Le secret des correspondances

Hervé Lehning

Agrégé de mathématiques,
journaliste et écrivain scientifique

À la fin du XIX^{e} siècle, les journaux étaient utilisés pour la communication entre particuliers. Ainsi, voici un extrait de la rubrique « correspondances personnelles » du *Figaro* du 1er janvier 1890 :

Correspondances personnelles

M. c. Mer ! Ai tor. N. sou. t. 2. beau. d. n. repro. récip. N. par. do. jam. d. bris. lie. q. n. ratta., hél !. si peu. Ec. souv.; vi. si du., p. v. surt. pa. c. 89 fin. d:l. larm ! W.

V. H. Mes meilleurs souhaits. Pense beaucoup à vous

M H Cpoof booff e'vo bnj cjfo nbmifvsfvy.

LILI — 1. w. m2. qs2n32s n2t w25y ci00. 100. w45e. 2us2. u. qs2t e w. o. q20t r. s2w.

EN3 Souh b et h on mon meill souven.

23 b. Rèc. comp. t. j. sur les mêmes heures, vois amie, let. frait gd pl. souh. et bon. fête, amit. t. à t.

La rubrique « correspondances personnelles » du *Figaro* du 1er janvier 1890.

Deux messages sont chiffrés dans cet extrait. Le premier, rédigé par M H, est limpide ; il correspond à un décalage d'une lettre et signifie : *« Bonne année d'un ami bien malheureux. »* Le second, proposé par LILI, semble correspondre à une substitution alphabétique. En collectant une cinquantaine de messages, dans différentes éditions du *Figaro*, portant le même indicatif LILI, il est possible de reconstituer la substitution.

Pour commencer, le symbole 2 étant le plus fréquent, il représente sans doute la lettre e, la lettre la plus fréquente en français. On cherche alors une faille pour casser LILI. Nous la trouvons dans le message du 12 janvier :

« LILI. Vot pens ne me quitte pas est tout mon bonh. voud. vs v. 32. u. 13. n2. »

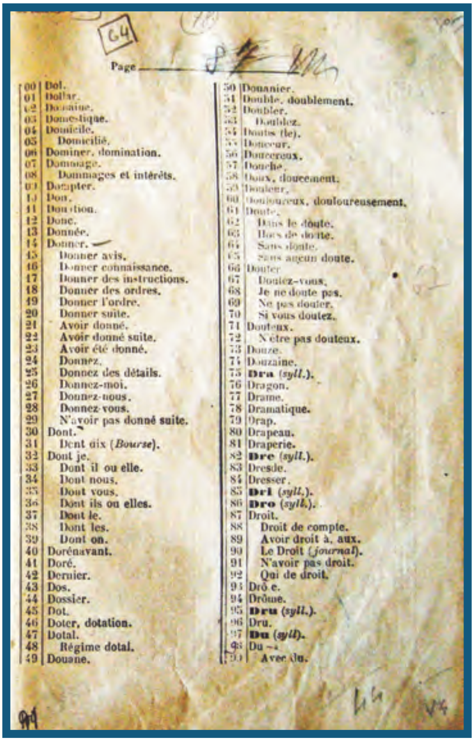
L'unique partie chiffrée, *« 32. u. 13. n2 »*, est un dernier mot que l'expéditeur a voulu cacher. La position des 2 fait penser à *« je t'aime »*, les lettres i et j étant confondues. Le chiffre s'écroule alors progressivement.

Aussi étrange que cela puisse paraître, ces décryptements ont eu un rôle dans l'histoire de la cryptologie. En effet, le commandant français Étienne Bazeries (1846–1931) s'amusait à les lire et, au mess des officiers de sa garnison, régalait ses collègues des histoires scabreuses qu'il lisait sans peine… jusqu'au jour où il annonça qu'il pouvait également lire les messages chiffrés de l'armée. Son général prit cette remarque au sérieux et lui demanda de décrypter quelques dépêches du ministère, ce que Bazeries fit aisément. C'est ainsi qu'il devint l'un des grands cryptologues de l'armée française, puis du ministère des Affaires étrangères de l'époque.

Des maths… plus sophistiquées… pour plus de sécurité !

Pour chiffrer, les entreprises de l'époque utilisaient plutôt des dictionnaires chiffrés ce qui, outre l'assurance d'un certain secret des correspondances, économisait le coût des messages.

