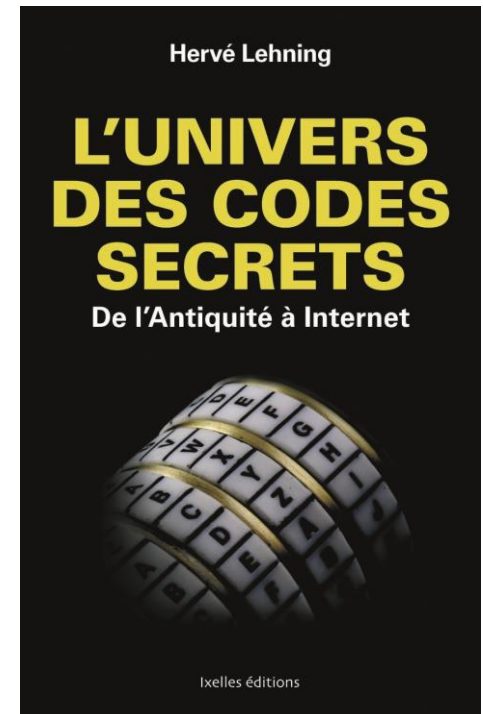


# Etienne Bazeris et le secret des correspondances à la Belle époque

Par Hervé Lehning

[www.lehning.eu](http://www.lehning.eu)

<http://blogs.futura-sciences.com/lehning/>



## Correspondances personnelles

**M** e. Mer! Ai tor. N. sou. t. 2. beau. d. n. repro. récip.  
**M**. 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  
**MYOSOT.** Entour milie. Ai. inef! Souv. fid. ét! Ame.

**L** U. V. A toi mes v. sois h. moi ma vie est bri-  
**L**, sée car je toujours autant à toi. Je souf. et  
s. atrocem, malh. Pense qqfois à moi.

**M H** Cpoof booff e'vo bnj cjfo nbmifvsfvy.

**L** ILI — 1. w. m2. qs2n32s n2t w25y c400. 100. w45e.  
**L** 2us2. u. qs2t e w. o. q20t r. s2w.

Figaro du premier janvier 1890

Figaro du 12 janvier 1890

**Correspondances personnelles**

**B**leuet : D4nqm. s2ulcm. S2ous. 1 Q1s3t t2n. qs4di.  
T2s. i25s. r3 q45w. w4 w. n2sds2e. 4 h. Mil. amit.

Man. Chér. prends lett. rue M. A toi. F.

**L**ILI. Vot pens ne me quitte pas est tout mon  
bonh. voud. vs v. 32. u. 13. n2.

**V**H. — Ai écrit 2 fois. Ma pensée ne varie pas.  
Tout à vous de cœur. Supplie répondre.

Une erreur de chiffrement classique qu'on retrouvera dans l'armée napoléonienne

Hypothèse :

32. u. 13. n2. signifie « je t'aime »

i et j étant confondus

1 -> a 2 -> e 3 -> i

u -> t n -> m

Les voyelles sont chiffrées par des nombres :

a -> 1 e -> 2 i -> 3 o -> 4 u -> 5 y -> 6

Et les consonnes par la lettre suivante

b -> c c -> d etc.

# Retour au premier janvier pour vérification

1. w. m2. qs2n32s n2t w25y c400. 100. w45e.  
2us2. u. qs2t e w. o. q20t r s2w.

1. w. m2. qs2n32s n2t w25y c400. 100. w45e.  
2us2. u. qs2t e w. o. q20t r s2w.

a v le premier mes veux bonn ann vould  
etre t pres d v n pens q rev

1. w. m2. qs2n32s n2t w25y c400. 100.  
w45e. 2us2. u. qs2t e w. o. q20t r s2w.

a v le premier mes veux bonn ann voud  
etre t pres d v n pens q rev

A vous le premier mes vœux de bonne  
année. Je voudrais être près de vous. Je ne  
pense qu'en rêve.



## Correspondances personnelles

**B**leuet : D4nqm. s2u1cm. S2ous. 1 Q1s3t t2n. qs4di.  
T2s. i25s. r3 q45w. w4 w. n2sds2e. 4 h. Mil. amit.

Man. Chér. prends lett. rue M. A toi. F.

**L**ILI. Vot pens ne me quitte pas est tout mon  
L bonh. voud. vs v. 32. u. 13. n2.

**V**H. — Ai écrit 2 fois. Ma pensée ne varie pas.  
Tout à vous de cœur. Supplie répondre.

D4nqm. s2u1cm. S2ous. 1 Q1s3t t2n. qs4di.  
T2s. i25s. r3 q45w. w w. n2sds2e. 4 h. Mil.  
amit.

Compl. retabl. Rentr. A Paris sem. Proch.  
Ser. heur. si pouv. v v. mercred. 4 h Mil. amit.

D4nqm. s2u1cm. S2ous. 1 Q1s3t t2n. qs4di.  
T2s. i25s. r3 q45w. w w. n2sds2e. 4 h. Mil. amit.

Compl. retabl. Rentr. A Paris sem. Proch.  
Ser. heur. si pouv. v v. mercred. 4 h Mil. amit.

Complètement rétabli. Rentre à Paris la  
semaine prochaine. Je serais heureux si je  
pouvais vous voir mercredi à 4 heures. Mille  
amitiés.

Il faut chercher jusqu'au 23 janvier pour trouver autre chose que le chiffre de César et celui de Lili.

### Correspondances personnelles

180 — Pens ne vs quitte pas. Le soir, la nuit même.  
je vs écr. seul moyen causer av. maman. — Amit.

H. J. 94. Vais b. mieux ; vous ai écrit à C. demandez.

Y7. fh. qli. Jzq. huxe. nuf. jhk3. f. zv. F. uxh. Dulv. yzq.

Girou ferai mêm voyag. s. seule. A. bie. 10.

