Genève, le 23 novembre 1953.

Mr. William F. Friedman
310, Second Street, S.E.
WASHINGTON 3, D.C.

Monsieur,

Le Professeur B. van der Pol, qui vous a rencontré le mois dernier à Londres, me fait savoir qu'il vous intéresserait de connaître mon décryptement d'une lettre écrite par le mathématicien Euler à son ami Goldbach ; ce cryptogramme avait résisté pendant deux siècles à tous les efforts.

Je me fais un plaisir de vous envoyer, par pli séparé, une copie de ma publication à ce sujet. Comme vous le verrez vous-même, il s'agit d'un procédé élémentaire qui toutefois a été utilisé très intelligemment.

Veuillez agréer, Monsieur, l'expression de ma haute estime et considération.

P. Speziali

Pierre Speziali
2, chemin de Roches
GENEVE (Suisse)

Tirage à part: «Stultifera navis», Bulletin de la Société suisse des bibliophiles
10me année, No. 1/2, avril 1953

P. Speziali / Le logogriphe d'Euler[1]

Dans la lettre que le grand mathématicien bâlois Léonard Euler, étoile de première grandeur au firmament scientifique du XVIIIe siècle, adressait le 4 juillet 1744 à son ami Christian Goldbach se trouve, à la suite d'une longue dissertation sur le calcul différentiel, le passage que voici:

«Ich habe vor einiger Zeit nachfolgenden logogryphum entworfen, worin alle characteres Buchstaben bedeuten und der Text latein ist:

Pxqſwlznjdvynſtiddkqxhleebfpxdfgtlzbccfbkfodxokfng lqxnſshejmlckzxhrfwjgfhxvzjnbgyxcdgixkoxjmlncoigdx vzflme ſnfyjqfangvnylrcxfonbfjalrkw ſnbfpjoizoxqknub rofadgiaxwkcbrbcklofrnjwngfzfhgjfcbcfvqjtxeevtbzfyjsb zhfmlnbgſsqjwglnxvzfkonbcoigdxvrkfjalzxtſnilenfgvcbo ofcfxnnfgnkbcjnnjynxvplgnbfzfoxeejdgxbcjcnfdyvdbhzln vyxmbcblobbcyfekonbceiobfplwsxzxfjcndbhrlzqxsfonbcol jfſyqfmjeevhleexoiexmgicfdnktwoldxnfbxofcktvpxrnv

Ungeachtet hier die Bedeutung der characterum nicht veränderlich ist, so deucht mich doch, daß dergleichen Schrift nicht leicht dechiffrirt werden kann[2].»

Nous ne savons si Goldbach a trouvé la clef de ce chiffre, ni si Euler lui a communiqué la solution. Dans leur correspondance ultérieure, du moins dans celle que nous possédons encore, il n'est plus fait mention de ce problème.

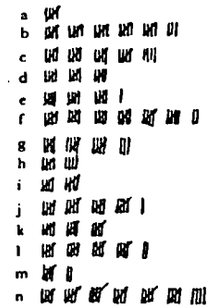
Nombreux sont ceux que le logogriphe d'Euler a intrigués depuis deux siècles.

Ceux que cette question pourrait encore intéresser aujourd'hui en trouveront la solution dans cet article, dont le principal but est de proposer une méthode et de donner des directives à quiconque viendrait, un jour ou l'autre, à se trouver en présence d'un texte aussi incompréhensible que celui d'Euler et voudrait essayer d'en trouver la clef.

Euler lui-même nous donne déjà trois indications précieuses: le texte est en latin, chaque signe garde la même signification dans tout le message et tous les signes ont un sens.

Il faut d'abord se familiariser avec la physionomie du latin[3]. Si l'on n'a pas une table indiquant la fréquence des lettres de cette langue, on prendra un texte quelconque d'un millier de lettres, on comptera combien de fois intervient la lettre A, puis le B, etc. et on dressera un tableau de fréquence en %. En rangeant les lettres de l'alphabet par ordre de fréquence décroissante on obtiendra la suite: I E U T A M S N R O D L V C P Q B F G X H, qui ne peut être qu'approximative, car elle est certainement faussée si le texte contient des répétitions de mots formés par des lettres rares.

Faisons ensuite une statistique des lettres qui composent notre cryptogramme.



