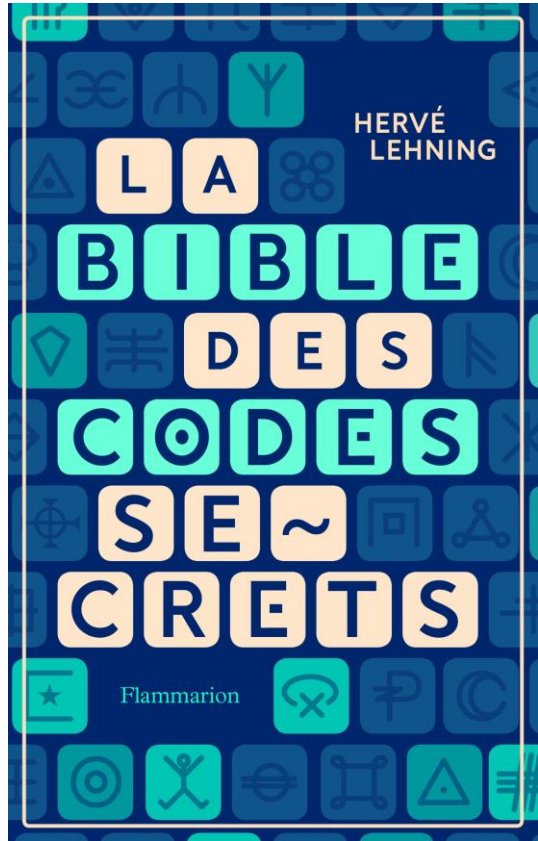
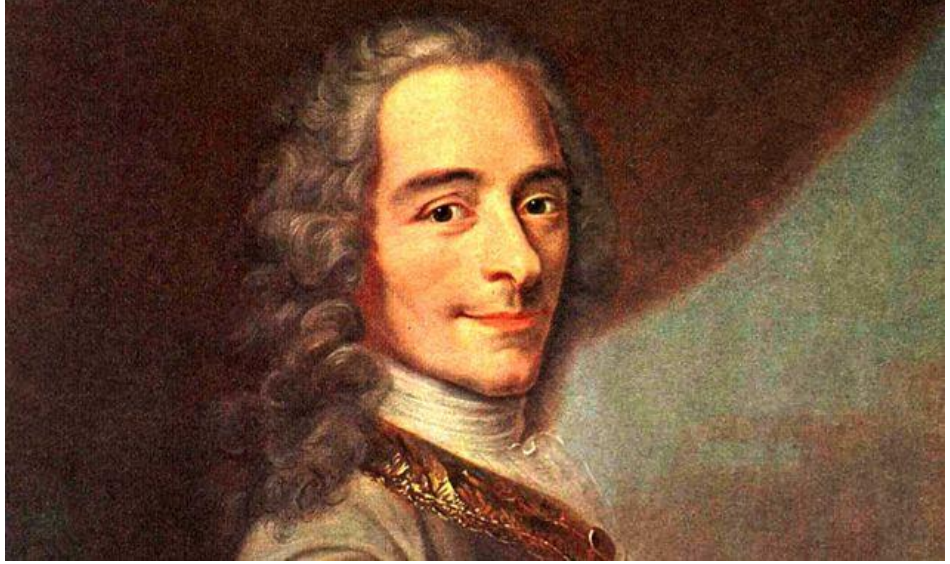
L’incroyable confiance des origines