L'expression « dommages et intérêts » pouvait ainsi se coder en 9108, soit quatre lettres au


Page

00	Dol.	50	Douanier.
01	Dollar.	51	Double, doublement.
02	Domaine.	52	Doubler.
03	Domestique.	53	Doublez.
04	Domicile.	54	Doubs (le).
05	Domicilié.	55	Douceur.
06	Dominer, domination.	56	Doucereux.
07	Dommage.	57	Douche.
08	Dommages et intérêts.	58	Doux, doucement.
09	Dompter.	59	Douleur.
10	Don.	60	Douloureux, douloureusement.
11	Donation.	61	Doute.
12	Donc.	62	Dans le doute.
13	Donnée.	63	Hors de doute.
14	Donner.	64	Sans doute.
15	Donner avis.	65	Sans aucun doute.
16	Donner connaissance.	66	Douter
17	Donner des instructions.	67	Doutez-vous.
18	Donner des ordres.	68	Je ne doute pas.
19	Donner l'ordre.	69	Ne pas douter.
20	Donner suite.	70	Si vous doutez.
21	Avoir donné.	71	Douteux.
22	Avoir donné suite.	72	N'être pas douteux.
23	Avoir été donné.	73	Douze.
24	Donnez.	74	Douzaine.
25	Donnez des détails.	75	**Dra** (*syll.*).
26	Donnez-moi.	76	Dragon.
27	Donnez-nous.	77	Drame.
28	Donnez-vous.	78	Dramatique.
29	N'avoir pas donné suite.	79	Drap.
30	Dont.	80	Drapeau.
31	Dont dix (*Bourse*).	81	Draperie.
32	Dont je.	82	**Dre** (*syll.*).
33	Dont il ou elle.	83	Dresde.
34	Dont nous.	84	Dresser.
35	Dont vous.	85	**Dri** (*syll.*).
36	Dont ils ou elles.	86	**Dro** (*syll.*).
37	Dont le.	87	Droit.
38	Dont les.	88	Droit de compte.
39	Dont on.	89	Avoir droit à, aux.
40	Dorénavant.	90	Le Droit (*journal*).
41	Doré.	91	N'avoir pas droit.
42	Dernier.	92	Qui de droit.
43	Dos.	93	Drôle.
44	Dossier.	94	Drôme.
45	Dot.	95	**Dru** (*syll.*).
46	Doter, dotation.	96	Dru.
47	Dotal.	97	**Du** (*syll.*).
48	Régime dotal.	98	Du
49	Douane.	99	Avec du.

Une page du *Code télégraphique chiffré* de F.-J. Sittler (Lefebre, 1879). Le numéro de la page est écrit au crayon et plusieurs fois modifié car il fait partie du chiffre. Si le numéro de la page est ici 91, « dragon » se chiffre 9176 (ou 9716… selon la convention passée entre les correspondants).

© Hervé Lehning

lieu de dix-huit, quand on utilisait le *best-seller* des dictionnaires chiffrés de l'époque, celui de Sittler, qui eut cours de 1890 à 1920 environ.

Même si la numérotation personnalisée des pages compliquait le décryptement, celui-ci restait relativement élémentaire. Tous les messages chiffrés arrivant à la poste étaient envoyés au ministère des Affaires étrangères, pour lequel Étienne Bazeries travaillait. Ils étaient ainsi décryptés.

L'autre grand nom de la cryptographie de la fin du XIX^{e} siècle fut le Néerlandais Auguste Kerckhoffs (1835–1903). Il fut le premier à énoncer le principe de base de la cryptographie moderne : un système de chiffrement ne doit pas reposer sur son secret, mais sur celui d'une clef que l'on change périodiquement. Tous les systèmes que nous venons de voir sont défaillants de ce point de vue.

Dès la Renaissance, le diplomate français Blaise de Vigenère (1523–1596) avait pourtant conçu un système répondant au principe de Kerckhoffs, même s'il fut peu utilisé à l'époque. Son principe est simple mais son application à la main est pénible, il consiste en un décalage des lettres variant selon une clef. Par exemple, la clef « abc » correspond à un décalage de 0 pour la première lettre, de 1 pour la seconde, de 2 pour la troisième, puis on recommence (0 pour la quatrième lettre, 1 pour la cinquième…). Ainsi, « mathématiques » se chiffre en « mbvhfoaukqvgs ».

Bien entendu, les clefs sont en général plus complexes, mais le principe reste le même. Comme l'utilisation manuelle d'un tel chiffre est pénible, il existe des instruments pour le faire, comme la *réglette de Saint-Cyr*, utilisée autrefois dans cette école d'officiers pour l'enseignement de la cryptographie.

La *réglette de Saint-Cyr* permet de réaliser des décalages selon une clef (en italiques ici). Ainsi, la clef *i* transforme A en I, B en J, *etc*.

