LAPLULVWG-λA-CRYPTOG®aPH1ε-NVNBXZA

Chtulhu, Kult, Conspiracy X, Rétrofutur... Autant de JDR qui comptent parmi leur liste de compétences la **cryptographie** (les méthodes de chiffrement), sans pour autant que celle-ci n'intervienne souvent au cours de scénarios. En effet, soit le PJ ne fait qu'un jet, auquel cas il ne sert à rien de rentrer dans les détails mécanistiques de la **cryptanalyse** (les méthodes de déchiffrement), soit le PJ décrypte le texte en direct, auquel cas il passe le reste du scénario dessus. Une solution est de donner des devoirs à la maison pour les petits PJs entre scénario. Mais bon, ça nécessite qu'une campagne soit en cours.

Au lieu de cela, je vous propose ici un bref aperçu de cette science qui depuis des millénaires est en perpétuelle évolution, constamment motivée par la guerre entre chiffrement et déchiffrement, menant amateurs et professionnels à toujours aller plus loin. Ainsi, cette guerre pourra se reporter entre PJs et MJs, mais l'avantage sera à ceux qui ont acheté ce fanzine ! HA HA !

1001001000111100100101010100000100010010

La confidentialité des messages a toujours été une priorité chez l'homme, qu'il soit en temps de guerre ou non. De nombreux grands savants ont contribué à sa sophistication continuelle. Beaucoup sont inconnus du fait même que leurs travaux devaient rester secrets. Cependant, un certain nombre de connaissances finit par être révélé.

La stéganographie et les oeufs durs (L5A...)

Il existe trois types de chiffrement non exclusifs. La **stéganographie** est une technique qui consiste à cacher la présence du message. Tout le monde connaît le fameux jus de citron qui apparaît à la flamme d'une bougie, mais il en existe bien d'autres. En Chine, on écrivait sur une soie fine, glissée dans une minuscule boule recouverte de cire, et qu'un messager avalait. Au XVIème siècle, un scientifique italien, Giovanni Porta, décrivit un procédé selon lequel il suffisait d'écrire avec une encre composée de vinaigre et d'alun sur un oeuf dur, alors l'encre traverse la coquille poreuse, la laissant intacte, et se dépose sur le blanc d'oeuf. Le destinataire peut alors aisément lire le message après avoir épluché celui-ci. Quant à la technique du jus de citron, elle s'applique en réalité à tout liquide organique riche en carbone, l'urine comprise, ce qui peut être bien pratique. Les tatouages sur la tête sont efficaces mais nécessitent le temps que repoussent des cheveux.

Cependant, la stéganographie a aujourd'hui peu d'applications, bien qu'elle puisse s'avérer très efficace. Pendant la seconde guerre mondiale, les Allemands utilisaient le micropoint : un texte sans intérêt se terminait par un point final, et au-desssus de celui-ci se trouvait un microfilm d'un mm de diamètre contenant une page de texte A4 réduite. Sans microscope, sa lecture est impossible. Ceci met aussi l'accent sur un autre point fondamental de la cryptographie : elle dépend intimement de l'avancée technologique contemporaine, et cela dès le XIXème siècle.

La cryptographie par transposition

Vient ensuite la **cryptographie** à proprement parlé, qui elle a pour but non de cacher la présence du message, mais d'en cacher le contenu par cryptage. Son principe est le suivant : un envoyeur, Bernard, code un texte «clair» selon une technique de cryptage A avec sa clef 1. Le message crypté est transmis au receveur, Alice, qui applique le processus de décryptage inverse de A, et avec la clef 1 également. Si quelqu'un de mal intentionné, Eve, veut intercepter le message, il sera crypté. Mais elle peut comprendre qu'il est crypté par A. Cependant, elle n'a pas la clef 1, et seule cette clef peut permettre le déchiffrement.

Là, on peut discerner deux techniques de cryptographie, la **transposition** et la **substitution**.

