Comme suite à la lecture de « Histoire des codes secrets / de l'Egypte des pharaons à l'ordinateur quantique » de Simon Singh, voici un petit historique de la cryptographie et de la cryptanalyse au cours des siècles.

Définitions :

cryptographie : technique de chiffrement (cryptage par modification des caractères) ou de codage (cryptage par substitution de mots) d'un message pour en cacher le sens.

cryptanalyse : technique qui permet de déduire le texte en clair du texte chiffré (sans en connaître la clef), ou, plus rarement, codé.

Nota :

En cryptographie, la tradition veut que les descriptions d'échanges de messages mettent en scène des personnages fictifs nommés Alice (A) et Bernard (B). Un troisième personnage nommé Eve (E comme espion) cherche à intercepter le message.

-=-=-=-=-=-=-=-=-=-

Chiffre (cryptage par modification des caractères) par substitution de César : 1er siècle av. JC

Les arabes inventent la cryptanalyse (fin 8ème siècle), c'est-à-dire le décryptage (en l'occurrence le déchiffrage).

Apparition des codes (cryptage par substitution de mots et non de caractères) au 16ème siècle.

Blaise de Vigénère invente le mot-clef au 16ème siècle : les caractères successifs du message utilisent différents alphabets de substitution, déterminés à partir du mot-clef.

Arthur Scherbius fait breveter (1918) sa machine à chiffrer, nommée Enigma.

Alan Turing (mars 1940) met en service sa première bombe (machine programmable de déchiffrement) nommée Victoire.

Horst Feistel (1934) conçoit Lucifer : chiffrage classique, mais permet, grâce à l'apparition de l'ordinateur, de brouiller les bits ou les blocs de bits.

DES (Data Encryption Standard) (1976) : Lucifer à 56 bits.

Whitfield Diffie, Martin Hellman, Ralph Merkle inventent l'échange de clefs : Alice chiffre puis envoie, Bernard chiffre puis renvoie, Alice déchiffre puis renvoie, Bernard déchiffre. En fait, le système ne fonctionne pas car l'ordre des opérations n'est pas bon (en cas de non-commutativité des chiffres élaborés).

Hellman (1976) utilise l'arithmétique modulo pour qu'Alice et Bernard aient une clef commune sans se rencontrer, par la fonction à sens unique $Y^X \pmod P$ avec P premier et Y premier avec P. Ils conviennent de P et de Y par téléphone. Alice envoie $\alpha=Y^A \pmod P$. Bernard envoie $\beta=Y^B \pmod P$. Alice calcule $\beta^A \pmod P$. Bernard calcule $\alpha^B \pmod P$. Ils trouvent le même résultat. C'est la clef d'un chiffrement en DES.

Whitfield Diffie (1975) invente la clef asymétrique : Alice communique sa clef publique qui permet à Bernard de chiffrer le message qu'il envoie à Alice. Celle-ci le déchiffre avec sa clef privée (cohérente avec sa clef publique mais connue que d'elle même).

Ron Rivest, Adi Shamir et Léonard Adleman invente le RSA (1977) : Alice choisit deux nombres p et q premiers entre eux. Soit $N=pq$ et e tel que $e=(p-1)(q-1)$ a priori premier (raison technique). Alice diffuse e et N (sa clef publique). Bernard chiffre son message : $C=M^e \pmod N$ et l'envoie à Alice. Celle-ci calcule d tel que $ed=1 \pmod{(p-1)(q-1)}$ et déchiffre le message : $M=C^d \pmod N$.

Clifford Cocks, Nick Patterson et Malcom Williamson travaillent au sein du GCHQ (1973). Sur une idée de James Ellis, Cocks découvre une clef asymétrique proche du RSA (donc trois ans avant la formule d'échange de clefs de Hellman et quatre ans avant le RSA), mais cette découverte est restée secrète. Le GCHQ n'a même pas pu la breveter.

Phil Zimmermann met à disposition du public son logiciel PGP (version utilisable en 1991) qui procède comme suit pour accélérer les opérations : Alice veut envoyer un message à Bernard. Elle le chiffre avec une clef symétrique IDEA (similaire au DES) et l'envoie. Puis elle chiffre cette clef symétrique avec la clef publique de Bernard puis envoie le résultat. Bernard déchiffre la clef symétrique avec sa clef privée puis le message avec la clef symétrique. PGP (Pretty Good Privacy) se charge de l'ensemble des opérations : choix aléatoire de la clef symétrique, de la clef publique et de la clef privée.

PGP facilite aussi la signature numérique. Si Alice veut assurer authenticité et confidentialité : Alice chiffre préalablement le message avec sa clef privée, puis chiffre le résultat avec une clef symétrique IDEA et l'envoie. Puis elle chiffre cette clef symétrique avec la clef publique de Bernard puis envoie le résultat. Bernard déchiffre la clef symétrique avec sa clef privée puis le message avec la clef symétrique (confidentialité) puis avec la clef publique d'Alice (authenticité).

Peter Shor (laboratoire Bell / 1994) découvre un algorithme quantique (décomposition en facteurs premiers) capable de casser le RSA.

Lov Grover (laboratoire Bell / 1996) découvre un algorithme quantique (recherche d'une clef dans une liste) capable de casser le chiffre DES.

Stephen Wiesner (fin des années 60) propose une monnaie quantique : le numéro du billet (écrit en clair sur le billet) est codé par des qu-bits (présents sur le billet !) à base de photons dont la polarisation n'est connue qu'en consultant une base nationale. La lecture des qu-bits par un faussaire ne lui permettrait pas de connaître la polarisation, et même rendrait faux le billet.

Charles Bennett et Giles Brassard (1984) inventent la cryptographie quantique : Alice envoie à Bernard une série de photons sans lui préciser leur polarisation. Alice indique par téléphone à Bernard pour quels qu-bits il a choisi la bonne polarisation. Ils ne conservent que les valeurs des qu-bits lus avec la bonne polarisation par Bernard. C'est la clef jetable. Alice et Bernard testent quelques bits au hasard (test d'intégrité au cas où Eve ait lu donc modifié, ne connaissant pas, elle non plus, les polarisations). Alice et Bernard échangent un message chiffré avec la clef.

Septembre 2021