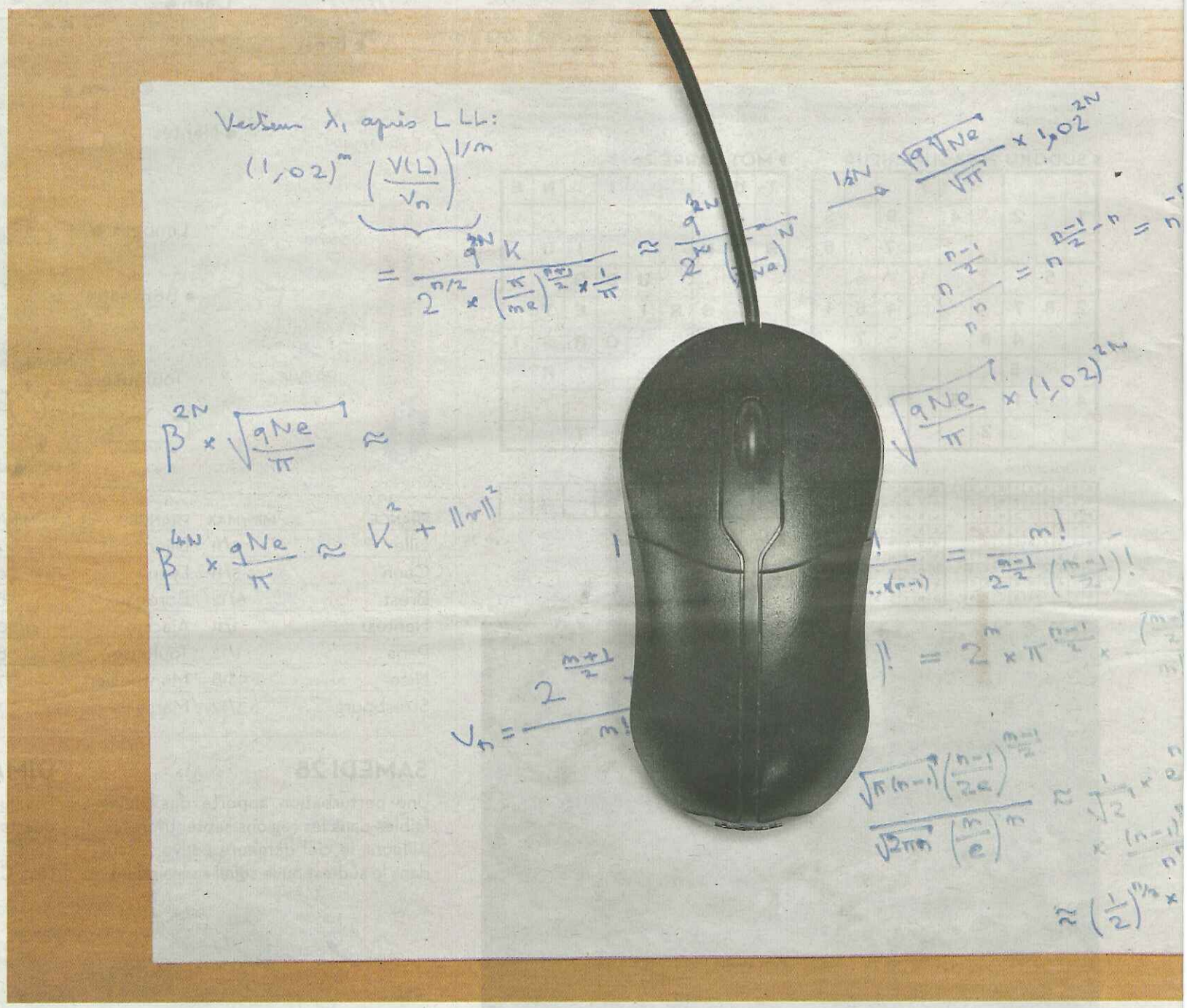
# *Cryptographie,*

**Puce des passeports, vote électronique, stockage dans le nuage, cartes bleues… Le chiffrement gagne tous les domaines, avançant au rythme des découvertes mathématiques. Son usage principal demeure l'authentification.**

Par **PIERRE ALONSO**
Photo **ERWAN FICHOU**



Un mathématicien a raccourci la Seconde Guerre mondiale, précipitant la victoire des alliés. Il s'appelait Alan Turing. Avec son équipe, réunie à 80 km au nord de Londres dans le manoir de Bletchley Park, il a disséqué jour et nuit les messages codés par les nazis. Jusqu'à les décrypter. Contre la machine des Allemands, baptisée Enigma, Alan en a inventé une autre, qui passait en revue une infinité de combinaisons mathématiques, beaucoup plus vite que n'importe quel cerveau humain. Elle constitue le premier prototype de l'ordinateur.

