FICHE 8
César et Al-Kindi, les premiers acteurs de la cryptographie

Les hommes ont toujours voulu protéger leurs communications, qu'il s'agisse d'envoyer des ordres militaires, d'espionner les puissances ennemies, de faire du commerce ou même d'échanger des lettres amoureuses. À l'époque de Jules César, très peu de personnes savent lire, et sa méthode de chiffrement, pourtant très simple, suffit dans la plupart des cas.

Au sortir de l'antiquité, ce chiffrement s'est raffiné : plutôt que simplement décaler l'alphabet, on mélange les lettres apparemment au hasard (en réalité, on utilise un mot- ou une phrase-clé). Les possibilités sont immenses et il est impossible, si l'on ne connait pas la clé, d'essayer tous les alphabets possibles. Ce chiffrement par « substitution mono-alphabétique » (à une lettre « en clair » correspond une, et une seule, lettre chiffrée) restera inviolé pendant près de 1 000 ans, jusqu'à ce qu'Al-Kindi invente une méthode (appelée « analyse de fréquence ») qui permet de le briser en quelques minutes.

Al-Kindi, de son vrai nom Abū Yūsuf Ya'qūb ibn Isāq al-Kindī, est l'un des plus grands savants arabes, auteur de plus de 290 manuscrits sur l'astronomie, les mathématiques, la médecine, la philosophie… Au IXe siècle après J.-C., alors que l'Occident s'enferme dans l'obscurantisme, les sciences arabes connaissent leur âge d'or. Al-Kindi remarque que certaines lettres sont beaucoup plus fréquentes que d'autres et que le chiffrement mono-alphabétique ne modifie pas ces fréquences. Par exemple, si « e » est chiffré en « L », la lettre « L » aura la même fréquence, dans le message chiffré, que la lettre « e » dans le message clair. Connaissant la fréquence des lettres dans une langue, il devient facile de retrouver le texte clair, si celui-ci est assez long. Al-Kindi devient le premier cryptanalyste de l'histoire.

Il faudra attendre le XVe siècle pour que Léon Battista Alberti invente le chiffrement par substitution poly-alphabétique, puis que Blaise de Vigenère le perfectionne. Cette méthode utilise plusieurs alphabets chiffrés et résiste à l'analyse de fréquence. Elle fera autorité pendant 3 siècles jusqu'à ce que Charles Babbage découvre une méthode pour la briser.

Depuis, la course continue entre les cryptographes (qui inventent des chiffrements) et les cryptanalystes (qui attaquent ces chiffrements). La cryptographie s'est mécanisée, puis informatisée. Les cryptographes actuels sont davantage mathématiciens que linguistes, mais les enjeux restent les mêmes. Cependant, comme nous le verrons, depuis l'essor d'Internet et la numérisation de nos communications, ces enjeux ont pris une dimension nouvelle :

- D'un côté, les États peuvent intercepter toutes les communications (e-mail, téléphone…) échangées entre deux individus, et souhaitent limiter l'usage de la cryptographie pour préserver la sécurité (espionner les terroristes, en particulier).
- D'un autre côté, les citoyens prennent conscience de l'importance qu'il y a de préserver leur intimité, qu'il s'agisse de leur vie de famille, leur santé, leurs opinions politiques, croyances religieuses, orientations sexuelles… Que peuvent devenir ces informations dans les mains d'un employeur, d'un assureur ou d'un gouvernement non démocratique ?