On retrouve ces messages les 30 et 31 janvier :

### Correspondances personnelles

**R**u. d'Amsterd. 4 h. dim. dern. chap. roug. mant. bleu  
défaut à g. revenez mêm. ru. heur. dim. Prière ard.

**F.21** — Avez lett Q. kiliqbgoiq 42. Vais b. Trist — A.

**75** — Kf wt beps. qfujuf nbnbo Bzfa dpvg. C, bw bou  
**J** upvu wpu. cpvi. Wt efn. tfvm. wpu. bggfdu.

**S L 55** env. tous souhaits mille amit.

**X. 3. L. s. nouv.** suis inquiet. Tâchez faire écr.

**Y7.** gqn. utth. Fhu3y. lked. 3zn. Fzxr. uxh. Hud. dqf.

**Urg<sup>t</sup>** v. parl. Suppl. écr. quand pauv. ch. Rose tend.

### Correspondances personnelles

**Y7.** julg. qlxqv. ushzlsud. z. lg. Nuf. l. jhked. j. ugjqkl.  
**J**nefk. rkm. ve. 3klv. Gkq. xzn3, jz. qli. — F. z.

**LILI.** — Voud. vs parl. quand puis-je esp. vs voir?

Les messages Y7 :

fh. qli. Jzq. huxe. nuf jhk3.f.zv.F.uxh.Dulv.yzq.

gqn. utth. Fhu3y. lked. 3zn. Fzxr. uxh. Hud.  
dqf.

julg. qlxqv. ufhzlsud.z.lg.Nuf.l.jhked.j.ugjqkl.  
Jnefk. rkm. ve. 3klv. Gkq. Xzn3, jz. Qli. – F.z.

fh. qli. Jzq. huxe. nuf jhk3.f.zv.F.uxh.Dulv.yzq.  
gqn. utth. Fhu3y. lked. 3zn. Fzxr. uxh. Hud. dqf.  
julg. qlxqv. ufhzlsud.z.lg.Nuf.l.jhked.j.ugjqkl.  
Jnefk. rkm. ve. 3klv. Gkq. Xzn3, jz. Qli. – F.z.

La lettre la plus fréquente est le u (au lieu du e),  
Le 3 est intrigant (seul nombre)  
a, b et c n'apparaissent pas ...

Hypothèse : l'alphabet est retourné (atbash)  
mais v et w sont confondus et m est chiffré en  
3, pour ne pas l'être en lui-même.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | x | y | z |
| z | y | x | v | u | t | s | r | q | p | o | n | 3 | l | k | j | i | h | g | f | e | d | c | b | a |

fh. qli. Jzq. huxe. nuf jhk3.f.zv.F.uxh.Dulv.yzq.

tr. inq. Pai. recu. let prom.t.ad.T.ecr.Vend.bai



|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | x | y | z |
| z | y | x | v | u | t | s | r | q | p | o | n | 3 | l | k | j | i | h | g | f | e | d | c | b | a |

gqn. utth. Fhu3y. lked. 3zn. Fzxr. uxh. Hud. dqf.

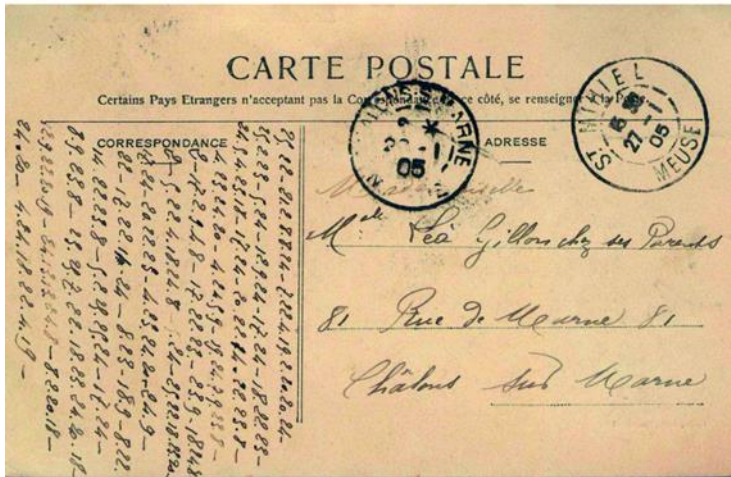
sil. effr. Tremb. nouv. mal. Tach. ecr. Rev. Vit.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | x | y | z |
| z | y | x | v | u | t | s | r | q | p | o | n | 3 | l | k | j | i | h | g | f | e | d | c | b | a |

julg. qlxqv. ufhzlsud.z.lg.Nuf.l.jhked.j.ugjqkl. Jnefk.  
 rkm. ve. 3klv. Gkq. Xzn3, jz. Qli. – F.z.

Pens incid etrange v a ns let n prouv p espion  
 pluto hom du mond sov calm pa inq - T.a.

# Les cartes à Léa





112 307  
109 8

# CARTE POSTALE

Certains Pays-Etrangers n'acceptant pas la Correspondance de ce Code, se renseigner à la Poste.



29.22-13.24.22-22.19.2.4.24.24-17.24-  
 18.22.23.24.14-19.24-18.22.23.24.20.18-19.24-  
 18.24-4.24.14.2.23.4-29.22.23.8-7.29.4  
 12.9.2.9.3-18.24.20.20.9.23.24.8-18.22  
 20.18-20.2.9.8-4.22.18.18.4.22.2.24.4.21  
 20.18-13.24-18.24.2.2.8-7.24.4.19.9-  
 12.24.22.20.19-17.24-8.24.4.22.23.8-15.  
 23.24.24-5.2.22.23.24.20.18-5.24-  
 10.22.23.18-23.18-12.9.24-17.24-20.24-  
 4.24.5.2.23.8-18.24.8-5.22.4.18.24.8-12.9.24-  
 13.24-8.2.23.4-18.22.20.14.25.8-12.9.24-17.24-  
 13.24.8-4.24.5.24.14.22.23.8-13.24-29.22.18.  
 23.20-9.20-15.2.20-15.22.23.8.24.4-

M<sup>rs</sup> Léa Gillois chez M. Parent  
 51 Rue de Carnot St  
 Chalons sur Marne



# CARTE POSTALE

Certains Pays Etrangers n'acceptant pas la Correspondance de ce Code, se renseigner à la Poste.