L'histoire d'Alan Turing, considéré comme le père fondateur de l'informatique, est restée secrète des dizaines d'années. Homosexuel, condamné à suivre un traitement hormonal en 1952, il se suicide deux ans plus tard, sans avoir jamais pu faire valoir sa participation décisive à la victoire contre le IIIe Reich. Le gouvernement britannique ne présentera ses excuses qu'en 2009, la reine son pardon en 2013… Le film *The Imitation Game*, sorti fin janvier, a popularisé la vie, romancée et lissée, du mathématicien de génie et cryptanalyste – c'est-à-dire casseur de codes.

Aujourd'hui, le chiffrement n'est plus réservé aux communications classifiées des armées. Ni même aux utilisateurs soucieux de préserver leur vie privée. «*Tout le monde utilise la crypto tous les jours*», corrige Damien Vergnaud, jeune maître de conférence en cryptologie à l'Ecole normale supérieure (ENS), rue d'Ulm à Paris. Pour trouver son bureau, il faut chercher le «*couloir cryptographie*», puis badger pour déverrouiller la porte. Le laboratoire de l'ENS est l'un des premiers du genre en France, longtemps dirigé par le père de la cryptologie, Jacques Stern, apôtre de sa libéralisation (obtenue en 2004 dans la loi, avec maintien d'une déclaration administrative préalable dans certains cas). Celui qui a lancé la discipline académique en France et a grandement contribué à sa démocratisation.

**«La NSA a compris qu'il était inutile de casser la crypto si elle pouvait récupérer les clés ailleurs. C'est un peu l'histoire de la porte blindée sur un mur en papier…»**

**Louis Goubin** professeur en cryptographie, évoquant le piratage de Gemalto par l'agence américaine

La «crypto» est désormais partout. «*Dans l'esprit des gens, la crypto sert à assurer la confidentialité des données, alors que l'usage principal de nos jours est l'authentification : garantir qu'un paiement est effectué, qu'on se connecte sur son wi-fi*», indique Damien Vergnaud. Les téléphones y recourent pour chiffrer la voix et authentifier l'utilisateur sur le réseau, de même que les cartes bleues. Internet, bien sûr, est truffé de cryptographie. Un phénomène historiquement corrélé au besoin de sécurisation des transactions bancaires.