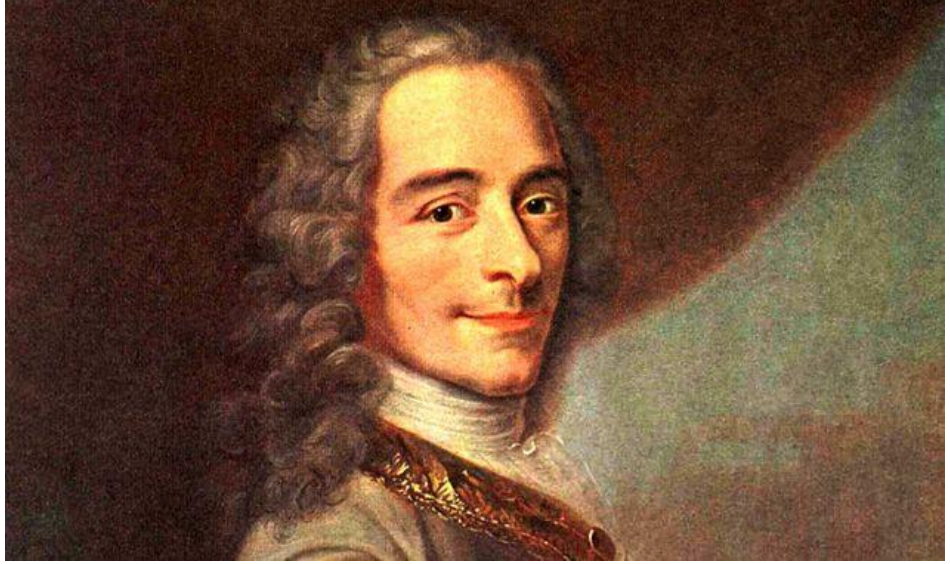
Blogs.futura-sciences.com/lehning/

www.lehning.eu



Voltaire ne croyait pas à la possibilité de décrypter les lettres à cause du nombre de possibilités.

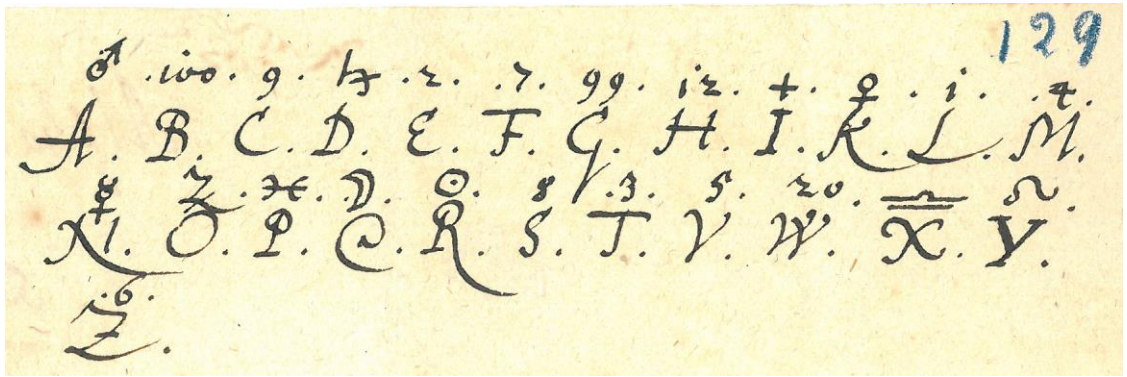
Telle est la loi de probabilités que dans un chiffre bien fait il y a deux cents, trois cents, quatre cents à parier contre un, que dans chaque numéro vous ne devinerez pas la syllabe dont il est représentatif.
Le nombre des hasards augmente avec la combinaison de ces numéros et le déchiffrement totalement impossible quand le chiffre est fait un peu d'art…



Voltaire ne croyait pas à la possibilité de décrypter les lettres à cause du nombre de possibilités.

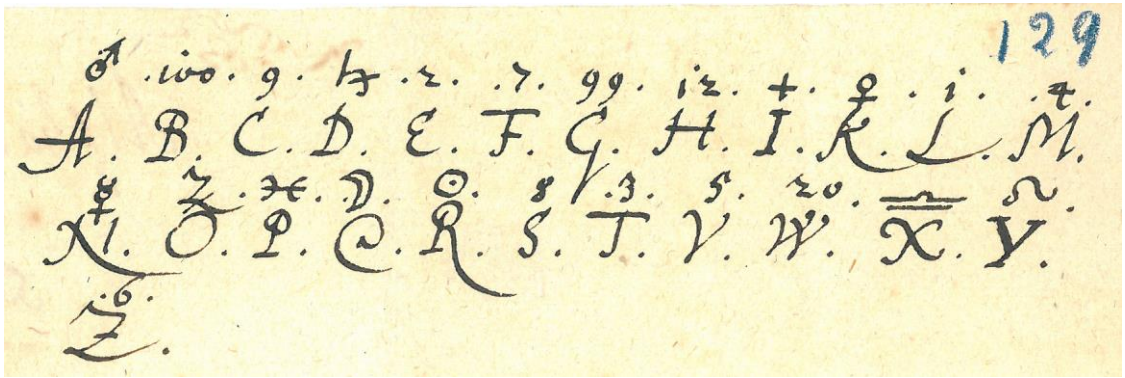
L’argument (erroné) de Voltaire a traversé les siècles.