ADRESSE

M<sup>rs</sup> Léa Gillois chez M. Parent  
 51 Rue de Carnot St  
 Chalons sur Marne

29.22-13.24.22-22.19.2.4.24.24-17.24-  
 18.22.23.24.14-19.24-18.22.23.24.20.18-19.24-  
 22.23.24-24.18-8.23-15.23.20-  
 19.24-18.2.23-18.23-2.24.4.21-22.  
 24.18-24.8.18-2.24.4.21-22.  
 24.18-24.8.18-2.24.4.21-22.  
 18.22-18.24.18.24-19.24-2.24.4.21-22.  
 18.22-23.2.20-7.24.24.29.23.24.4-4.24.21.  
 22.24.19-13.24-29.22.18.23.20-24.8.18-  
 2.29.4-18.2.23-12.9.24-17.24-5.24.  
 4.23-18.22.20.18-22.19.21.24.9-29.2.20  
 22.20.21.24-15.23.24.20-22.23.24.24-  
 9.20-29.23.13.13.23.2.20-17.24-15.22.23.8.24.4.8-



25.22 21.2.8.8.24 7.22.4.19.2.20.20.24 25.2.23  
5.24 12.9.24 17.24 18.22.23 24.5.4.23.18 17.24  
20.22.14.22.23.8 4.23.24.20 4.24.5.9 19.24.7.9.23.8  
2 17.2.9.4.8 17.22.23 23.9 18.24.8 2  
5.22.4.18.24.8 5.24 25.22.18.23.20 17.24 20.22.23  
4.23.24.20 24.9 22 17.22.14.24 8.23 18.9  
8.22.14.22.23.8 5.2.25.25.24 17.24 8.9.23.8  
23.25.7.22.18.23.24.20.18 12.9.22.20.19  
24.13.13.24.8 8.2.20.18 24.20 4.24.18.22.4.19  
22.9 4.24.14.2.23.4 25.2.20 22.20.21.24  
22.19.2.4.24 18.2.9.18 22 18.2.23

25.22 21.2.8.8.24 7.22.4.19.2.20.20.24 25.2.23  
5.24 12.9.24 17.24 18.22.23 24.5.4.23.18 17.24  
20.22.14.22.23.8 4.23.24.20 4.24.5.9 19.24.7.9.23.8  
2 17.2.9.4.8 17.22.23 23.9 18.24.8 2  
5.22.4.18.24.8 5.24 25.22.18.23.20 17.24 20.22.23  
4.23.24.20 24.9 22 17.22.14.24 8.23 18.9  
8.22.14.22.23.8 5.2.25.25.24 17.24 8.9.23.8  
23.25.7.22.18.23.24.20.18 12.9.22.20.19  
24.13.13.24.8 8.2.20.18 24.20 4.24.18.22.4.19  
22.9 4.24.14.2.23.4 25.2.20 22.20.21.24  
22.19.2.4.24 18.2.9.18 22 18.2.23

25.22 21.2.SSE 7.22.4.19.2.20.20.E 25.2.23  
5.E 12.9.E 17.E 18.22.23 E.5.4.23.18 17.E  
20.22.14.22.23.S 4.23.E.20 4.E.5.9  
19.E.7.9.23.S 2 17.2.9.4.S 17.22.23 23.9  
18.E.S 2 5.22.4.18.ES 5.E 25.22.18.23.20  
17.E 20.22.23 4.23.E.20 E.9 22 17.22.11.E  
S.23 18.9 S.22.14.22.23.S 5.2.25.25.E 17.E  
S.9.23.S 23.25.7.22.18.23.E.20.18  
12.9.22.20.19 ELLES S.2.20.18 E.20  
4.E.18.22.4.19 22.9 4.E.14.2.23.4 25.2.20  
22.20.21.E 22.19.2.4.E 18.2.9.18 22  
18.2.23

25.22 21.OSSE 7.22.4.19.ONNE 25.O.23 5.E  
12.9.E 17.E T.22.23 E.5.4.23.T 17.E  
N.22.14.22.23.S 4.23.EN 4.E.5.9  
19.E.7.9.23.S 2 17.O.9.4.S 17.22.23 23.9  
TES 2 5.22.4.TES 5.E 25.22.T.23.N 17.E  
N.22.23 4.23.ENE.9 22 17.22.11.E S.23 T.9  
S.22.14.22.23.S 5.O.25.25.E 17.E S.9.23.S  
23.25.7.22.T.23.ENT 12.9.22.N.19 ELLES  
SONT EN 4.ET.22.4.19 22.9 4.E.14.O.23.4  
25.ON 22.N.21.E 22.19.O.4.E TO.9.T 22  
TO.23



25.A 21.OSSE 7.A.4.19.ONNE 25.OI 5.E  
12.U.E 17.E TAI E.5.4.IT 17.E NA.14.AIS  
4.IEN 4.E.5.U 19.E.7.UIS 2 17.OU.4.S 17.AI  
I.U T.E.S 2 5.A.4.TES 5.E 25.A.T.I.N 17.E  
N.A.I 4.I.ENE.U A 17.A.11.E SI TU SA.14.AIS  
5.O.25.25.E 17.E SUIS I.25.7.ATIEN  
12.UAN.19 ELLES SONT EN 4.ETA.4.19 AU  
4.E.14.OI.4 25.ON AN.21.E A.19.O.4.E TOUT  
A TOI

Ma gosse, pardonne-moi ce que je t'ai écrit, je n'avais rien reçu depuis 2 jours. J'ai eu tes 2 cartes ce matin. Je n'ai rien eu à ja\*e. Si tu savais comme je suis impatient quand elles sont en retard. Au revoir mon ange. Tout à toi

## Les mêmes faiblesses du côté de Napoléon

- 1) Utilisation de chiffres dignes de celui des cartes à Léa
- 2) Mélange de passages en clair et de passages en chiffré

## Le message du commandant Pulier

En 1796, pendant la campagne d'Italie, alors qu'il se trouve en Ligurie, le commandant Pulier envoie le message suivant à son général (archives de l'armée) :

10000 20414 13120 70002 03001 91317  
00190 00705 11201 40011 etc

En tout 800 chiffres et quand on les regroupe par deux, on ne trouve que des nombres de 00 à 25 !