Première constatation: le logogriphe contient les 26 lettres de notre alphabet plus le signe *ſ*. Or l'alphabet latin ne compte que 21 lettres. Les cinq les plus fréquentes – ce sont, nous venons de le voir, I, E, U, T, A – représentent à elles seules la moitié environ d'un texte quel qu'il soit. Dans le nôtre, qui compte 408 lettres, elles devraient donc apparaître une quarantaine de fois chacune. Or le *n*, qui revient le plus souvent, n'y figure que 34 fois. Aucune n'atteint donc 40. Cela paraît signifier qu'Euler a employé au moins deux représentations pour les lettres les plus fréquentes. Il se serait donc servi du système que les cryptologues nomment «substitution à représentation multiple».

Cette hypothèse une fois admise, il faut examiner le cryptogramme et essayer de tirer le plus de renseignements possibles des redoublements de lettres et des groupes de lettres qui se répètent.

Les redoublements nous permettent de faire la distinction entre consonnes et voyelles. Les voici dans l'ordre, avec les deux lettres qui les encadrent: *iddk*, *leeb*, *bccf*, *xeev*, *booſ*, *xnnf*, *jnnj*, *xeej*, *obbc*, *jeev* et *leex*. Puisque toutes les lettres qui encadrent les redoublements ne se redoublent pas elles-mêmes, on en tire que *i*, *k*, *l*, *f*, *x*, *v*, *j* sont des voyelles. Le *b* fait exception, mais comme il encadre trois redoublements et comme *o* et *c* se redoublent en tant que consonnes, il n'y a aucun risque à supposer que *b* est une voyelle.

Le cas de la lettre *e* est intéressant. Elle intervient dans 5 redoublements et ne figure que 6 fois en tant que lettre simple. Une lettre plutôt rare que fréquente qui se redouble souvent en latin est le L (par ex. dans les mots *nullum*, *illa*, *bellum*, *augella*, *ancilla*, etc.); il suffit d'examiner un texte latin pour s'en apercevoir au premier coup d'œil.

On trouve des répétitions de 2, de 3 ou de plusieurs lettres. Elles correspondent à des bigrammes, trigrammes ou à des mots fréquents. Les petits mots, prépositions ou autres, tels que *in*, *ab*, *cum*, *est* et les désinences *us*, *um* peuvent être utiles, mais il est difficile de les repérer avant de posséder d'autres données sûres. Relevons plutôt les deux belles séquences *ſjalrkwſn* et *ſjalzxtſn*. Nous avons accepté *k* et *x* comme voyelles; s'ils représentent la même voyelle, il est probable que ces deux suites signifient exactement la même chose. Dès lors *r* et *z* correspondent à la même lettre du clair; il en sera de même pour *w* et *t*.

La suite *coigdxv* se répète. Il est curieux que ce mot, formé pourtant par des lettres fréquentes, soit chiffré les deux fois de la même façon: il y a là une intention manifeste de la part de l'auteur du cryptogramme. Cette répétition ne peut donner aucun point d'appui.

Nous avons distingué entre consonnes et voyelles. L'expérience prouve que l'identification des consonnes est plus aisée que celle des voyelles. En effet, un texte latin est en général composé par autant de consonnes que de voyelles. Les voyelles sont au nombre de 5, et ne se distinguent guère par leur fréquence; parmi les consonnes, au contraire, il y en a de rares, de très rares même, et de fréquentes. Si on commence par rechercher celles-ci, on risque de mettre sa patience à rude épreuve. Prenons, par exemple, les consonnes les plus fréquentes du latin: T, M, S, N. Supposons que les lettres *c*, *n*, *o*, *g* du logogriphe leur correspondent. Les essais qu'entraîne cette hypothèse peuvent demander beaucoup de temps. Nous ne voulons pas dire que la méthode soit mauvaise, ni qu'elle ne puisse conduire, après des recherches plus ou moins laborieuses, au résultat final. Le facteur chance joue aussi quelquefois en faveur de celui qui persévère. Cependant le risque est grand que certains impondérables du subconscient ne ramènent le chercheur à des hypothèses déjà examinées et rejetées: on y revient malgré tout, on s'y cramponne, on piétine et on ne trouve rien en définitive. J'en veux comme preuve le cas suivant.

Il y a quelque part, dans la première moitié du message, le groupe *nco*, formé par trois consonnes fréquentes. Les trigrammes clairs possibles sont MST, MTR, NTS, NTM, NTR, NST, RST, STR, STM, soit dans le corps d'un mot soit comme

[1] Quoique le contenu de cet article sorte du cadre de nos publications, nous n'avons pas voulu priver nos lecteurs de cette belle leçon de déchiffrement, qui apporte aux collectionneurs d'autographes, à côté de subtiles considérations sur les écritures secrètes, la clef de l'énigme proposée par notre grand mathématicien Léonard Euler.