Méthode classique de chiffrement : les alphabets chiffrés



A priori 26 ! (un nombre énorme) correspondances possibles entre les lettres et les symboles : Indécryptable par force brute ! Le même raisonnement a fait considérer la machine Enigma comme indécryptable

Méthode classique de chiffrement : les alphabets chiffrés



Indécryptable par force brute mais faciles à décrypter grâce à :

méthode des fréquences

méthode du mot probable

Un exemple moderne à l’origine de la vocation d’Etienne Bazeries :

Jeux cryptographiques dans les journaux

Ou correspondances personnelles à décrypter pour amuser ses collègues ?

C’était en 1890 et un jour, il annonça qu’il savait aussi bien décrypter les dépêches de l’armée. Loin de le punir, son général le mit au défi de le faire … ce qu’il fit et fut embauché par l’armée dans son service du chiffre.

Correspondances personnelles

M c. 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.

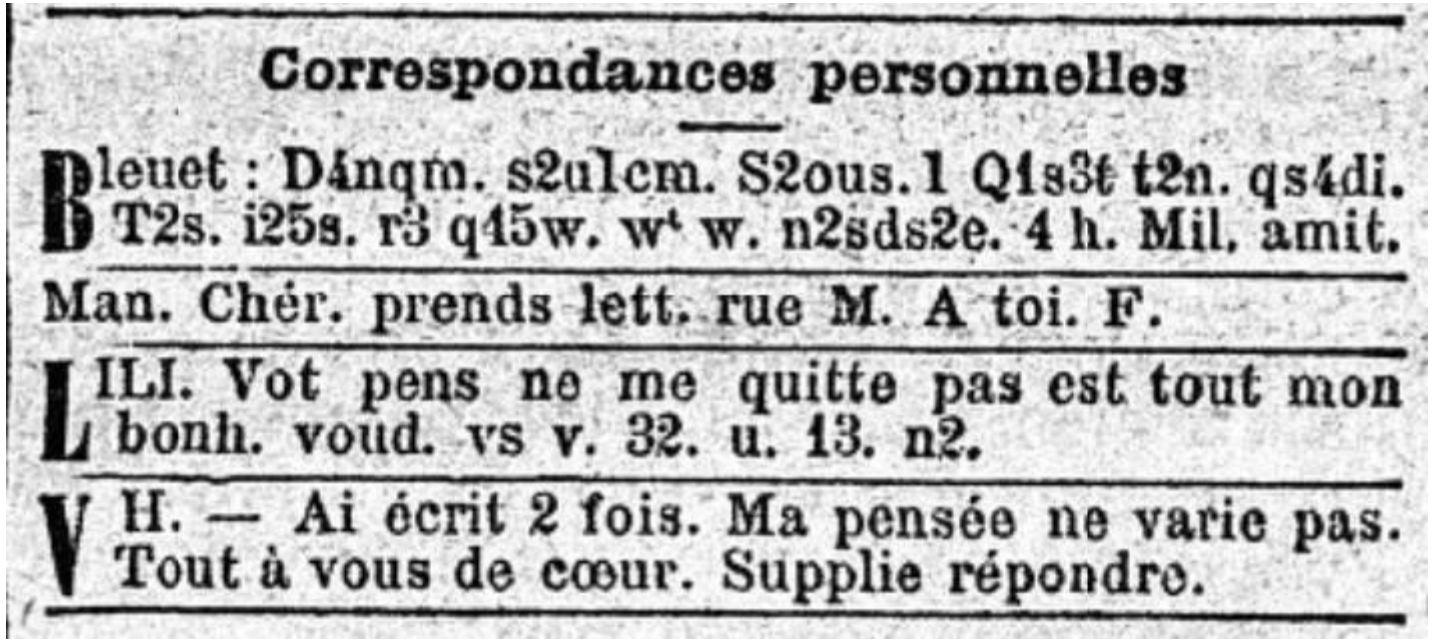
L U. V. A toi mes v. sois h. moi ma vie est bri-
L, sée car je toujours autant à toi. Je souf. et
s. atrocem, malh. Pense qqfois à moi.