Le Grand Chiffre de Louis XIV et ses successeurs :

Dictionnaires chiffrés avec nulles et annulant  
dont il fallait savoir bien se servir.

| A           | B        | C             | D        | E         | F   | G                 | H   | I        | K           | L         | M           | N        | O   | P                 | Q   | R                  | S         | T   | V                   | X   | Y   | Z   | de       | re        | se  |     |
|-------------|----------|---------------|----------|-----------|-----|-------------------|-----|----------|-------------|-----------|-------------|----------|-----|-------------------|-----|--------------------|-----------|-----|---------------------|-----|-----|-----|----------|-----------|-----|-----|
| 31<br>8     | 41<br>11 | 51<br>16      | 61<br>13 | 71<br>10  | 81  | 91                | 101 | 111<br>9 | 121         | 131<br>15 | 141<br>18   | 151<br>7 | 161 | 171<br>5          | 181 | 191<br>19          | 201<br>12 | 211 | 221<br>14           | 231 | 241 | 251 | 261<br>6 | 271<br>20 | 281 | 291 |
| an          | 23       | de            | 24       | general   | 25  | Lo                |     | 26       | Marriage    | 27        | pe          |          | 28  | Regale            | 29  | Vous               |           | 30  | Nuls                |     |     |     |          |           |     |     |
| au          | 32       | di            | 33       | guerre    | 34  | Lu                |     | 35       | Momieur     | 36        | pi          |          | 37  | Rome              | 38  | Notre              |           | 39  | N. N. 301           |     |     |     |          |           |     |     |
| avec        | 40       | do            | 42       | Ha        | 43  | Lur               |     | 44       | Ngr         | 45        | po          |          | 46  | Republique        | 47  | an                 |           | 48  | Annulars            |     |     |     |          |           |     |     |
| ainsy       | 49       | du            | 50       | he        | 52  | Luy               |     | 53       | Madame      | 54        | pu          |          | 55  | La                | 56  | voir               |           | 57  |                     |     |     |     |          |           |     |     |
| ausy        | 58       | dans          | 59       | hi        | 60  | Les               |     | 62       | Ministre    | 63        | pour        |          | 64  | Le                | 65  | vr                 |           | 66  | 311. 321. 331       |     |     |     |          |           |     |     |
| alliance    | 67       | des           | 68       | ho        | 69  | Le Roy            |     | 70       | Mantoué     | 72        | paix        |          | 73  | Si                | 74  | venise             |           | 75  | ce qui est entre    |     |     |     |          |           |     |     |
| avec        | 76       | En            | 77       | hu        | 78  | Le R. de Conty ou |     |          | Modene      | 80        | pas         |          | 82  | So                | 83  | Viene              |           | 84  | ces chiffres ne son |     |     |     |          |           |     |     |
| ambassade   | 85       | elle          | 86       | homme     | 87  | Le R. de Pologne  |     | 79       | Madrid      | 88        | Prince      |          | 89  | Su                | 90  | La                 |           | 92  | de vien             |     |     |     |          |           |     |     |
| allemans    | 93       | est           | 94       | honneur   | 95  | Ulloc desaxe      |     | 96       | Milan       | 97        | pologne     |          | 98  | Sans              | 99  | xe                 |           | 100 | 341. 351.           |     |     |     |          |           |     |     |
| Autriche    | 102      | cue           | 103      | hollande  | 104 | Le C. Radzinski   |     | 105      | Pa          | 106       | personne    |          | 107 | Les               | 108 | xi                 |           | 109 |                     |     |     |     |          |           |     |     |
| Allemagne   | 110      | ens           | 112      | hongrie   | 113 | Le pape           |     | 114      | te          | 115       | particulier |          | 116 | Son               | 117 | xo                 |           | 118 |                     |     |     |     |          |           |     |     |
| Ba          | 119      | ent           | 120      | Ja        | 122 | Le C. Spada       |     | 123      | ni          | 124       | pendant     |          | 125 | Sur               | 126 | xu                 |           | 127 |                     |     |     |     |          |           |     |     |
| be          | 128      | Eminence      | 129      | je        | 130 | Le C. Pancianici  |     | 132      | no          | 133       | Barme       |          | 134 | Sasainte          | 135 | La                 |           | 136 |                     |     |     |     |          |           |     |     |
| de          | 127      | je            | 139      | je        | 139 | Le C. Albanj      |     | 140      | nu          | 142       | qua         |          | 143 | Sam <sup>te</sup> | 144 | Ze                 |           | 145 |                     |     |     |     |          |           |     |     |
| do          | 146      | Excexcellence | 138      | jo        | 148 | Le C. Harboer     |     | 149      | nous        | 150       | que         |          | 152 | Sauoye            | 153 | Zi                 |           | 154 |                     |     |     |     |          |           |     |     |
| du          | 155      | Epagne        | 147      | ju        | 157 | La France         |     | 158      | notre       | 159       | que         |          | 162 | Suede             | 162 | Zo                 |           | 163 |                     |     |     |     |          |           |     |     |
| bien        | 164      | Electeur      | 156      | ju        | 166 | l'Empire          |     | 167      | Naples      | 168       | qui         |          | 169 | Ta                | 170 | Zu                 |           | 172 |                     |     |     |     |          |           |     |     |
| bon         | 173      | Fa            | 165      | je        | 175 | l'Empereur        |     | 176      | negociation | 177       | quo         |          | 178 | te                | 179 | Angletene          |           | 274 |                     |     |     |     |          |           |     |     |
| beaucoup    | 180      | fe            | 174      | in        | 175 | Leg. Duc          |     | 184      | neanmoins   | 193       | quand       |          | 186 | ti                | 187 | Prusse             |           | 275 |                     |     |     |     |          |           |     |     |
| bulles      | 188      | fi            | 182      | interest  | 183 | les Curves        |     | 199      | nonce       | 200       | quoy        |          | 194 | to                | 195 | Le C. de Briord    |           | 360 |                     |     |     |     |          |           |     |     |
| Brandebourg | 196      | fo            | 189      | intention | 190 | les Tartars       |     | 207      | on          | 208       | quit        |          | 202 | tu                | 203 | Le C. de Kinski    |           | 361 |                     |     |     |     |          |           |     |     |
| Ca          | 204      | fu            | 197      | Italie    | 198 | les Moscovites    |     | 215      | ont         | 216       | quille      |          | 209 | tou               | 210 | Le P. de Salm      |           | 362 |                     |     |     |     |          |           |     |     |
| ce          | 212      | faire         | 205      | Impeneaux | 206 | Ka                |     | 214      | oit         | 224       | Ra          |          | 217 | tant              | 218 | Le P. Dietricstein |           | 363 |                     |     |     |     |          |           |     |     |
| ci          | 219      | fait          | 213      | Ke        | 222 | Ma                |     | 223      | orient      | 232       | re          |          | 225 | troupes           | 226 | Le C. Davach       |           | 364 |                     |     |     |     |          |           |     |     |
| co          | 227      | faut          | 220      | Ki        | 229 | Me                |     | 230      | ou          | 238       | ri          |          | 233 | tion              | 234 | Le M. de Villars   |           | 365 |                     |     |     |     |          |           |     |     |
| cu          | 235      | Ga            | 228      | Ko        | 237 | Mi                |     | 238      | ordre       | 247       | ro          |          | 240 | Va                | 242 | Le M. de Pries     |           | 366 |                     |     |     |     |          |           |     |     |
| cour        | 243      | ge            | 236      | Ku        | 245 | no                |     | 246      | ou          | 255       | ru          |          | 248 | Ve                | 249 | M. de Chomas       |           | 367 |                     |     |     |     |          |           |     |     |
| contre      | 253      | gi            | 244      | La        | 253 | nu                |     | 254      | ordinaire   | 263       | rient       |          | 256 | vi                | 257 | M. de de Sauoye    |           | 368 |                     |     |     |     |          |           |     |     |
| comme       | 250      | go            | 252      | La        | 253 | mais              |     | 262      | Pa          | 270       | vont        |          | 264 | vo                | 265 | M. de Carignan     |           | 369 |                     |     |     |     |          |           |     |     |
| camp        | 252      | gu            | 259      | Le        | 260 | ment              |     | 269      | Roy         |           | 272         |          | 272 | vu                | 273 | M. de Harcourt     |           | 370 |                     |     |     |     |          |           |     |     |
| Cardinal    | 258      | grand         | 267      | Li        | 268 |                   |     |          |             |           |             |          |     |                   |     | M. de Callard      |           | 371 |                     |     |     |     |          |           |     |     |
| Da          | 266      |               |          |           |     |                   |     |          |             |           |             |          |     |                   |     | M. de Royalle      |           | 372 |                     |     |     |     |          |           |     |     |
|             |          |               |          |           |     |                   |     |          |             |           |             |          |     |                   |     | M. de Royalle      |           | 373 |                     |     |     |     |          |           |     |     |
|             |          |               |          |           |     |                   |     |          |             |           |             |          |     |                   |     | M. de de Bourgoye  |           | 374 |                     |     |     |     |          |           |     |     |
|             |          |               |          |           |     |                   |     |          |             |           |             |          |     |                   |     | M. de de Brillon   |           | 375 |                     |     |     |     |          |           |     |     |



