrement* et *exposant de déchiffrement*. Bob **publie alors le grand nombre et l'exposant de chiffrement** (ils sont donc connus de tous, alors que **les deux nombres premiers et l'exposant de déchiffrement restent secrets**).

Afin d'envoyer son message à Bob, l'ordinateur d'Alice le **crypte au moyen de l'exposant de chiffrement et du grand nombre** (cela passe par des calculs de puissances et de restes de divisions). Quand Bob reçoit le message chiffré, son ordinateur le décrypte en faisant le même genre de calculs, mais cette fois avec **l'exposant de déchiffrement**.



Et toute **la sécurité du système repose sur le fait qu'il est très difficile de retrouver les deux nombres premiers** et donc de **retrouver l'exposant permettant de déchiffrer** les messages d'Alice.

[3] La consultation dudit décret peut se faire via le site https://www.whitehouse.gov/the-press-office/2015/07/29/executive-order-creating-national-strategic-computing-initiative (consulté le 26/02/2016).

Mais la lutte continue

Alors, tout va pour le mieux dans le meilleur des mondes ? Jamais nous n'aurons de problèmes de sécurité dans nos transferts de données ? Pas tout à fait, car la cryptographie doit faire face à une double évolution dans le temps.

Tout d'abord, la recherche en mathématiques, et en particulier en arithmétique, se poursuit. Des méthodes ont déjà été mises au point pour diminuer drastiquement le nombre d'opérations à effectuer pour décomposer un nombre en nombres premiers. Pour le moment, elles nécessitent encore tellement de calculs que cela n'aide pas les pirates informatiques. Pourquoi ne pas interdire la recherche sur les nombres premiers, vous demandez-vous peut-être ? Car, en-dehors de l'amélioration des connaissances en arithmétique que les nombres premiers procurent, il vaut simplement mieux qu'une équipe de mathématiciens fasse une grande découverte à leur sujet au vu et au su de tous, plutôt qu'un brillant *hacker* « dans son coin »… En attendant, soyez rassurés : d'autres techniques de cryptage ont déjà été développées et pourront remplacer le RSA si cela devenait un jour nécessaire. On peut citer par exemple le *chiffrement d'El Gamal* ou la cryptographie sur les *courbes elliptiques*, tous deux partiellement basés sur les nombres premiers mais dont la sécurité repose cette fois sur la notion de « logarithme discret »[4].

Ensuite, l'accroissement de la puissance des ordinateurs se poursuit elle aussi. Par exemple, d'après le site *Phoronix*, **une tablette en 2012 est aussi rapide que le superordinateur Cray-2 de 1985**, premier ordinateur à avoir dépassé la barre du milliard de calculs par seconde. Et ce phénomène se poursuivra dans le futur, avec notamment **le développement des ordinateurs quantiques** (cf. encadré ci-contre). Ainsi, les ordinateurs mettront de moins en moins de temps pour faire des opérations données (comme par exemple une décomposition en nombres premiers). Suivant l'ampleur de cette évolution, la cryptographie devra **accroître en conséquence le niveau de sécurité de ses techniques**. Dans ce contexte, la découverte d'un nombre premier à 22 millions de chiffres en janvier 2016 offre une nouvelle marge de protection au chiffrement RSA.

Le monde des ordinateurs quantiques

Les **ordinateurs quantiques** fonctionnent sur base des propriétés de la matière étudiées en physique quantique. Leur développement est en cours. Ils pourraient avoir une **capacité de calculs phénoménale** en comparaison avec les ordinateurs actuels : d'après Google, un prototype qui lui appartient a réalisé un calcul **100 millions de fois plus vite** qu'un ordinateur conventionnel. Ils pourraient ainsi **bouleverser la cryptographie** s'ils sont un jour commercialisés, en rendant vulnérables les techniques actuelles, mais aussi en permettant la mise en place de la cryptographie dite « quantique ».

[4] Le logarithme discret est une notion bien plus complexe que celle des nombres premiers. En quelques mots, elle consiste à rechercher des exposants au sein de structures algébriques abstraites.

Cependant, d'ici l'apparition de nouvelles techniques mathématiques ou informatiques, les nombres premiers gardent de beaux jours devant eux. Et ils pourront de la sorte continuer, pendant au moins quelques années, à protéger nos données.

Loïc Demeulenaere (FNRS)
Université de Liège

Pour plus d'infos/références :

Agrawal, M., N. Kayal et N. Saxena. Primes is in P. *Annals of Mathematics.* 2004, **160** (2), p. 781-793.

DALRYMPLE, G. Brent. *The age of the Earth in the twentieth century: a problem (mostly) solved. Special Publications, Geological Society of London. 2001, **190** (1), p. 205–221*

http://rue89.nouvelobs.com/2015/08/11/savez-compter-petaflops-top-10-superordinateurs-sans-france-260697 (site consulté le 26/02/2016)

http://www.lesechos.fr/30/07/2015/lesechos.fr/021238115945_le-supercalculateur-le-plus-puissant-du-monde-annonce-par-barack-obama.htm (site consulté le 26/02/2016)

http://www.phoronix.com/scan.php?page=news_item&px=MTE4NjU, (site consulté le 08/03/2016)

http://www.journaldunet.com/solutions/dsi/1137545-l-informatique-quantique-la-quete-du-graal-numerique/ (site consulté le 09/03/2016)

http://www.lesechos.fr/idees-debats/sciences-prospective/021678126130-lordinateur-quantique-reste-a-construire-1198237.php (site consulté le 09/03/2016)

http://www.sciencesetavenir.fr/high-tech/informatique/20151214.OBS1309/les-incroyables-promesses-de-l-ordinateur-quantique.html (site consulté le 09/03/2016)

http://www.lesechos.fr/idees-debats/sciences-prospective/021678126130-lordinateur-quantique-reste-a-construire-1198237.php (site consulté le 09/03/2016)

https://cel.archives-ouvertes.fr/file/index/docid/92955/filename/cel-29.pdf (cours sur l'informatique quantique ; site consulté le 09/03/2016)

http://www.lumenogic.com/www/static/pdf/colossus-servan-schreiber.pdf (article sur la création du *Colossus* ; site consulté le 09/03/2016).