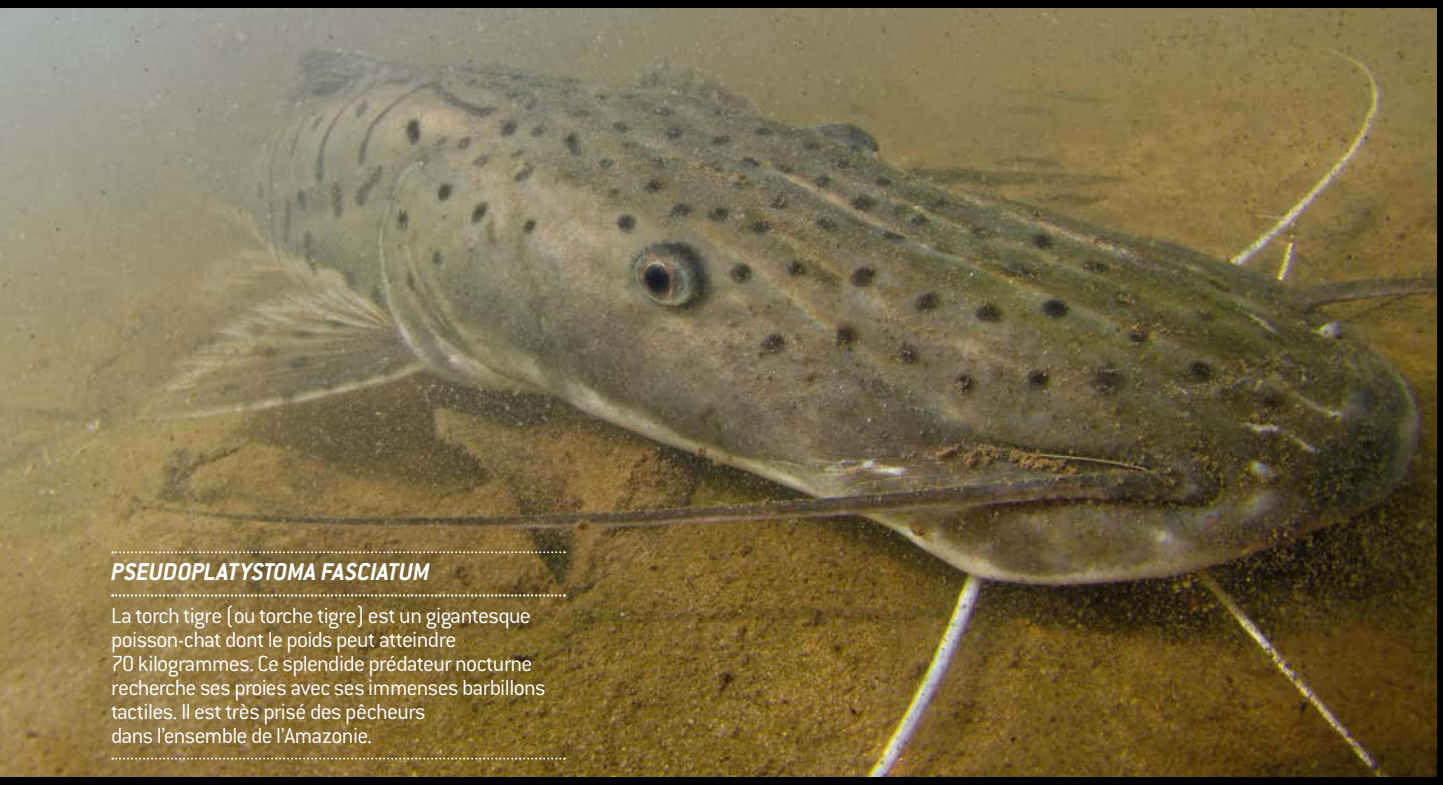


PSEUDOPLATYSTOMA FASCIATUM

La torch tigre (ou torche tigre) est un gigantesque poisson-chat dont le poids peut atteindre 70 kilogrammes. Ce splendide prédateur nocturne recherche ses proies avec ses immenses barbillons tactiles. Il est très prisé des pêcheurs dans l'ensemble de l'Amazonie.

CORYDORAS SP.

Les corydoras sont des petits poissons-chats sud-américains qui passent leur vie à fouiller le sable à l'aide de leurs barbillons. Cette espèce, pourtant rencontrée non loin de Cayenne, n'est pas encore identifiée. Il s'agit sans doute de l'une des multiples espèces inconnues et non décrites qui peuplent les cours d'eau de Guyane. Les corydoras sont parmi les poissons les plus recherchés par les aquariophiles.

POTAMOTRYGON HYSTRIX

Les raies d'eau douce, dont la queue est dotée d'un ou plusieurs dards venimeux, constituent le principal danger lié aux poissons en Guyane. Elles fréquentent des milieux sableux, propices à la baignade ou à la marche dans l'eau. Leur habitude de s'enfouir dans le sable et leur robe mimétique conduisent à un risque très réel de marcher dessus.

Frédéric MELKI, docteur en pharmacie et naturaliste photographe, est président-directeur général de Biotope, maison d'édition et entreprise d'ingénierie écologique. Les photographies de ce portfolio sont extraites de son livre *Poissons d'eau douce de Guyane – plongée dans les eaux de l'Amazonie française* (Biotope, 2016).