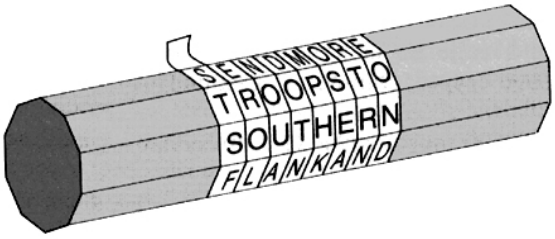
La transposition consiste en la redistribution des lettres d'un message selon un processus donné, le hasard étant le plus haut niveau de sécurité, mais impossible à décrypter. Un des plus simples mais efficace est la transposition en dents de scie :

Prenez cet exemple.

P E E C T X M L
R N Z E E E P E.

PEECTXMLRNZEEPE.

Voici un autre exemple, la scytale spartiate. Bernard enroulait un ruban autour du morceau de bois, la scytale, écrivait le message ainsi, et le ruban était déroulé, transmis



et décrypté par Alice grâce à sa propre scytale.

Venons cependant au principal, le chiffrement par substitution. C'est de très loin cette technique qui fut et reste la plus utilisée, car elle laisse cours à nombre de procédés possibles, ayant permis d'accéder à une sécurité théoriquement impénétrable, nous le verrons ensuite.

Le chiffre de César (Vampire : Dark Ages...)

Tout débute pendant la guerre des Gaules. César nous raconte comment un message codé fut envoyé par lui à Cicéron qui s'apprêtait à se rendre, lui annonçant l'arrivée imminente de renforts.

Le code consiste à substituer la lettre claire par celle qui de trois lettres la suivait dans l'alphabet :

a b c d e f g h i j k l m n o p q r s t u v w x y z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
veni, vidi, vici
YHQL, YLGL, YLFL

Le principe de ce *chiffre de César* fut ensuite largement utilisé, en décalant de trois ou de n'importe quel autre nombre compris entre 1 et 25 (on appellera à partir de maintenant ce nombre la clef, qui peut être un chiffre comme 3 ou une lettre, ici D qui code a). Il resta indéchiffré jusqu'au jour où le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oomran ibn Ismaïl al-Kindi (eh oui, pas de chance...), versé dans la linguistique et les mathématiques, comprit que chaque langue comprenait des lettres de fréquence donnée. Par exemple, la lettre la plus fréquente en français est toujours le e. Ainsi, si le texte crypté est assez long, on peut établir les fréquences de chaque lettre codée. Ainsi, si le X est la plus fréquente, on a peu de chance de se tromper en affirmant qu'elle code le e (en français), et on peut ensuite en déduire toutes les autres lettres car il ne nous reste qu'à appliquer un chiffre de César de clef 19. Le premier pas dans la cryptanalyse était fait, la science du déchiffrement. Voici pour vous la fréquence usuelle des lettres en français :

A	9.42%	J	0.89%	S	7.90%
B	1.02%	K	0.00%	T	7.26%
C	2.64%	L	5.34%	U	6.24%
D	3.39%	M	3.24%	V	2.15%
E	15.87%	N	7.15%	W	0.00%
F	0.95%	O	5.14%	X	0.30%
G	1.04%	P	2.86%	Y	0.24%
H	0.77%	Q	1.06%	Z	0.32%
I	8.41%	R	6.46%		

Le carré de Vigenère (7éme mer...)

Il fallait donc trouver une nouvelle méthode de chiffrement, sachant que le déchiffrement ci-dessus peut tout de même être limité dans le cas de textes courts non représentatifs, ou de textes volontairement biaisés en telle ou telle lettre (le meilleur exemple étant le roman de 200 pages de George Pérec «La disparition» sans le moindre e). Une première technique fut un décalage comme le chiffre de César, où chaque lettre n'est plus chiffrée par un seul caractère mais par un nombre de caractères différents proportionnel à sa fréquence dans un texte clair normal. Ainsi, le e à 15,87% sera chiffré par 16 graphes qui lui seront propres. Le résultat est qu'une analyse de fréquences montre une centaine de graphes différents qui ont tous une fréquence égale. On ne peut donc pas utiliser cette technique. On peut cependant recourir à la fréquence des couples de lettres, aussi bien caractérisées que celles des lettres seules. Par exemple, le q et le u sont toujours en pair... Donc pas de quoi assurer une sécurité absolue pourtant toujours nécessaire.

