de sécurité, tandis que les ITSEC vérifiaient leur pertinence et leur efficacité.

Bientôt émergea l'idée de critères universels acceptables des deux côtés de l'Atlantique et même au-delà. C'est ainsi que naquirent les « Critères Communs » bientôt transformés en norme ISO, à la rédaction desquels la France prit une part déterminante, la présidence du groupe de travail lui étant revenue.

De fait, alors que les États-Unis et le Royaume-Uni se concentraient sur la certification de différents systèmes d'exploitation et dispositifs de sécurité tels les pare-feu, la France trouva dans la carte à puce un champ d'application privilégié. Son expertise dans ce domaine l'amena même à exercer une sorte de monopole. À ce titre, des firmes prestigieuses coréennes, japonaises et même américaines telle Motorola en vinrent à lui confier les évaluations de leurs produits. Cette grande compétence était le fait d'une petite équipe de chercheurs de France Télécom répartie entre Grenoble et Caen. Une dizaine de personnes qui avaient su, en collaboration avec le SCSSI, développer les méthodes d'investigation à la fois sur le matériel et sur le logiciel et automatiser la recherche de failles. Cette équipe fut ensuite transférée au sein du Laboratoire des technologies de l'information (LETI) du CEA.

Ce travail sur la sécurisation des composants de cartes à puce impliquait un effort considérable de la part des industriels se lançant dans le processus et parfois des changements substantiels dans l'organisation de la chaîne de production à l'intérieur même des salles blanches, pour lesquelles les investissements avaient été considérables. C'est ainsi qu'en 1999 à Tours, lors de l'opération de lancement de Moneo, ce porte-monnaie électronique qui malheureusement n'a pas eu le succès escompté, un PDG de la société, en recevant officiellement son certificat de sécurité, déclara que ce certificat lui avait coûté 20 % de logiciel et de dépenses supplémentaires, un dépassement de 30 % des délais, et 50 % de sueur et de stress en plus pour les premiers composants. Mais il se félicitait du gain en rapidité de développement et de mise au point obtenu ensuite.

Longtemps, la carte à puce ainsi sécurisée fut réputée comme le moyen de paiement le plus sûr, avec une fraude affichée de 0,03 %. Ce taux ne militait pas pour un renforcement de la sécurité. Ainsi la taille des clés, pourtant jugée bien trop faible par les experts, fut maintenue bien trop longtemps. Aussi, quand le GIE Carte bancaire fut confronté à l'affaire Humpich, un vent de panique souffla sur ce bel optimisme.

Sécurisation et législation

Un des problèmes rencontrés pour sécuriser la carte a été la législation française, car les moyens cryptologiques, classés dans la catégorie des armes de guerre, étaient soumis au régime défini par le décret de 1939. Ainsi, lors d'une réunion du Directoire de la cryptologie, vers 1985, le représentant du ministère de l'Industrie, en entrant à Matignon, s'excusa d'avoir pénétré dans ce lieu en portant une arme de deuxième catégorie : sa carte bancaire… Celle-ci contenait en effet un algorithme cryptographique qui interdisait sa possession. Un aménagement au décret fut donc adopté pour ne pas pénaliser cette technologie dont on commençait à percevoir le potentiel… Arme de guerre ou non ? La question refait surface alors que la carte est utilisée pour des moyens de télécommunication ou de diffusion tels que la télévision à péage ou la téléphonie mobile.

L'affaire Humpich

En 1997, Serge Humpich, ingénieur autodidacte de la puce, réussit à casser la signature RSA, alors statique et stockée dans la carte, notamment à l'aide du processus décrit page 74. Il réalisa ensuite des cartes trompant les terminaux de la RATP (les yescards) qui n'exigeaient pas une identification forte, car traitant des transactions d'un faible montant. Il tenta de monnayer son savoir-faire, mais se fit interpeller dans le cadre de la loi Godfrain. Son procès en 2000 suscita quelque effroi, car lui et ses soutiens étaient en mesure de compromettre la clé RSA en la diffusant.

En fait, les fraudes d'origine technologique sont généralement restées d'assez bas niveau, l'essentiel des escroqueries étant à imputer à une incroyable naïveté des victimes et à l'habileté des escrocs en matière d'ingénierie sociale. Pourtant, une vraie vulnérabilité est apparue lorsque les cartes ont été dotées d'une capacité « sans contact ». Il s'est en effet avéré que cette technologie était piratable à courte distance et entraînait le risque d'exfiltration d'informations hautement sensibles. La Commission nationale de l'informatique et des libertés (CNIL) s'en est émue et impose désormais aux banques de désactiver cette fonctionnalité sur demande du porteur ou de lui fournir un étui « cage de Faraday » évitant la sollicitation électromagnétique non désirée.

Mais un risque bien plus inquiétant se profile. Avec ou sans contact, la carte à puce est un instrument de sécurité en elle-même. Or on entend beaucoup qu'elle pourrait disparaître en raison des offres nouvelles des géants de l'Internet et de la téléphonie. Que le téléphone utilise une puce SIM ayant de nouvelles capacités ou qu'il remplisse lui-même ces nouvelles fonctions, il n'y aurait alors plus de séparation entre l'outil de communication et le moyen d'identification et d'authentification – la puce. Une situation qui devrait faire le bonheur des pirates… et offrir aux géants du Web Google, Apple, Facebook et Amazon la mainmise sur un des rares domaines pas encore complètement sous la domination américaine. ■

BIBLIOGRAPHIE

Carte à puce et cryptographie : je t'aime moi non plus, conférence de J.-L. Desvignes et J.-J. Quisquater au Musée des arts et métiers du Cnam, 2015 : http://bit.ly/29mT1Lk

S. Bouzefrane et P. Paradinas, **Les Cartes à puce,** Hermès Science Publications, 2013.

C. Tavernier, **Les Cartes à puce. Théorie et mise en œuvre,** 2e édition, Dunod, 2011.

W. Rankl et W. Effing, **Smart Card Handbook,** 4e édition, Wiley, 2010.

M. Éluard et S. Lelievre, **YesCard, entre mythe et réalité ou un aperçu du système bancaire français,** MISC, hors-série n° 002, novembre 2008.