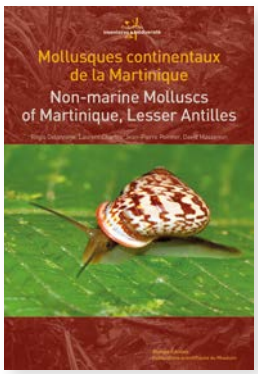
© Pour la Science - n° 466 - Août 2016

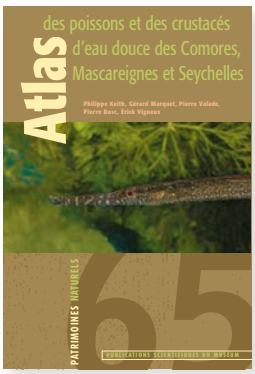
MUSÉUM
NATIONAL D'HISTOIRE NATURELLE

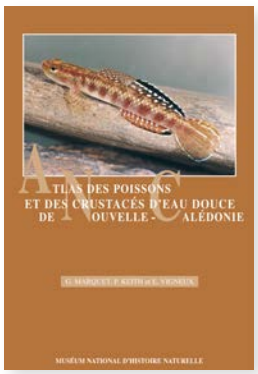
..... biodiversité - eau douce .....

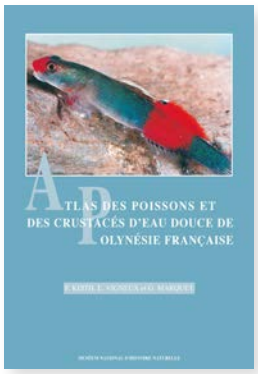
ESPÈCES DULÇAQUICOLES EN ZONE TROPICALE

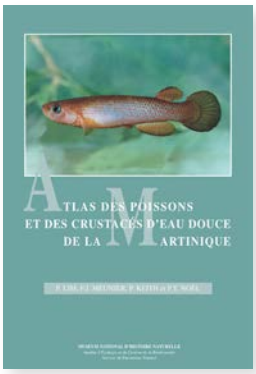
Atlas et inventaires

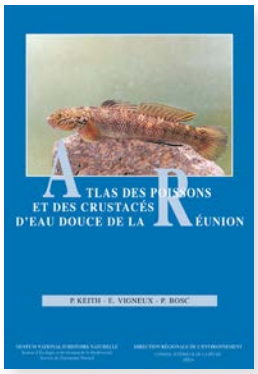




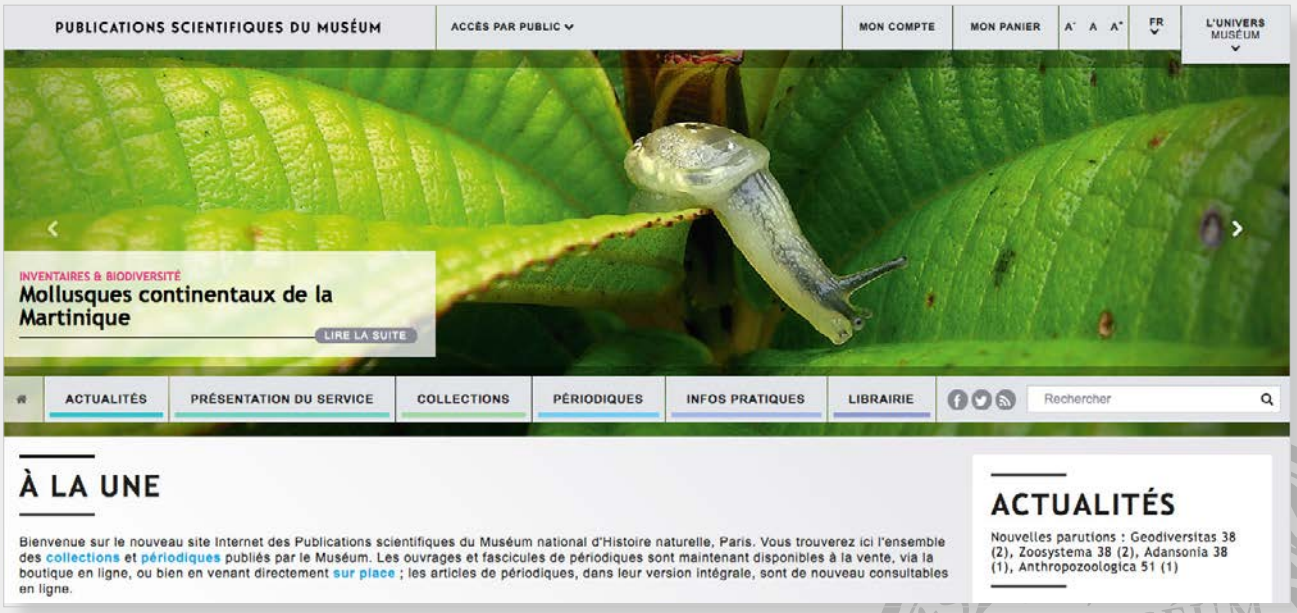








plus de renseignements et de contenus
sur la librairie en ligne des Publications scientifiques



Commandez vos ouvrages depuis le **monde entier** sans intermédiaire. Navigation transversale par **Moteur de recherche**, **Thèmes** et **Géozones**.

Téléchargez gratuitement les articles des revues *Geodiversitas*, *Zoosystema* et *Adansonia* (publiés depuis 2000). D'autres revues sont consultables ou référencées...

Composez votre propre sélection en éditant un **catalogue** personnalisé au format PDF (A4).