Afin de montrer l'importance historique de la cryptographie, on peut citer la mort de Marie Stuart, reine d'Ecosse, dont le complot contre la reine d'Angleterre fut démasqué par le cryptanalyste Phelippes, ou l'identité du masque de fer, un simple général des armées de Louis XIV qui avait fui devant l'ennemi autrichien, laissant là ses troupes, et fut puni par emprisonnement, obligé de porter le masque en question.

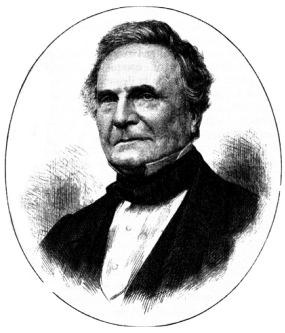
C'est seulement en 1586 que Blaise de Vigenère publia «le traité des chiffres» qui devait révolutionner la cryptographie. Il avait en effet mis au point une méthode prétendue infaillible. C'est simple, au lieu de décaler toutes les lettres d'un texte de la clef 3, comme pour le chiffre de César, on attibue à chaque lettre une clef différente. Par exemple, le mot Chtulhu, crypté selon la clef *drap* donne :

Chtulhu	(texte clair)
drapdra	*(clef)*
FYTJOYU	(texte crypté)

Ainsi, je veux coder la lettre c par la clef *d*, je prends l'alphabet décalé où a est codé en D (la même chose q'une clef de 3, voir ci-dessus). J'obtiens F. On voit également que le code de clef *a* ne transforme pas le texte clair. En bref, on fait la même chose que César, mais avec un alphabet différent à chaque lettre. La clef est un mot facile à retenir, qui est répété autant de fois que le texte le nécessite. Les cryptanalystes rentrent chez leur maman et pleurent. Rien ne peut briser ce code. Tout du moins c'est ce qu'on a cru jusqu'au XIXème siècle.

Babbage contre de Vigenère (Maléfice...)

Blaise de Vigenère


Charles Babbage

Sans entrer dans des considérations historiques, voici comment Babbage décrypta le chiffre de Vigenère. Tout d'abord, si le mot-clef utilisé est de taille assez petite, comme *drap*, on peut finir par voir une même suite de caractères comme FYTJOYU répétée dans le texte crypté, car le mot Chtulhu est répété dans le texte clair, et il se trouve que la clef pour les deux est *drapdra* (et pas *rapdrap* par exemple).

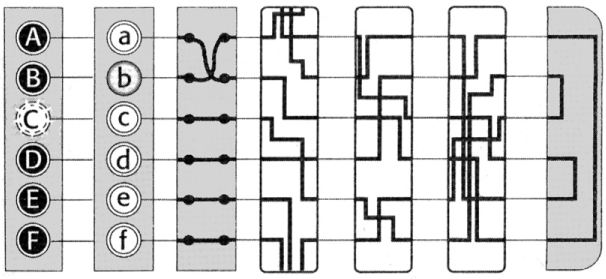
Ensuite, on compte le nombre de lettres entre les deux FYTJOYU, on trouve 24. On trouve également d'autres suites de caractères répétés, qui eux sont séparés par 16 et 36. Le seul dénominateur commun entre ces trois nombres est quatre. Donc la clef fait quatre lettres (24=**4**x6, 16=**4**x4, 36=**4**x9). Et alors, vous allez me dire ? Mais les enfants, le problème est résolu ! Il suffit alors de mettre ensemble toutes les lettres cryptées par la 1ère lettre de la clef (ici *d*), c'est-à-dire en position 1, 5, 9, 13... qui à eux seuls forment un texte certes incompréhensible, mais tout à fait adapté pour l'analyse de fréquences. Il suffit alors de refaire la même chose avec les lettres cryptées qui sont en 2ème, 6ème position... (position 2+4n, où n est vaut 1, 2, 3...), puis tous les 3+4n, et finalement tous les 4n. Babbage a terrassé la Bête Vigenèrienne. Cela nécessite cependant un mot-clef court. On peut tout à fait utiliser comme clef un texte entier bien connu, comme la déclaration d'Indépendance aux USA. En 1817, un américain du nom de Beale, accompagné d'une trentaine d'autres hommes, a trouvé selon la légende une mine d'or, représentant 20 millions

