Du message chiffré au système cryptographique

Marie-José Durand-Richard

DU MESSAGE CHIFFRE AU SYSTEME CRYPTOGRAPHIQUE

Marie-José DURAND-RICHARD[1]

Le décryptement d'un message chiffré en mode polyalphabétique par le mathématicien anglais Charles Babbage (1791-1871) en 1846 marque sans doute un premier rapprochement entre cryptologie et mathématiques. Et ce rapprochement peut paraître continu à la lecture des « lois de Kerckhoffs », telles qu'elles sont aujourd'hui présentées, sous forme mathématisée, pour introduire les systèmes de sécurité dans l'enseignement de la cryptologie. Pourtant, Auguste Kerckhoffs (1835-1901) ne faisait alors qu'énoncer en 1883, un ensemble de critères cherchant à caractériser un système cryptographique. Plaquer l'état de nos connaissances présentes sur l'histoire de la cryptologie des 19e et 20e siècles est donc un raccourci brutal qui ne permet pas de comprendre comment s'est opérée la rencontre entre cryptologie et mathématiques. Celle-ci n'est pas seulement le fruit d'une convergence technique ou opératoire. Elle a été marquée par une transformation profonde des significations épistémologiques et sociales, tant des conditions d'exercice de la cryptologie que de celles du calcul. Ainsi, au temps de César, le chiffre qui porte son nom[2] ne s'énonçait pas en termes d'addition modulo 26 sur l'ensemble des permutations dans un ensemble à 26 éléments ! Et l'énoncé de Kerckhoffs ne contient aucune référence à une quelconque écriture ensembliste ou fonctionnelle qui n'est pas encore advenue, et qui mettra du temps à pénétrer le milieu cryptographique. La référence à ces auteurs ne cherchera pas ici à repérer des précurseurs ou des

[1] mjdurand.richard@gmail.com. Université Paris Diderot, Sorbonne Paris Cité, SPHERE-REHSEIS, UMR 7219, CNRS, F-75205 Paris, France.

[2] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » pp. 24-25.

anticipations fructueuses de la situation actuelle, mais à percevoir les enjeux spécifiques d'un tel rapprochement.

Au 19e siècle, les pratiques cryptologiques restent le fait de manipulations scripturales. Elles vont d'abord évoluer par le biais de pratiques matérielles nouvelles, suscitées par la mise en place de réseaux techniques – télégraphe, téléphone, téléscripteurs, *etc.* – qui feront système bien avant que la théorie des systèmes ne s'empare des théorisations informatiques ou cybernétiques au milieu du 20e siècle. Or, l'existence de ces réseaux, qui relève de la raison d'être de cette cryptologie en voie de mathématisation, se trouve pour le moins masquée – ou reste pour le moins implicite – dans les présentations générales des dernières avancées de la cryptologie. Celles-ci préfèrent se référer aux échanges inter-individuels entre Alice et Bob[3]. Référence trompeuse s'il en est, qui traduit des échanges collectifs d'ordre commercial ou militaire en histoires personnelles ! Ce chapitre vise donc à expliciter les conditions de mathématisation de la cryptologie liées à l'existence de ces réseaux de communication.

Ainsi la mathématisation de la cryptologie se trouve-t-elle médiatisée par la nécessité de travailler matériellement sur des systèmes de codes liés à des systèmes techniques nouveaux. C'est bien la naissance du télégraphe qui modifie radicalement l'exercice de la cryptographie, entre les savantes recherches privées de Charles Babbage et l'article d'Auguste Kerckhoffs sur *La cryptographie militaire.* Lorsque Gilbert S. Vernam (1890-1960), ingénieur à la section télégraphique de *l'American Telephon & Telegraph Company* (AT&T) à Manhattan, conçoit son système à bandes chiffrantes au sortir de la Première Guerre Mondiale, il travaille à la sécurité des téléscripteurs. Il ne mobilise pas l'addition sur le groupe {0, 1} d'une théorie des groupes finis encore inexistante ! Il travaille sur des impulsions électriques et sur des rubans perforés dont les trous et les espaces correspondent aux signes du code Baudot[4], et c'est bien la matérialité technique qui constitue le support de ses pratiques et de sa réflexion. Claude E. Shannon (1916-2001) travaille initialement dans un tout autre contexte – celui de l'optimisation du fonctionnement d'une machine destinée à

[3] De très nombreux manuels de cryptologie, y compris des exposés de chercheurs, ainsi que les ouvrages de vulgarisation, présentent les échanges cryptographiques comme devant préserver le secret (bien souvent amoureux) entre deux acteurs, nommés Alice et Bob, parfois Bernard, et laissent implicite la question de la sécurité du système tout entier. Voir par exemple Rémi, « La cryptographie à clé publique », p. 48 ; Misarsky, « Cryptanalyse et spécification des schémas de redondance RSA », p. 8.

[4] Ce code, dit code *Murray* par les Anglo-saxons, est aussi appelé code télégraphique ou alphabet international (AI) n° 2, ou code CCITT n° 2. C'est un des premiers codes binaires ainsi mis en œuvre sur une machine.

résoudre les équations différentielles[5] – lorsqu'il remarque, en 1937, que les connexions d'un circuit électrique peuvent s'exprimer dans les mêmes termes qu'une algèbre de Boole. Ingénieur et mathématicien, Shannon élabore un nouveau langage, exprimant le fonctionnement de ces circuits en termes mathématiques. Mais c'est bien en tant que cryptologue qu'il élabore sa célèbre théorie de l'information au sortir de la Seconde Guerre Mondiale. Quant au cryptologue Horst Feistel (1915-90), il est déjà chargé d'élaborer des algorithmes cryptographiques chez IBM (*International Business Machines*) lorsqu'il conçoit ses algorithmes de chiffrement par blocs, qu'il exprime en termes d'algèbre binaire. Ce sont ces textes que j'ai retenus pour mieux cerner quelques moments décisifs de la mathématisation de la cryptologie associés à la maîtrise des réseaux de communication.

BABBAGE ET LE DECRYPTEMENT DU CHIFFRE DE VIGENERE

Charles Babbage est aujourd'hui surtout reconnu comme mathématicien. Il est souvent considéré comme un pionnier en matière d'ordinateur – une projection rétro-historique parmi tant d'autres ! – parce qu'il a conçu les plans d'une machine, *The Analytical Engine*, à la suite de sa *Difference Engine* partiellement construite. En effet, la « machine analytique » peut être assimilée à une calculatrice automatique à programme externe, dont la structure opératoire[6] est effectivement la même que celle d'un ordinateur classique d'architecture von Neumann, distinguant et isolant mémoire, organes de calcul, et organes de contrôle, organes d'entrée et de sortie. Mais Babbage est également l'auteur de recherches trop méconnues en cryptologie.

Les travaux de décryptement de Babbage

Le manuscrit aujourd'hui conservé à la *British Library*, « Philosophy of Deciphering »[7], témoigne d'une activité constante en ce domaine, et au moins reconnue par ses pairs, de 1831 à 1870. Il accumule des matériaux destinés à une publication, à laquelle il semble pourtant renoncer faute de temps[8]. Fondateur de la *Statistical Society* en 1834, il échange avec le

[5] L'analyseur différentiel a été conçu et construit au MIT (*Massachusetts Institute of Technology*) par Vannevar Bush (1890-1974) en 1927. Il a rapidement été reproduit en Angleterre, à Manchester, puis à Cambridge, par Douglas R. Hartree (1897-1958).

[6] Durand-Richard, « Charles Babbage : de l'école algébrique anglaise à la 'machine analytique' ».

[7] Babbage, Add. Mss 37 205.

[8] Babbage fait de nombreuses références à cet ouvrage qu'il voudrait publier, et au temps qui

célèbre astronome et statisticien belge Adolphe Quetelet (1796-1874) dès 1831 sur l'analyse des fréquences des différents langages[9]. Il établit des tableaux de fréquences des lettres en analysant d'importants ouvrages : pour la langue anglaise, les *Sermons* de Hugh Blair (1718-1800) publiés en 5 volumes de 1771 à 1801, et pour la langue allemande, *Die Phosphorescenz der Körper* (1811-15) de Placidus Heinrich (1758-1825)[10]. Babbage offre la première trace du décryptement d'un message chiffré par une substitution alphabétique de type Vigenère, même si ce résultat reste en partie ignoré, au moins jusqu'à ses échanges avec un certain Mr Thwaites dans les colonnes du *Journal of the Society of Arts* en 1854-55. Cependant, bien que les idées de Babbage soient innovantes, aussi bien en cryptologie qu'en mathématiques, il reste un auteur charnière, un « gentleman amateur » qui élabore ses machines dans l'atelier qu'il a fait équiper dans sa propre demeure, un « polymath » qui se préoccupe de l'harmonie entre tous les aspects de la « philosophie naturelle », plutôt que de chercher la spécialisation des disciplines. S'il enquête longuement pour son *Treatise on the Economy of Machines and Manufactures* (1832), c'est avant tout pour mobiliser les hommes de pouvoir afin de coordonner les développements industriels, alors facteurs de profonds déséquilibres politiques et sociaux.

Ses travaux de cryptologie coïncident avec les débuts du télégraphe, dont il appréhende tout à fait l'importance socio-économique, tout comme il enquête en tant qu'expert pour s'assurer de la sécurité des chemins de fer. Charles Wheastone (1802-75)**Erreur ! Source du renvoi introuvable.**, l'inventeur du télégraphe en Angleterre, est un de ses amis. Il invente aussi, en 1854, un procédé de chiffrement par substitution de digrammes, qui se trouve répertorié dans le manuscrit de Babbage[11]. Ce mode de chiffrement est communément appelé « carré de Playfair », du nom du baron Lyon Playfair (1818-98) qui le présentera aux autorités. Wheatstone, comme Playfair, a le souci d'éviter que les textes des télégrammes puissent être lus par tous, au moins pour certains sujets sensibles[12]. Cependant, contrairement à Wheatstone en 1854, contrairement aussi à John H. B. Thwaites au même moment, Babbage n'aborde pas la question du secret des correspondances télégraphiques. Il ne considère que les messages privés échangés au sein de cette élite cultivée qu'il veut convertir à la science et où il fait autorité[13]. La

lui manque, trop absorbé sans doute par la conception et les tentatives de fabrication de ses machines. Babbage, Add. Mss 37 205, folios 211, 214.

[9] Babbage, « On the proportion of Letters Occurring in Various Languages ». Quetelet traduit cette lettre en français et la publie en 1831. Add. Mss 37 205, folio 230.

[10] Franksen, *Mr Babbage's Secret*, p. 211.

[11] Babbage, Add. Mss 37 205, folio 80.

[12] Un appareil qui mécanise ce procédé, le cryptographe de Wheatstone, porte également son nom. Davies, « Wheatstone's Cryptograph ».

[13] Durand-Richard, « Le regard français de Charles Babbage ».

cryptologie reste pour Babbage une activité réservée à cette élite, une aristocratie proche du pouvoir, celle qu'il reçoit dans ses dîners mensuels et à laquelle il fait admirer sa « machine aux différences ». Auteur charnière entre les pratiques scripturales et le développement des réseaux, Babbage se considère lui-même comme un philosophe – au sens de la « philosophie naturelle » – selon le titre de son autobiographie[14].

C'est donc avec les érudits et aristocrates de ses amis et connaissances que Babbage se consacre à la cryptographie, une activité à laquelle il s'adonne tout à fait régulièrement, et qui semble le fasciner suffisamment pour qu'il entreprenne d'en répertorier les principales méthodes, qu'il puise essentiellement dans le traité de cryptographie du révérend John Wilkins, évêque de Chester, *Mercury or the Secret and Swift Messenger* (1641). C'est d'ailleurs à Wilkins – dont les œuvres viennent alors d'être rééditées – et non à Vigenère, que Babbage attribue le chiffrement polyalphabétique, signe de l'importance des traditions nationales en ce domaine. Les *agony columns,* ces messages du journal *The Times* où s'échangent soupirs et rendez-vous galants, sont une source importante d'exemples des modes de chiffrement élémentaires pour Babbage, qu'il utilise en deux exemplaires dans son manuscrit, l'un comme explication, l'autre comme exercice. Babbage et Wheatstone n'ont donc aucun mal à les décrypter, ce dernier allant jusqu'à s'immiscer dans ces correspondances pour mettre en garde les protagonistes ou s'en moquer[15]. Plus sérieusement, et très systématiquement, Babbage dresse un inventaire chronologique et conceptuel des systèmes de chiffrement, et accumule des matériaux d'aide au décryptement[16] : dictionnaires, inventaires, répertoires, analyse de fréquences sur des lettres et des mots courts, recherche d'équations simultanées. Il est régulièrement sollicité pour décrypter des correspondances, et insiste auprès de ses interlocuteurs sur les difficultés du décryptement en l'absence d'une bonne connaissance du contexte ou de la langue, surtout quand il s'agit d'analyses historiques. En 1835, il aide l'astronome Francis Baily (1774-1844) à reconstituer le sens d'une lettre datée de 1722, de l'assistant de l'astronome royal John Flamsteed (1646-1719), écrite comme une sorte de sténographie, afin de déterminer l'origine des erreurs constatées dans les observations de son arc mural[17]. En 1854, il intervient dans un procès, décryptant une abondante correspondance chiffrée afin de rétablir l'honneur de la famille du capitaine Childe[18]. Enfin, en 1858, il détermine pour Mrs Green[19] que les lettres qu'elle possède doivent être attribuées au roi Charles II plutôt qu'à

[14] Babbage, *Life of a Philosopher.*
[15] Babbage, Add. Mss 37 205, folios 66, 80.
[16] *ibid.*, folios 211, 214.
[17] Franksen, *Mr Babbage's secret*, p. 18.
[18] Babbage, Add. Mss 37 205, folios 81 à 130.
[19] *ibid.*, folios 209 à 214.

Charles I. Dès le début des années 1830, Babbage innove dans ses échanges avec ses amis, Davies Gilbert (1767-1839) – président de la *Royal Society* de 1827 à 1830 – ainsi que le géologiste William H. Fitton (1780-1861) et sa sœur Mrs James, composant un système auto-clé, et discutant de ses possibilités et inconvénients selon que le mot-clé utilisé est soit le texte clair, soit le texte chiffré[20].