SCIENCEPRESS.MNHN.FR

MUSÉUM NATIONAL D'HISTOIRE NATURELLE
PUBLICATIONS SCIENTIFIQUES

Comment on a sécurisé

Jean-Jacques Quisquater et Jean-Louis Desvignes

Dans les années 1980, on s'est aperçu que la carte à puce n'était pas sans faille. Un mariage avec la cryptographie, domaine alors en pleine renaissance, s'imposait d'urgence...

la carte à puce

© Gettyimages/David Gould

L'ESSENTIEL

- À son apparition dans les années 1980 en France, la carte à puce était considérée comme inviolable.
- Mais bien vite, les premières attaques sont venues et il a fallu sécuriser davantage cette invention, d'autant que le ministère de la Défense envisageait son utilisation pour renforcer la sécurité de certains équipements de chiffrement.
- A commencé alors une course pour intégrer à la puce, malgré sa faible capacité, des algorithmes de cryptographie suffisamment puissants.

Depuis son lancement il y a quatre ans, le paiement sans contact connaît un succès croissant. Trois milliards de transactions ont eu lieu en Europe avec une carte Visa sans contact entre mai 2015 et mai 2016, soit près de trois fois plus qu'un an plus tôt, a annoncé la société Visa Europe. Dans les commerces de proximité, une transaction sur cinq est effectuée par ce moyen, contre une sur soixante en 2013. En France, l'adoption de ce mode de paiement a augmenté de 230 % en un an, conduisant à 194 millions de transactions sur douze mois, concernant plus de 2 milliards d'euros. La confiance accordée à ce mode de paiement est grande. Pourtant, fondé sur une communication en champ proche (un lecteur communique par ondes radio avec la puce de la carte bancaire à l'aide d'une minuscule antenne si la distance qui les sépare est inférieure à 10 centimètres), il est loin d'être inviolable : certes, des précautions empêchent que l'on vide votre compte (plafond de retrait à 20 euros, nombre de paiements sans contact limité par jour...), mais aucune mesure de sécurité n'a été installée au sein de la carte pour bloquer ce type d'attaque. Rien non plus n'empêche un hacker d'intercepter vos données bancaires en passant un lecteur près de la poche où vous conservez votre carte.

Un million de dollars sur un plateau

En fait, le paiement sans contact n'est que le dernier rebondissement d'une longue histoire, celle de la sécurisation de la carte à puce, dont nous avons été tous deux des témoins et acteurs, l'un (Jean-Jacques Quisquater) pour la partie technologique, l'autre (Jean-Louis Desvignes) en tant que gardien de l'usage de la cryptographie, alors dédiée à des utilisations militaires et gouvernementales. Ce qu'il montre surtout, c'est que l'histoire se répète. Au début de l'usage de la carte à puce, dans les années 1980, il était commun de croire que celle-ci était incassable et digne d'une confiance totale. Cette confiance était si ancrée qu'elle nous offrit un million de dollars sur un plateau.

Lors d'une grande exposition à Bruxelles, vers 1985, un directeur de Philips avait imaginé de distribuer plusieurs dizaines de milliers de cartes à puce, avec comme mission pour les participants de trouver le code d'accès de quatre chiffres, le code PIN. Le premier qui réussirait gagnerait un million de dollars. Or un simple calcul de probabilités montrait que, statistiquement, vu le nombre de cartes distribuées et le nombre de participants,

quelqu'un trouverait forcément le code de sa carte. Cela n'avait rien à voir avec la sécurité. L'un de nous (J.-J. Quisquater) en a fait la remarque au directeur, qui ne l'a pas cru. Avec Louis Guillou, un des pionniers de la sécurisation de la carte à puce, nous avons donc imaginé une attaque afin de montrer que l'on pouvait réellement casser le code de la carte *(voir page 74)*. La boîte de Pandore était ouverte.

Nous n'allons pas raconter ici l'histoire de la carte à puce, qui demanderait bien un livre pour rendre justice à tous et à tous les essais, mais nous allons tenter de montrer comment la carte à puce est devenue à la fois un objet de confiance, grâce à l'introduction de la cryptographie, et la gardienne des clés secrètes, un ingrédient essentiel… de la cryptographie elle-même.

Un objet inviolable par nature, pensait-on

Lors de son apparition, la carte à puce semblait être, de par sa nature même, une enceinte à l'abri des investigations malveillantes et un obstacle à la fraude pour les applications essentiellement monétaires auxquelles on la destinait. Il est vrai que la barrière technologique que constituait un circuit électronique pour le commun des mortels était déjà bien au-delà des compétences nécessaires à la lecture et à la manipulation de la simple bande magnétique des cartes alors en usage. Aussi les premiers développements et brevets n'utilisaient-ils pas vraiment la cryptographie. Que ce soient les Gondas dans *La Nuit des temps* de René Barjavel (1968) – une civilisation disparue qui, pour ses paiements, connectait une clé à un ordinateur central –, les premiers brevets japonais, allemands ou américains, ou encore la « bague » à puce conçue par Roland Moreno en 1974, rien n'indiquait que la puce devait contenir de la cryptographie, bien que des éléments de sécurité fussent évoqués *(voir l'encadré page 74)*.

Tout naturellement, la carte bancaire fut la destination privilégiée de la carte à puce, la simple carte en relief et son « fer à repasser » ou la carte à bande magnétique apparaissant vite, du moins aux banques européennes, comme insuffisamment sûres. Néanmoins, c'est une application imprévue qui fit décoller l'industrialisation de masse de cette technologie : la télécarte, simple réservoir d'unités de communication, qui permit de résoudre la question épineuse des milliers de monnayeurs des cabines téléphoniques. Une autre application de moindre étendue, mais touchant une population influente, contribua aussi à la visibilité de la carte à puce : la télévision à péage. C'est d'ailleurs celle-ci qui, alors que je (J.-L. Desvignes) dirigeais le Service central de la sécurité des systèmes d'information (SCSSI, devenu aujourd'hui l'Agence nationale de la SSI ou ANSSI), me conduisit à me pencher sur la sécurisation de cette technologie et à alerter le gouvernement sur la nécessité de s'en occuper d'urgence.