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.

La rubrique « correspondances personnelles » du Figaro le premier janvier 1890

Figaro du 12 janvier 1890



Correspondances personnelles

Bleuet : D4nqm. s2ulcm. S2ous. 1 Q1s3t t2n. qs4di. T2s. i25s. r3 q15w. w⁴ w. n2sds2e. 4 h. Mil. amit.

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

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

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

Une erreur de chiffrement classique : mélanger clair et chiffré. On la retrouvera au long de l'histoire.

Hypothèse (vu le contexte) :

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.

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.

Même si on utilisera encore longtemps des alphabets chiffrés plus ou moins améliorés, du temps de Voltaire, on sait mieux faire grâce à Antoine Rossignol, ce qui mènera au grand chiffre de Louis XIV en particulier.

A	B	C	D	E	F	G	H	J	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	&	nt	rt	st
31 8	41 11	51 16	61 13	71 10	81	91	101	111 9	121	131 15	141 18	151 7	161	171 5	181	191 1 19	201 3 12	211 4	221 2 14	231	241	251	261 6	271 20	281	291

an	23	de	24	general	25	Lo	26	Mariage	27	pe	28	Regale	29	Vous	30	Nuls
au	32	di	33	guerre	34	Lu	35	Monsieur	36	pi	37	Rome	38	Vostre	39	u. 22. 301 et tous les autres nombres qui ne sont pas dans le chiffre
auec	40	do	42	Ha	43	Leur	44	Mgr	45	po	46	Republique	47	vn	48	Annulans
ainsy	49	du	50	he	52	luy	53	Madame	54	pu	55	Sa	56	Voir	57	311. 321. 331
aussy	58	dans	59	hi	60	Les	62	Ministre	63	pour	64	Se	65	vr	66	Ce qui est entre ces chiffres ne sert de rien
alliance	67	des	68	ho	69	LeRoy	70	Mantoüe	72	paix	73	Si	74	Venise	75	341. 351.
auec	76	En	77	hu	78	LeP. de Conty ou leR. de Pologne	79	Modene	80	pas	82	So	83	Vienne	84	
ambassade	85	elle	86	homme	87	l'Elec. de Saxe	96	Madrid	88	Prince	89	Su	90	Xa	92	
allemans	93	est	94	honneur	95	le Cal. Radziowski	105	Milan	97	pologne	98	Sans	99	xe	100	
autriche	102	eux	103	hollande	104	le pape	114	Na	106	personne	107	Ses	108	xi	109	
allemagne	110	ens	112	hongrie	113	le Cal. Spada	123	ne	115	particulier	116	Son	117	xo	118	
Ba	119	ent	120	Ja	122	le Cal. panciatici	132	ni	124	pendant	125	Sur	126	xu	127	
be	128	Eminence	129	je	130	le Cal. albanj	140	no	133	Parme	134	Sa Sainteté	135	Za	136	
bi	137	Excellence	138	ji	139	le Cal. Barberin	149	nu	142	qua	143	Santé	144	Ze	145	
bo	146	Espagne	147	jo	148	la france	158	nous	150	que	152	Sauoye	153	Zi	154	
bu	155	Electeur	156	ju	157	l'Empire	167	nostre	159	qui	160	Suede	162	Zo	163	
bien	164	Fa	165	jl	166	l'Empereur	176	Naples	168	quo	169	Ta	170	Zu	172	
bon	173	fe	174	in	175	le gd. Duc	184	negociation	177	quu	178	te	179	Angleterre	274	
beaucoup	180	fi	182	jnterest	183	la Reyne	192	necessaire	185	quand	186	ti	187	Prusse	275	
bulles	188	fo	189	jntention	190	les Turcs	199	neanmoins	193	quoy	194	to	195	Le C. de Briord	360	
Brandebourg	196	fu	197	Italie	198	les tartares	207	Nonce	200	quil	202	tu	203	le C. de Kinski	361	
Ca	204	faire	205	Imperiaux	206	les Moscovites	215	On	208	quelle	209	tou	210	le P. de Salms	362	
ce	212	fait	213	Ka	214	Ma	223	ont	216	Ra	217	tant	218	le P. Dietristein	363	
ci	219	faut	220	Ke	222	Me	230	oit	224	re	225	troupes	226	le C. Harach	364	
co	227	Ga	228	Ki	229	Mi	238	oient	232	ri	233	tion	234	le M. de Villars	365	
cu	235	ge	236	Ko	237	Mo	246	ons	239	ro	240	Va	242	le M. de Priés	366	
cour	243	gi	244	Ku	245	Mu	254	ordre	247	ru	248	Ve	249	M. de St. Thomas	367	
contre	293	go	252	La	253	mais	262	ou	255	vient	256	Vi	257	M. le D. de Sauoye	368	
comme	250	gu	259	Le	260	ment	269	ordinaire	263	vont	264	Vo	265	M. de Carignan	369	
camps	292	grand	267	Li	268			Pa	270	Roy	272	Vu	273	M. d'Harcourt	370	
Cardinal	258													M. de Tallard	371	
Da	266													Me. Royalle	372	
														Me. la D. Royalle	373	
														Me. la D. de Bourgogne	374	
														M. le Cal. de Boüillon	375	