Premier décryptement du mode polyalphabétique

C'est entre février et mars 1846 que Babbage va décrypter un message chiffré en mode polyalphabétique, à l'occasion d'un jeu avec son neveu Henry Hollier qu'il a initié à la cryptologie lorsqu'il était enfant, et qui l'aide à établir ses dictionnaires de déchiffrement – répertoires de mots et analyse de fréquences sur des mots courts. L'intérêt du manuscrit « Philosophy of Deciphering » est de rassembler ses nombreux essais, dont la collecte est malheureusement incomplète, et qui, à l'évidence, n'est pas rangée dans le bon ordre[21]. Le message chiffré est le suivant :

```
PYRI  ULOFV

POVVMGN  MK  UO  GOWR  HW  LQ  PGFJHYQ OJAV  MSN
WIJHEEHPR  BRVGRUHEGK, EFF WJSR  RVY
CPOY  VSP,  PX  OKLN  PI  XXYSNLA  SELF  XG
FEEWTALV  LJIU, WR  MOI  EGAP  HMFL  ML  YINZ
TNGDDG  YQIV  UYEAP-BQL
     WJQV  PGYK  STRITLMHFOFI EWTAWK
               TIEJC
```

Babbage découvre assez vite qu'il s'agit d'un mode de chiffrement polyalphabétique. Il fait à ce sujet de nombreuses analyses de fréquences à partir des mots courts, de 2, 3 et 4 lettres. La première difficulté de son travail provient du fait que le message a été chiffré à partir de trois clés différentes, difficulté que Babbage devra d'abord identifier avant de parvenir au texte clair. Après quelques tentatives infructueuses pour écrire et résoudre des systèmes d'équations simultanées – ces systèmes étant incomplets –, Babbage repère d'abord qu'il est possible d'associer, à chaque lettre de l'alphabet, le nombre qui correspond à son rang.

Alors, pour chaque lettre du chiffré, du clair et du mot-clé qui se correspondent, Babbage découvre l'existence d'une opération entre les

[20] *ibid.*, folios 8-9. Babbage, *Life of a Philosopher*, p. 175-176.
[21] *ibid.*, folios 43 à 63.

nombres qui leur sont associés, à condition toutefois de soustraire 26 dès que ce nombre excède 26, ce qu'il écrit :

> « Take 26 from all the +s exceeding 26 »

Babbage met longuement en œuvre cette opération dans ses essais pour trouver les mots-clés, avant de l'exprimer pour la première fois par une formule mathématique :

$$\text{Cypher} = \text{Key} + \text{Translation} - 1 \qquad (1)$$
$$\text{Translation} = \text{Cypher} - \text{Key} + 1$$

Partant de cette constatation, sa méthode va consister à conjuguer la recherche des mots-clés avec celle de mots probables, comme « *affectionate* », « *nephew* », *dear uncle* », *etc*. Il écrit victorieusement : « *Decyphered completely, Thursday, March 19, 1846 – Friday morning 1 1/2 a.m.* »[22], et donne la solution obtenue avec les trois clés différentes MURRAY, CACOETHES et SUMMERSET :

```
  PYRI   ULOFV
  murr  aymur
  dear  uncle

POVVMGN  MK  UO  GOWR  HW  LQ  PGFJHYQ
cacoeth  es  ca  coet  he  sc  acoethe
nothing  is  so  easy  as  to  perform

OJAV  MSN  WIJHEEHPR  BRVGRUHEGK, EFF WJSR  RVY
scac oet   hescacoet  hescacoeth, esc acoe  the
what  you  perfectly  understand, and when  you

CPOY  VSP,  PX  OKLN  PI  XXYSNLA  SELF  XG
scac  oet,  he  scac  oe  thescac  oeth  es
know  how,  it  will  be equally   easy  to

FEEWTALV  LJIU, WR  MOI EGAP  HMFL  ML  YINZ
cacoethe  scac  oe  the scac  oeth  es  caco
decipher  this  in  the mean  time  it  will

TNGDDG  YQIV  UYEAP-BQL
ethesc  acoe  thesc-aco
puzzle  your  brain-box

       WJQV  PGYK  STRITLMHFOFI EWTAWK
       some  rset  somersetsome rsetso
       ever  your  affectionate nephew
```

[22] *ibid.*, folios 58-59. Ces feuillets sont datés du 24 février, élément qui témoigne du désordre de leur classement.

```
TI EJC
me rse
hen ry
```

Sur la même page où Babbage donne cette solution se trouvent également les trois petits tableaux suivants :

	Table 1			Table 2			Table 3	
	N°	Rem Substract		N°	Rem Substract		N°	Rem Substract
6)	0	24	9)	0	18	8)	0	19
	1	12		1	2		1	18
	2	20		2	0		2	14
	3	17		3	2		3	12
	4	17		4	14		4	4
	5	0		5	4		5	17
				6	19		6	18
				7	7		7	14
				8	4			

En face de chaque reste est ainsi indiquée la lettre de l'alphabet correspondante. Par exemple, pour la troisième clé :

```
 0   1   2  3   4   5   6   7
 T   S   O  M   E   R   S   E
19  18  14  12  4  17  18   4
```

Ces tableaux traduisent une étape supplémentaire dans la réflexion de Babbage concernant la correspondance entre nombres et lettres de l'alphabet. Cette fois, Babbage n'associe plus à chaque lettre son *numéro* d'ordre dans l'alphabet, mais un *nombre* de 0 à 25, c'est-à-dire leur reste dans la division par 26, à savoir les classes de résidus dans une relation de congruence modulo 26. Comme en témoignent les correspondances numériques qui se trouvent dans les feuillets de recherche de ce type :

```
19  20  18   9  20  12  13   8   6  15   6   9
 S   T   R   I   T   L   M   H   G   O   F   I
18  14  12   4  17  18   4  19  18  14  12   4
 A   F   F   E   C   T   I   O   N   A   T   E
 1   6   6   5   3  20   9  15  14   1  20   5
 S   O   M   E   R   S   E   T   S   O   M   E
```

et la présence constante du terme (+1) dans les formules (1), ce n'est pas au cours de sa recherche[23], mais seulement dans sa présentation finale, que

[23] O. Franksen affirme que Babbage utilise les congruences de Gauss pour mener sa

Babbage fait le rapprochement entre son travail et la théorie des congruences de C. F. Gauss (1777-1855), dont il connaît par ailleurs les *Disquisitiones Arithmeticae* (1801).

Le seul travail publié de décryptement : la controverse avec Thwaites

Par contre, Babbage utilise dans le détail cette théorie des congruences lorsqu'en 1854, il montre à Thwaites, chirurgien-dentiste à Bristol, que cette invention qu'il croît toute nouvelle n'est autre que le chiffrement polyalphabétique : on le trouve déjà chez Wilkins, il a déjà été décrypté – par Babbage lui-même –, et le système de règles coulissantes que Thwaites a fait breveté existe aussi déjà, en carton ou en bois, y compris sous d'autres formes, comme le système des disques concentriques. Thwaites avait envoyé son « invention » à la *Society of Arts*, pour qu'elle en fasse connaître l'intérêt, affirmant que ce système valait pour tout langage, et qu'il était très sûr, puisqu'il était, selon lui, impossible de décrypter le message sans connaître la clé. Il se référait même à l'*Essay on Probabilities*, publié par Augustus de Morgan (1806-71) en 1838 dans le *Penny Cyclopaedia*, pour affirmer que : « De par cette communication, je revendique la primeur de la découverte de la correspondance secrète utilisant le principe de permutation »[24]. Cette invention lui semble cruciale pour maintenir le secret dans les échanges télégraphiques, tant pour les établissements publics que dans les échanges commerciaux, donnant l'exemple d'une faillite qui aurait pu être évitée si une information confidentielle avait pu être envoyée chiffrée par télégramme.

Contacté comme expert, Babbage répond d'abord sarcastiquement que « il ne vaut pas la peine de considérer un chiffrement comme impénétrable, sauf si l'auteur a lui-même décrypté quelque chiffrement très difficile ». Mais il n'aura finalement d'autre recours pour convaincre Thwaites de sa méprise que de décrypter le message de sa seconde lettre, un extrait de *The Tempest* de Shakespeare, chiffré deux fois successivement avec deux clés différentes.

Le clair :

> Soft, sir, one word more,
> They are both in either's powers : but this swift business
> I must uneasy make, lest too light winning
> Make the pne word more, I charge thee

recherche, alors qu'il utilise seulement la correspondance entre numérotation et lettres de l'alphabet.

[24] « *By this communication I claim precedence in the discovery of secrecy correspondence on the principle of permutation.* »

That thou attend me, thou dost here usurp
Upon this island as a spy, to win it
From me, the lord on't.

Le chiffré :

UTMU[25], DQV, UKS, LKZT, LRWN, FLHL, HPG,
SVUS, QR, KFHWAZI, ORBNDW, EHA, RJZZ,
THQJZ, YHIEVURV, N, VGWW, HUCCJF,
NLSI, RBGI, PWE, KLLQF, ALAUGPX, TBVM,
XNB, DGEHU, KLLQF, SQR, DMTU, TPCM, M
IEOGCM, JGHJ, CTEW, GOMW, RAUPVH, SB,
HWKC, TNVY, QQVH, HZSTG, BQZV, XNFG
XOTQMG, FB, M, WSL, AM, YZU, JE, NVUJ,
AT, PPU, KRWM, AR'W.

Babbage s'amuse alors de ce que Thwaites ignore : « [Il] ne semble pas connaître les principes sur lesquels sont construits de tels chiffrements, car il semble avoir employé deux chiffrements successifs, à savoir le mot TWO à partir de *p*, et le mot COMBINED à partir de *e*. Plus encore, il semble ignorer que l'ordre des chiffrements successifs est indifférent ». Ce que démontre Babbage sur le premier vers du texte, avec les deux clés trouvées : TWO et COMBINED, sans révéler pour autant comment il les a trouvées. Mais cette fois, il présente en détail comment, à partir de cette clé composée de 24 lettres (3 fois 8), il peut obtenir pour chaque lettre du chiffré, la lettre correspondante du clair. Partant d'un tableau du même type que ceux qu'il avait donnés pour les trois clés du message de son neveu :

[25] Après avoir trouvé les deux clés avec lesquelles le message a été chiffré, Babbage corrigera la 2ème lettre du 1er mot du chiffré, qui doit être *v* et non *t*.

Reste	Nb tabulaire	Reste	Nb tabulaire
0	24	12	22
1	2	13	8
2	17	14	16
3	7	15	25
4	1	16	3
5	11	17	5
6	8	18	9
7	4	19	12
8	6	20	4
9	23	21	3
10	14	22	13
11	15	13	7

Babbage « calcule » alors pour chaque lettre du chiffré la lettre correspondante du clair. Ainsi, pour le mot GOMW du chiffré :

w est la 145e lettre du chiffré et 145 = 6 fois 24 + 1

Dans le tableau, en face du reste 1 se trouve le nombre 2, et la lettre *w* est la 23e lettre de l'alphabet naturel. La différence 23 – 2 = 21 donne la place de la lettre du clair dans l'alphabet, soit *u*.

Babbage renvoie alors la balle dans le camp de Thwaites, le mettant au défi de décrypter à son tour un chiffré issu de la même pièce de Shakespeare, défi que Thwaites ne relèvera pas[26].

Le caractère privé des échanges de Babbage est essentiel pour appréhender à la fois ses méthodes et l'absence de diffusion de son travail. La non publication de « Philosophy of Deciphering » est souvent attribuée à la guerre de Crimée (1853-54), et au souci de ne pas rendre public ce qui aurait pu avantager l'adversaire russe. Mais outre la dispersion de Babbage lui-même entre tous ses travaux[27], l'écart entre les recherches savantes et l'état des pratiques sur le terrain peut également avoir été déterminant. Lorsqu'au même moment, Lyon Playfair propose le chiffrement de Wheatstone au Foreign Office, celui-ci juge son utilisation trop compliquée pour les praticiens de la cryptographie. Le fossé déjà signalé au chapitre

[26] Tous ces échanges sont publiés dans le *Journal of the Society of Arts*, 1855, vol. 2, pp. 253-258, et compilés dans le manuscrit de Babbage sur la « Philosophy of Deciphering ». Add. Mss 37205, folios 133 à 179, avec les articles de ce journal, la correspondance avec le journal, et les essais de décryptement de Babbage.

[27] Babbage est également l'auteur d'une « Philosophy of Analysis », écrite dans les années 1820, et non publiée. Il en partagera cependant les idées dans sa correspondance avec George Peacock, l'auteur d'un *Treatise on Algebra* qui initie à Cambridge une conception purement symbolique de l'algèbre.

« L'ancrage de la cryptologie dans les jeux d'écriture »[28], entre avancées conceptuelles et état de l'art est donc encore très prégnant au milieu du 19e siècle. Et Babbage cherche avant tout la reconnaissance de son milieu social. Lorsque Thwaites insiste sur les avantages commerciaux de sa proposition au moment où se développe l'utilisation du télégraphe, Babbage se contente de démontrer l'existence du décryptement, il ne renchérit pas sur la possibilité de lui donner une plus vaste audience.

C'est donc à Friedrich W. Kasiski (1805-81) qu'est en général attribué le décryptement du chiffrement de Vigenère, qu'il publie à Berlin en 1863 dans *Die Geheimschriften und die Dechiffrir-Kunst*. À juste titre d'ailleurs, puisque Kasiski donne cette fois une méthode générale de décryptement, un raffinement de l'analyse des fréquences. Pour l'appliquer, il faut au préalable découvrir la longueur de la clé, ce qui se fait en repérant, sur un texte assez long, des répétitions de groupes de lettres qui laissent supposer qu'un même mot a pu être chiffré à différents endroits avec les mêmes lettres-clé. La distance, en nombre de lettres, entre ces répétitions donne alors un multiple du nombre de lettres de la clé. Une fois ce nombre déterminé, il ne reste plus qu'à découper le message en sous-messages, formés des lettres chiffrées avec la même lettre de la clé.

L'ouvrage de Kasiski a été publié alors qu'il était officier d'infanterie prussien à la retraite. Il a travaillé en amateur sans mesurer tout l'intérêt de ses avancées. Sa démarche reste attachée au message, contrastant avec l'approche de Kerckhoffs qui énoncera ses lois dans une perspective plus globale liée au système de communication.

KERCKHOFFS ET LE SYSTEME TELEGRAPHIQUE

Dans la seconde partie du 19e siècle, les militaires s'emparent de l'usage du télégraphe. Leurs échanges secrets sont désormais transmis par ce nouveau support, ce qui change radicalement les conditions auxquelles la cryptologie se trouve confrontée. Là où Babbage continuait à traiter des messages entre individus, Kerckhoffs va examiner frontalement les nouvelles exigences qu'impose au secret l'utilisation d'un réseau télégraphique par les personnels militaires, du commandement aux exécutants.