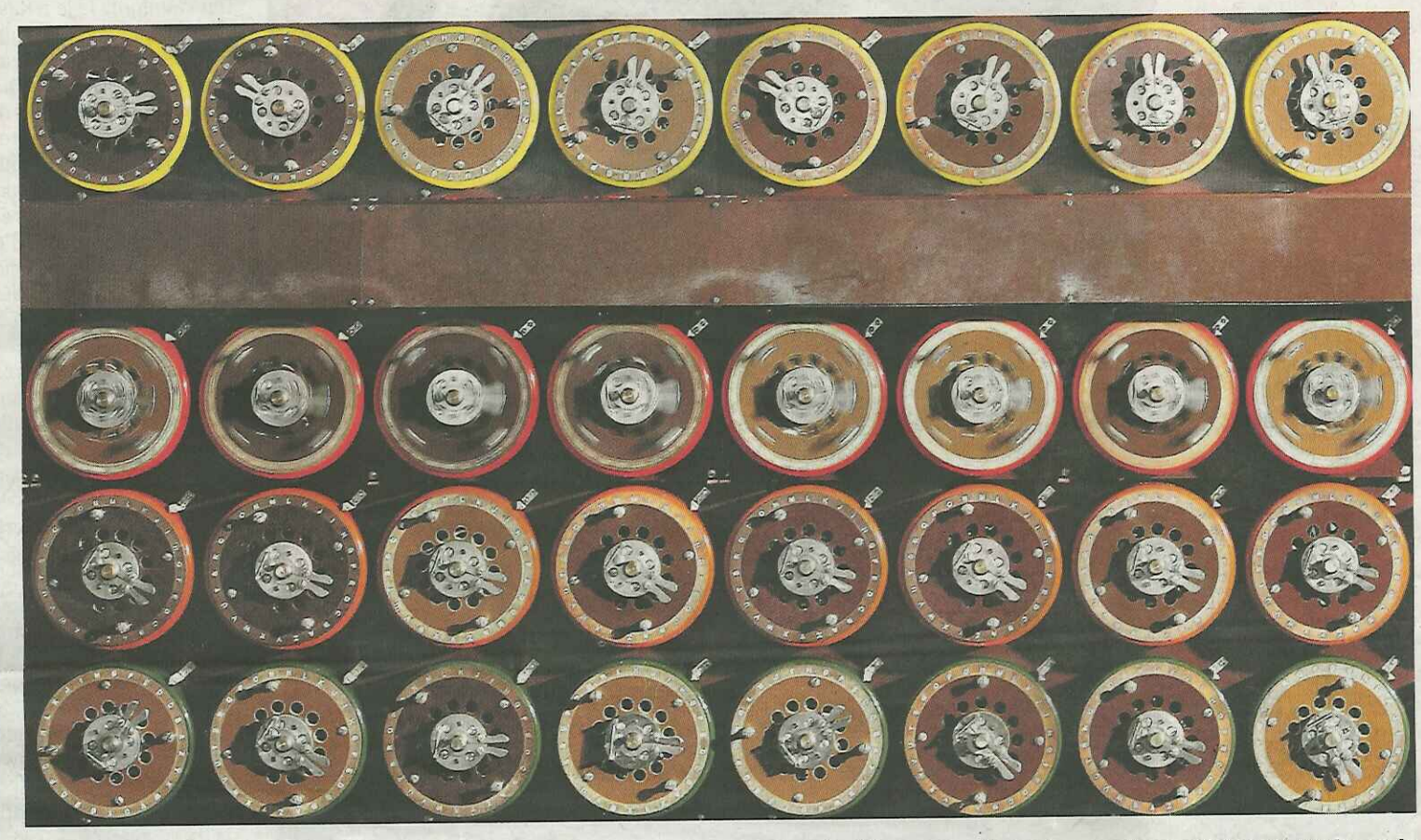
## «Informations biométriques»

Louis Goubin, responsable du master en cryptographie Secrets à l'université de Versailles-Saint-Quentin, cite de nouveaux usages et de nouveaux défis : «*Les passeports comportent maintenant une puce pour faire passer dans un canal sécurisé les informations biométriques entre le passeport et le terminal ; le vote électronique met en jeu des problèmes inédits : il faut déchiffrer les votes seulement une fois agrégés pour ne pas savoir qui vote pour qui ; le cloud computing* [l'informatique dans «le nuage», ndlr] *nécessite de manipuler des données cryptées.*»

Son bureau surplombant le campus de l'université et, au loin, le château, ne ressemble pas vraiment à un laboratoire militaire, pas plus qu'à un repère de hackers – forcément méchants, tels qu'Hollywood aime les caricaturer.

Louis Goubin fait avant tout des mathématiques. Il explique : «*En cryptologie, il y a deux scénarios.*

# monde clés



La Bombe du mathématicien britannique Alan Turing, à Bletchley, en Angleterre. Cette machine servit à déchiffrer les messages codés par la machine «Enigma» des nazis durant la Seconde Guerre mondiale.
PHOTO REUTERS

Au laboratoire de cryptographie de l'Ecole normale supérieure (ENS), 45 rue d'Ulm à Paris.

*Soit, comme à l'époque d'Enigma, des gens conçoivent un algorithme de chiffrement et d'autres essaient de le casser. Soit on part d'un problème mathématique et on construit un algorithme pour lequel on peut prouver que le casser revient à casser le problème mathématique.*» Exemple : sur une feuille de papier, Louis Goubin écrit une multiplication simple, 7×13. 91 s'empresse-t-on de répondre. Certes, mais le but est de faire l'inverse : «*Il est facile de retrouver que 91 est égal à 7×13. Mais prenons 912357926851, c'est beaucoup plus compliqué. Et complètement infaisable avec un nombre de 200 chiffres. C'est ce qu'on appelle le problème de la factorisation.*» Un problème que le mathématicien Fermat a identifié au XVIIe siècle.