de dollars. Il crypta trois textes, avec un texte-clef différent pour chacun. Ils contiennent l'histoire, l'emplacement et les noms des propriétaires du trésor. Evidemment, le texte indiquant l'emplacement n'a toujours pas été décrypté, car aucun texte clef essayé n'a fonctionné, contrairement à la page de l'histoire dont la clef était cette Déclaration d'Indépendance. Dans ce genre de cas, il faut essayer comme clef tous les textes connus, en supposant qu'il soit connu. C'est donc quasiment impossible. Un clef longue permet donc une sécurité absolue mais n'est pas pratique du tout en terme de rapidité le décryptage, ce qui est absolument nécessaire en cas de guerre.

La machine Enigma (Rétrofutur)

Face à la faiblesse de ses codes pendant la 1ère guerre mondiale, ce qui a participé à sa défaite, l'Allemagne prit les devants pendant la seconde guerre mondiale. Il fallait un chiffre sûr et pratique. Les responsables des communications du IIIème Reich optèrent pour un projet d'un dénommé Scherbius, qui avait inventé une machine baptisée Enigma. Voici son principe.

La machine est composée de plusieurs parties : un clavier, où l'on tape le texte clair à chiffrer, un tableau lumineux indiquant les lettres chiffrées correspondantes, puis, reliant l'un à l'autre, un réseau de connexions complexe. Ce réseau est composé de trois rotors qui peuvent tourner sur eux-mêmes, comme le montre la figure suivante, permettant un nombre de chemins possibles très grand entre lettres du clavier et lettres du panneau. En plus de cela, on peut utiliser le tableau de connexions, qui sert à inverser des chemins entre eux, augmentant le nombre de possibilités. Le dernier composant est le réflecteur. Voilà comment ça marche. On tape sur la lettre b sur le clavier, un courant électrique suit les cables jusqu'à atteindre la diode sous le C du panneau lumineux. Le réflecteur ne complexifie pas le chemin, il permet le déchiffrement. En effet, en tapant le texte chiffré sur le clavier, on obtient le texte clair sur le panneau lumineux, condition indispensable à l'utilisation de toute machine de cryptage. La clef ici correspond à l'ordre des trois rotors, tous différents les uns des autres, et leur position de rotation. Les connexions du tableau de connexions font aussi partie de la clef.



panneau lumineux | clavier | tableau de connexions | 3 rotors amovibles | réflecteur