En 1996, une chaîne de télévision britannique, BSkyB, avait été victime d'un piratage à grande échelle de la part d'une société irlandaise. Celle-ci commercialisait ouvertement de fausses cartes d'accès aux programmes à prix bradé, et les rustines successives imaginées pour contrer ce piratage ne résistaient pas au trésor de guerre rapidement constitué par les pirates. C'est cet exemple de développement d'une industrie mafieuse permis par l'absence d'une prise en compte sérieuse des questions de sécurité au départ du projet que j'utilisai à l'époque afin de convaincre le ministère de la Santé d'adopter une démarche sécuritaire pour ses propres cartes : la carte Vitale et la carte des professionnels de santé. Inutile de décrire les risques qu'aurait comportés la distribution de telles cartes duplicables et falsifiables à souhait.

L'usage public de la carte à puce n'était pas le seul enjeu. Dix ans plus tôt, alors que j'étais « Officier chiffre » à l'état-major des armées, je m'étais occupé de la gestion des clés des équipements de chiffrement, et celle-ci était alors loin d'être satisfaisante. Comme tout responsable de ce domaine à l'époque, j'avais en tête la trahison de Hans-Thilo Schmidt, cet employé du chiffre allemand qui, plusieurs années avant la Seconde Guerre mondiale, avait monnayé auprès du service de renseignement français la fourniture du manuel d'utilisation d'Enigma – la machine à chiffrer allemande dont les décryptements ont été conduits successivement par les Polonais aidés des Français, puis par les Britanniques,

Les rustines successives imaginées pour contrer ce piratage ne résistaient pas au trésor de guerre rapidement constitué

■ **LES AUTEURS**


Jean-Jacques QUISQUATER est professeur émérite de cryptologie à l'université catholique de Louvain, en Belgique.

Jean-Louis DESVIGNES, général, est président de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI).

© Pour la Science - n° 466 - Août 2016

notamment le mathématicien Alan Turing – et de ses tableaux de clés, les paramètres de la machine qui permettaient de déchiffrer les messages. Ces renseignements avaient notablement facilité les travaux de cryptanalyse. Or jusqu'aux années 1990, les réseaux de chiffrement gouvernementaux tels que ceux de l'Alliance atlantique avaient peu évolué. Il s'agissait toujours de systèmes à clé secrète – ou systèmes symétriques (la même clé, privée, était utilisée pour chiffrer et déchiffrer) – dont l'initialisation (l'introduction de la même clé dans toutes les machines) était manuelle et permettait donc aux opérateurs d'y avoir accès physiquement.

Quelle que soit la rigueur du processus de sélection de ces opérateurs, il n'était pas exclu de recruter un individu susceptible de compromettre les éléments secrets qu'il manipulait. Certes, des efforts avaient été accomplis pour diminuer cette vulnérabilité en recourant à différentes astuces : des blocs de feuillets détachables journellement évitaient que la compromission des clés s'étale sur une période trop longue. Les techniques de grattage empruntées à certains jeux avaient aussi été envisagées. Sont ensuite apparus des conteneurs de bandes perforées impossibles à rembobiner après lecture (des sortes d'escargot), puis des injecteurs électroniques quelque peu blindés, simples mémoires dotées d'interfaces exotiques impossibles à lire pour un profane, mais d'un coût élevé.

Pour ma part, afin d'augmenter la sécurité des réseaux les plus étendus, j'avais paradoxalement commencé par allonger la cryptopériode de certaines clés pour diminuer le nombre d'exploitants amenés à les manipuler ! En passant de 24 heures à une semaine, je divisais par 5 ou 6 le risque de confier nos plus grands secrets à une brebis égarée.

C'est pourquoi, dès que la carte à puce est apparue, et notamment la carte Bull CP8 au milieu des années 1980, je cherchai à exploiter ses capacités pour initialiser à un coût modeste les nouveaux équipements de chiffrement. Au départ, la carte ne fut donc qu'un réservoir sécurisé de clés secrètes, comme dans le cas de l'équipement de cryptophonie gouvernemental DCS500 de Sagem *(voir la figure ci-contre en bas)*. Il fallut attendre la fin des années 1990 pour que la Défense utilise la carte à puce comme élément contenant les certificats de sécurité dans le cadre d'une « infrastructure de gestion de clés », c'est-à-dire recourant à des systèmes cryptologiques asymétriques. Ceux-ci, communément dits à clé publique (ces systèmes ont deux clés, une publique pour le chiffrement, une privée pour le déchiffrement), étaient apparus au milieu des années 1970, mais leur développement à grande échelle n'intervint qu'avec celui d'Internet.

© Wikimedia commons/ Papardelle

CES ANCÊTRES DE LA CARTE BANCAIRE *(en haut, la carte à deux puces de Philips, en bas, la carte CP8 de Bull)* portent l'élément clé qui rendit possible la sécurisation de la carte à puce : un processeur.

LE DCS500 DE SAGEM fut le premier équipement de cryptophonie numérique recourant à une carte à puce pour sa mise à la clé (l'introduction de la clé permettant de chiffrer et déchiffrer les messages). Il a été utilisé par les hautes autorités de l'État et les forces armées à partir des années 1990.