## Valise diplomatique

Les deux scénarios renvoient aux deux grandes familles de la crypto : symétrique et asymétrique. Chacune a son algorithme star : AES (Advanced Encryption Standard, «Standard de cryptage avancé», inventé en 2000) pour le premier, RSA (du nom des trois créateurs, Ronald Rivest, Adi Shamir, Leonard Adleman, trouvé en 1977) pour le second. Chacune a ses propriétés et des usages propres. «*Le téléphone rouge utilisait un système de chiffrement symétrique, un schéma appelé le "masque jetable" ou* "one-time pad"», rappelle Damien Vergnaud. Par valise diplomatique, la Maison Blanche et le Kremlin s'envoyaient une clé de chiffrement, qu'ils utilisaient lors d'un échange, puis la modifiaient. «*On peut démontrer que cette technique est parfaitement sûre. Un attaquant, même avec une puissance de calcul infinie, ne pourra jamais trouver le message.*» La solution est pourtant loin de se prêter à tous les contextes. «*La clé, utilisée une seule fois, doit être aussi longue que le message*», précise Damien Vergnaud. Pour chiffrer un disque dur selon ce principe, il faudrait… un autre disque dur. Sans compter que la fameuse clé de décryptage doit être partagée de façon parfaitement confidentielle. Ce qui était valable pour les dirigeants des deux plus grandes puissances l'est moins pour le quidam souhaitant faire un achat en ligne. «*Tout dépend du modèle de menace*, résume François Morain, professeur d'informatique à l'Ecole polytechnique. *Le système de cryptographie est fonction de l'évaluation de la menace et des moyens disponibles. Il n'y a pas de crypto absolue, pas plus que de système universel.*»

Ceux qui font les codes sont aussi, souvent, ceux qui les cassent. La cryptologie marche ainsi sur ses deux jambes : la cryptographie pour concevoir des algorithmes et la cryptanalyse pour les briser. C'est particulièrement vrai pour le chiffrement symétrique, qui ne repose pas sur un problème mathématique identifié. «*Il s'agit davantage de constructions empiriques. Des batteries d'attaques sont menées sur un chiffrement symétrique pour vérifier sa solidité*», détaille Louis Goubin, de l'université de Versailles. Ce qui n'exclut pas qu'un cerveau génial, comme celui de Turing, surgisse et trouve une solution jusqu'ici inimaginée.

## Courbes elliptiques

Les recherches en cryptologie suivent donc les découvertes en mathématiques. Des nouveaux champs émergent. Damien Vergnaud, de l'ENS, travaille ainsi sur les courbes elliptiques, qui font appel à des mathématiques plus récentes. Nadia el-Mrabet, du Laboratoire d'informatique avancée de Saint-Denis (université Paris-VIII), se concentre sur un autre aspect, tout aussi crucial pour garantir l'intégrité d'un protocole de cryptographie : son «*implémentation*», «*sa traduction en langage informatique*», explicite la chercheuse. Ici, le but est de faire parler, ou taire, un algorithme lorsqu'il est soumis à des attaques «*physiques*». Mesurer la consommation électrique d'une carte à puce, ou envoyer des signaux pour perturber son fonctionnement, peut fournir des informations précieuses sur le mode d'implantation de la cryptographie, donc sur de potentielles faiblesses.

Tous nos interlocuteurs répètent que les failles ne se trouvent presque jamais dans la cryptographie elle-même. Louis Goubin en veut pour preuve la dernière affaire qui a ébranlé le géant des cartes à puce, Gemalto. Le site d'enquête The Intercept révélait en février que la puissante agence de renseignement américaine (NSA) avait piraté l'entreprise pour dérober les clés de chiffrement des cartes SIM. «*La NSA a bien compris qu'il était inutile de casser la crypto si elle pouvait récupérer les clés à d'autres endroits. C'est un peu l'histoire de la porte blindée sur un mur en papier…*» commente Goubin.

Le secteur de la défense conserve évidemment un appétit intact pour la crypto. Les échanges entre le monde industriel et les universités sont courants. De même entre acteurs civils et militaires. Dans les conférences de cryptographie, que François Morain a vu se remplir ces trente dernières années, se côtoient képis et costards. Les profils de spécialistes s'arrachent. Y compris pour les services secrets. Sur son site, la DGSE indique recruter des «*cryptomathématiciens*». Si possible, le prochain Alan Turing.