|     |            |     |                                     |      |                    |      |                   |      |                |      |           |      |                      |
|-----|------------|-----|-------------------------------------|------|--------------------|------|-------------------|------|----------------|------|-----------|------|----------------------|
| 1.  | R          | 51. | C                                   | 98.  | pologne            | 143. | qua               | 186. | quand          | 228. | ga        | 269. | ment                 |
| 2.  | V          | 52. | be                                  | 99.  | Sans               | 144. | sa ma.            | 187. | ti             | 229. | Ki        | 270. | pa                   |
| 3.  | S          | 53. | luy                                 | 100. | Xe                 | 145. | Ze                | 188. | bulles         | 230. | me        | 271. | nt                   |
| 4.  | T          | 54. | Madame                              | 101. | h                  | 146. | bo                | 189. | fo             | 231. | x         | 272. | Roy                  |
| 5.  | P          | 55. | pu                                  | 102. | Autriche           | 147. | Espagne           | 190. | intention      | 232. | orient    | 273. | Vu                   |
| 6.  | R          | 56. | sa                                  | 103. | eux                | 148. | jo                | 191. | R              | 233. | ri        | 274. | Angleterre           |
| 7.  | N          | 57. | Voir                                | 104. | hollande           | 149. | le Card. barberin | 192. | La Reine       | 234. | tion      | 275. | Prusse               |
| 8.  | A          | 58. | ainsy                               | 105. | le Card. Radzinski | 150. | nous              | 193. | neantmoins     | 235. | cu        | 281. | rt                   |
| 9.  | J          | 59. | dans                                | 106. | Na                 | 151. | n.                | 194. | quoy           | 236. | ge        | 291. | st                   |
| 10. | E          | 60. | hi                                  | 107. | personne           | 152. | que               | 195. | to             | 237. | Ko        | 360. | le C. de Briord      |
| 11. | B          | 61. | D                                   | 108. | Se                 | 153. | sauoye            | 196. | Brandebourg    | 238. | mi        | 361. | le C. de Kinoki      |
| 12. | S          | 62. | les                                 | 109. | Si                 | 154. | Li                | 197. | fu             | 239. | ons       | 362. | le P. de Salms       |
| 13. | D          | 63. | Ministre                            | 110. | Allemagne          | 155. | bu                | 198. | Italie         | 240. | ro        | 363. | le P. Dietristin     |
| 14. | V          | 64. | pour                                | 111. | J                  | 156. | Etatow            | 199. | les Turcs      | 241. | y         | 364. | le C. Darach         |
| 15. | L          | 65. | se                                  | 112. | ens                | 157. | ju                | 200. | Nonce          | 242. | va        | 365. | le m. de Kiltaw      |
| 16. | C          | 66. | sr                                  | 113. | hongrie            | 158. | la france         | 201. | S              | 243. | couw      | 366. | le m. de Pries       |
| 17. | T          | 67. | alliance                            | 114. | le pape            | 159. | notre             | 202. | qu'il          | 244. | gi        | 367. | M. des Thomas        |
| 18. | M          | 68. | des                                 | 115. | ne                 | 160. | qui               | 203. | tu             | 245. | Ku        | 368. | M. le D. de Fauoye   |
| 19. | R          | 69. | ho                                  | 116. | particulier        | 161. | o                 | 204. | ca             | 246. | mo        | 369. | M. de Saignan        |
| 20. | nt         | 70. | le Roy                              | 117. | son                | 162. | Suede             | 205. | faite          | 247. | ordre     | 370. | M. d'harours         |
| 21. | an         | 71. | E                                   | 118. | Xo                 | 163. | zo                | 206. | Impériaux      | 248. | ru        | 371. | M. de Tallard        |
| 22. | de         | 72. | Mantoue                             | 119. | ba                 | 164. | bien              | 207. | les Tartars    | 249. | Ve        | 372. | M. le Royale         |
| 23. | general    | 73. | paix                                | 120. | ent                | 165. | fa                | 208. | on             | 250. | comme     | 373. | M. la D. Royale      |
| 24. | lo         | 74. | Si                                  | 121. | K                  | 166. | il                | 209. | quelle         | 251. | Z         | 374. | M. la D. de Bourg.   |
| 25. | Mariage    | 75. | Venise                              | 122. | Ja                 | 167. | l'Empire          | 210. | tout           | 252. | go        | 375. | M. le C. de Bouillon |
| 26. | pe         | 76. | auec                                | 123. | le Card. Spada     | 168. | Naples            | 211. | J              | 253. | la        |      |                      |
| 27. | Regale     | 77. | en                                  | 124. | ni                 | 169. | quo               | 212. | ce             | 254. | mu        |      |                      |
| 28. | Sous       | 78. | hu                                  | 125. | pendant            | 170. | ta                | 213. | fait           | 255. | ou        |      |                      |
| 29. | A          | 79. | Le P. de Comy, ou le Roy de Pologne | 126. | sw                 | 171. | p                 | 214. | Ka             | 256. | rien      |      |                      |
| 30. | au         | 80. | Madere                              | 127. | xu                 | 172. | zu                | 215. | les Moscouites | 257. | vi        |      |                      |
| 31. | di         | 81. | J.                                  | 128. | be                 | 173. | bon               | 216. | ont            | 258. | Cardinal  |      |                      |
| 32. | guerre     | 82. | pas                                 | 129. | Eminence           | 174. | fe                | 217. | Ra             | 259. | gu        |      |                      |
| 33. | lu         | 83. | si                                  | 130. | je                 | 175. | in                | 218. | tant           | 260. | le        |      |                      |
| 34. | Monsieur   | 84. | Vienn                               | 131. | J                  | 176. | l'Empereur        | 219. | ci             | 261. | R         |      |                      |
| 35. | pi         | 85. | Ambassade                           | 132. | le Card. pancingij | 177. | negociation       | 220. | saut           | 262. | mais      |      |                      |
| 36. | Rome       | 86. | elle                                | 133. | no                 | 178. | que               | 221. | V              | 263. | ordinaire |      |                      |
| 37. | voire      | 87. | honne                               | 134. | Madrid             | 179. | te                | 222. | Ke             | 264. | ront      |      |                      |
| 38. | auec       | 88. | Madrid                              | 135. | sa Saintete        | 180. | beaucoup          | 223. | ma             | 265. | vo        |      |                      |
| 39. | B.         | 89. | Prince                              | 136. | za                 | 181. | Q                 | 224. | oit            | 266. | Da        |      |                      |
| 40. | do         | 90. | Su                                  | 137. | bi                 | 182. | fi                | 225. | re             | 267. | grand     |      |                      |
| 41. | ha         | 91. | g.                                  | 138. | Excellence         | 183. | intrest           | 226. | co             | 268. | Li        |      |                      |
| 42. | leur       | 92. | xa                                  | 139. | ji                 | 184. | le P. Dur         |      |                |      |           |      |                      |
| 43. | Mgr.       | 93. | allemand                            | 140. | le Card. albany    | 185. | necessaire        |      |                |      |           |      |                      |
| 44. | Mgr.       | 94. | est                                 | 141. | M                  |      |                   |      |                |      |           |      |                      |
| 45. | po         | 95. | honneu                              | 142. | nu                 |      |                   |      |                |      |           |      |                      |
| 46. | Republique | 96. | l'Elec. de saxe                     |      |                    |      |                   |      |                |      |           |      |                      |
| 47. | sr         | 97. | Milan                               |      |                    |      |                   |      |                |      |           |      |                      |
| 48. | ainsy      |     |                                     |      |                    |      |                   |      |                |      |           |      |                      |
| 49. | du         |     |                                     |      |                    |      |                   |      |                |      |           |      |                      |
| 50. |            |     |                                     |      |                    |      |                   |      |                |      |           |      |                      |