Le décryptement est d'autant plus difficile que la clef est longue et choisie aléatoirement. L'idéal est qu'elle soit aussi longue que le message et qu'on ne l'utilise qu'une fois, on parle alors de *masque jetable*. C'est le chiffre utilisé dans le fameux téléphone rouge, qui relie Washington et Moscou depuis 1963. Ce chiffre est aussi l'un des chiffres des espions de la guerre froide, d'où les petits carnets étranges ci-dessous.

Carnet de nombres aléatoires avec loupe.
© Archives de la DGSE. Exposition Archives nationales : Le secret de l'État.

Le principe est simple. On chiffre d'abord le message en une suite de nombres par la méthode que l'on veut (par exemple, A = 01, B = 02…), puis on ajoute au message obtenu un nombre aléatoire de même longueur (sans effectuer de retenue). Ainsi, « mathématiques » devient d'abord :

13 01 20 08 05 13 01 20 09 17 21 05 19.

On lui ajoute ensuite les vingt-six premiers chiffres du carnet, le message chiffré est donc :

03691 91070 16694 49382 63998 8.

Clair	13012	00805	13012	00917	21051	9
+ clef	90689	91275	03682	49475	42947	9
= chiffré	03691	91070	16694	49382	63998	8

Si l'on connaît la clef, c'est-à-dire les nombres du carnet, on déchiffre ce message en faisant la différence entre le message chiffré et la clef :

Chiffré	03691	91070	16694	16694	63998	8
– clef	90689	91275	03682	49475	42947	9
= clair	13012	00805	13012	00917	21051	9

Ce système de chiffrement est solide mais repose sur la sécurité de transmission de la clef. Il est très probablement utilisé dans les *stations de nombres*.

Surveillance de masse : prise de conscience et solutions

De nos jours, la confidentialité des communications sur Internet est assurée par des systèmes de ce type, que l'on dit *symétriques* car chiffrement et déchiffrement sont symériques l'un de l'autre. Ces deux opérations s'opèrent à la vitesse de l'addition, c'est-à-dire instantanément. La transmission de la clef est assurée par un chiffrement *asymétrique* (où savoir chiffrer ne suffit pas pour déchiffrer). Le plus célèbre de ces chiffres est le code RSA, inventé par Ronald Rivest, Adi Shamir et Leonard Adleman en 1976 et fondé sur la difficulté de la factorisation des nombres. Son chiffrement repose sur une exponentiation, donc est très lent et gourmand en énergie, ce qui explique que l'on limite son utilisation à la transmission des clefs. Le système PGP (Pretty Good Privacy, en français Assez bonne confidentialité) repose sur ce principe.

A priori, nous pouvons disposer ainsi de chiffrements pratiquement indécryptables. C'est le cas du système de communication des hautes personnalités de l'État créé par Thalès et nommé TEOREM (*sic.*).

Le TEOREM de Thalès,
téléphone sécurisé des personnalités de l'État.
© *Hervé Lehning*

Bien entendu, ceci ne peut que déplaire aux services de renseignements. Une solution serait de demander à chacun de laisser ses clefs chez un tiers de confiance qui ne les donnerait qu'aux autorités autorisées, sur décision de justice.

Edward Snowden (né en 1983) a révélé la surveillance de masse de la NSA.
© *Laura Poitras*

Selon Edward Snowden, la National Security Agency (NSA, l'agence de sécurité américaine) a préféré adopter une autre démarche et a demandé aux fournisseurs de logiciels américains de créer des portes dérobées permettant de contourner leurs algorithmes de chiffrement.

Le pire ennui de cette méthode est que, si une porte dérobée existe pour pénétrer dans une citadelle, tout le monde peut la découvrir et l'utiliser ! La NSA a ainsi créé une faiblesse dans tous les systèmes de chiffrements qu'elle contrôle. Aussi, pourquoi des *hackers*, des entreprises ou d'autres organismes se priveraient-ils de les utiliser ?

À l'inverse, ces portes dérobées pourraient disqualifier les entreprises américaines et créer une opportunité extraordinaire aux sociétés françaises. D'autant plus que le marché de la cryptologie est florissant. Pour satisfaire le désir de l'État de surveiller les escrocs et les terroristes, il suffirait alors de créer un tiers de confiance gardant les clefs de chacun, et d'instaurer une législation prévoyant d'y faire appel dans le cadre de certaines enquêtes.

H.L.

Pour en savoir (un peu) plus :

Les archives du Figaro (1890), disponibles en ligne *via* Gallica, Bibliothèque nationale de France.

L'univers des codes secrets, de l'Antiquité à Internet, Hervé Lehning, Ixelles, 2012.

Les stations de nombres, radio des espions, Philippe Baudouin, Arte radio, 2013.