Toutefois, pour que de telles utilisations soient possibles et fiables, encore fallait-il que la carte à puce soit réellement un système sécurisé. Si l'on veut éviter certaines attaques, il faut associer à la puce une certaine puissance de calcul. Prenons le cas simple du mot de passe stocké sur la carte et utilisé pour avoir accès à une ressource, comme c'était le cas au début de la télévision à péage et du Minitel. Supposons une carte, associée à un utilisateur par un code PIN, qui tente de prouver son identité en communiquant ce mot de passe. Pour stocker ce mot de passe, il faut que la puce ait une mémoire inviolable et, par extension, qu'elle soit elle-même inviolable.

La cryptographie, une nécessité

En outre, si le mot de passe est transmis tel quel, en clair, il est facile à copier. Sa transmission ne doit donc pas se faire directement, mais en utilisant un détour, par exemple une question non prévue au sujet de ce mot de passe. En pratique, l'idée est d'utiliser des nombres aléatoires ou le mot de passe en coordination avec un algorithme cryptographique, par exemple une fonction de chiffrement ou un algorithme sans transfert de connaissance (visant à montrer qu'on connaît la solution d'un problème sans la révéler et, inversement, à contrôler la solution d'un problème sans en prendre connaissance).

Or cette idée qu'il fallait introduire une cryptographie forte dans la carte à puce faisait vite son chemin entre 1980 et 1984, notamment chez Bull avec Michel Ugon (inventeur de l'algorithme Telepass), au Centre commun d'études de télévision et télécommunications avec Louis Guillou (inventeur de l'algorithme GOC, générateur d'octets chiffrants) et chez Philips avec l'un de nous (J.-J. Quisquater). J'avais (J.-J. Quisquater) eu la chance, en 1976, de lire l'article *New directions in cryptography* de Whitfield Diffie et Martin Hellman, chercheurs à l'université

© Saul mention contraire, les photographies sont des auteurs

Stanford en Californie (qui ont reçu le prix Turing 40 ans après, en 2015, pour leurs travaux), au moment de sa publication. Alors qu'à l'époque, seule la cryptographie à clé secrète – symétrique – était utilisée, les deux cryptologues y proposaient le concept de système à clé publique et montraient l'intérêt de l'arithmétique des grands nombres premiers pour cette approche. Je travaillais alors comme chercheur dans un laboratoire de Philips à Bruxelles dédié aux mathématiques appliquées et, fasciné, je demandai à mon patron la permission de me lancer dans la cryptomathématique. Il accepta et, à sept, nous commençâmes à explorer le domaine, avant même que le premier système à clé publique, l'algorithme de chiffrement RSA, des initiales de ses trois inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman, toujours utilisé aujourd'hui, soit publié (il fut annoncé en 1977 par Martin Gardner dans *Scientific American*).

En décembre 1979, Philips France prit contact avec nous pour nous demander de participer à un appel d'offres du groupement d'intérêt économique (GIE) Carte à mémoire, rassemblant alors la Direction générale des télécommunications et des banques françaises, appel d'offres qui visait à tester la viabilité technique et économique de la carte à puce dans la vie réelle. Deux concurrents, Schlumberger et Bull, relevaient le défi, et Philips France voulait aussi tenter sa chance. Or l'équipe en charge du projet avait le sentiment qu'il fallait mettre de la cryptographie dans la carte à puce, au moins pour l'authentification. D'où son appel, puisque nous étions devenus le laboratoire de Philips dédié à la cryptographie. Ainsi, en 1981, le GIE Carte à mémoire lança trois tests grandeur nature de la carte à puce, respectivement à Blois avec Bull, à Caen avec Philips et à Lyon avec Schlumberger, comptant chacun plusieurs centaines de terminaux et plusieurs dizaines de milliers de cartes à puce. Et en préparation de cette expérience, dès début 1980, nous eûmes des réunions pour ajouter des fonctions cryptographiques et des protocoles de sécurité à la carte à puce.

Seule l'expérience de Blois fut jugée convaincante, et la carte à puce de Bull fut développée par la suite. Néanmoins, les cartes à puce étaient encore loin d'une sécurisation correcte, pour une raison simple : si les protocoles de sécurité entraient bien dans la carte, les algorithmes de cryptographie étaient trop

Trouver un code PIN en 1985

Étant donné la carte à puce, il suffisait d'essayer un premier chiffre du code PIN, de déterminer, avec un oscilloscope, la durée du calcul de vérification effectué par la carte et de stopper à temps l'alimentation de la puce afin d'éviter l'enregistrement d'une tentative erronée dans la mémoire de la carte. Vu l'implantation de l'époque, quand le chiffre était juste, le temps de calcul était moins long que quand il était faux. Par essais successifs, on déterminait ainsi le premier chiffre, puis chacun des suivants selon la même méthode.

L'invention de la carte à puce

La carte à puce est un morceau de plastique portant au moins un circuit intégré contenant de l'information. On peut donc faire remonter son aventure à 1958, année où Jack Kilby, de Texas Instruments, inventa le premier circuit intégré : il assembla plusieurs transistors sur un support de silicium, ce qui conduisit à la production de processeurs (Intel 4004 en 1969, puis 8008 en 1972) permettant de réaliser de véritables petits ordinateurs miniatures, sur une seule puce.

Cette miniaturisation poussa très tôt à imaginer des dispositifs portables pour traiter des paiements. Dès les années 1960, l'auteur de science-fiction René Barjavel décrivait dans son roman *La Nuit des temps* un système de paiement au moyen d'une « bague ». Et entre 1968 et 1972, plusieurs brevets ont été déposés dans ce sens au Japon, en Allemagne, en Grande-Bretagne et aux États-Unis, décrivant des cartes plastiques munies de mémoires électroniques.