+ 293... contre

**Nuls**  
 21. 22. 301.  
 et tous les autres nombres qui  
 ne sont pas dans ce chiffre

annulans  
 311. 321. 331.

Ce qui est entre ces  
 chiffres ne sort de  
 rien.  
 341. 351.

La ville fortifiée de Rodrigo est assiégée par les Britanniques quand le général Montbrun, commandant la division cavalerie de Marmont écrit à son gouverneur. Dans le premier paragraphe, Montbrun prend acte du précédent message de la ville puis continue ainsi :

*Je m'empresse d'en transmettre le contenu à 25. 13. 8. 9. 38. 19. 18. 37. 14. 10. 33. 28. 17. 34. 14. 17. 26. 5. 19. 21. 23. 31. 32 qui m'a ordonné de communiquer avec vous.*



Qui peut bien être le personnage désigné par les  
23 nombres :

*25. 13. 8. 9. 38. 19. 18. 37. 14. 10. 33. 28. 17.  
34. 14. 17. 26. 5. 19. 21. 23. 31. 32*

?

George Scovell, le décrypteur de Wellington, devine qu'il s'agit de Marmont désigné avec tous ses titres. Il finit par trouver:

*S.E. Le Maréchal, Duc de Raguse*

*25. 13. 8. 9. 38. 19. 18. 37. 14. 10. 33. 28. 17. 34.  
14. 17. 26. 5. 19. 21. 23. 31. 32*

... il en déduira le décryptement de toutes les dépêches de l'armée française.