1. R
2. Y
3. S
4. T
5. P
6. K
7. N
8. A
9. I
10. E
11. B
12 S
13. D
14. V
15. L
16. C
17. T
18. M
19. R
20. nt
23. an
24. de
25. general
26. lo
27. Mariage
28. pe
29. Regale
30. Vous
31. A
32. au
33. di
34. guerre
35. Lu
36. Monsieur
37. pi
38. Rome
39. votre
40. auec
41. B.
42. do
43. ha
44. leur
45. Mgr.
46. po
47. Republique
48. Vn
49. ainsy
50. du
51. C
52. he
53. luy
54. Madame
55. pu
56. sa
57. Voir
58. aussy
59. dans
60. hi
61. D
62. les
63. Ministre
64. pour
65. se
66. Vr
67. alliance
68. des
69. ho
70. le Roy
71. E
72. Mantoue
73. paix
74. Si
75. Venise
76. auec
77. en
78. hu
79. Le P. de Comty, ou le Roy de Pologne
80. Modene
81. F.
82. pas
83. so
84. Vienne
85. Ambassade
86. Elle
87. homme
88. Madrid
89. Prince
90. Su
91. g.
92. xa
93. allemans
94. est
95. homneur
96. l'Elec. de saxe
97. Milan
98. pologne
99. Sans
100. Xe
101. h
102. Autriche
103. eux
104. hollande
105. le card.l Radzioski
106. Na
107. personne
108. Ses
109. xi
110. Allemagne
111. J
112. ens
113. hongrie
114. Le pape
115. ne
116. particulier
117. Son
118. Xo
119. ba
120. ent
121. K
122. Ja
123. le card.l Spada
124. ni
125. pendant
126. Suo
127. xu
128. be
129. Eminence
130. je
131. L
132. le card.l panciatici
133. no
134. Parme
135. Sa Saintete
136. Za
137. bi
138. Excellence
139. ji
140. le card.l albani
141. M
142. nu
143. qua
144. sa Ma.te
145. Ze
146. bo
147. Espagne
148. jo
149. le card.l barberin
150. nous
151. n.
152. que
153. Sauoye
154. Zi
155. bu
156. Electeur
157. ju
158. la france
159. notre
160. qui
161. O
162. Suede
163. Zo
164. bien
165. fa
166. jl
167. l'Empire
168. Naples
169. quo
170. ta
171. p
172. Zu
173. bon
174. fe
175. in
176. l'Empereur
177. negociation
178. quu
179. te
180. beaucoup
181. Q
182. fi
183. interest
184. leg.d Duc
185. necessaire
186. quand
187. ti
188. bulles
189. fo
190. intention
191. R
192. la Reine
193. neantmoins
194. quoy
195. to
196. Brandebourg
197. fu
198. Italie
199. Les Turcs
200. Nonce
201. S
202. quil
203. tu
204. ca
205. faire
206. Imperiaux
207. les Tartares
208. on
209. quelle
210. tout
211. T
212. ce
213. fait
214. Ka
215. les Moscouites
216. ont
217. Ra
218. tant
219. ci
220. faut
221. V
222. Ke
223. ma
224. oit
225. re
226. troupes
227. co
228. ga
229. Ki
230. me
231. x
232. oient
233. ri
234. tion
235. cu
236. ge
237. Ko
238. mi
239. ons
240. ro
241. y
242. va
243. cous
244. gi
245. Ku
246. mo
247. ordre
248. ru
249. Ve
250. comme
251. Z
252. go
253. la
254. mu
255. ou
256. rient
257. Vi
258. Cardinal
259. gu
260. le
261. K
262. mais
263. ordinaire
264. ront
265. vo
266. Da
267. grand
268. Li
269. ment
270. pa
271. nt
272. Roy
273. Vu
274. angleterre
275. Prusse
281. rt
291. st
+ 292 camp
+ 360. le.t de Briord
361. le.t de Kinski
362. le P. de Salmo
363. le P. Dietristin
364. le.t Darach
365. le M. de Villars
366. le M. de Prie
367. M. des.t Thomas
368. M. le D. de Savoye
369. M. de Carignan
370. M. d'harcourt
371. M. de Tallard
372. M.r Royale
373. M.r la D. Royale
374. M.r la D. de bourg.
375. M. le.t al de Bouillon