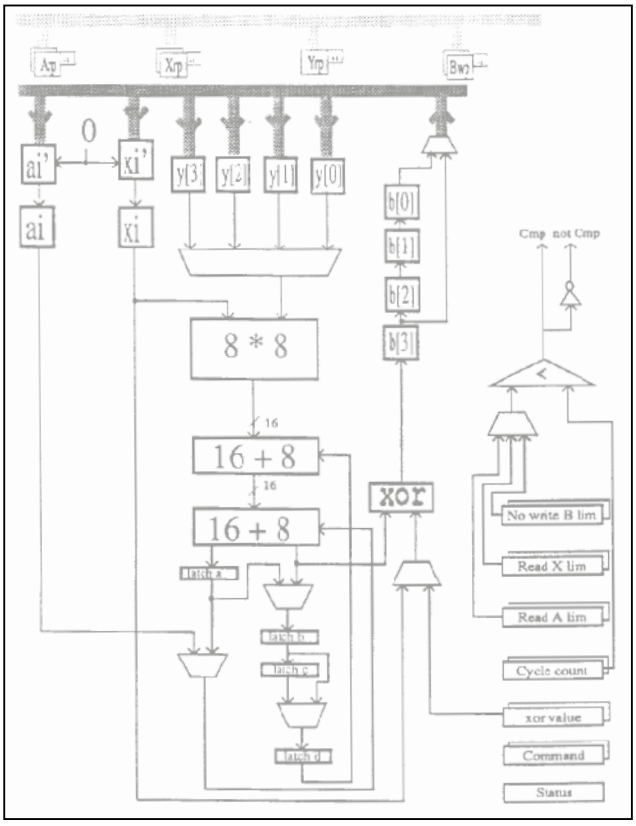
La paternité de la carte à puce à mémoire est souvent attribuée au Français Roland Moreno, qui déposa en 1974 le brevet de la carte à mémoire avec l'aide de Jean Moulin. Mais l'ingénieur français Michel Ugon *(médaillon)*, alors chez Bull, est le véritable père de la carte à puce dite intelligente. C'est lui qui inventa, en 1977, la carte intégrant aussi un microprocesseur, indispensable aux applications exigeant une capacité de calcul à des fins de sécurisation. C'est d'ailleurs Michel Ugon qui, en France, s'impliqua le plus, durant de nombreuses années, dans la sécurisation de l'ensemble de la filière Carte à puce.

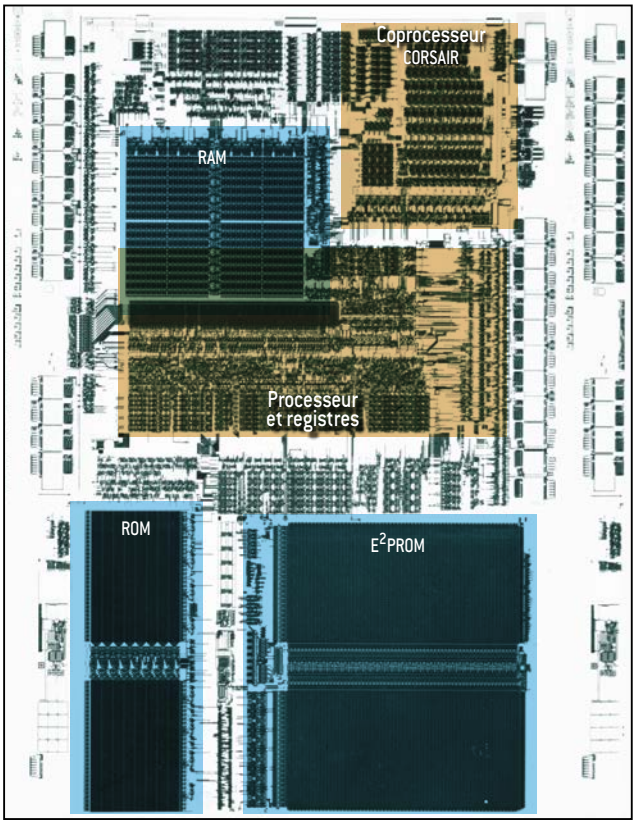
En 1977 et 1978, Michel Ugon déposa les deux principaux brevets sur les cartes à microprocesseurs. En mars 1979, il fabriqua la première carte à microprocesseur (à deux puces) et, en octobre 1981, la première carte monopuce à microprocesseur, la carte CP8 de Bull, qui conférait une meilleure sécurité. Les premières commandes industrielles furent lancées, qu'il s'agisse de la télécarte à puce ou de la carte bancaire. Toutefois, la cryptographie n'y était pas d'un très haut niveau, même si on y pensait. À une exception notable près, cependant : dans les années 1970, les travaux chez IBM sous la direction de Carl Meyer furent très tôt orientés vers l'utilisation de la cryptographie, et une version expérimentale de carte, très différente du modèle actuel, fut testée avec l'algorithme cryptographique Lucifer, ancêtre du DES, dans le cadre d'une expérience de transfert de données à Londres. Mais IBM ne poursuivit pas dans cette voie, sa banque sponsor n'ayant pas été convaincue et la technologie des cartes n'étant alors pas assez avancée. La carte à puce intelligente n'en était alors qu'à ses balbutiements…

– J.-J. Q. et J.-L. D.