Comme pour Kasiski, les renseignements sont rares quant aux biais par lesquels Kerckhoffs est arrivé au contact de la cryptologie. En particulier, il est difficile d'apprécier en quoi consistent ses relations avec le monde militaire. David Kahn[29] nous apprend seulement qu'il a eu des difficultés

[28] Voir p. 24.
[29] Kahn, *The Codebreakers*, pp. 230-240.

politiques après la défaite de 1870. Mais rien dans sa biographie n'indique spécifiquement comment il a été conduit à publier deux importants articles sur « La cryptographie militaire » dans deux numéros successifs du *Journal des sciences militaires*, en janvier et février 1883. Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwerhof (1835-1901), issu d'une riche famille flamande, diplômé en lettres et en sciences à l'Université de Liège, a beaucoup voyagé en Europe avant de s'installer en France où il va enseigner, d'abord essentiellement les lettres et les langues modernes en province – à Meaux et à Melun – puis l'allemand à l'Ecole des Hautes Etudes Commerciales et à l'Ecole Arago à Paris à partir de 1881. Il est l'auteur de divers ouvrages, qui vont du théâtre à des grammaires de langue étrangère. C'est après ses publications en cryptographie qu'il se fera propagandiste d'un nouveau langage, le *Volapuk*, qui vient d'être inventé par le prêtre catholique allemand Martin Schleyer (1831-1912), et qui se répand comme une traînée de poudre en France et dans le monde entier dès sa création en 1880. Kerckhoffs devient même président de l'*Académie Internationale de Volapuk* au 2e congrès de *Volapuk* tenu à Munich en 1887. Malgré ces débuts fulgurants, le *Volapuk* est moribond dès 1890 : il n'a pas résisté aux oppositions quant à la « nature » de cette nouvelle langue, entre l'idée d'une langue la plus littéraire possible envisagée par Schleyer et celle d'une langue la plus simple possible voulue par Kerckhoffs. L'érudition linguistique de ce dernier a sans aucun doute constitué une forme d'expertise tout à fait propice à penser une réorganisation des enjeux de la cryptographie militaire. Mais les éléments connus de sa biographie laissent néanmoins dans l'ombre le détail de son élaboration.

Les exigences de la cryptographie télégraphique

Dans les cours de cryptologie à l'université aujourd'hui, les lois de Kerckhoffs sont énoncées dans un cadre mathématisé, se référant à l'algorithme qui préside au secret des échanges. Elles apparaissent, du fait de cette dénomination, comme une sorte d'anticipation des critères de sécurité d'un système cryptographique transmis par voie électronique, alors qu'il n'y a bien sûr pas trace de référence à une quelconque notion d'algorithme chez Kerckhoffs, cette notion n'étant, à l'évidence, pas formalisée à son époque. Par contre, il a parfaitement perçu et explicité les conditions nouvelles imposées par la transmission télégraphique des messages, à la fois pour rendre applicable leur chiffrement, et pour adapter les services cryptographiques de l'armée à ce nouveau système de transmission. Analysant les conséquences organisationnelles de l'utilisation

du télégraphe pour les services du chiffre, Kerckhoffs énonce ce qu'il appelle les « desiderata de la cryptographie militaire »[30] :

> « 1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable,
> 2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi,
> 3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants,
> 4. Il faut qu'il soit applicable à la correspondance télégraphique,
> 5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes,
> 6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer »[31].

Kerckhoffs insiste sur le fait que ce mode de communication fait intervenir plusieurs niveaux de responsabilité et de très nombreux intervenants, dont les compétences sont très différentes. Il relève la difficulté qui a si longtemps bloqué l'utilisation des modes de chiffrement les plus élaborés : il serait vain d'exiger des personnels peu formés d'effectuer des manipulations trop compliquées. Il s'agit de rendre compatible le secret des informations avec cet usage collectif des échanges à l'extérieur comme à l'intérieur de la chaîne de transmission. C'est cette analyse qui conduit Kerckhoffs à distinguer pour la première fois sans doute entre deux types de difficulté : la difficulté matérielle et la difficulté mathématique. Et c'est aux difficultés matérielles et organisationnelles qu'il s'attache : le « système » dont il traite est celui qui régit la transmission télégraphique de l'ensemble des messages dans l'armée. On est loin des correspondances privées auxquelles Babbage appliquait ses recherches mathématiques :

> « Il faut bien distinguer entre un système d'écriture chiffrée, imaginée pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré, et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains […]. Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas, dans le

[30] Guillot, « Auguste Kerckhoffs et la cryptographie militaire ».
[31] Kerckhoffs, « La cryptographie militaire », I, p. 12.

> second, il faut un système remplissant certaines conditions exceptionnelles »[32].

Ce sont ces conditions exceptionnelles, liées au mode de transmission télégraphique, qui constituent ce que Kerckhoffs nomme pour la première fois un « système cryptographique », et dont il énonce les « desiderata ». C'est bien dans ce domaine qu'il innove, et non en mathématiques. Il précise en outre que les messages chiffrés sont désormais écrits en séparant les lettres des messages chiffrés en tranches de cinq lettres, du fait de leur transmission télégraphique. S'il présente un inventaire érudit des méthodes et des instruments de chiffrement, il n'en produit pas de nouveau.

L'organisation de la cryptographie en tant que « système » n'est pas seulement une question de définition couchée sur le papier. Kerckhoffs accorde beaucoup d'importance aux différents systèmes de chiffrement utilisables sur le champ de bataille. Rendre ces « desiderata » effectifs impose tout un ensemble d'adaptations qui ne vont pas de soi au sein de l'armée, du moins en ce qui concerne les services du chiffre. Comment rendre compatible la hiérarchie du commandement militaire avec la circulation des messages chiffrés entre tous les niveaux de l'armée ? Exiger un secret absolu supposerait que dans un corps d'armée, toutes les instructions chiffrées émanent ou du moins passent dans les mains d'un seul, ce qui serait réduire la correspondance secrète à un rôle singulièrement modeste. Kerckhoffs attribue d'ailleurs, au moins en partie, la défaite de 1870 à un manque de communication entre les généraux de Paris et ceux de la province. Le procédé étant désormais commun à tous, le secret doit donc porter essentiellement sur la clé.

Corollaire de la mise en place de ce système de communications : l'extension de l'enseignement de la cryptologie dans les écoles militaires, dont Kerckhoffs souligne l'importance. Il en fait état en France depuis 1874, et en Allemagne au moment où il écrit en 1883. Le système cryptographique doit être également compatible avec les exigences du caractère public de cet enseignement :

> « L'administration doit absolument renoncer aux méthodes secrètes et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles militaires, que nos élèves seront libres de communiquer à qui leur plaira et que nos voisins pourront adopter et même copier si cela leur convient »[33].

---

[32] *ibid.*, I p. 12.
[33] *ibid*., I, pp. 14-15.

Au-delà de l'inventaire des méthodes cryptographiques, c'est bien l'enjeu principal des articles de Kerckhoffs : convaincre le système hiérarchique de l'armée de la nécessaire réorganisation des services du chiffre du fait de ce nouveau mode de transmission des messages.

Les débuts d'un enseignement de la cryptographie militaire

Conséquence du travail de Kerckhoffs ou de la défaite de 1870 : la France a considérablement renforcé son service cryptographique. Selon David Kahn en effet, il s'agit d'ailleurs d'une pratique manifeste dans les pays ayant connu une défaite militaire, ce que les vainqueurs négligent de faire en général. Le travail de Kerckhoffs structure ce que David Kahn appelle une véritable école de cryptographie[34], constituée pour beaucoup d'officiers issus de l'Ecole Polytechnique, et qui va assurer la suprématie de la France en ce domaine jusqu'à la Première Guerre Mondiale. Le marquis Gaëtan de Viaris (1847-1901) – Gaëtan Henri Léon Viarizio di Lesegno – réorganise le Service du Chiffre en 1890, conçoit quelques machines de chiffrement, et produit plusieurs articles dans *Le Génie Civil*, où il traduit en équations algébriques les relations entre les lettres du clair et du chiffré pour tous les chiffrements polyalphabétiques déductibles de celui de Vigenère. Paul-Louis-Eugène Valério publie une dizaine d'articles dans le *Journal des sciences militaires* dans les années 1890, ainsi qu'un ouvrage en deux volumes, *De la cryptographie, essai sur les méthodes de déchiffrement* (1893-96). Il interviendra dans le procès de Rennes qui condamne une seconde fois le capitaine Dreyfus, avant que ne lui soit accordée une grâce présidentielle en 1899. La tradition de la cryptographie comme activité érudite se poursuit également, comme en témoigne le *Traité élémentaire de cryptographie* (1901) de Félix M. Delastelle (1840-1902), administrateur des tabacs à Marseille, qui se consacre à une classification des modes de chiffrement au moment où il prend sa retraite. Et le lieutenant Etienne Bazeries (1846-1931) s'est initié par lui-même à la cryptanalyse, en décryptant les messages chiffrés parus dans les colonnes des journaux, avant de devenir si efficace au Bureau du Chiffre du Ministère des Affaires Etrangères. Il cassera le fameux « Grand Chiffre de Louis XIV », et publiera *Les chiffres secrets dévoilés* (1901), avant de travailler pour l'armée jusqu'après la Première Guerre Mondiale, ne se retirant qu'en 1924. N'oublions pas George-Jean Painvin (1886-1980) qui, s'il fut formé à l'Ecole Polytechnique, enseignait la géologie et la paléontologie avant de devenir LE cryptanalyste qui permit à l'armée française le succès que l'on

[34] Kahn, *The Codebreakers*, pp. 240-242.

sait dans les derniers moments de la Première Guerre Mondiale [35]. Au cours de cette guerre, le lieutenant Henry Olivari (1868-1955), polytechnicien, est envoyé à Petrograd (Russie) sous les ordres du général Maurice Janin (1862-1946), dans le cadre d'une mission militaire française chargée d'organiser un encadrement des services français insuffisamment dotés à l'ambassade, de recueillir des radiogrammes allemands sur le front de l'est, et aussi d'établir des liens avec l'état-major russe, et d'enseigner à la Stavka certaines méthodes, dont Olivari précise : « Étant mieux qui quiconque au courant de ce qui avait été fait à Paris, je savais fort bien ce qu'il convenait de dire et de cacher ». À son retour, il déplorera que cette collaboration n'ait pas été plus loin du fait de dissensions au sein du Service du Chiffre[36]. Tous ces travaux seront largement repris dans le *Cours de cryptographie* du colonel Marcel Givierge (1871-1931), qui servira longtemps de manuel aux cryptologues français, jusqu'après la Seconde Guerre Mondiale. Il connaîtra plusieurs éditions, et traversera l'Atlantique, puisque Shannon le cite comme une source importante[37] dans sa *Theory of Secrecy Systems* en 1949. Quoi qu'il en soit, de part et d'autre de l'Atlantique, les militaires vont développer un enseignement de la cryptologie spécifique aux systèmes télégraphiques, sans que les manuels ne se montrent innovants pour autant[38]. À tel point qu'en 1915, le lieutenant Parker Hitt (1878-1971), instructeur en cryptologie de l'école du Signal de l'armée à Fort Leavenworth, est tellement conscient de la vulnérabilité des méthodes de chiffrement enseignées aux États-Unis qu'il demande – en vain – à ses chefs de partir – à ses frais ! – en France pour s'initier à des méthodes plus élaborées. L'autorisation lui en sera refusée, mais, devenu *Chief Signal Officier of the First Army* en 1918, il exercera ses talents sur le front en France au sein de l'*American Expeditionary Forces.* Il saura combler le fossé entre les pratiques de la cryptologie militaire et les avancées technologiques des nouveaux moyens de communication (télégraphe, téléphone, radio). Son *Manual for the Solution of Military Ciphers* (1916), premier livre de ce type outre-Atlantique, sera utilisé en particulier par le couple de cryptanalystes William F. Friedman (1891-1969) et Elizabeth W. Friedman (1892-1980) pour former des générations de cryptologues pendant l'entre-deux-guerres[39].

[35] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » p. 90.
[36] D'autres membres de la mission étaient polytechniciens ou normaliens. Certains d'entre eux resteront en URSS après la Révolution d'Octobre en 1917. Olivari, *Mission d'un colonel français en Russie 1916*, p. 36.
[37] Voir dans ce chapitre : « Mathématisation de la cryptographie ».
[38] Slater, *Telegraphic Code* ; Hill, *Manual for the Solution of Military Ciphers.*
[39] Smoot, « Fighting the Damned Huns ».

VERNAM ET LA PROTECTION DES ECHANGES PAR TELESCRIPTEUR

La façon dont l'armée investit le télégraphe pour son système de communications secrètes fait passer au second plan l'importance de la cryptologie dans les correspondances secrètes et les relations commerciales. À partir de la fin du 19e siècle, elle sera de ce fait le plus souvent référée aux échanges diplomatiques et militaires[40]. Pourtant, évoquée entre Babbage et Twaites pour les échanges commerciaux, elle se maintient aussi dans les milieux cultivés, comme en témoigne l'investissement d'un Edgar A. Poe (1809-49) sur le sujet dans ses *Histoires extraordinaires*[41]. L'introduction des téléscripteurs aux États-Unis, en faisant converger échanges privés, échanges commerciaux et mécanisation des moyens de transmission, correspond au moment du déploiement généralisé des communications, et à leurs besoins de confidentialité. La technique de chiffrement inventée par Gilbert S. Vernam, ingénieur chez AT&T (*American Telegraph and Telephon Company*) à Manhattan depuis 1915, contribuera d'ailleurs largement au développement du téléscripteur lui-même. Mais elle n'est le fait ni d'un mathématicien, ni d'un linguiste, et s'exprime dans le vocabulaire spécifique de l'ingénieur, en termes d'impulsions électriques.

Le chiffrement automatique des messages transmis par téléscripteur

Vernam est alors chargé de la sécurité des téléscripteurs à la section télégraphe du département *Develepment and Research*, et son invention est inscrite dans la nature même de ce type de transmission. Elle intègre le chiffrement et le déchiffrement au processus d'émission, de transmission et de réception des messages par voie télégraphique. Une fois de plus, il n'y a pas trace d'algorithme de chiffrement dans le brevet[42] qu'il obtient en 1919. Le texte de ce brevet décrit avant tout un dispositif technique, le « *printing telegraphic system* », formé d'électro-aimants et de commutateurs rotatifs, qui produit et contrôle automatiquement la façon de rendre inintelligibles les messages au cours de leur transmission. Il y est question de circuits ouverts ou fermés, de connexions et d'impulsions électriques. Les opérations dont traite Vernam sont celles qui caractérisent les différentes étapes de fonctionnement des parties du système : dispositifs d'émission, de

[40] Il est en général ignoré que la machine *Enigma*, utilisée comme machine de chiffrement par les services allemands de la défense pendant la Seconde Guerre Mondiale, fut d'abord conçue pour le commerce et utilisée dans les banques dans les années 1920. Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 19.