+ 293 . . . contre

Nuls

21. 22. 301.

et tous les autres nombres qui ne sont pas dans cet chiffre

annulans

311. 321. 331.

Ce qui est entre ces chiffres ne sert de rien.

341. 351.

Difficile à décrypter si la méthode est bien utilisée comme les concepteurs le demandent, comme dans la table de Puisieulx de 1750 :

Vous trouverez, Monsieur, Dans ce paquet trois nouvelles tables de chiffre savoir un ordinaire, ou de réserve et un de correspondance avec une instruction sur la manière de s'en servir. Vous sentirez aisément combien il importe que vous recommandiez à vos secrétaires de se conformer scrupuleusement à cette instruction.

Il ne faut absolument pas mettre dans les articles chiffrés aucun mot en clair, et être très attentif que le chiffre ne paraisse avoir aucune raison avec ce qui le précède ou ce qui le suit en clair, et que ce qui précède ou ce qui suit ne puisse fournir aucune lumière sur les articles chiffrés. […]

Importance des protocoles et donc de la formation des chiffreurs. Un bon chiffre mal utilisé peut être une catastrophe. Aujourd'hui comme hier !

En commençant la dépêche ou l'article qui doit être chiffré après avoir mis dans la première ligne 6 ou 7 nombres pris au hasard, on chiffrera ce qui doit l'être jusqu'à la fin ; alors on se servira du nombre qui marque la fin et on mettra en Suite quelques nombres pris au hasard […]

On ne se servira du chiffre de réserve que lorsque l'on aura lieu de soupçonner que le chiffre ordinaire n'est plus sûr. Alors on ne se servira en aucun cas du chiffre ordinaire et les dépêches seront chiffrées du chiffre de réserve.

La manière de se servir d’un chiffre est aussi importante que le chiffre lui-même.

Exemple avec l’armée Napoléonienne à Rodrigo.

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.

Parmi les erreurs classiques et toujours d’actualité :
Transmettre le même message en clair et en chiffré.

L’armée napoléonienne l’a fait … et d’autres ont continué sur cette voie.

L’inconvénient principal de ces tables de chiffrement est qu’une fois le secret percé, on ne peut le reconstruire…

La solution sera trouvée à la fin du XIX° siècle : le secret ne doit pas reposer sur la méthode mais sur une clef qu’on change régulièrement.

Moralité : les méthodes changent, les erreurs restent. De ce côté, l'histoire du chiffre a beaucoup à nous apprendre.