Chaque jour, les soldats allemands devaient décider d'une clef. Là est la faiblesse de tous ces modes de cryptage. La transmission de la clef présente un grand risque. Aussi avaient-ils établi un carnet de clefsjetables renouvelés tous les mois. Il n'était donc pas soumis à une transmission trop dangereuse. Ce que les nazis ne savaient pas cependant, c'est qu'un polonais déçu par l'Allemagne avait communiqué les plans d'Enigma à l'Angleterre, rendant l'immense tâche de décryptage envisageable. Rejewski, c'est son nom, non content de cela, lança aussi les bases du décryptage du chiffre généré par Enigma. Mais les moyens du Biuro Szyfrow, le bureau de décryptage polonais, n'étaient pas suffisants, bien qu'ayant une avance théorique énorme et insoupçonnée sur tout le reste du monde dans ce domaine. Il se basait sur le principe que la répétition est l'ennemie de la sécurité. Or par souci de sécurité justement, les messages allemands étaient codés par une clef propre à chaque message, elle-même précisée au début du texte, mais cryptée selon la clef du jour disponible sur les carnets. En effet, si le message n'était codé que par la clef du jour, et si celle-ci était découverte, tous les messages du jour seraient décryptés. Cette clef propre au message était répétée deux fois, par sûreté. Cette prudence fut leur perte.

A ce stade, je ne veux pas rentrer dans les détails du déchiffrement d'Enigma, ce serait trop technique et inutile. Quoiqu'il en soit, là encore on peut voir l'avantage que la cryptanalyse a pu donner aux Alliés pendant la guerre, interceptant et traduisant de nombreux messages nazis, évitant de nombreux morts, l'embargo sur l'Angleterre, mais aussi permettant le choix du lieu de débarquement en Normandie...

Il est par contre important de souligner ici le comportement du gouvernement anglais. En effet, le Commandant Alaistair Dennison, dirigeant ces opérations, avait une politique bien particulière. Premièrement, tous les décrypteurs travaillaient sous le serment de ne rien dire de leurs activités, rendant anonymes leurs efforts de guerre, comme pour Alan Turing qui en faisait partie. Certains furent traités après la guerre comme des collabos, car tout le monde croyait qu'ils n'avaient pas oeuvré pour la victoire Alliée. Deuxièmement, le Commandant faisait travailler ces hommes alors qu'il connaissait lui-même les clefs à trouver, via des espions français. En effet, il s'attendait bientôt à ne plus avoir accès aux carnets, et ne voulait pas que l'on soit dépendant des réussites irrégulières des résistants. Troisièmement, les informations tirées des messages n'étaient pas forcément exploitées, quelque soit leur importance. Si les nazis voyaient tous leurs navires coulés par des croiseurs anglais allant directement à leur position, ils se seraient inquiétés et auraient renforcé leur Enigma, en rajoutant des rotors, par exemple. Tout aurait été à refaire. Ils savaient donc ce qui allait se passer, mais se taisaient, sacrifiant ça et là des positions pour conserver leur avantage via l'accès aux messages ennemis. C'est là d'où vient la principale difficulté de gestion en temps de guerre.

Puis la guerre prit fin, laissant sa trace indélébile. Mais déjà la cryptographie avait un autre cheval de bataille.

Clés privée et publique (Conspiracy X,...)

L'avénement des ordinateurs a permis à la cryptographie de faire un véritable bond, comme ça a été le cas dans de nombreux autres domaines. Il fallait un système de cryptage adapté au système binaire des bits. Ce code répond pour les lettres à la convention ASCII suivante :

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000110	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Ainsi le texte DRAP se code 1000100 1010010 1000001 1010000.

Le système de brouillage encore utilisé actuellement se nomme le DES (Data Encryption Standard), appelé originellement Lucifer, inventé par Horst Feistel, un immigré allemand aux USA.. La NSA (Agence nationale de sécurité) avait proposé un concours pour trouver un algorithme confidentiel pour assurer les communications gouvernementales américaines. Ils reprochèrent d'abord à l'inventeur ses origines, mais finirent par choisir Lucifer car il était de loin le plus efficace. Il s'agit d'une transformation opérée sur un texte clair en binaire, consistant en un remaniement très complexe de l'ordre des nombres, mais totalement réversible et déterminée par la clef.

