La cryptographie à l'honneur : Diffie et Hellman, prix Turing 2015

Antoine Joux [1] et Cécile Pierrot [2]

Ouvrons une fenêtre sur le futur : San Francisco, Juin 2016. Sous les applaudissements des participants au banquet annuel, le président de l'ACM [3] remet le prix Turing à Whitfield Diffie, 72 ans, longtemps à la tête de la sécurité de Sun Microsystems, et Martin E. Hellman, d'un an son cadet, professeur émérite d'ingénierie électronique à l'université de Stanford. Doté d'un million de dollars et financé par Google, ce prix souvent perçu comme le Nobel inexistant de l'informatique récompense – enfin – « leurs contributions primordiales à la cryptographie contemporaine ». Un joli clin d'œil pour Alan Turing, considéré d'ordinaire comme le premier cryptographe moderne.

Parions que le président Alexander Wolf déclarera, fidèle à l'annonce de l'ACM en ligne : « Aujourd'hui, les communications chiffrées représentent un thème dominant des médias ; elles sont perçues comme un problème de sécurité nationale, affectent les relations entre les gouvernements et le secteur privé, attirent des milliards de dollars dans la recherche et le développement. » Il marquera une pause pour mieux reprendre : « En 1976, Diffie et Hellman imaginèrent un futur où nous communiquerions au quotidien via des réseaux électroniques, exposant ainsi la correspondance de chacun d'entre nous au vol ou à l'altération numérique. Quarante ans plus tard, on ne peut que saluer leurs prévisions extralucides. »

1. Université Pierre et Marie Curie (Chaire de cryptologie de la Fondation de l'UPMC), Laboratoire d'Informatique de Paris 6.

2. Laboratoire d'Informatique de Paris 6.

3. *Association for Computing Machinery.*

Pour mieux comprendre tout l'enthousiasme qui percera dans la voix du président, revenons quelque peu en arrière.

Alan Turing ou la cryptographie moderne

Jusqu'à la fin du XIX^{e} siècle la science des « codes secrets » s'attacha principalement à décrire des procédés de chiffrement, c'est-à-dire à convertir un message brut et clair en un texte illisible auquel seul un petit nombre d'élus pouvait rendre le sens initial. L'idée naïve consistait par exemple à échanger chaque lettre par une autre, ou à réarranger l'ordre de celles-ci. Parallèlement, les premières cryptanalyses allaient bon train : à chaque chiffrement répondait une tentative des adversaires pour « casser le code ». Ce n'est qu'avec l'avènement de la radio en 1903 et les enjeux de la première guerre mondiale que la cryptographie marqua son premier tournant vers la modernité. L'électricité et l'automatisation permirent un chiffrement progressivement plus complexe. En plus de la confidentialité des messages – l'information n'est accessible qu'à ceux dont l'accès est autorisé – on chercha, sans succès d'abord, à garantir leur authenticité – l'identité de celui qui nous écrit est certifiée – tout comme leur intégrité – une vérification atteste que les données n'ont pas été altérées pendant la transmission du message. L'horreur de la seconde guerre mondiale et la nécessité de ramener la paix donnèrent naissance au premier des cryptographes modernes : Alan Turing. En achevant la cryptanalyse de la machine Enigma utilisée par les allemands, Turing créa non seulement de toutes pièces ce que l'on considère comme le premier des ordinateurs mais ouvrit aussi le champ d'une cryptographie nouvelle, portée par l'électronique. L'informatique balbutiait. La cryptographie quittait l'enfance.

Un souci majeur contraria pourtant son développement pendant trois décennies successives. Si l'on comparait souvent le chiffrement à la dissimulation d'un message dans un coffre, suivi du verrouillage de celui-ci par une clef donnée, le déchiffrement devait permettre à tout détenteur de cette même clef, après voyage du coffre, de l'ouvrir pour révéler son contenu. La transmission du coffre-message pouvait prétendre à la meilleure sécurité possible, qu'en était-il de la clef ? En effet, celle-ci adopta très tôt, loin de l'objet matériel, une réalité plus abstraite recouverte par une correspondance de symboles, un mot, ou dorénavant un nombre plus ou moins grand d'octets. Le souci reposait alors sur l'existence de méthodes permettant de transmettre en amont cette information par des voies non sécurisées... Retour à la case départ.

L'avènement de la clef publique

New Directions in Cryptography parut en 1976. Petite révolution dans le domaine comme son titre le laissait déjà présager, cet article fondateur de Diffie et Hellman impulsa un changement de paradigme en formalisant la notion de cryptosystème

FIGURE 1. Whitfield Diffie (à gauche) et Martin E. Hellman (à droite)

asymétrique, c'est-à-dire de protocole où l'expéditeur et le destinataire n'ont aucune clef commune préalable. Exit alors le souci de sa transmission. Le schéma toujours d'actualité recommande la création non plus d'une clef partagée mais de deux clefs différentes associées ; l'une d'entre elles n'est pas secrète et peut être distribuée librement, c'est la clef publique, la seconde, privée donc, ne quitte en revanche jamais son propriétaire. Ainsi pour chiffrer un message il convient d'utiliser la clef publique de son destinataire, tandis que ce dernier se sert uniquement de la clef privée associée, sa clef, pour déchiffrer. Le cryptosystème RSA dessina l'année suivante une illustration exemplaire du chiffrement asymétrique.

Diffie et Hellman décrivirent au sein du même article une méthode de signature digitale, résolvant ainsi de manière satisfaisante le problème de l'authentification. Ici, le procédé est inversé : l'auteur d'un message utilise cette fois-ci sa propre clef privée pour signer ses écrits, tandis que tout un chacun peut vérifier son identité grâce à la clef publique qu'il aura préalablement distribuée. Les signatures numériques surpassent leurs homologues de papier en ce sens qu'elles permettent la détection d'une altération éventuelle : changer un mot dans le texte après sa signature rend celle-ci invalide. L'ajout malicieux de zéros sur les chèques de banque deviendrait ridicule avec une propriété similaire ; la signature manuscrite apposée reste malheureusement d'apparence valable, même une fois le montant modifié.

Et de nos jours ?

L'usage des chiffrements et signatures asymétriques est aujourd'hui indispensable aux transactions bancaires, aux serveurs de courriers électroniques comme aux sites en ligne. Qu'il en soit conscient ou non tout utilisateur d'Internet est familier de leur emploi : une URL qui commence par *https* indique par exemple, par la présence du *s* de *sécurité*, que le site fait appel à un protocole cryptographique. D'ordinaire celui-ci combine la cryptographie asymétrique – celle de Diffie et Hellman, qui permet de

nos jours de s'échanger une clef sans secret commun préalable – et la cryptographie symétrique, pour chiffrer ensuite les communications sous-jacentes.

Aussi sommes-nous heureux de voir cette distinction, même tardive, venir récompenser à la mesure de leurs découvertes ces pionniers de la cryptographie contemporaine. Leur récompense s'ajoute aux autres prix Turing décernés dans le domaine : le premier à Blum en 1995, le second à Rivest, Shamir et Adleman en 2002 pour la publication du système RSA un an après la révolution de Diffie et Hellman, et le dernier à Micali et Goldwasser en 2012.