[41] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 19.

[42] Vernam présente son invention chez AT&T dans une note du 17 décembre 1917. Le brevet est daté du 22 juillet 1919, mais il est signé par Vernam en date du 08 septembre 1918.

transmission et de réception, et dispositifs de chiffrement et de déchiffrement. Les explications qui concernent le mode de chiffrement et de déchiffrement portent essentiellement sur la manière technique de le réaliser. Elles ne sont pas données en termes mathématiques.

Les signes du code Baudot
avec le mode de symbolisation de Vernam

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	+	−	−	−	+	3	−	−	−	+	−	4	−	+	−	−	−
8	+	+	+	+	+	(+)	+	+	−	+	+	9	−	−	+	−	−	/	−	−	−	−	−

(3 = carriage return, 4 = line feed, 8 = letter shift, + = figure shift,
9 = space, / = null)

Les téléscripteurs représentent les lettres d'un message en utilisant le code Baudot, un codage binaire également appelé code télégraphique ou alphabet international, l'équivalent du code Morse pour ce type de transmission. Chaque lettre de l'alphabet y est codée par cinq unités qui, à partir de la frappe sur le clavier, vont se traduire par le passage du courant électrique ou par son absence. Les différentes combinaisons possibles de ces cinq unités permettent donc de transmettre 32 signes. Et le système dispose en outre de deux modes, qui permettent de distinguer minuscules et majuscules, et de représenter d'autres signes (ponctuation, chiffres). Dans une émission normale du message, pour chaque lettre transmise, les cinq impulsions correspondantes s'inscrivent sur le ruban de papier perforé, sous la forme d'un trou ou d'une absence de trou. Des ergots entrent dans ces trous pour faire contact et reproduire une impulsion. Ce codage sur ruban perforé peut alors être retranscrit au destinataire sous forme de lettres imprimées.

L'invention de Vernam utilise l'équipement du téléscripteur pour chiffrer ou déchiffrer automatiquement les messages. Elle associe au ruban du message un autre ruban qui fait office de clé. Lettre à lettre, les deux informations sont alors combinées électro-mécaniquement, afin de ne transmettre sur la ligne que le message chiffré. Cette clé n'est donc plus nécessairement un mot de la langue, elle n'est pas davantage un objet mathématique, elle n'est qu'un ruban de papier perforé dont les marques sont produites au hasard, même si Vernam précise qu'elles peuvent représenter une lettre de l'alphabet. Ce dispositif ouvre donc la voie au caractère aléatoire de la clé. Si la règle de combinaison est

traditionnellement présentée dans les ouvrages comme une addition sur l'ensemble {0,1}, ou comme l'opération du connecteur logique « ou exclusif » sur ce même ensemble, le brevet la décrit comme une combinaison des signes « + » et « – », où « + » représente une impulsion électrique, et « – » l'absence d'une telle impulsion. Encore ne la décrit-il que sur un exemple :

> « Supposons que le premier caractère du message à transmettre soit un *A*. Le *A* est codé par les signaux « + + − − − », où « − » représente une impulsion ouverte ou « espace », et « + » représente une impulsion fermée ou « marque ». Dans le système décrit ici, il faut comprendre que des impulsions de courant positives et négatives peuvent être utilisées à la place de circuits fermés ou ouverts si il y a besoin. Pour chiffrer et déchiffrer le message aux deux bouts de la ligne, on utilise des bandes identiques où est enregistrée une série de signaux codés qui sont de préférence choisis au hasard, mais qui, si on le veut, peuvent représenter une série prédéfinie de lettres ou de mots. Supposons que la lettre *B* soit présente dans l'émetteur chiffrant en même temps que la lettre *A* est transmise dans l'émetteur normal. Le code de la lettre *B* est « + − − + + ». L'envoi du *A* par l'émetteur normal signifie que les contacts 25 et 26 seront fermés alors que les contacts 27, 28 et 29 seront ouverts. Par conséquent, les relais 14 et 15 seront alimentés et leurs contacts seront fermés, alors que les relais 16, 17 et 18 resteront non alimentés. La présence de la lettre *B* dans le code transmis signifie que les contacts 36, 39 et 40, représentant les impulsions positives du *B* seront en contact avec la ligne 32 qui est connectée à la batterie, et les contacts 37 et 38, représentant les impulsions négatives de ce caractère, seront en contact avec la ligne 33 qui est mise à la masse.
> Il résulte de cette combinaison de contacts dans les deux émetteurs, […] puisque le bras de distribution 10 tourne autour des contacts 1 à 5, qu'une impulsion sera transmise sur la ligne à partir des contacts 2, 4, et 5, et qu'aucune impulsion ne le sera à partir des contacts 1 et 3. Cela signifie que le signal «− + − + + » sera transmis sur la ligne, et cela représente la lettre *G*, et non pas la lettre *A* qui était le caractère du message à transmettre »[43].

---

[43] *« Let us suppose that the first character of the message to be transmitted is* A. *The code signal of* A *is « + + – – – », where « – » represents an « open » or « spacing » impulse and « + » represents* a *« closed » or « marking » impulse in the system here illustrated although it will be understood that positive and negative current impulses may be used instead of closed and open circuit operation if desired. For ciphering and deciphering the message, the ciphering devices at the opposite ends of the line are provided with identical sections of tape upon which are recorded a series of code signals which are preferably selected at random but if desired may themselves represent a predetermined series of letters or words. Let us suppose that the letter* B *happens to be in the ciphering transmitter at the same moment that the letter* A *is being sent from the normal transmitter The code for the letter* B *is « + – – + + ». The sending of* A *from the normal transmitter means that the contacts 25 and 26 will be closed, while the contacts 27, 28 and 29 are open. Thus, relays 14 and 15 will be energized, and close their contacts, while relays 16, 17 and 18 remain unergized* [sic]. *The presence of the letter* B *in the code transmitter means that contacts 36, 39 and 40, representing the plus*

Dans ce système cryptographique, le chiffrement et le déchiffrement sont des opérations identiques, ce que Vernam ne montre que sur le seul exemple précédent. Autrement dit, appliquer deux fois la clé sur un message redonne le message lui-même.

Cette propriété présente un double intérêt technique. Il n'y a qu'un seul type de réalisation électromécanique à mettre en place. Et les opérations de chiffrement et de déchiffrement s'effectuent automatiquement, sans aucune intervention humaine : elles font intégralement partie du processus de transmission. Le chiffre de Vernam signe en quelque sorte l'acte de naissance de la cryptographie automatique, le « chiffrement en ligne », en même temps que celui du caractère aléatoire de la clé.

En outre, et contrairement à bien d'autres systèmes ultérieurs – celui de l'*Enigma* par exemple –, le message clair parvient au destinataire directement sous forme imprimée. Et si ce n'est pas là une totale nouveauté[44], cette impression directe à l'arrivée du téléscripteur se conjugue avec la vitesse de la frappe au clavier pour rendre particulièrement efficace ce mode de transmission chiffré. En tous cas, puisque le code Baudot est public, le secret du système de Vernam repose exclusivement sur celui du ruban-clé, ce qui correspond aux *desiderata* de Kerckhoffs.

---

impulses for B *will be in contact with the bus-bar 32, which is connected to battery and that contact 37 and 38, representing the negative impulses for this character will be in contact with bus-bar 33 which is grounded.*
As a result of this combination of contacts in the two transmitters, […] as the distributer arm 10 rotates over the contacts 1 to 5, impulses will be transmitted to the line from contacts 2, 4 and 5, and none from the contacts 1 and 3. This means that signal « – + – + + » will be transmitted over the line and this signal represents the letter G *and not the letter* A *which is the character of the message to be transmitted* ». Vernam, « Secret Signaling system ».

[44] Kahn, *The Codebreakers*, p. 397.

Exemple de chiffrement d'un message utilisant le système de Vernam

Le mode de chiffrement de Vernam	Le chiffrement d'un message	
« + » associé à « + » donne « – »	Clair	+ + – – –
« + » associé à « – » donne « + »	Clé	+ – – + +
« – » associé à « + » donne « + »	Chiffré	– + – + +
« – » associé à « – » donne « – »		

Le déchiffrement du chiffré

Chiffré	– + – + +
Clé	+ – – + +
Clair	+ + – – –

Vers le « one-time pad system »

Ce système est installé chez AT&T dès la note de Vernam du 17 décembre 1917. Et la *Navy* en est rapidement informée par le biais de la *Western Electric Company*, entreprise fabricante de AT&T. Il est adopté dès 1918 par le *Signal Armed Corps*, où le Major Joseph O. Mauborgne[45] (1881-1971), cryptologue et responsable du service des transmissions, en reconnaît immédiatement l'intérêt. Mauborgne a établi les premières liaisons radio aéroportées dès avant la guerre. Formé à l'école de Hitt, il dirigera la division *Engineering and Research* et le laboratoire du *Signal Corps* au Bureau des Standards après la Première Guerre Mondiale. Comme Hitt avant lui, il participe amplement à établir les conditions d'une cryptologie efficace avec les nouveaux moyens de communication mobilisés par l'armée. Impliqué dans la réalisation de l'invention de Vernam, il va en dégager les caractéristiques théoriques que son inventeur ne faisait qu'indiquer dans le texte de son brevet.

Mauborgne se penche sur la question de la réalisation de rubans perforés de caractère erratique. Afin d'éviter la manipulation de rubans trop longs, il combine d'abord deux rubans, de 1000 et 999 marques respectivement, produisant ainsi une clé de 999 000 caractères sans répétition. Mauborgne établit, sinon formellement, du moins sur l'exemple de deux clés particulières, qu'une telle combinaison présente certaines faiblesses. Fidèle aux leçons de Hitt qui déclarait dès 1914 qu'une bonne clé devait être « comparable en longueur au message lui-même »[46], il conjugue les deux

[45] Mauborgne a déjà publié en 1914 le premier décryptement connu du chiffre de Playfair, et en 1917, il a imposé à l'armée le cylindre de chiffrement élaboré par Hitt, qui sera intégré à la réalisation du M-94 en 1922.

[46] Cette condition n'est pas nouvelle. L'amorce d'une telle idée se trouve chez Vigenère et chez Babbage, conscients que plus la clé sera longue, plus le décryptement s'avérera difficile.

exigences susceptibles d'assurer l'inviolabilité du système : une clé « *endless and senseless* », c'est-à-dire aussi longue que le message et dépourvue de signification. Encore faut-il qu'elle ne soit utilisée qu'une seule fois. Mauborgne caractérise ainsi ce qui est aujourd'hui connu, depuis la démonstration formelle de Shannon de cette inviolabilité, sous le nom de « *one-time pad system* ».

Ce système de chiffrement automatique, en dépit de toutes ces qualités nouvelles, sera néanmoins très lourd à utiliser. En période de guerre, la quantité de messages transmis est colossale, et affecte tous les niveaux de l'armée, du commandement au soldat sur le champ de bataille. L'énorme quantité de clés à produire, à enregistrer et à distribuer est donc un obstacle majeur, auquel il faut ajouter la nécessité de contrôler la destruction des clés après leur première utilisation. Le volume du travail à produire déborde de beaucoup les moyens et les effectifs chargés de la transmission des messages.

> La réutilisation deux fois d'un ruban-clé peut être fatale, surtout en temps de guerre. Historiquement, il est arrivé que le décryptement de certains messages soit rendu possible par une telle erreur d'utilisation.
> Si on connaît déjà un autre message clair chiffré avec la même clé, on peut trouver le clair du second message. Il suffit pour cela de combiner les deux chiffrés. Puisque la combinaison de la clé avec elle-même annule toute impulsion, la combinaison des deux chiffrés est identique à celle des deux messages clairs. En combinant ce résultat avec le message clair connu, on obtient alors le message clair inconnu.

L'usage du « *one-time pad system* » ne sera donc pas généralisé, mais restera privilégié pour les communications particulièrement sensibles. La confection de clés réservées à un seul message sera ainsi proposée en Allemagne en 1921 par Werner Kunze (1908-86), Rudolf Schauffler et Eric Langlotz, et en 1926 par les Soviétiques à partir d'une indiscrétion d'un Britannique du *Governement Code and Cypher Service* (GC&CS). Pendant la Seconde Guerre Mondiale, la machine de la compagnie Lorenz contre laquelle ce même service élaborera le premier ordinateur, le *Colossus*, utilisait des clés générées pseudo-aléatoirement à partir de roues codeuses. Elle était réservée au chiffrement des communications entre le quartier général de Hitler et ceux des différents groupes d'armées. Et le « téléphone rouge » n'est autre qu'une ligne réservée aux échanges directs entre Washington et Moscou, installée en 1963 après la crise de Cuba. Les bandes

---

Et Porta insistait déjà sur l'intérêt d'utiliser des clés longues et dénuées de sens. La réalisation matérielle du système de Vernam rend cette intuition efficiente et permet de l'expliciter.

aléatoires étaient transmises par valise diplomatique et détruites après chaque utilisation.

L'invention de Vernam se cristallise donc en une réalisation technique impulsée par les nouveaux moyens de communication. La découverte récente d'un système de même type, élaboré par un banquier aux États-Unis dans les années 1880, mais resté lettre morte[47], illustre parfaitement cette nécessaire existence de besoins techniques et culturels pour que la nouveauté d'une idée se transforme en innovation investie socialement. Dans les années 1920, le travail de Vernam reste malgré tout dans le domaine de l'ingénierie. Pendant l'entre-deux-guerres, mathématiciens et ingénieurs travaillent et s'expriment – à quelques exceptions près – chacun dans leur milieu et leur langage. La restructuration des milieux scientifiques aux États-Unis pendant la Seconde Guerre Mondiale permettra leur convergence.

MATHEMATISATION DE LA CRYPTOGRAPHIE

Les travaux de Claude E. Shannon constituent une étape essentielle du basculement des pratiques matérielles vers la formalisation mathématique. Shannon est reconnu comme l'auteur d'une théorie nouvelle, la théorie mathématique de l'information, élaborée entre 1943 et 1949, et fondée sur une notion nouvelle qu'il appelle la « quantité d'information », reposant sur la théorie des probabilités. Mais dès 1937, la double formation technique et mathématique de cet ingénieur le conduit d'abord à élaborer un langage commun aux ingénieurs et aux mathématiciens, en traduisant en termes d'algèbre de Boole l'organisation logique d'une machine analogique : l'analyseur différentiel. Pendant la Seconde Guerre Mondiale, Shannon va investir la théorie des probabilités comme langage unificateur entre la cryptologie – qu'il utilise comme outil heuristique – et la théorie de l'information dont il élabore les concepts.