© Michel Ugon

© Pour la Science - n° 466 - Août 2016





LA PREMIÈRE PUCE À RSA, CORSAIR *(à droite)*, comportait, outre différentes mémoires (ROM, RAM, E²PROM) et un processeur, un coprocesseur qui facilitait la multiplication de grands nombres – le principe sur lequel est fondé l'algorithme RSA. Le schéma décrit l'algorithme de ce coprocesseur. On y distingue un multiplieur de nombres de 8 bits (octet) et deux additionneurs d'octets. Le reste concerne des sélecteurs, pointeurs et des chaînes de registres qui servent à gérer les paramètres de l'ensemble et les adresses des données à traiter. C'est le plus petit coprocesseur jamais conçu. En un seul coup d'horloge, il réalise l'opération $x \times y + a + b$ où chaque élément est un octet. Cette opération est assez magique, car si on imagine que chaque élément est un chiffre décimal entre 0 et 9, le plus grand nombre pouvant être obtenu est $9 \times 9 + 9 + 9 = 99$, soit un nombre de deux chiffres sans report final vers la gauche. Cette opération seule suffit pour réaliser simplement toute multiplication de grands nombres entiers ainsi que leur division avec reste.

gros par rapport aux capacités des cartes pour y être intégrés, surtout ceux à clé publique. Or les contraintes venant du SCSSI étaient grandes: il fallait éviter le détournement des objets qui utilisaient la cryptographie forte, et la carte à puce ne pouvait donc devenir un réservoir de clés secrètes ou fournir des certificats de sécurité que si elle répondait à ces contraintes. En d'autres termes, ses algorithmes devaient être suffisamment puissants pour empêcher qu'un chiffrement soit facilement associé à un déchiffrement.

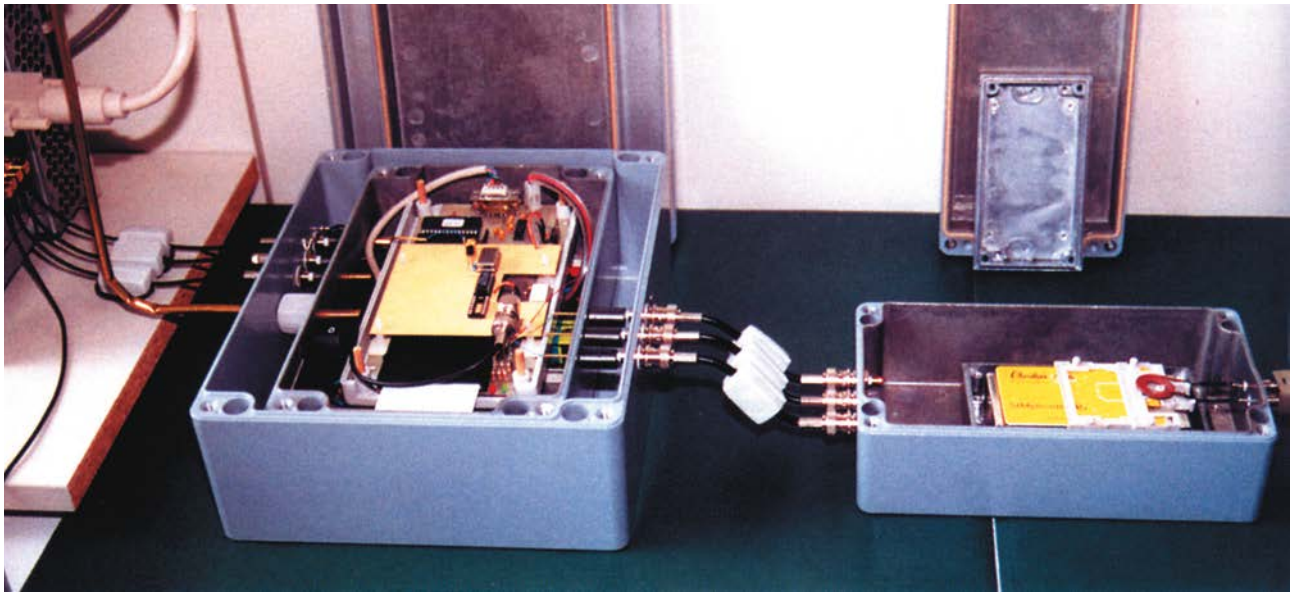
La course à l'algorithme

Au début, la carte comportait deux puces, l'une avec le processeur, l'autre avec la mémoire, ce qui offrait *a priori* plus de place pour l'algorithme. Mais on s'était aperçu que la connexion entre les deux, fort visible, permettait d'espionner les échanges processeur-mémoire (en détectant les variations d'intensité du courant consommé, par exemple). La monopuce avait résolu ce problème, mais pas celui de la capacité.

Les premiers algorithmes cryptographiques pour la carte à puce furent donc des algorithmes cryptographiques soit à sens unique, soit inversibles, mais toujours à clé secrète (Telepass 1, TDF, Telepass2, Videopass…). Ces algorithmes étaient bien adaptés à leur contexte restreint en vitesse et en mémoire ainsi qu'aux processeurs 8 bits en usage. Ils utilisaient entre 200 et 300 octets pour leur implémentation complète, ce qui est certainement un exploit. Cependant, l'absence de publication de ces algorithmes en rendait certainement l'usage plus restreint et la diffusion en dehors de la France difficile.

