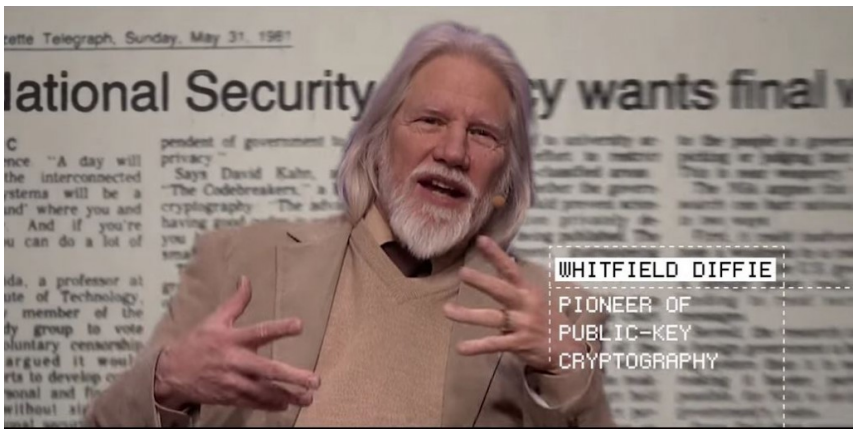
Symbolique : deux experts du chiffrement remportent le prestigieux prix Turing

Comme un symbole. Alors que le chiffrement s'est invité au centre des débats politiques – c'est vrai aux Etats-Unis avec l'affaire opposant Apple au FBI, mais aussi de ce côté-ci de l'Atlantique -, ce sont deux cryptographes de renom, **Whitfield Diffie et Martin E. Hellman**, qui se sont vu attribuer le prestigieux prix Turing, l'équivalent du Nobel pour l'informatique. Remis par une association (Association for Computing Machinery), la récompense, annoncée cette année lors de la RSA Conference, qui se tient cette semaine à San Francisco, est accompagnée d'une **prime d'un million de dollars**.

Le nom des deux chercheurs est associé à un algorithme essentiel du chiffrement, une méthode d'échanges de clefs qui fait partie des briques élémentaires de la cryptographie. Elle permet à deux personnes ne se connaissant pas de s'entendre sur un secret commun, et de communiquer dans des échanges à priori impossibles à déchiffrer par un tiers n'ayant pas ce secret en main. Cet algorithme est exploité dans l'initialisation de nombreux protocoles de sécurisation des communications : VPN, HTTPS, SMTPS…

Les inventeurs du chiffrement à clefs publiques

Comme le raconte le *New York Times*, les travaux de Whitfield Diffie, alors jeune programmeur au sein du laboratoire d'intelligence artificielle de l'Université de Stanford, trouvent leur origine dans une conférence d'un chercheur appelé John McCarthy, à Bordeaux, en 1970. Celui-ci y décrivait ce qu'on appelle aujourd'hui l'informatique en réseau : des terminaux connectés à des serveurs via des réseaux téléphoniques. La lecture des travaux de McCarthy amène Diffie à se poser la question de la signature de ces futurs échanges dématérialisés. Après des années d'effort, et avec l'aide de Martin E Hellman, un ingénieur de Stanford, il invente **en 1976** la technique du chiffrement à clefs publiques, permettant à des **personnes ne se connaissant pas d'échanger de façon confidentielle** des informations.



Martin Hellman et Whitfield Diffie ont également des positions bien tranchées en matière politique. Le premier milite contre les armes nucléaires et a indiqué qu'il utiliserait la part de la récompense qui lui revient pour poursuivre ce combat. Le second (en photo ci-dessus), qui a notamment travaillé pour Sun Microsystems comme directeur de la sécurité, est un défenseur de la protection des données personnelles. Il entend désormais se consacrer à écrire l'histoire du domaine qu'il a contribué à créer : la cryptographie.

Rappelons qu'une étude récente, à laquelle participaient des chercheurs de l'Inria et du CNRS, a montré que l'implémentation de l'algorithme d'échange de clefs Diffie-Hellman – et non l'algorithme lui-même – comporte une faiblesse, qui rend les échanges qu'il protège accessibles à une organisation ayant les moyens d'un état. De nombreux experts pensent que cette faiblesse pourrait expliquer l'architecture du système de déchiffrement des communications VPN de la NSA (appelé Turmoil), une architecture décrite dans un document Snowden publié par *Der Spiegel*.

A lire aussi :

L'Enisa très critique sur les contournements du chiffrement

Sécurité : 85 % des VPN SSL sont des passoires

Crédit photo : ACM