Shannon n'est certes pas le premier, surtout à cette époque, à faire entrer les mathématiques dans le champ de la cryptologie. Déjà au cours des années 1930, Lester S. Hill (1890-1961) avait explicité le chiffrement en termes d'algèbre modulaire, et appliqué le calcul matriciel à la cryptographie[48]. Et William Friedman, déjà cité, utilise le calcul des

[47] Bellovin, « Frank Miller, Inventor of the One-Time Pad ».

[48] Hill, « Cryptography in an Algebraic Alphabet », « Concerning Certain Linear Transformations Apparatus of Cryptography ». Professeur de mathématiques à *New York City University*, il a beaucoup travaillé en cryptologie pour l'armée des États-Unis, la Marine et le Département d'Etat pendant l'entre-deux-guerres et la Seconde Guerre Mondiale. Il a enseigné à l'université américaine de Biarritz pendant sa courte existence en 1945-46. L'essentiel de ses recherches en cryptologie reste classé confidentiel.

probabilités en cryptologie pour élaborer son « indice de coïncidence »[49] en 1921. Dans ces deux cas, les mathématiques interviennent comme un outil ponctuel dans un corpus dont la présentation générale ne change pas. Parallèlement, d'autres auteurs ont abordé la mathématisation des circuits de téléphone : Paul Ehrenfest (1880-1933) en 1910 en Russie, Vladimir I. Shestakov (1907-87) en 1945 en URSS, et Akira Nakashima (1908-70) en 1935 au Japon[50]. Mais aucun d'eux n'a bénéficié d'un contexte aussi pluridisciplinaire que celui de Shannon, qui a assuré à la fois l'extension et la postérité de ses nouvelles théories. Le travail de Shannon va beaucoup plus loin : il excelle dans la formulation mathématique des problèmes qu'il rencontre en tant qu'ingénieur, et va restructurer parallèlement la cryptologie et la théorie de l'information à partir de leur reformulation analytique, précisant soigneusement la signification des théorèmes mathématiques pour l'une et l'autre de ces applications. Il produit ainsi une théorie mathématique de la cryptographie fondée sur la notion d'information.

L'expression algébrique du montage de l'analyseur différentiel

La formation mathématique de Shannon comme ingénieur dans les années 1920 est tout à fait nouvelle. Il étudie à l'Université du Michigan, l'une des récentes universités d'état qui entrent alors en compétition avec les anciennes universités privées de l'est des États-Unis[51]. L'une des principales innovations est précisément l'introduction des mathématiques dans le cursus des ingénieurs. Et le *Massachussetts Institute of Technology* (MIT), où Shannon va travailler comme assistant-chercheur à partir de 1936, est un centre de recherches mathématiques tout à fait exceptionnel, où l'étude des

[49] Friedman, *The Index of Coincidence.* S'il a commencé ses recherches dans le laboratoire privé d'un millionnaire états-unien à Riverbanks, il intègre le département de la Défense en 1921, et dirigera ensuite le *Signals Intelligence Service* (SIS) pendant plus d'un quart de siècle. Cryptanalyste de premier plan, il participe très activement à l'enseignement et à la mécanisation de la cryptologie pendant l'entre-deux-guerres et pendant la Seconde Guerre Mondiale. Il a brisé le code japonais *Purple* en 1939, qui utilisait une machine à chiffrer à rotors de même type qu'*Enigma*. Il a contribué à l'élaboration d'un vocabulaire spécifique, introduisant en particulier le terme « cryptanalyse ».

[50] Ségal, *Le zéro et le un*, pp. 76 et 261. Trogemann, Nitussov et Ernst, *Computing in Russia*, pp. 57-68. Stankovic et Ascoal, *From Boolean Algebra to Switching Circuits and Automata*, pp. 121-124 et 163-166. L'histoire des mathématiques regorge de semblables cas d'inventions simultanées – dont celle du calcul infinitésimal par Newton et Leibniz est sans doute la plus célèbre – et qui relativise grandement la notion de « génie ».

[51] Créées à l'époque coloniale, elles sont regroupées sous le nom de *Ivy League.* Il s'agit des universités de Harvard à Cambridge, de Yale à New Haven, de Princeton, de Pennsylvanie à Philadelphie, Columbia à New York, Brown à Providence, de Darmouth à Hannover et Cornell à Ithaca.

mathématiques pures s'accompagne d'une philosophie utilitariste explicite. Entre 1927 et 1931, l'équipe de Vannevar Bush (1890-1974) y a conçu et construit une imposante machine, l'analyseur différentiel, qui permet d'obtenir graphiquement la solution d'équations différentielles dont les conditions initiales sont connues. Chargé de la maintenance de cet analyseur, Shannon va s'employer à optimiser son fonctionnement, en simplifiant l'organisation logique de ses circuits, qui connectent des intégrateurs analogiques à des organes d'opérations, et comportent de nombreuses boucles de rétroaction. Ces circuits sont spécifiques à différentes classes de problèmes, et leur montage nécessite la collaboration des ingénieurs, des physiciens et des mathématiciens[52]. Dès l'été 1937, Shannon fait un stage au *Bell Telephon Laboratories*, où il entrera pour quinze ans en 1941, et qui est alors le plus grand laboratoire privé du monde en matière de communications, avec plus de 1400 chercheurs dès les années 1920, travaillant sur les systèmes de contrôle automatiques et les analyses de stabilité. Dès avant la guerre, Shannon est donc déjà au cœur des meilleures institutions de recherche en mathématiques appliquées, dont le caractère stratégique au cours de la Seconde Guerre Mondiale va encore accroître l'importance. En 1956, le MIT créera spécialement pour lui une chaire de théorie de l'information au département du Génie électrique.

Comme il le confie lui-même, Shannon a étudié la logique symbolique et l'algèbre de Boole à l'université du Michigan, et c'est fort de cet enseignement qu'il a l'idée d'interpréter les circuits à relais et commutateurs en termes logiques, bien avant la conception et la mise au point des premiers ordinateurs. En notant $X_{ab} = 0$ le cas où le courant passe, et $X_{ab} = 1$ le cas où le courant ne passe pas entre deux points *A* et *B* du circuit, ainsi que (+) la combinaison de deux circuits en série et (•) celle de deux circuits en parallèle, il établit une « parfaite analogie » entre l'étude des circuits et le calcul propositionnel, qui lui permet d'opérer sur les circuits en termes d'opérations algébriques[53]. Son mémoire, intitulé « A Symbolical Analysis of Relay and Switching Circuits », montre comment traduire un tel circuit en un ensemble d'équations logiques dont les termes, représentant les relais et les commutateurs, ne peuvent prendre que les valeurs 0 et 1.

Mais ce travail n'est pas une simple application des mathématiques. Shannon s'y réfère à l'ensemble des auteurs qui ont développé l'algèbre de la logique, non seulement George Boole (1815-64) et Edward Huntington (1874-1952), mais aussi Louis Couturat (1868-1914) et Alfred Whitehead (1861-1947). Il a parfaitement saisi l'approche symbolique de la logique

[52] Bush, « The Differential Analyzer » ; Durand-Richard, « Planimeters and Integrpahs in the 19th century ».
[53] Ségal, *Le zéro et le un*, pp. 72-88. Shannon, « A Symbolic Analysis of Relay and Switching Circuits », p. 475.

mathématique et l'importance des analogies opératoires par lesquelles cette école de pensée s'autorise le transfert d'un système symbolique à un autre pour peu que les propriétés opératoires s'expriment avec les mêmes formules[54]. Il écrit :

> « Nous sommes maintenant en mesure de montrer l'équivalence de ce calcul avec certaines parties élémentaires du calcul des propositions. L'algèbre de la logique initialement développée par Boole, est une méthode symbolique pour étudier les relations logiques. Les symboles de l'algèbre booléenne admettent deux interprétations logiques. […] Si […] ses termes sont pris pour représenter des propositions, nous avons le calcul des propositions, dans lequel les variables sont limitées aux valeurs 0 et 1, […] »[55].

Pour sa part, Shannon procède par « induction parfaite », démontrant au cas par cas à partir des tables de vérité, la possibilité de simplifier les circuits en obtenant les formes normales des propositions logiques correspondantes. La détermination des formes normales permet d'optimiser le circuit correspondant.

Ce mémoire, soutenu en 1937 et publié en 1938 dans une revue technique d'électricité, recevra le prix Alfred Noble en 1940. Il sera immédiatement exploité aux *Bell Labs* et connaîtra une diffusion exceptionnelle pour un travail de Master. Howard Gardner le qualifie de « mémoire le plus important du siècle ». Ce langage commun aux ingénieurs et aux mathématiciens fait entrer un champ entier de l'ingénierie parmi les applications de la logique mathématique. Il débouche sur le basculement des préoccupations de l'ingénieur en communication, de l'étude des phénomènes physiques de propagation à l'analyse des circuits. Celle-ci pourra à son tour être transférée à l'analyse de toutes sortes de réseaux. Ce travail de Shannon sur l'analyseur différentiel ne s'arrête pas là. Il approfondit son propos en 1941 dans « A Mathematical Theory of the Differential Analyzer », qui sera de première importance dans la réalisation des grands calculateurs et des premiers ordinateurs au cours de la Seconde Guerre Mondiale[56]. Parallèlement, Shannon s'oriente plus directement vers

---

[54] Durand-Richard, « De l'algèbre symbolique à la théorie des modèles ».

[55] « *We are now in a position to demonstrate the equivalence of this calculus with certain elementary parts of the calculus of propositions. The algebra of logic originated by George Boole, is a symbolic method of investigating logical relationships. The symbols of Boolean algebra admit of two logical interpretations. […]. If […] the terms are taken to represent propositions, we have the calculus of propositions to which variables are limited to the values 0 and 1, […]* ». Shannon, « A Symbolical Analysis of Relay and Switching Circuits », p. 474.

[56] Au cours de la Seconde Guerre Mondiale, Bush, alors directeur du NDRC, a lancé un grand projet d'analyseur différentiel électronique, le *Rockfeller Differential Analyzer*, qui devait être un des plus grands instruments scientifiques des temps modernes » à la sortie de la guerre. Ce projet a été développé en collaboration avec Samuel J. Caldwell (1904-60), au département

des études de mathématiques[57] au MIT, préparant une thèse sous la direction de Bush, « An Algebra for Theoretical Genetics », soutenue en 1940, où il poursuit le travail de formulation mathématique qui lui permet de généraliser certaines lois connues de la dynamique des populations. Cette solide formation mathématique sera constamment mobilisée et enrichie dans ses travaux ultérieurs sur la théorie de l'information et la cryptographie.

Cryptographie et théorie de l'information

Dès 1940, Shannon est impliqué dans l'effort de guerre, qui se traduit aux États-Unis par un renforcement très structuré des relations entre la Défense, l'Industrie et les Universités au sein du *National Development and Research Committee* (NDRC), dirigé par Bush. Shannon travaille à l'élaboration d'une arme automatique anti-aérienne, le M-9, qui doit optimiser la trajectoire de tir[58], au sein de la section D2 du contrôle de tir, à laquelle sont associées les *Bell Labs* et le MIT. Le calcul prédictif des coordonnées de la position de la cible en vol, à partir de la transmission de ses coordonnées par radar, recourt à l'analyse statistique et au calcul des probabilités, ainsi qu'à la technique de lissage des données transmises. Il s'agit d'éliminer les fluctuations du signal et les effets du bruit. La voie est ainsi ouverte à Shannon pour mener de front l'analyse des processus de communication en termes discrets comme en termes continus. Le rapport commun rédigé en 1946 par Ralph B. Blackman (1904-90), Hendrik W. Bode (1905-82) et Shannon, « Data Smoothing and Prediction in Fire-control System », traite déjà du problème du contrôle de tir en termes de transmission, manipulation et utilisation du « renseignement » – « *intelligence* » en anglais –, terme qui se réfère alors au secret et à l'information. Aussi bien l'article sur ce sujet publié en 1950 par Bode et Shannon[59], que la contribution de Shannon à l'article collectif « The Philosophy of Pulse Code Modulation », publié en 1948, hériteront directement de cette ligne de recherche.

Mais l'étape la plus déterminante, et trop souvent ignorée, du travail de Shannon pour l'élaboration de sa théorie mathématique de l'information réside sans nul doute dans ses travaux de cryptologie menés aux *Bell Labs* pour la division D2 du NDRC de 1943 à 1945. En septembre 1945, Shannon

---

d'Ingénierie du MIT. Mais il a été supplanté par l'ENIAC (*Electronic Numerator Integrator Analyzer and Computer*) à l'issue de la guerre.

[57] Il suit à cette époque les cours de Norbert Wiener (1890-1964). Ségal, *Le zéro et le un*, p. 81.

[58] De nombreux exemplaires du M-9 seront fabriqués et joueront un rôle essentiel au moment de la bataille d'Angleterre et du débarquement allié du 6 juin 1944, *ibid*., pp. 93-99.

[59] Bode et Shannon, « A simplified Derivation ».

rédige un rapport confidentiel, « A Mathematical Theory of Cryptography », qui sera déclassifié, et associé à des matériaux de 1946 pour être publié en 1949 sous le titre « Communication Theory of Secrecy Systems ». Entre temps, il aura publié en 1948 sa célèbre « Mathematical Theory of Communication », dont il a déjà conçu un mode de représentation dès 1939, sans toutefois introduire à cette époque le calcul des probabilités[60]. Même s'il présente le second texte publié comme une application du premier, leur élaboration a donc été menée en parallèle. Quiconque en douterait pourrait vérifier que le texte qui porte sur la théorie de l'information est beaucoup plus lisible après la lecture du texte qui traite des systèmes secrets. C'est à partir d'analogies opératoires désormais fondées sur la théorie des probabilités que Shannon peut identifier système crypté et canal de communication bruité, tous deux intervenant désormais aussi bien dans le domaine militaire que dans le domaine civil.