LOGIQUE & CALCUL

Est-il vrai que 0,999... = 1 ?

Les développements décimaux des nombres sont universellement utilisés. Cependant, certains nombres ont deux développements possibles. Il existe des approches qui tentent de l'éviter et de soutenir rigoureusement que 0,999... < 1.

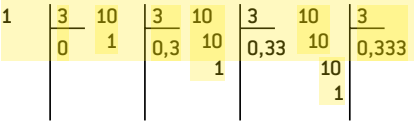
Jean-Paul DELAHAYE

Les notations aident à comprendre et soutiennent la pensée mathématique. De nombreux progrès sont dus à l'introduction de bons symboles et de règles précises qui en fixent la manipulation. Le système de numération décimal de position dû aux mathématiciens indiens des Ve, VIe et VIIe siècles de notre ère permet à tous de représenter des nombres très grands ou très petits et de calculer avec. Ce fut une invention extraordinaire sans laquelle la science n'aurait sans doute pas pu se développer, ni le commerce ou l'industrie moderne.

Il existe cependant des cas où une notation engendre des confusions dont il est difficile de s'échapper. C'est le cas, du moins en première analyse, du problème qui nous intéresse ici. La question est : « Est-il vrai que 0,999... = 1 ? » ou, au contraire, 0,999... < 1 ? »

L'expression 0,999... se réfère bien évidemment à la notation décimale des nombres réels. Les points de suspension signifient ici que la suite de chiffres 9 se poursuit indéfiniment. Cela n'a de sens que moyennant l'idée que n'importe quelle suite de chiffres avec une virgule, par exemple 192,252525..., désigne un nombre bien défini. Nous allons revenir sur le sens précis que l'on attribue aujourd'hui à cette notation. Mais auparavant, sans faire de théorie, et en appliquant quelques règles élémentaires de calcul, énumérons plusieurs des démonstrations que les professeurs de mathématiques proposent aux étudiants afin de les persuader que l'affirmation 0,999... = 1 est vraie.

Démonstration 1. Personne ne doute que 1/3 = 0,333... Imaginons en effet que l'on pose la division de 1 par 3. On trouve 0 ; puis 0,3 ; puis 0,33 ; puis 0,333. On est alors convaincu que cela se poursuit indéfiniment et donc que 1/3 = 0,333...



Partant de l'égalité 1/3 = 0,333..., en multipliant de chaque côté du signe égal par 3, on arrive à 3 × 1/3 = 3 × 0,333... ce qui donne 1 = 0,999...

De même, partant de 1/9 = 0,111... obtenu en posant la division, on arrive, en multipliant par 9 de chaque côté du signe égal, encore à 1 = 0,999...

Plusieurs démonstrations

Démonstration 2. Posons $u = 0{,}999...$ Multiplions de chaque côté par 10 (on remarque que multiplier par 10 un nombre en écriture décimale revient à déplacer la virgule d'une case vers la droite) : $10u = 9{,}999...$

Soustrayons maintenant $u = 0{,}999...$ de chaque côté de l'égalité : $10u - u = 9$ (car bien sûr 9,999... – 0,999... = 9). Cela donne $9u = 9$, donc $u = 1$. On a ainsi à nouveau prouvé que 1 = 0,999...

Démonstration 3. Faisons l'hypothèse que 0,999... < 1. Considérons la moyenne *m* des deux nombres 0,999... et 1. C'est un nombre inférieur à 1 et supérieur à 0,9, car la moyenne de deux nombres se situe toujours entre les deux nombres considérés. L'écriture décimale de *m* commence donc par 0,9. Cette moyenne *m* est aussi supérieure à 0,99 et inférieure à 1 ; c'est donc un nombre dont l'écriture décimale commence par 0,99.

En poursuivant, on établit que le développement décimal de *m* est nécessairement 0,999... La moyenne *m* est donc égale au plus petit des deux nombres considérés. C'est absurde, car la moyenne entre deux nombres différents n'est égale à aucun d'eux. L'hypothèse de départ, 0,999... < 1, est donc fausse. Comme il ne se peut pas que 0,999... > 1, on a nécessairement 1 = 0,999...

Il existe une autre fin possible pour ce raisonnement. On pose $u = 0{,}999...$ Nous avons établi que $m = (u + 1)/2 = u$, donc $u + 1 = 2u$, ce qui donne $u = 1$.

Toutefois, les enseignants de mathématiques le savent bien : même après l'exposé de telles démonstrations, si on interroge les étudiants en leur laissant vraiment la parole, ils exprimeront encore des doutes sur la validité de l'égalité. De nombreuses études réalisées en divers endroits du monde confirment que même après une ou plusieurs démonstrations en bonne et due forme, tout le monde n'est pas convaincu de l'égalité.

Des dizaines d'articles de didactique des mathématiques ont porté sur cette étrangeté. Il me semble qu'elle a une