Il restait cependant un problème majeur pour l'application du DES à Internet : l'échange de cette clef, étape indispensable et qui rend vulnérable tout système de cryptage. Il fallait donc trouver un moyen de contrer cette faiblesse. Ceci est l'oeuvre de plusieurs scientifiques, un premier anglais travaillant sous serment qui ne fut reconnu que très tard comme l'inventeur originel, et deux équipes de trois hommes, Diffie-Hellman-Merkle et Rivest-Shamir-Adleman.

C'est le concept révolutionnaire de clefs privée et publique. Revoilà Bernard qui veut écrire à Alice. Il consulte un annuaire de clefs publiques accessibles à tous, et trouve celle d'Alice. Il crypte ce message selon cette clef. Alice reçoit le message crypté, et utilise sa clef privée pour le décrypter. C'est la seule à pouvoir le faire. Donc ni Eve ni Bernard ne peuvent décrypter le message, car ils n'ont pas la clef privée, gardé bien secrète par Alice. Ce concept se base sur l'existence d'un mode de cryptage asymétrique. Je m'explique. Le texte clair est normalement crypté par un algorithme A donné, avec une clef 1, puis décrypté selon l'algorithme exactement inverse avec la meme clef 1. Pour ce système asymétrique, le décryptage nécessite une clef différente de 1, et c'est la clef privée. Ceci est permis par l'existence de fonctions irréversibles, asymétriques. a donne G selon telle fonction, mais le passage de G à a nécessite une autre transformation. Il existe très peu de fonctions de ce type et ce fut le principal obstacle de ces chercheurs. Ils finirent par mettre au point la fonction RSA, encore utilisée actuellement. Cette fonction est une fonction modulo, qui fonctionne comme un cadran horaire. Modulo de base 12 transforme 1 et 1, mais aussi 13 en 1, 17 en 5, comme on lit l'heure l'après-midi. Il existe des modulo de n'importe quelle base. Cette base est en fait la clef publique. Elle est le produit de 2 chiffres très grands, la clef privée. Trouver ces deux chiffres à partir de la clef publique prendrait des millions de fois l'âge de l'univers avec les ordinateurs actuels. Donc c'est pas mal. Mais, un hic, théorique du moins... à voir au paragrahe suivant.

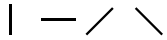
Je tiens juste à faire remarquer que le système RSA couplé au DES sont associés dans le logiciel PGP, accessible sur Internet sur www.pgpi.com (version internationale, pas américaine ! Sinon, vous serez poursuivis par la NSA). Pour la petite histoire, ce logiciel a été mis en ligne gratuitement dans les années 70 par Zimmermann, un américain qui luttait pour le respect de vie privée. Il n'avait pas payé les droits sur le RSA au NSA, car il était déjà certain qu'il se le verrait refusé. En effet, le NSA veut conserver son emprise sur les communications, afin d'assurer la sécurité fédérale par l'écoute et le décryptage des échanges entre citoyens. Un certain nombre de réseaux criminels ont été démantelés ainsi. Mais Zimmerman voulait que ces pratiques cessent, pour éviter que Big Brother n'observe chacune des ses pensées intimes. Quelques mois plus tard, Zimmerman fut jugé pour traffic d'armes (eh oui, les codes comme celui-là sont considérés comme armes lourdes dans les mains des méchants terroristes). Le FBI et le NSA débarquèrent chez lui plusieurs fois... De quoi devenir parano. Quoiqu'il en soit, le système fédéral n'a rien pu faire contre lui car aucune loi ne concernait le transfert d'informations sans support matériel. Aujourd'hui, PGP est utilisé à travers le monde, par les entreprises surtout. Elle permet une sécurité absolue, sauf évidemment si Eve est équipée d'un système *tempest-attack*, un détecteur de signaux électromagnétiques portable permettant de savoir sur quelles touches de votre clavier vous tapez, la machine n'ayant cependant q'uune portée de quelques mètres. Mais pour éviter qu'on ne vous chope votre clef ainsi, rien de tel qu'un bon écrantage sur les murs de votre appartement ! Il faut cependant une licence gouvernementale pour acquérir ce matériel.