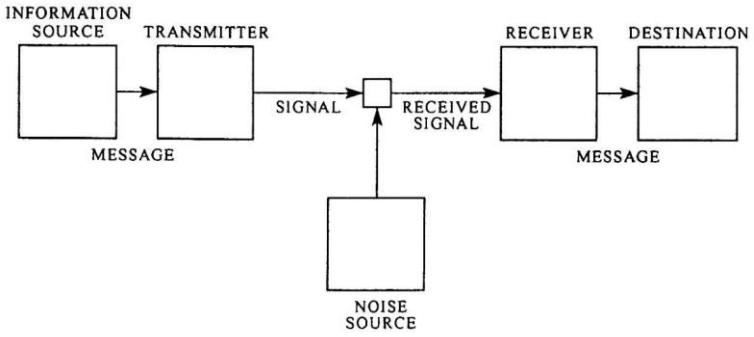

Fig. 1—Schematic diagram of a general communication system.

Le schéma devenu classique que donne Shannon d'un canal de communication présente la même structure pour ces deux types de systèmes : elle distingue la source, le transmetteur, le canal proprement dit, le récepteur, et le destinataire du message. Selon le cas, le transmetteur transforme le message en signal ou en chiffré et le récepteur effectue l'opération inverse.

[60] Shannon, lettre à Vannevar Bush du 16 février 1939, *Collected Papers*, p. 455-456.

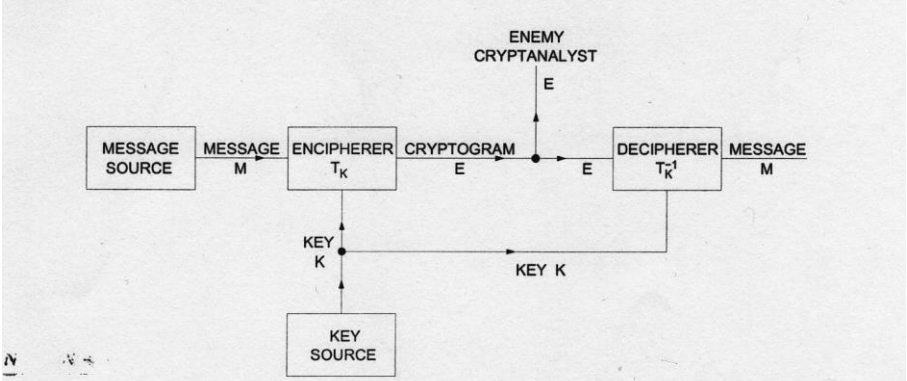

Fig. 1. Schematic of a general secrecy system

Dans ses deux articles, Shannon s'appuie sur les plus récents développements des mathématiques : théorie des ensembles, théorie des fonctions[61] et théorie moderne de la mesure, se référant directement à Andrei N. Kolmogoroff (1903-87), Maurice Fréchet (1878-1973), John von Neumann (1903-57) et Oskar Morgenstern (1902-77), ainsi qu'à Norbert Wiener (1894-1964)[62] lorsqu'il aborde les probabilités continues. La formulation mathématique qu'il propose concerne le système dans sa globalité :

> « L'aspect significatif est que le message présent est un, *sélectionné à partir d'un ensemble* de messages possibles. Le système doit être conçu pour opérer sur chaque sélection possible, et non pas seulement sur celle qui est présentement choisie, puisque celle-ci est inconnue au moment de la conception du système »[63].

Sa définition de la quantité d'information d'un système est d'abord explorée sur des exemples de « langages artificiels » que produit Shannon comme approximations de plus en plus raffinées du caractère stochastique du langage naturel. La cryptologie y intervient explicitement comme outil heuristique, permettant d'approcher cette formulation mathématique, puisque les approximations probabilistes produites pour les lettres, les

---

[61] Shannon utilise abondamment les diagrammes de représentation des fonctions, où des flèches – les clés – relient les éléments de l'ensemble de départ – les messages clairs – aux éléments de l'ensemble d'arrivée – les cryptogrammes.

[62] Voir la note 57.

[63] « *The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design* », Shannon, « A Mathematical Theory of Communication », p. 5.

digrammes et les trigrammes d'un message en anglais proviennent d'analyses cryptographiques[64]. Et la définition elle-même n'intervient qu'à la suite d'une longue discussion des conditions qu'elle doit remplir pour être opératoire pour l'ingénieur. C'est ainsi que Shannon parvient à la « seule définition qui satisfasse ces conditions » :

$$H = -K\sum_{i=1}^{n} p_i \log p_i$$

Dans cette formule, Shannon pose $K = 1$ pour pouvoir identifier cette définition à l'entropie d'un système donnée par le théorème de Boltzmann, telle qu'elle a été antérieurement définie en mécanique statistique[65]. Elle mesure aussi bien le choix que l'incertitude que représente un message parmi tous les messages possibles, les p_i représentant les probabilités d'occurrence de chacun d'entre eux. Elle est donc maximale lorsque la situation est la plus incertaine, à savoir dans le cas de l'équiprobabilité. Elle concerne aussi bien le cryptanalyste cherchant à retrouver le message clair à partir du cryptogramme, que l'ingénieur face au bruit perturbant la qualité de la transmission et que Shannon considère pour la première fois comme une variable aléatoire[66]. Dans les deux cas, il identifie la connaissance avec « un ensemble de propositions auxquelles sont associées des probabilités »[67].

De ce fait, un système secret est défini abstraitement comme un ensemble d'opérations ou de transformations T_i d'un espace – l'ensemble des messages possibles – dans un autre – l'ensemble des cryptogrammes possibles. Le cryptogramme E résulte de l'application à un message M d'une telle transformation T caractérisée par la clé i – devenue clairement aléatoire – de telle sorte que :

$$E = T_i\,(M)$$

Shannon prend soin de préciser que ces transformations doivent avoir un inverse unique, afin que le message clair puisse être retrouvé à partir du cryptogramme par la transformation :

$$M = T_i^{-1}(E)$$

---

[64] Pratt, *Secret and Urgent.* Dewey, *Relative Frequency of English Speech Sounds.*

[65] Shannon, « A Mathematical Theory of Communication », p. 11. Shannon se réfère ici à Tolman, *Principles of Statistical Mechanics.* Cette identification de la mesure de l'information à l'entropie d'un système donnera lieu à de très nombreuses interrogations philosophiques, notamment dans ses applications à l'informatique. Atlan, *Entre le cristal et la fumée*, pp. 5-129.

[66] Shannon, « A Mathematical Theory of Communication », p. 19.

[67] Shannon, « Communication Theory of Secrecy Systems », p. 657.

Et les différents modes de chiffrement connus, de César à Vernam, sont alors réinterprétés dans cette formulation mathématique. À chaque clé et à chaque message sont associées des probabilités *a priori*, qui proviennent du caractère stochastique du langage, et qui sont donc connues du cryptographe et du cryptanalyste. Si par exemple, les messages possibles sont les suites de lettres de longueur *N* dans une langue, les probabilités *a priori* ne sont autres que les fréquences des occurrences des lettres de ces suites dans cette langue. Comme l'écrivait déjà Kerckhoffs, il faut penser que « l'ennemi[68] connaît le système utilisé »[69]. Celui-ci, ayant intercepté le message, peut alors calculer les probabilités *a posteriori* des messages et des clés susceptibles d'avoir produit ce cryptogramme. Toute l'étude de Shannon porte sur les relations entre ces probabilités *a priori* et *a posteriori*[70], et le problème général de la cryptanalyse n'est autre, pour Shannon, que le calcul de ces probabilités *a posteriori*.

Ces définitions marquent une mutation essentielle de la cryptologie, dans la mesure où elles permettent à Shannon – et à ses successeurs – de structurer son analyse de la cryptologie à partir des propriétés mathématiques des systèmes secrets, celles qui proviennent de cette définition ensembliste, comme celles qui découlent des probabilités associées à chaque message et à chaque clé, qui sont en général celles des suites possibles de lettres en anglais.

Analyse mathématique des systèmes secrets

La structure statistique du langage est donc au cœur de toutes les analyses de Shannon dans ces deux articles. Chaque message y est considéré comme une suite de lettres dont chacune est choisie dans un ensemble donné – l'alphabet en général – avec une probabilité donnée. Dans le cas le plus fréquent, celui du langage naturel, chacune de ces probabilités dépend des choix précédents, ce qui permet de caractériser l'ensemble des suites de lettres comme un processus de Markov discret, qu'il suppose ergodique, c'est-à-dire statistiquement homogène. Shannon utilise alors toutes les propriétés de l'entropie élaborées en mécanique statistique pour explorer celles de la quantité d'information. Dans le cas d'un canal bruité, l'entropie s'applique aux signaux transmis comme aux signaux reçus ; dans le cas d'un

[68] Tenant compte du contexte élargi dans lequel il travaille, Shannon prend soin de préciser que ce terme provient des applications militaires, et qu'il « est couramment utilisé dans le vocabulaire cryptographique pour dénoter quiconque est susceptible d'intercepter un cryptogramme ». *ibid* ., p. 657.

[69] Il peut même disposer d'un équipement spécial pour intercepter et enregistrer les messages.

[70] Elles font intervenir le théorème de Bayes, qui joue un rôle central dans la théorie des probabilités.

système secret, elle concerne l'ensemble des messages aussi bien que l'ensemble des clés. Dans les deux cas, Shannon caractérise l'ambiguïté du signal reçu par l'entropie conditionnelle du message transmis connaissant le message reçu, qu'il nomme l'équivocation[71] : c'est l'information additionnelle qui doit être fournie pour restituer le message reçu. L'incertitude correspondante – fortuite dans le premier cas et délibérée dans le second – peut être compensée en envoyant l'information sous une forme redondante, qui peut utiliser un encodage approprié ou la redondance propre au message, exprimant précisément « de quels éléments il peut être réduit sans perdre aucune information »[72]. La spécification mathématique de la redondance joue un rôle important dans ces travaux. Dans le domaine des télécommunications, Shannon a d'abord travaillé à réduire la bande de fréquence utilisée en s'appuyant sur le fait que la voix humaine est très redondante. Et c'est à partir de cette recherche d'une réduction de la redondance qu'il a envisagé que la quantité d'information transmise soit d'autant plus grande que la redondance est plus faible.

Quant aux transformations de l'espace des messages possibles dans l'espace des cryptogrammes possibles, elles sont susceptibles d'être combinées, en tant qu'opérations sur les systèmes, soit afin d'engendrer de nouveaux types de systèmes secrets, soit d'en fournir de possibles décompositions, donc de contribuer à la résolution de cryptogrammes. La plupart du temps, ces deux espaces étant identiques, ces transformations sont des endomorphismes, dit Shannon, et les systèmes secrets ont une structure d'« algèbre associative linéaire », dont toutes les propriétés peuvent donc être attribuées aux systèmes secrets. Shannon intègre à cette approche théorique l'ensemble des systèmes connus, dont il renvoie l'étude pratique aux ouvrages de cryptographie existants[73]. Cette analyse débouche notamment sur une classification théorique des systèmes secrets qui permet d'optimiser le travail du cryptanalyse, et qui s'accompagne d'une analyse pratique de la quantité de travail requis pour le décryptement, ce qui garde une grande importance pour Shannon. Il distingue :

– le secret pur, pour lequel toutes les clés sont équivalentes, au sens où elles conduisent toutes au même ensemble de probabilités *a posteriori*. Il forme un groupe et se décompose en sous-systèmes fermés disjoints, stables dans les opérations de chiffrement. Un cryptogramme intercepté ne permet de spécifier qu'une sous-classe de messages clairs.

---

[71] L'équivocation est un indice théorique du secret, théorique en ce sens qu'elle ne tient aucun compte de la limitation de temps dans laquelle travaille le cryptanalyste. Elle donne une approximation de la quantité de messages à intercepter pour obtenir une solution cryptanalytique.

[72] Par exemple, la lettre *u* suivant toujours la lettre *q*, elle peut être omise sans perdre aucune information.

[73] Notamment Givierge, « Cours de cryptographie », et Gaines, « Elementary Cryptanalysis ».

– les systèmes semblables, dont les cryptogrammes se correspondent terme à terme avec les mêmes probabilités *a posteriori.*
– le secret parfait, où les probabilités *a posteriori* sont égales aux probabilités *a priori* et pour lequel intercepter un message ne donne donc aucune information au cryptanalyste[74]. Un tel système est particulièrement utile pour les correspondances entre les plus hauts niveaux de commandement, mais il requiert une énorme quantité de clés. C'est par exemple le cas du chiffrement de Vernam.
– le système idéal, pour lequel l'équivocation de la clé et celle du message ne s'annulent pas quand le nombre de lettres interceptées augmente, laissant le cryptanalyste dans l'impossibilité théorique de déterminer une solution unique pour un cryptogramme intercepté.

Le travail de Shannon, essentiellement connu pour avoir fondé la théorie mathématique de l'information, est donc tout aussi déterminant pour la cryptologie. Celle-ci a manifestement une fonction heuristique considérable pour inciter Shannon à penser la quantité d'information en termes de probabilités, et indépendamment de la signification des messages. Mais au-delà de cette fonction heuristique, elle s'est trouvée elle-même totalement renouvelée par la restructuration qu'opère Shannon en y introduisant les concepts dégagés en théorie de l'information. Cette reformulation mathématique de la cryptologie permet de synthétiser l'ensemble des méthodes existantes[75]. Mais surtout, elle offre aux successeurs de Shannon un vaste champ théorique, structuré par l'ensemble des possibles, et qui conjugue les préoccupations de l'ingénieur à celles du mathématicien.

Information et signification

Historiens et enseignants insistent de manière récurrente sur le fait que le travail de Shannon autorise un abandon de toute référence à la signification des messages échangés. Et cette question fait l'objet de discussions réitérées autour de l'idée selon laquelle la transmission des messages sur les canaux de communication est indépendante de toute signification. Tout se passe comme si l'existence de ces systèmes de communication rendait superflue la référence au sens. Cette affirmation soulève un problème philosophique majeur, dès lors qu'est prise en compte l'importance de la fonction signifiante pour l'humain, aussi bien au plan individuel que collectif

[74] Shannon, « Communication Theory of Secrecy Systems », pp. 679-683.
[75] Le lecteur est souvent impressionné par le niveau d'abstraction de ces articles. Or, non seulement Shannon était à la fois ingénieur et mathématicien, mais surtout, il n'a pas été autorisé à montrer dans ses articles les éléments qui auraient pu permettre au lecteur d'en déduire les usages applicatifs. Roch, *Claude E. Shanon, spielzeug, leben*, p. 136.