Autre erreur : envoyer le même message deux fois,  
une fois complètement chiffré et une autre fois  
avec des parties en clair !

Péterswald, ce 17 septembre 1813,  
Monsieur le Maréchal,  
L'empereur ordonne que vous vous portiez le plus tôt possible 167. 138. 169. 106. 171. 15. 117 avec son infanterie, sa cavalerie et son artillerie, en ne laissant 15. 164. 138. 169. 176. 166. 35. 138. 169. 81 que ce que Sa Majesté a désigné pour 106. 78. Son principal but sera de rester 107. 87. 176. 169. 53. 52. 167. 52. 35. 138. 6. 85. 82. 52. 106. 171. 171. 15. 117 et de chasser 117. 107. 156. 169. 145. 171. 115. 167. 68 qui manœuvrent dans 20. 176. 131. 75. Vous pouvez vous rendre en droite ligne 156. 169. 40. 35. 138. 169. 81. 167. 138. 169. 87. 53. 91.  
Le Prince Vice-Connétable, Major Général,  
Berthier

Péterswald, ce 17 septembre 1813,

Monsieur le Maréchal,

L'empereur ordonne que 175. 138. 167. 164. 90. 138. 167. 152. 169. 145.  
53. 166. 117. 137. 103. 157. 176. 152. 167. 134. 37. 37. 117. 174. 169. 106.  
171. 15. 117. 15. 132. 6. 175. 176. 126. 48. 164. 153. 126. 32. 50. 175. 176.  
126. 25. 68. 94. 105. 122. 171. 115. 176. 15. 164. 118.169. 166. 35. 138.  
169. 81. 136. 20. 173. 138. 53. 171. 107. 87. 82. 131.. 15. 52. 134. 81. 94.  
137. 90. 138. 169. 106. 51. 169. 116. 168. 115. 175. 176. 126. 137. 148.  
115. 6. 119. 156. 90. 3. 176. 177. 146. 146.52.169. 82. 131. 169. 107. 92.  
126. 52. 167. 23. 53. 35. 138. 6. 61. 167. 52. 106. 171. 39. 53. 50. 52. 6. 72.  
167. 177. 169. 117. 167. 137. 22. 145. 171. 115. 167.68.154. 107. 94. 138.  
164. 126. 115. 176. 16. 115. 167. 20. 176. 131. 67. 126. 6. 145. 175. 138.  
167. 126. 115. 23. 126. 68. 23. 159. 92. 53. 93. 81. 94. 137. 22. 6. 90. 35.  
138. 169.81. 174. 169. 119.53. 115.15.

Le Prince Vice-Connétable, Major Général,

Berthier

Cela suffit pour décrypter le message.

Ce type d'erreurs de procédures se retrouveront plus tard dans les deux guerres mondiales.

Principe de Kerckhoffs :

La cryptographie ne doit pas reposer sur le secret du système mais sur une clef qu'on change périodiquement.

Exemple : chiffre de Boulanger quand il était ministre de la guerre (1886)

Substitution poly-alphabétique de Vigenère plus une transposition très simple (écriture à l'envers).



Avec la clef CROIX, le message « Boulanger a fait adopter le fusil Lebel » devient d'abord :

|          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| <b>B</b> | <b>O</b> | <b>U</b> | <b>L</b> | <b>A</b> | <b>N</b> | <b>G</b> | <b>E</b> | <b>R</b> | <b>A</b> | <b>F</b> | <b>A</b> | <b>I</b> | <b>T</b> | <b>A</b> | <b>D</b> | <b>O</b> |
| <b>C</b> | R        | O        | I        | X        | C        | R        | O        | I        | X        | C        | R        | O        | I        | X        | C        | R        |
| <b>D</b> | F        | I        | T        | X        | P        | X        | S        | Z        | X        | H        | R        | W        | B        | X        | F        | F        |
|          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |
| <b>P</b> | T        | E        | R        | L        | E        | F        | U        | S        | I        | L        | L        | E        | B        | E        | L        |          |
| <b>O</b> | I        | X        | C        | R        | O        | I        | X        | C        | R        | O        | I        | X        | C        | R        | O        |          |
| <b>D</b> | B        | B        | T        | C        | S        | N        | R        | U        | Z        | Z        | T        | B        | D        | V        | Z        |          |

Soit DFITX PXSZX HRWBX FFDBB TCSNR UZZTB DVZ

DFITX PXSZX HRWBX FFDBB TCSNR UZZTB DVZ

Qu'on écrit à l'envers :

ZVDBT ZZURN SCTBB DFFXB WRHXZ SXPXT IFD.

Décryptement d'un message chiffré ainsi par  
Bazeries :

AWAQQ KQZKG STNVX MWFKH WTQRO WQCMP  
WAIFX WRGVJ UIQJP AWAJG DBBFU JQFMW  
GKSUC KMZZE ANTZF KCZGU WTGKG JKSJU WT

AWAQQ KQZKG STNVX MWFKH WTQRO  
WQCMP WAIFX WRGVJ UIQJP AWAJG DBBFU  
JQFMW GKSUC KMZZE ANTZF KCZGU WTGKG  
JKSJU WT

Ces répétitions (AWA et UWT) peuvent être des coïncidences. Elles peuvent être aussi dues au fait que les mêmes lettres ont été chiffrées par la même partie de la clef... ce qui trahit sa longueur.

AWAQQ KQZKG STNVX MWFKH WTQRO  
WQCMP WAIFX WRGVJ UIQJP AWAJG DBBFU  
JQFMW GKSUC KMZZE ANTZF KCZGU WTGKG  
JKSJU WT

Les AWA sont à une distance de 45 et les UWT à une distance de 10. La longueur de la clef serait un diviseur commun donc égale à 5 (méthode de Kasiski).

Si cette hypothèse est juste, les cinq groupes suivant ont été chiffrés par une substitution mono-alphabétique :

AKSMW WWWUA DJGKA KWJW  
WQTWT QARIW BQKMN CTKT  
AZNFQ CIGQA BFSZT ZGS  
QKVKR MFVJJ FMUZZ GKJ  
GGXHO PXJPG UWCEF UGU

Le premier groupe correspond à la clef S puisque  $S+E=W$  ( $18+4=22$ ). Les autres groupes ne donnent rien car il y a des ex-aequo.