La cryptographie quantique (Cyberpunk)

Nouveauté : le DES ne fonctionnerait plus si l'ordinateur quantique existait , étant sa capacité théorique de calcul. Comme je suppose que la mécanique quantique vous réserve encore ses secrets, petit exposé succinct.

La lumière est composée de corpuscules indivisibles nommées photons, aux propriétés ondulatoires. Ceci fut mis en évidence par Young (par ailleurs grand cryptographe ayant lançé les bases du déchiffrement des hiéroglyphes égyptiens), envoya un faisceau lumineux vers une plaque percée de 2 fentes parallèles relativement éloignées. Il vit sur l'écran disposé juste derrière des bandes clair-obscur, et conclut qu'il s'agissait des interactions entre les ondes lumineuses séparées par les fentes.

Cependant, les physiciens actuels peuvent reproduire l'expérience mais avec un fin filament, qui n'émet les photons qu'un par un. On ne devrait donc pas voir les bandes clair-obscur sur l'écran, car il n'y a pas interaction entre un seul photon et lui-meme. Et là, c'est le drame. Eh merde, qu'ils dirent en voyant les petites bandes sur l'écran. Ne pouvant remettre en cause l'indivisibilité des photons, les physiciens proposèrent deux hypothèses, la superposition d'états de Schrodinger, et celle des multivers. En gros (limite faux), le photon a deux états probables superposés entre son émission et son interception par l'écran : passage par la fente 1 ou par la 2. Le seul fait de percevoir les bandes sur l'écran contraint le photon à choisir entre ces deux états équiprobables. Pour les multivers, au contraire, le photon a un seul état mais passe par différentes réalités parallèles. Ces concepts mettent tout le monde mal à l'aise, alors ne vous inquiétez pas. Quoiqu'il en soit, un ordinateur basé sur des photons peut profiter de ses états superposés, car 128 calculs devraient pouvoir être faits en même temps au lieu d'un pour nos ordinateurs actuels. La factorisation de la clef publique n'est plus qu'une question de jours. Mais, comme vous allez le deviner, les cryptographes n'ont pas attendu que cet ordinateur soit sorti pour trouver un système de cryptage adapté à cette technologie. Et oui, la cryptographie quantique, mise au point par Stephen Wiesner et Charles Bennett, répond à toutes les attentes théoriques, car c'est le seul chiffre qui est absolument indéchiffrable, tant qu'on ne réfute les bases de la mécanique quantique. Elle se base sur le fait que les photons ont quatre états possibles suivants, appelés spins :



Quand un photon de spin vertical passe par une fente verticale, il est inchangé, et par une fente horizontale il ne passe pas. Quand le photon de spin oblique passe par une fente verticale, il devient de spin vertical. Prenons un exemple. Le texte clair est transcrit en une séquence de photons de spins vertical, vertical, oblique, horizontal, oblique. On le fait passer par une fente verticale, le texte crypté en sortant est vertical, vertical, vertical, rien, vertical. Maintenant, faisons passer la séquence par une fente en croix, donc horizontale et verticale. La séquence en sortant sera vertical, vertical, indéterminé, horizontal, indéterminé. En effet, comme on l'a vu ci-dessus, le photon de spin oblique va avoir plusieurs états possibles superposés en sortant de la fente, horizontal ou vertical. De cette manière, on a appliqué un chiffrement asymétrique : un photon de spin horizontal à la sortie de la fente peut provenir d'un photon horizontal ou oblique. Le déchiffrement est donc impossible, sauf dans certaines conditions que je ne préciserai pas ici, et qui peuvent être transmises comme clef de Bernard à Alice.

Voilà un bref tableau de l'histoire de la cryptographie, pouvant servir aussi bien dans le cadre de scénarios, que dans une petite séance de déchiffrement pour PJs. La clef du chiffre peut alors être précisée au PJ selon son niveau en cryptographie, voire le texte directement déchiffré.