Il est vrai qu'en 1948, dans « A Mathematical Theory of Communication », Shannon affirme d'emblée que les « aspects sémantiques de la communication ne sont pas pertinents pour le problème de l'ingénieur »[76]. Ce qui ne signifie pas pour autant qu'il s'en détourne totalement. La rédaction même de ses articles témoigne au contraire du soin qu'il prend à préciser pour l'ingénieur la signification des mathématiques qu'il introduit. Il adopte une démarche tout à fait constructive en examinant soigneusement les conditions que doit remplir la quantité d'information pour constituer une grandeur mesurable, sur laquelle l'ingénieur pourra pratiquer des opérations mathématiques conformes à sa propre expérience. C'est en cherchant la fonction mathématique qui va lui permettre d'exprimer le mieux cette notion qu'il définit l'unité de mesure correspondante, le fameux *binary digit* (bit)[77]. Quand il traite des probabilités *a priori* et *a posteriori*, il prend soin de discuter des enjeux épistémologiques attachés à l'intervention du théorème de Bayes et aux relations entre probabilités objectives et probabilités subjectives[78]. Et surtout, de manière tout à fait caractéristique, tous les théorèmes énoncés sous forme mathématique sont suivis d'un énoncé spécifique, significatif pour l'ingénieur dans son travail. Par exemple, ayant défini la redondance D_N pour N lettres d'un message par la formule :

$$D_N = log\ G - H(M),$$

où G est le nombre total de messages de longueur N, et $H(M)$ l'incertitude attachée au choix du message M, Shannon établit la formule :

$$H(K) - H_E(K) \leq D_N,$$

où $H(K)$ est l'incertitude attachée à la clé, et $H_E(K)$ l'incertitude conditionnelle attachée à la clé connaissant le cryptogramme. Il précise alors :

[76] « *These semantic aspects of communication are irrelevant to the engineering problem* », Shannon, « A Mathematical Theory of Communication », p. 5.

[77] Si ses prédécesseurs aux *Bell Labs*, Ralph V.L. Hartley (1888-1970) et Harry Nyquist (1889-1976), avaient déjà envisagé l'introduction d'une mesure logarithmique de la quantité d'information, Shannon est le premier à dégager l'intérêt d'une mesure probabiliste lorsqu'il traite de front cryptologie et communication.

[78] Shannon, « Communication Theory of Secrecy Systems », p. 646.

> « Ceci montre que, dans un système fermé par exemple, la diminution de l'équivocation de la clé après l'interception de *N* lettres n'est pas plus grande que la redondance de *N* lettres du langage »[79].

Shannon fait suivre le théorème :

> « Une condition nécessaire et suffisante pour avoir un secret parfait est que :
>
> $$P_M(E) = P(E)$$
>
> pour tout *M* et tout *E*, où *M* est le message, *E* le cryptogramme, [*P*(*E*) la probabilité *a priori* du cryptogramme, et $P_M(E)$ sa probabilité conditionnelle si *M* est choisi, c'est-à-dire la somme des probabilités de toutes les clés qui produisent *E* à partir de *M*.] C'est-à-dire que $P_M(E)$ doit être indépendant de *M* ».

de l'explication suivante :

> « Dit autrement, la probabilité totale de toutes les clés qui transforment M_i en un cryptogramme donné *E* est égale à celle de toutes les clés qui transforment *Mi* en un même cryptogramme *E* pour tous les M_i et *E* »[80].

En fait, le travail de Shannon permet de renouveler fondamentalement la question de la signification d'un énoncé. Il pose clairement, d'un point de vue technique, la question du lieu de l'énonciation, là où d'autres que lui la poseront d'un point de vue philosophique. En tant qu'ingénieur, et comme il l'écrit à plusieurs reprises : « Le problème fondamental de la communication est celui de reproduire un message sélectionné en un point, soit exactement, soit approximativement, en un autre point »[81]. De fait, la formule par laquelle il définit la quantité d'information – the « *amount of information* » – traduit bien le changement de point de vue qu'engage la conceptualisation mathématique de la notion de système. Avec cette définition, qui prend en compte l'ensemble de tous les messages et de toutes les clés possibles, Shannon ne se situe pas à l'intérieur du système, mais

---

[79] « *This shows that, in a closed system, for example, the decrease in equivocation of key after* N *letters have been intercepted is not greater than the redundancy of* N *letters of the language* ». *ibid.*, p. 689.

[80] « *A necessary and sufficient condition for perfect secrecy is that* $P_M(E) = P(E)$ *for all* M *and* E. *That is,* $P_M(E)$ *must be independent of* M.
Stated in another way, the total probability of all keys that transform M_i *into a given cryptogram* E *is equal to that of all key transforming* M_j *into the same* E *for all* M_i, M_j *and* E ». *ibid.*, p. 680.

[81] « *The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point* », Shannon, « A Mathematical Theory of Communication », p. 5.

totalement à l'extérieur de ce système, cherchant à expliciter les conditions qui vont lui permettre d'en maîtriser l'ensemble des communications. Il insiste abondamment sur le fait qu'un système secret ne signifie pas une transformation, mais un ensemble de transformations – les clés possibles étant aussi importantes que les clés effectivement choisies – et qualifie de « vrais systèmes secrets » les systèmes cryptographiques définis par Kerckhoffs, ceux qui, par opposition aux « systèmes privés », sont destinés à être utilisés collectivement et publiquement[82]. La signification n'a donc pas disparu du champ des préoccupations de Shannon. Mais ce qui signifie pour Shannon ingénieur diffère radicalement de ce qui signifie pour Alice et Bob, simples acteurs du système parmi d'autres. Son travail est hautement significatif pour les développements des communications, du point de vue de l'ingénieur certes, mais plus généralement du point de vue des praticiens des systèmes de communication, et plus encore du point de vue de tous les pouvoirs pour lesquels ils sont mis au point et organisés. Shannon rend donc tout simplement manifeste le fait que la signification d'un énoncé dépend du point de vue de celui qui l'énonce.

Au sortir de la guerre, la production naissante des ordinateurs hérite largement de ce langage commun, forgé par Shannon pour les ingénieurs et les mathématiciens, qui conservaient encore des approches distinctes au moment de leur collaboration autour de l'analyseur différentiel. Ce langage commun contribuera très efficacement à la mutation de l'approche analogique vers l'approche digitale dans la conception et la réalisation des grands calculateurs. À partir des années 1950, la mise en réseau des ordinateurs se heurte à la nécessité de garantir la confidentialité des échanges informatiques, ouvrant de nouveaux défis et de nouvelles perspectives pour la cryptologie.

CRYPTOLOGIE ET INFORMATIQUE

Dans la course aux armements inaugurée par la guerre froide dans les années 1950, l'ordinateur a été une des clés du système de défense, investie dans les recherches sur l'armement nucléaire et dans la surveillance des territoires[83]. La transition des besoins militaires vers le domaine civil sera

[82] Shannon, « Communication Theory of Secrecy Systems », p. 656.

[83] Mis au point au début des années 1950, le programme SAGE (*Semi Automatic Ground Environment*) est un réseau de défense anti-aérienne automatisé qui couvre l'ensemble du territoire des États-Unis. Les ordinateurs en constituent le centre nerveux. Le *Whirlwind*, premier ordinateur à travailler en temps réel, sera réalisé au MIT dans ce cadre. La firme IBM fut alors chargée d'analyser le *Whirlwind* afin d'en produire industriellement pour les besoins de la défense. Ses modèles IBM 701 et IMB 702, respectivement destinés à des fins militaires et civiles, s'en inspireront directement.

grandement favorisée par la collaboration entre défense, universités et industrie, inaugurée aux États-Unis pendant la guerre. L'amenuisement des budgets militaires à la fin de la guerre a conduit les entreprises commerciales à chercher de nouveaux débouchés. Cette évolution a concrétisé l'ancrage de l'informatique dans le monde civil[84] dès le début des années 1970.

Conjugué à l'algébrisation de la logique et au travail de Shannon, l'architecture von Neumann des ordinateurs[85] ouvre la possibilité d'identifier données numériques et instructions, et installe la notion d'algorithme au cœur de la production des logiciels, qui délivrent sous forme abstraite ce que réalisait initialement le montage des calculateurs sous forme câblée.

L'enjeu du secret change une fois de plus de dimension. Comme l'écrit Horst Feistel en 1973, du fait de leur fonctionnement en réseaux : « Les ordinateurs constituent, ou vont constituer, une menace pour la liberté individuelle. Ils contiennent des données personnelles et sont accessibles à partir de terminaux très éloignés »[86]. Contrairement à la formulation de Feistel, il ne s'agit d'ailleurs pas tant de liberté individuelle, celle que recherchent « les amoureux et les voleurs », mais de la sécurité des échanges internationaux et des libertés commerciales, qui ne concernent plus seulement les militaires et les diplomates, mais constituent une « affaire publique ». Sous la pression d'une demande civile de normalisation de plus en plus forte, émanant en particulier du monde bancaire, la NSA (*National Securité Agency*), créée[87] en 1952 aux États-Unis pour assurer le développement et la sécurité de tous les moyens de chiffrement du gouvernement et de l'OTAN, va promouvoir la publication d'algorithmes cryptographiques. Une nouvelle étape est ainsi franchie quant à la nature du secret : l'accroissement de la puissance du chiffrement, et donc, sa résistance à la cryptanalyse, réduisent la part secrète, concrétisant ainsi les principes de Kerckhoffs.

---

[84] Breton, *Une histoire de l'informatique,* pp. 115-137.

[85] L'architecture Von Neumann est caractérisée par une mémoire unique pour les données et les programmes.

[86] « *There is a growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy* ». Feistel, « Cryptography and Computer Privacy », p. 15.

[87] Son existence est restée secrète jusqu'en 1957. Les journalistes la surnomment alors la *No Such Agency*. Elle est à l'origine du système mondial d'espionnage des communications commerciales ECHELON, élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande, et installé en 1980. Voir l'introduction de cet ouvrage page 17.

Le chiffrement par blocs

C'est dans ce contexte que Feistel va inventer un nouveau dispositif de chiffrement symétrique qui mobilise pleinement la notion d'algorithme et le codage en écriture binaire. D'abord utilisé dans l'algorithme *LUCIFER*[88], en 1973, ce mode de chiffrement est qualifié de chiffrement par blocs, par opposition au mode traditionnel de chiffrement, dit chiffrement par flots. Il alimentera de nombreux algorithmes cryptographiques dont une variante de *LUCIFER* qui sera immédiatement utilisée pour la banque en ligne, et surtout le DES (*Data Encryption Standard*), premier algorithme public de chiffrement symétrique, qui sera homologué par le *National Bureau of Standards* des États-Unis au terme d'une compétition remportée par IBM (*International Business Machines*) à la suite d'un appel d'offres lancé en 1977 pour produire un système cryptographique utilisable par les entreprises.

Emigré d'Allemagne en 1934, et citoyen des États-Unis depuis 1944, Horst Feistel a fait des études de physique au MIT avant de travailler pour l'AFCRC (*Air Force Cambridge Research Center*) sur la mise au point du dispositif IFF (*Identification Friends and Foes*), puis à la conception du chiffrement au *Thomas Watson Research Center* de la firme IBM. Il est un des premiers chercheurs non gouvernementaux à travailler sur la théorisation des modes de chiffrement. Son premier article sur le sujet, « Cryptography and Computer Privacy », est publié en 1973 dans le *Scientific American.* Il analyse d'emblée l'évolution des enjeux : il s'agit désormais de protéger les systèmes informatiques eux-mêmes, ainsi que les banques de données. Feistel écrit notamment :

> « Le système lui-même doit être tel qu'il soit invraisemblable qu'une personne non autorisée mais habile et subtile puisse soit y entrer, soit y supprimer, soit en altérer des commandes ou données »[89].

Une question nouvelle émerge donc : il s'agit d'authentifier l'origine de tout message, et au-delà, de toute instruction informatique, ceci afin d'assurer la sécurité des opérations effectuées par ordinateur. Le problème est donc ici beaucoup plus vaste que la seule protection du secret des messages. Il concerne également les risques de panne et le fait que les réseaux d'ordinateurs sont très ouverts à la corruption délibérée des échanges, car la moindre altération peut fausser tous les résultats ultérieurs

---

[88] Ce nom proviendrait du mot « Demon », obtenu par troncature du mot « Demonstration », qui était alors trop long pour pouvoir être traité par le système d'exploitation.

[89] « *The system itself must make it extremely unlikely that an unauthorized but clever and sophisticated person can either enter, withdraw or alter commands or data in such a system* ». Feistel, « Cryptography and Computer Privacy », p. 15.

des opérations du système. Une nouvelle exigence entre en jeu : si le cryptanalyste dispose d'un laps de temps non négligeable pour travailler, dans un système informatique au contraire, les corrections doivent intervenir en temps réel pour que sa fiabilité soit garantie à ses utilisateurs.

Le travail de Feistel s'inscrit dans le prolongement direct de l'article de Shannon de 1949 sur les systèmes secrets. Il présente toutes ses analyses, à commencer par celle du système de Vernam, en termes d'opérations sur les symboles 0 et 1 en arithmétique modulaire : le chiffrement et le déchiffrement ne sont autres qu'une seule et même opération, l'addition en base 2. Feistel insiste sur l'intérêt d'une clé aléatoire pour le chiffrement polyalphabétique en arithmétique binaire, qui détruit toute régularité d'ordre syntaxique susceptible de servir d'indice au cryptanalyste : toute possibilité de s'appuyer sur la signification des messages se trouve ainsi éliminée, et le cryptogramme produit devient potentiellement indéchiffrable, puisque la recherche d'un mot clair à partir de toutes les substitutions possibles donne tous les mots ayant le même nombre de caractères, sans pouvoir en privilégier aucun.

Outre la difficulté de produire des clés pseudo-aléatoires de longueur suffisante, et en très grand nombre, le système de Vernam souffre d'un autre grave défaut. Dans un environnement d'ordinateurs, où sont transmises beaucoup de données numériques, la moindre erreur de chiffrement peut provoquer une avalanche d'erreurs de calcul. Pour surmonter ce nouveau handicap, Feistel reprend l'idée de fractionner le message, qu'il trouve déjà dans le mode de chiffrement ADFGVX utilisé par les militaires allemands[90] pendant la Première Guerre Mondiale, et celle de chiffrement-produit, théorisée par Shannon dans son article de 1949 alors que son intérêt s'était estompé pendant l'entre-deux-guerres avec le développement des machines à rotors. Dans la section de son article consacrée à la pratique du secret, Shannon envisageait également différents procédés possibles pour renforcer la puissance des systèmes de chiffrement, selon les principes de confusion et de diffusion, que Feistel va s'employer à réaliser concrètement dans le chiffrement par blocs. Ces méthodes visent à contrarier l'analyse statistique menée sur la propagation de certaines propriétés du clair et du chiffré. La diffusion doit disperser les probabilités associées aux lettres du message, tandis que la confusion doit brouiller la relation entre les probabilités associées aux lettres du cryptogramme et à celles de la clé.