A : WQ**TWT** Q**ARIW** BQKMN C**TKT**  
 B : VP**SVS** PZQH**V** **APJLM** B**SJS**  
 C : **UORUR** OYP**GU** Z**OIKL** **ARIR**  
 D : **TNQTQ** N**XOFT** Y**NHJK** ZQH**Q**  
 E : **SMPS**P MW**NES** XMGI**J** YPG**P**  
 F : **RLORO** LVMD**R** W**LFHI** X**OFO**  
 G : QKN**QN** K**ULCQ** VK**EGH** W**NEN**  
 H : PJMP**M** JTKBP **UJDFG** VM**DM**  
 I : **OILOL** IS**JAO** T**ICEF** **ULCL**

Analyse du second groupe selon les clefs possibles. Les lettres en gras sont celles de E SAINT URLO, 80 % des lettres en français.

On détermine ainsi la clef, SIORC, ce qui donne :

IOMZE SILTE ALZEV UORTF ELCAM EIOVN ESUOV  
EJSEH CACSN IOMSE LTNOS RIRVU OCEDA SELIC  
IFFID SULPS ELSTE RCESS EL

En l'inversant, on obtient :

LE SSECR ETSLE SPLUS DIFFI CILES ADECO UVRIR  
SONTL ESMOI NSCAC HESJE VOUSE NVOIE MACLE  
FTROU VEZLA ETLIS EZMOI



Ce qui se décrypte en :

*Les secrets les plus difficiles à découvrir sont les moins cachés. Je vous envoie ma clef. Trouvez-la et lisez-moi.*

## **Retour sur saint Urlo :**

Avec humour, certains considèrent saint Urlo comme le saint patron des cryptologues ...

L'étonnant est qu'il existe bien un saint Urlo.



## Chapelle de Saint Urlo à Lanvénege (Morbihan)

Au XI<sup>e</sup> siècle, Urlo fut le premier abbé de l'abbaye Sainte-Croix de Quimperlé. Il ne fut canonisé que difficilement car personne n'avait été témoin d'un seul miracle qu'il aurait réalisé.

N'est-ce pas une preuve supplémentaire de son lien avec la cryptologie ? (les exploits des décrypteurs sont effectivement tenus secrets longtemps)

# Georges Painvin et le chiffre ADFGX

Pour les offensives de 1918, les Allemands changèrent de chiffre : ils n'émettaient plus que les lettres ADFGX en morse !

# Pourquoi ?

1. Eloignement des codes morses de ces cinq lettres :

● — A — ● ● D ● ● — ● F — — ● G  
— ● ● — X

2. Cinq codes permettent de chiffrer 25 lettres

Carré de Polybe  
avec phrase clef, ici « chiffre des  
télégraphistes en allemand » soit  
« Geheimschrift der Funker »,

|   | A | D | F | G | X |
|---|---|---|---|---|---|
| A | G | E | H | I | M |
| D | S | C | R | F | T |
| F | D | U | N | K | A |
| G | B | L | O | P | Q |
| X | V | W | X | Y | Z |

|   |   |   |   |   |   |
|---|---|---|---|---|---|
|   | A | D | F | G | X |
| A | G | E | H | I | M |
| D | S | C | R | F | T |
| F | D | U | N | K | A |
| G | B | L | O | P | Q |
| X | V | W | X | Y | Z |

« Attaquez demain à quatre heures » devient :

FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX  
 GX FD FX DX DF AD AF AD FD DF AD DA



# Surchiffrement par transposition,

FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX GX FD FX  
DX DF AD AF AD FD DF AD DA

| N | E | B | U | L | E | U | X |
|---|---|---|---|---|---|---|---|
| 5 | 2 | 1 | 6 | 4 | 3 | 7 | 8 |
| F | X | D | X | D | X | F | X |
| G | X | F | D | A | D | X | X |
| F | A | A | D | A | X | F | X |
| A | G | F | F | F | X | G | X |
| F | D | F | X | D | X | D | F |
| A | D | A | F | A | D | F | D |
| D | F | A | D | D | A | G | X |

Clef : nebuleux

| N | E | B | U | L | E | U | X |
|---|---|---|---|---|---|---|---|
| 5 | 2 | 1 | 6 | 4 | 3 | 7 | 8 |
| F | X | D | X | D | X | F | X |
| G | X | F | D | A | D | X | X |
| F | A | A | D | A | X | F | X |
| A | G | F | F | F | X | G | X |
| F | D | F | X | D | X | D | F |
| A | D | A | F | A | D | F | D |
| D | F | A | D | D | A | G | X |

Nous écrivons les colonnes dans l'ordre indiqué :

DFAFF AAXXA GDDFX DXXXD ADAAF DADFG  
 FAFAD XDDFX FDFXF GDFGX XXXFD X

# Messages indécryptables du 5 Mars au 5 Avril 1918

Le 4 Avril, Georges Painvin détecta deux messages similaires. Imaginons par exemple que nous ayons chiffré le message suivant :  
« attaquez demain à cinq heures ».

FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX  
DD AG FF GX AF AD FD DF AD DA

Après transposition :

DFAFF FGXXA GGDAX DXXXF NDAAF GDXFG  
FAAAD XDDFF DXFXF DAAXX XXDFD X

Au lieu de :

DFAFF AAXXA GDDFX DXXXD ADAAF DADFG  
FAFAD XDDFX FDFXF GDFGX XXXFD X

La coïncidence des deux messages en tête s'est transformée en des répétitions toutes les sept lettres (la longueur des colonnes).

DFAFFAA XXAGDDF XDXXXDA DAAFDAD  
FGFAFAD XDDFXFD FXFGDFG XXXXFDX

DFAFFFG XXAGGDA XDXXXFD DAAFGDF  
FGFAAAD XDDFFDX FXFDAAA XXXDFDX

On retrouve la longueur des colonnes donc la longueur de la clef de transposition, première étape du décryptement.

# Une amélioration désastreuse : le chiffre ADFGVX ... et la victoire