[2] Le texte intégral de la lettre est dans la *Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIe siècle*, par P.-H. Fuss, St. Pétersbourg, 1843, tome I, pp. 278–293.

[3] Il existe une abondante littérature traitant des écritures secrètes. Citons deux ouvrages théoriques parmi les meilleurs: le *Cours de Cryptographie* de Givierge, Paris, 1936, et le *Manuale di Crittografia* de Sacco, 3e éd., Rome 1947. Le second contient une notice historique très intéressante, une liste bibliographique des plus complètes et 28 tables de fréquences, dont une pour le latin.

fin et début. En examinant tous ces cas, on n'aboutit absolument à rien. On se dit alors: *n* et *c* se redoublent, ils interviennent dans des répétitions de bigrammes et de trigrammes; ce sont donc bien deux lettres fréquentes dans un texte clair. En serait-il autrement du *o*? Serait-ce une lettre d'ordinaire rare, fréquente dans ce texte? Mais laquelle?

Il est donc plus simple de porter son premier effort sur les lettres rares du cryptogramme. Elles correspondent probablement à des lettres rares du texte clair. Prenons le *a*, qui n'apparaît que 5 fois et précisément dans les groupes *fangv*, *jalrk*, *fadgiaxwkc*, *jalzx*. Examinons attentivement *ang* et *adg*. Nous admettrons pour *n* une des lettres T, M, S ou N; *g* est moins fréquent, dont N, R ou D. Que prendre pour *a*? Après deux essais seulement notre choix s'est porté sur la lettre X. Dès lors les possibilités se réduisent à une seule, *ang* = XTR, ce trigramme étant bien encadré par deux voyelles. La voyelle qui le précède est certainement *e*, donc *fang* = EXTR.

Passons à *adg*; *d* est moins fréquent que *g* et se redouble. Ce pourrait être P, B ou F. Après le X nous mettrons P; *adg* correspondrait donc à XPR.

Puisque nous avons posé *n* = T, reprenons la lettre fréquente *c*. Elle doit valoir M ou S; la substitution de *c* par M dans tout le texte ne donne rien de plausible, tandis que *c* = S nous fait apparaître quelque chose qui nous plaît beaucoup:

n c o i g d x v z f
T S R P E

où *i*, *x* et *v* sont des voyelles. Allons chercher *x* dans la séquence contenant deux fois le *a*, écrite plus haut.

a	*d g i a x w k c*
X	P R X S

En séparant comme nous le faisons et en nous rappelant que nous avons admis que *x* et *k* représentent la même lettre, nous repérons sans peine le mot PROXIMIS.

Cela étant, nous pouvons compléter le groupe précédent:

c o i g d x v z f
S O R P I E

Nous avons ailleurs, dans notre cryptogramme, le groupe *nxvzf* qui, d'après ce que nous avons déjà identifié, correspond à TI..E; immédiatement nous pensons à la terminaison TIONE. En reportant dans le texte les lettres que nous venons d'identifier ainsi, toutes nos suppositions se confirment. Il reste la lettre *o*, qui nous a donné tant de mal; c'est une lettre généralement rare en latin, mais fréquente dans ce texte: le C. On a ainsi le mot SCORPIONE.

Une douzaine de lettres sont déjà identifiées. En les reportant partout où elles figurent, ce sera désormais chose facile de compléter le texte entier, qui prendra l'aspect suivant:

p x q f w l z n j d v y n f t i d d k q x h l e e
QUIDAMANTEPORTAMOPPIDIGALL

b f p x d f g t l z b c c f b k f o d x o k f n g
UEQUIPERMANUSSEUIACPICIETR

l q x n f s h e j m l c k z x h r f w j g f h x v
ADITAFGLEBASINIGNEMEREGIO

z j n b g y x c d g i x k o x j m l n c o i g d x
NETURRISPROIICIEBATSCORPI

v z f l m e f n f y j q f a n g v n y l r c x f o
ONEABLATEREDEXTROTRANSIEC

n b f j a l r k w f n b f p j o i z o x q k n u b
TUEEXANIMATUEQUECONCIDITHU

r o f a d g i a x w k c b r b c k l o f r n j w n
NCAXPROXIMISUNUSIACENTEMT

g f z f h g j f c b c f v q j t x e e v t b z f y
RANEGREESUSEODEMILLOMUNER

j s b z h f m l n b g f s q j w g l n x v z f k o
EFUNGABATURAFDEMRATIONEIC

n b c o i g d x v r k f j a l z x t f n i l e n f
TUSCORPIONIEEXANIMATOALTE

g v c b o o f c f x n n f g n k b c j n n j y n x
ROSUCCESEITTERTIUSETTERTI

v p l g n b f z f o x e e j d g x b c j c n f d y
OQUARTUENECILLEPRIUSESTAPR

v d b h z l n v y x m b c b l o b b c y f e k o n
OPUGNATORIBUSUACUUSRELICT

b c e i o b f p l w s x z x f j c n d b h r l z q
USLOCUEQUAMFINIEESTPUGNAND

x s f o n b c o l j f f y q f m j e e v h l e e x
IFACTUSCAEEARDEBELLOGALLI

o i e x m g i c f d n k t v o l d x n f b x o f c
COLIBROSEPTIMOCAPITEUICAS

k t v p x r n v
IMOQUINTO

La fin nous apprend qu'il faut chercher ce texte dans le «De bello gallico» de J. César et précisément au 25e chapitre du VIIe livre, où nous lisons en effet:

«Quidam ante portam oppidi Gallus, qui per manus sebi ac picis traditas glaebas in ignem e regione turris proiciebat, scorpione ab latere dextro traiectus exanimatusque concidit. Hunc ex proximis unus iacentem transgressus eodem illo munere fungabatur; eadem ratione ictu scorpionis exanimato alteri successit tertius et tertio quartus, nec prius ille est a propugnatoribus vacuus relictus locus, quam restincto aggere atque omni ex parte submotis hostibus finis est pugnandi factus[4].»

Remarquons que le *f* du chiffré signifie tantôt E, tantôt S, ce qui veut dire que dans le manuscrit original, aujourd'hui introuvable, il y avait deux *f* de type différent. C'est probablement là une des causes des difficultés qu'a présentées le décryptement de ce texte. Les erreurs de chiffrement sont peu nombreuses. La fin du texte latin est quelque peu contractée.

La clef du chiffre est donnée par les deux tables suivantes:

a) *alphabet chiffrant:*

A B C D E F G H I L M N O P Q U R S T U V X
l m o q j s h u k e t r i d p g c n b a
f f x w z v y f

b) *alphabet déchiffrant:*

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 f
X U S P L E R G O E I A B T C Q U D N F M H O M I R N A
V

[4] En voici la traduction: «Il y avait devant une porte un Gaulois qui jetait vers la tour en feu des boules de suif et de poix qu'on lui passait de main en main; un trait parti d'un scorpion *(sorte de catapulte qui ressemblait à une grosse arbalète montée sur pied)* lui perça le flanc droit et il tomba sans connaissance. Un de ses voisins, enjambant son corps, le remplaça dans sa besogne; il tomba de même, frappé à son tour par le scorpion; un troisième lui succéda, et au troisième un quatrième; et le poste ne cessa d'être occupé par des combattants jusqu'au moment où l'incendie ayant été éteint et les ennemis repoussés sur tout le front de la bataille, le combat prit fin.»

Ce qui précède paraîtra long, et d'un abord pénible au profane. Parfois on parvient au but plus rapidement par une méthode assez expéditive, dite du «mot probable». Elle consiste à rechercher dans le texte des mots susceptibles de s'y trouver.

Si Euler nous avait prévenu qu'il s'agissait d'un passage de César, nous aurions essayé d'y placer des termes fréquents dans la langue militaire, tels que *bellum*, *hostis*, *pugnare*, etc. et nous aurions trouvé sans grand-peine la solution. Mais il s'est bien gardé de nous faciliter ainsi la tâche.

Il est piquant de rappeler que César lui-même (Euler le savait-il?) chiffrait les ordres qu'il donnait à ses lieutenants au moyen d'un système très simple, qui consistait à décaler chaque lettre de quelques rangs dans l'alphabet. Ce système, qui devait suffire à faire perdre son latin à Vercingétorix, porte de nos jours encore le nom de Jules César.

Notons en terminant que le latin est particulièrement difficile à décrypter, la fréquence des lettres ne présentant pas les mêmes écarts que dans la plupart des langues modernes.

C'est pour cette raison que, tout récemment, un de mes amis, qui cherchait lui aussi à percer le secret du logogriphe d'Euler, s'était fait chiffrer par sa fille quelques passages de César, dans le dessein d'étudier les moyens d'attaquer les cryptogrammes latins.

Warum denn in die Ferne schweifen,
Sieh, das Gute liegt so nah!