Dans l'algorithme *LUCIFER* que décrit Feistel dans son article de 1973, la force du système est obtenue par une combinaison de chiffrements successifs, qui alternent substitutions et permutations. Les substitutions bouleversent le nombre et la répartition des 0 et des 1, et assurent la

[90] Voir le chapitre « Les travaux de la Section du Chiffre pendant la Première Guerre Mondiale » p. 87.

confusion des probabilités qui sont associées aux lettres initiales du message. Quant aux permutations, elles ne font que mélanger les symboles, et engendrent la diffusion de ces probabilités. Ces transformations sont effectuées électroniquement par des dispositifs nommés respectivement boîtes S et boîtes P, qui alternent en plusieurs couches à travers lesquelles passe le message. Le système décrit en 1973 – mais qui n'est pas le premier établi par Feistel et ses collègues – travaille sur des blocs de 128 symboles binaires. Il utilise une clé de même longueur, qui sélectionne les substitutions à mettre en œuvre sur des blocs de 4 symboles binaires. À la sortie, les chiffres sont devenus des fonctions très sophistiquées, et surtout non linéaires, de tous les chiffres d'entrée. Le but du concepteur est évidemment « d'empêcher un adversaire de retracer le processus inverse »[91]. Ces produits de transformations ouvrent, selon Feistel, des possibilités presque illimitées d'invention, de conception et de recherche.

Le message transmis est complété par plusieurs éléments : un mot de passe pour garantir l'authenticité du message, un code correcteur pour juguler les éventuels brouillages de transmission, et un autre mot de passe pour restreindre l'échange des messages à un groupe prédéterminé de destinataires. Le chiffrement par blocs mélange judicieusement les chiffres du message initial et de ces ajouts, de telle sorte qu'un adversaire ne puisse les distinguer.

Ainsi le chiffrement par blocs conjugue-t-il la force du système de chiffrement à une bonne résistance à la corruption – fortuite ou intentionnelle – des messages. Feistel est donc très confiant dans ce nouveau système de chiffrement, investissant la cryptographie d'origine militaire pour assurer la confidentialité des échanges civils.

La publication du DES en 1977 marque un nouveau tournant : c'est le premier algorithme à clé secrète rendu public. La possibilité de rendre public les modes de chiffrement est désormais reconnue par tous. Cette publicité n'est d'ailleurs pas sans risque : elle ne correspond à un choix raisonnable que si l'algorithme sur lequel repose le mode de chiffrement est sûr. Or, l'intervention de la NSA dans la conception ultime du DES a conduit ses utilisateurs à soupçonner l'existence de trappes qui lui auraient permis de décrypter les échanges[92]. Le DES a cependant été le système de chiffrement à clé secrète le plus utilisé pendant une vingtaine d'années. L'augmentation considérable de la puissance des ordinateurs a cependant rendu possible, dès 1997, la recherche de la clé par calcul exhaustif. Pour y

[91] Feistel, « Cryptography and Computer Privacy », p. 21.

[92] Ce soupçon n'est pas totalement gratuit, puisque la NSA a continué à fournir à ses allés des machines *Enigma* pendant la guerre froide, sans révéler que son système avait été décrypté en Grande-Bretagne et aux États-Unis pendant la guerre précédente. Voir l'introduction p. 17.

pallier, la NSA a standardisé un triple DES, puis le système AES en 2000, à la suite d'un appel d'offres cette fois international.

CONCLUSION

Si la cryptologie traite toujours de messages chiffrés, les conditions et l'extension du chiffrement ont donc connu des mutations profondes depuis le début du 19e siècle. L'écriture des cryptogrammes a abandonné la technique du papier-crayon pour s'effectuer au moyen d'instruments et de machines, devenues électroniques au 20e siècle. Mais surtout, les principes propres à l'exercice de la cryptologie ont renoncé au secret des messages particuliers, pour s'attacher aux conditions qui garantissent le secret de l'ensemble des messages susceptibles d'être échangés par le biais d'un système technique donné : système télégraphique et téléphonique au 19e siècle, télégraphie sans fil, téléscripteurs et ordinateurs au 20e. Le développement de ces nouveaux systèmes de communication a été déterminant dans cette mutation de la cryptologie, tout comme les techniques d'écriture avaient présidé à ses balbutiements. L'analyse des conditions de sécurité susceptibles de garantir le caractère sinon privé, du moins réservé, des communications, a présidé à la mathématisation du domaine, et la cryptologie a finalement joué un rôle capital dans l'extension des réseaux d'ordinateurs. Et au fur et à mesure que la puissance des méthodes cryptographiques se renforçait, le secret s'est de plus en plus restreint à la question des clés de chiffrement, la méthode elle-même pouvant s'exposer publiquement.

Il n'empêche que la publicité faite au système ne concerne pas la société civile dans son ensemble. Qu'il s'agisse du système télégraphique ou des réseaux d'ordinateurs, seul un cercle restreint d'utilisateurs initiés est susceptible de s'approprier la connaissance du procédé de chiffrement. Il s'agit des militaires dans le texte de Kerckhoffs, des techniciens du téléscripteur dans le système de Vernam, et des praticiens de l'informatique aujourd'hui. La publicité faite aux systèmes de chiffrement témoigne en fait de l'extension du spectre des personnels concernés par le fonctionnement de ces systèmes. En dépit des déclarations fracassantes sur l'universalité du mode de communication qu'autorise l'informatique aujourd'hui, les modes d'échanges reproduisent de fait les rapports sociaux existants dans la société, tout en décuplant la puissance des détenteurs d'information.

Avec l'extension qu'a connue la théorie de l'information depuis les années 1950, l'importance prise par la notion de système dans ce mode d'échanges a dépassé de très loin le point de vue de l'ingénieur qu'était Shannon. Dans cette perspective nouvelle, il serait pourtant réducteur d'ignorer toute caractérisation du sujet autre que son appartenance à un

quelconque système, ou de considérer tout élément extérieur au système comme « ennemi ». Si la question de la signification des messages n'est pas pertinente pour l'ingénieur, elle reste hautement pertinente, d'un point de vue philosophique, pour le sujet pris dans le fonctionnement de multiples systèmes. Réduire le sujet à l'état d'élément communicant de tels systèmes va à l'encontre de la conception humaniste soucieuse de l'autonomie du sujet, et pour laquelle la signification est centrale dans les échanges humains. En ce sens, il est essentiel pour le sujet de porter un regard extérieur sur ces systèmes de communication. Tels qu'ils sont organisés par la cryptologie, ils ne fonctionnent pas *ex nihilo*. Ils ont une fonction sociale déterminée pour les organisateurs du système lui-même, auxquels il offre toute la puissance de son réseau d'échanges instantanés. Et il devient donc particulièrement urgent de penser cette fonction sociale des systèmes dans leur ensemble.

BIBLIOGRAPHIE

Atlan, H., *Entre le cristal et la fumée, Essai sur l'organisation du vivant.* Paris, Seuil, Points Sciences, 1979.

Babbage, Ch., *The Works of Charles Babbage*, (dir.) M. Campbell-Kelly, London, William Pickering, 11 vols, 1989.

— *Life of a Philosopher, in Works,* vol. 9.

— « Philosophy of Deciphering », Add. Mss. 37205, *British Library, Manuscript Room.*

Bellovin, S. M., « Frank Miller : Inventor of the One-Time Pad », Columbia University, Academic Commons, 2011, http://hdl.handle.net/10022/AC:P:10665.

Bode, H. W. et Shannon, C. E., « A simplified Derivation of Linear Least Squares Smoothing and Prediction Theory », Decimal Classification : R 150. Reprinted *in Shannon's Collected Papers,* pp. 628-656.

Breton, Ph., *Une histoire de l'informatique,* Paris, Seuil, 1990.

Bush, V., « The Differential Analyzer. A New Machine for Solving Differential Equations », *Journal of the Franklin Institute,* 1931, vol. 212, pp. 447-88.

Davies, D. W., « Wheatstone's Cryptograph and Plett's Cipher Machine », *Cryptologia,* 1985, vol. 9, n° 2, pp. 155-160.

Dewey, G., *Relative Frequency of English Speech Sounds,* Boston, Harvard University Press, 1923.

Durand-Richard, M.-J., « Charles Babbage (1791-1871) : de l'Ecole algébrique anglaise à la "machine analytique", *Mathématiques, Informatique et Sciences Humaines*, 1992, 30° année, n° 118, 5-31 ; et n° 120, 79-82.

— « Planimeters and integraphs in the 19th century, before the differential analyzer », *Nuncius*, 2010, vol. XXIV, n° 1, pp. 101-124.
— « Le regard français de Charles Babbage (1791-1871) sur le déclin de la science en Angleterre », *Documents pour l'histoire des techniques*, numéro thématique sur « Les techniques et la technologie entre la France et l'Angleterre XVIIe-XIXe siècles », (dir.) P. Bret, I. Gouzévitch et L. Perez, n° 19, 2e sem. 2011, pp. 287-304.
— « De l'algèbre symbolique à la théorie des modèles : structuration de l'analogie comme méthode démonstrative », *in Le statut de l'analogie dans la démarche scientifique, Perspective historique* (éd.) Marie-José Durand-Richard, Paris, L'Harmattan, 2008, pp. 131-169.
Feistel, H., « Cryptography and Computer Privacy », *Scientific American*, 1973, vol. 128, n° 5, pp. 15-23.
Franksen, O. I., *Mr Babbage's Secret, the tale of a cypher and APL,* Vedbaek (Denmark), Strandberg Forlag, 1984.
— « Babbage and Cryptography. Or, the mystery of Admiral Beaufort's cipher », *Mathematics and Computers in Simulation*, 1993, n° 35, pp. 327-367.
Friedman, W. F., *The Index of Coincidence and its Applications to Cryptolgraphy,* Laguna Hills, California, Aegean Park Press, 1921.
Fréchet, M., *Méthode des fonctions arbitraires, théorie des événements en chaîne dans le cas d'un nombre fini d'états possibles*, Pairs, Gauthier-Villars, 1938.
Givierge, M., *Cours de cryptographie,* Paris, Herman, 1939.
Guillot, P., « Auguste Kerckhoffs et la cryptographie militaire », 2012, http://www.bibnum.education.fr/calculinformatique/cryptologie/la-cryptographie-militaire#.
Hill, L. S., « Cryptography is an Algebraic Alphabet », *American Mathematical Monthly*, 1929, n° 36, pp. 306-312.
— « Concerning Certain Linear Transformations Apparatus of Cryptography », *American Mathematical Monthly*, 1931, n° 38, pp. 135-154.
Hitt, P. *Manual for the Solution of Military Ciphers*, Fort Leavenworth, KS, Press of the Army Service School, 1916.
Kolmogoroff, A., *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin, Springer, 1933.
Minarsky, J.-F., « Cryptanalyse et spécification de schémas de signature RSA avec redondance », *Thèse de l'université de Caen,* Spécialité : Mathématiques et leurs applications, Caen, Université de Basse-Normandie, 1999.
Olivari, H., *Mission d'un colonel français en Russie (1916)*, Paris, L'Harmattan, 2009.

Pratt, M. F., *Secret and Urgent, the Story of Codes and Ciphers*, Garden City New York, American Cryptogram Association, Blue Ribbon Bookds, 1939.

Rémy, F., « La cryptographie à clé publique », *Pour la Science*, dossier « L'art du secret », juillet/octobre 2003, n° 36, pp. 44-51.

Roche, A., *Claude E. Shannon, Spielzeug, Leben und die gheime Geschichte seiner Theorie der Information*, Berlin, Gegenstalt Verlag, 2, Auflage, 2010.

Segal, J., *Le zéro et le un, histoire de la notion scientifique d'information au 20e siècle*, Paris, Syllepse, 2003.

Shannon, C. E., *Collected Papers of C.E. Shannon*, (eds.) Sloane, N. J. A. et Wyner, A. D. New York, IEEE Press, 1993.

— « A Symbolical Analysis of Relay and Switching Circuits », *Transactions of the American Institute of Electrical Engineers*, 1938, n° 57, pp. 713-723, *in Shannon's Collected Papers,* pp. 471-495. http://paradise.caltech.edu/CNS188/shannon38.pdf.

— A letter from Shannon to Vannevar Bush, dated : 16th February 1939, *in Shannon's Collected Papers*, pp. 455-456

— « An algebra for Theoretical Genetics », Ph. D. Doctoral mathematical Dissertation, 1948, *in Shannon's Collected Papers,* pp. 891-920.

— « Mathematical Theory of the Differential Analyzer », *Journal of Mathematics and Physics*, 1941, vol. 20, pp. 337-354, *in Shannon's Collected Papers*, pp. 493-513.

— « Communication Theory of Secrecy Systems », *The Bell System Technical Journal*, 1946-49, vol. 28, pp. 656-711, *in Shannon's Collected Papers*, pp. 656-711.

— « The Philosophy of PCM », *Decimal Classification* : R 148.6. Original manuscript received by the Institute may 24, 1948, *in Shannon's Collected Papers*, pp. 151-176.

— « A Mathematical Theory of Communication », *The Bell System Technical Journal*, july-october 1948, vol. 27, pp. 379-423 et 623-656, *in Shannon's Collected Papers*, pp. 5-82.

Slater, R., *Telegraphic Code, to Ensure Secrecy on the Transmission of Telegrams*, London, W. R. Gray, 1870.

Smoot, B. R., « Pioneers of US Military Cryptology : Colonel Parker Hitt and his wife Genevieve Young Hitt », *Federal History*, 2012, pp. 87-100.

Stankovic, R. S. et Ascola, I., *From Boolean Logic to Switching Circuits and Automata*, Berlin Heidelberg, Springer Verlag, 2011.

Tolman, R.C., *Principles of Statistical Mechanics*, Oxford, Clarendon Press, 1938.

Trogemann, G., Nitussov, A. et Ernst, W., *Computing in Russia, The History of Comuter Devices and Information Technology revealed*, traduction anglaise par A. T. Nitussov, Wiesbaden, Vieweg & Sohn Verlag, 2001.

Vernam, G. S., « Secret Signaling System », *United States Patent Office*, patented July 22, 1919.

Von Neumann, J. et Morgenstern, O., *Theory of Games and Economic Behavior*, Princeton, Princeton University Press, 1944.

Wilkins, J., *The Mathematical and Philosophical Works*, London, Vernor and Hood, 1802, 2 vols.