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).