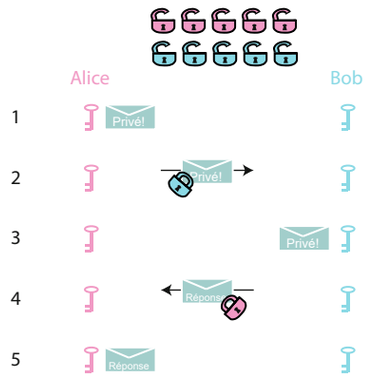
FICHE 9
Histoire de la cryptographie à clé publique

Dans les années 1960, l'informatique se développe et ouvre de nouvelles possibilités. La cryptographie, jusque-là réservée aux seules agences gouvernementales, devient accessible aux entreprises, voire aux particuliers. Mais, si deux personnes souhaitent communiquer secrètement, elles doivent se mettre d'accord sur une clé servant au chiffrement et au déchiffrement. L'échange des clés, qui a toujours été un casse-tête dans l'histoire de la cryptographie, devient un problème insurmontable à mesure que la cryptographie se démocratise.

Whitfield Diffie et Martin Hellman vont résoudre ce problème en 1976, dans un article intitulé New directions in cryptography resté fameux. Ces deux mathématiciens montrent qu'il est possible de communiquer secrètement en utilisant un chiffrement asymétrique. Le chiffrement asymétrique utilise 2 clés, l'une publique, l'autre privée. La clé publique permet de chiffrer le message, mais seule la clé privée permet de le déchiffrer.



Deux ans plus tard, Ron Rivest, Adi Shamir et Leonard Adleman améliorent cette idée pour créer l'algorithme RSA (nommé d'après leurs initiales). L'algorithme RSA utilise, pour simplifier, un très grand nombre, N, que l'on peut décomposer comme le produit de 2 nombres premiers *p* et *q*. N=*p*x*q*. N est la clé publique, tandis que *p* et *q* constituent la clé privée. N permet de chiffrer un message, mais l'opération de déchiffrement nécessite de connaître *p* et *q*. La sécurité de RSA repose sur le fait qu'il est très difficile de calculer les diviseurs d'un très grand nombre (on dit aussi « factoriser » un nombre). Même avec les meilleurs calculateurs, la factorisation peut prendre des années si le nombre est suffisamment grand. Pour cette raison, RSA est l'algorithme de chiffrement le plus utilisé dans le monde.

RSA est très sûr mais nécessite des moyens de calcul importants. Paul Zimmermann a résolu ce problème en 1991 en inventant un logiciel appelé PGP (*pretty good privacy*) qui est un compromis entre un chiffrement « classique » à clé privée et un chiffrement RSA. PGP a permis de démocratiser la cryptographie en la rendant accessible aux ordinateurs grand public. Cela lui a valu des poursuites judiciaires de la part du gouvernement américain. Certains gouvernements tentent en effet de limiter l'usage de la cryptographie de manière à pouvoir continuer d'intercepter les communications. Pour cela, ils exigent en général :

• Soit de limiter la taille des clés utilisées : une clé de taille « moyenne » est trop difficile à casser pour un ordinateur classique, mais pas pour un supercalculateur. Ainsi, la confidentialité est assurée vis-à-vis des particuliers, mais pas des agences gouvernementales ni des très grandes entreprises qui possèdent des supercalculateurs.

• Soit de déposer ses clés privées dans un « coffre » géré par un organisme « de confiance » (une agence gouvernementale par exemple). Ainsi, les communications sont secrètes pour tout le monde sauf pour ceux qui ont accès au coffre.

Longtemps réservée aux armées et aux diplomates, la cryptographie est aujourd'hui utilisée par de nombreux services : les banques (cartes bancaires, transactions sécurisées sur Internet), le commerce électronique, les messageries électroniques (carte SIM, e-mail…), les services médicaux (carte Vitale…), le vote électronique, etc.