Le vrai départ s'est produit à Eurocrypt 1984, première conférence internationale publique sur la cryptographie, à Paris. Louis Guillou y présenta la carte à puce et l'accès conditionnel. Et lorsqu'on lui demanda pourquoi il n'utilisait pas l'algorithme DES, un algorithme à clés secrètes de 56 bits adopté comme standard en 1976, il répondit: « C'est impossible, car la ROM [mémoire vive] est bien trop petite. » Un défi que je proposai alors à mon équipe de relever. Il y avait en effet au même moment en Belgique un projet de transmission interbancaire sécurisée dénommé TRASEC, dont l'idée était de stocker les clés secrètes des transactions dans une carte à puce sous le contrôle d'un code PIN. Toutefois, l'exécution de l'algorithme DES avec cette clé s'effectuait dans un ordinateur non sécurisé. Intégrer l'algorithme à la carte permettrait d'obtenir

© Pour la Science - n° 466 - Août 2016



© EISS

AVEC UN DISPOSITIF MODESTE D'ANALYSE DES CARTES À PUCE branché sur un ordinateur, on mesure facilement des temps de calcul ou la consommation électrique, des informations très utiles pour retrouver la clé secrète utilisée dans le cryptosystème RSA des cartes.

cette sécurité manquante. Durant plusieurs mois, nous avons gagné octet par octet, déplaçant les permutations en usage dans le DES et les repliant. Nous avons ainsi réduit l'implantation à un total de 668 octets : chaque octet a coûté environ un jour de travail à une personne…

Le RSA sur une puce

Cependant, pour chacun de nous, le graal cryptographique de la carte à puce n'était pas le DES, mais le RSA. Cet algorithme fondé sur la détermination de deux grands nombres premiers à partir de leur produit était devenu le standard de la cryptographie. L'intégrer à la carte permettrait la signature, la distribution des clés, etc. Paul Barrett, de l'université d'Oxford, en Grande-Bretagne, inventa alors, en 1986, un nouvel algorithme pour le RSA, plus spécifiquement dédié à des processeurs pour traitement du signal. Nous sommes donc partis de cet algorithme. Après quelques tests sur une carte à puce, nous sommes arrivés à près de 100 secondes pour exécuter un algorithme RSA à 512 bits. Et à l'aide de quelques astuces (le stockage des multiples du module public et l'utilisation du théorème des restes chinois, qui permet de résoudre des équations d'arithmétique modulaire), nous avons fourni, toujours pour un module RSA de 512 bits, une signature en moins de 20 secondes. Un beau résultat, mais encore trop lent et trop gourmand en ressources pour être utilisé.

En 1989, Henri Molko, de Philips France et Allemagne, nous proposa un projet audacieux : créer un coprocesseur RSA en symbiose avec un processeur 80C51 pour réaliser une signature RSA sur 512 bits en moins d'une seconde (nous ferons 0,2 seconde). Sans moyens financiers, nous nous sommes lancés dans le projet CORSAIR *(Coprocessor RSA In a Rush)*. En cinq semaines, plusieurs versions du coprocesseur ont été imaginées à partir d'un nouvel algorithme que j'avais trouvé peu avant. Cela conduisit à une première accélération du RSA pour carte à puce par un facteur 500. Un premier prototype en silicium fut obtenu début 1990 : tout fonctionna, sauf l'écriture dans la mémoire morte effaçable de la carte (E^2PROM), « trop » optimisée en aval de notre projet *(voir la figure page 75)*.

Un nouvel algorithme, l'algorithme de Quisquater, avait donc été imaginé. Il se différenciait des autres par le fait que le coprocesseur était indépendant de la longueur de la clé et que l'exécution avait lieu à temps constant de bout en bout, car aucun test n'était effectué en cours de calcul, ce qui, *a priori*, évitait les attaques par mesure du temps d'exécution de l'algorithme.

Une course aux coprocesseurs de deuxième génération fut lancée parmi les fabricants : Fortress, Siemens, Infineon… et Philips. En 1995, Philips élabora un nouveau projet pour reprendre le dessus : FAME, qui nous conduisit à une nouvelle version 500 fois plus rapide que celle de CORSAIR. Son secret ? L'amélioration des circuits électroniques, avec l'ajout d'un multiplieur d'horloge qui augmentait de 16 fois sa fréquence, un multiplieur calculant le produit de nombres codés sur 32 bits (au lieu de 8), un bus (la ligne de transmission de l'information) plus large, une mémoire RAM à double accès très vaste et une meilleure chaîne de traitement au sein du coprocesseur. Ce coprocesseur est toujours utilisé dans des variantes optimisées. Au total, en dix ans, une accélération d'un facteur 250 000 a été obtenue entre la première version logicielle en 8 bits et celle de FAME.

Le développement des grandes applications de la carte à puce coïncida avec la volonté de plusieurs pays de définir une méthodologie pour évaluer la sécurité des systèmes informatiques. Les premiers, les Américains proposèrent à l'Otan, à travers l'*Orange Book*, les critères à respecter pour obtenir un niveau de sécurité donné. Ceux-ci apparaissant vite comme une arme de concurrence efficace pour imposer les produits américains, certains pays européens réagirent en proposant chacun un livre de couleur différente : vert pour les Allemands, jaune pour les Britanniques et… bleu-blanc-rouge pour les Français ! Finalement, la Commission européenne s'empara du sujet et ainsi naquirent les ITSEC (critères d'évaluation de la sécurité de la technologie de l'information) qui permirent aux pays européens de mettre en place leur schéma de certification. Notons que les ITSEC différaient de l'*Orange Book* : celui-ci vérifiait la présence de mécanismes

© Pour la Science - n° 466 - Août 2016

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…

1	3	10	3	10	3	10	3				
	0	1	0,3	10	0,33	10	0,333				
				1		10					
						1					

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

© Pour la Science - n° 466 - Août 2016