Méthode de Jules César

Méthode :

On décale chaque lettre de 3 positions dans l'alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ

- Chiffrement : décalage vers la droite (+)
- Déchiffrement : décalage vers la gauche (-)

Exemple :

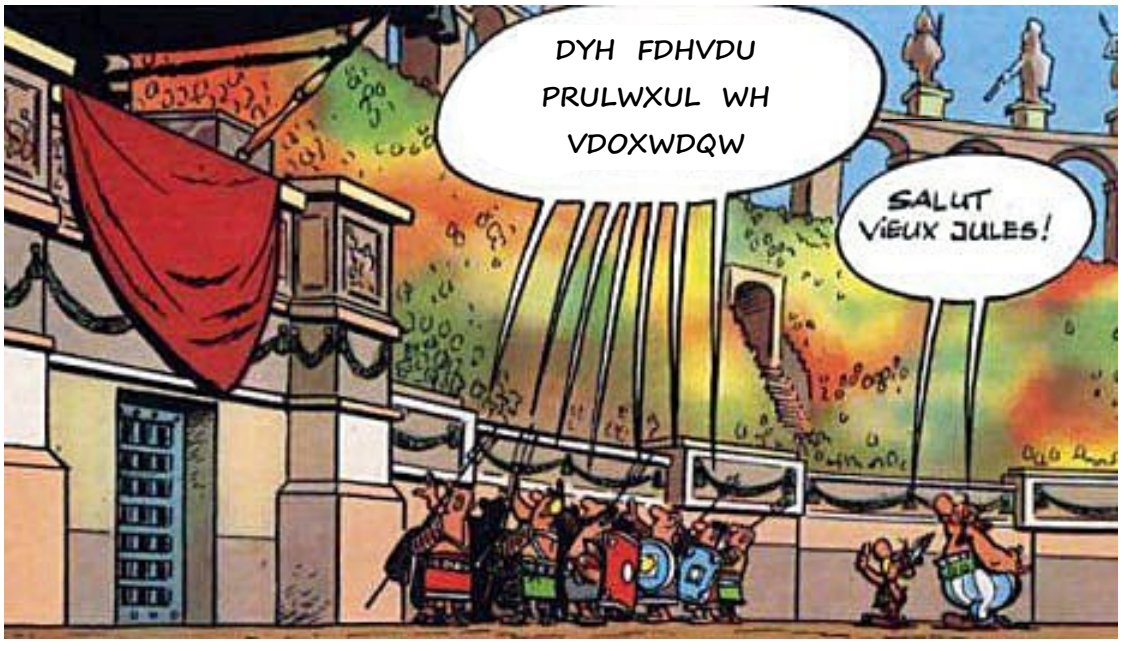
Texte clair : B O N J O U R

Message chiffré: E R Q M R X U

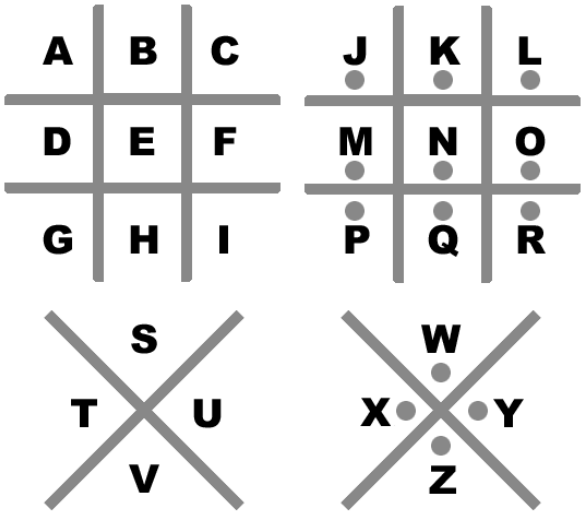
Enigme 1 : (en Français) Age : > 7 ans

FHVDU QH YLHLOOLW SDV, LO PXULW ! DYH PRL !

Enigme 2 : (en LATIN) Age : > 12 ans



Le Chiffre des francs maçons (XVIII)



Clair: B O N J O U R

Crypto: ⌴ ⊏ ⊡ ⌟ ⊏ < ⌜

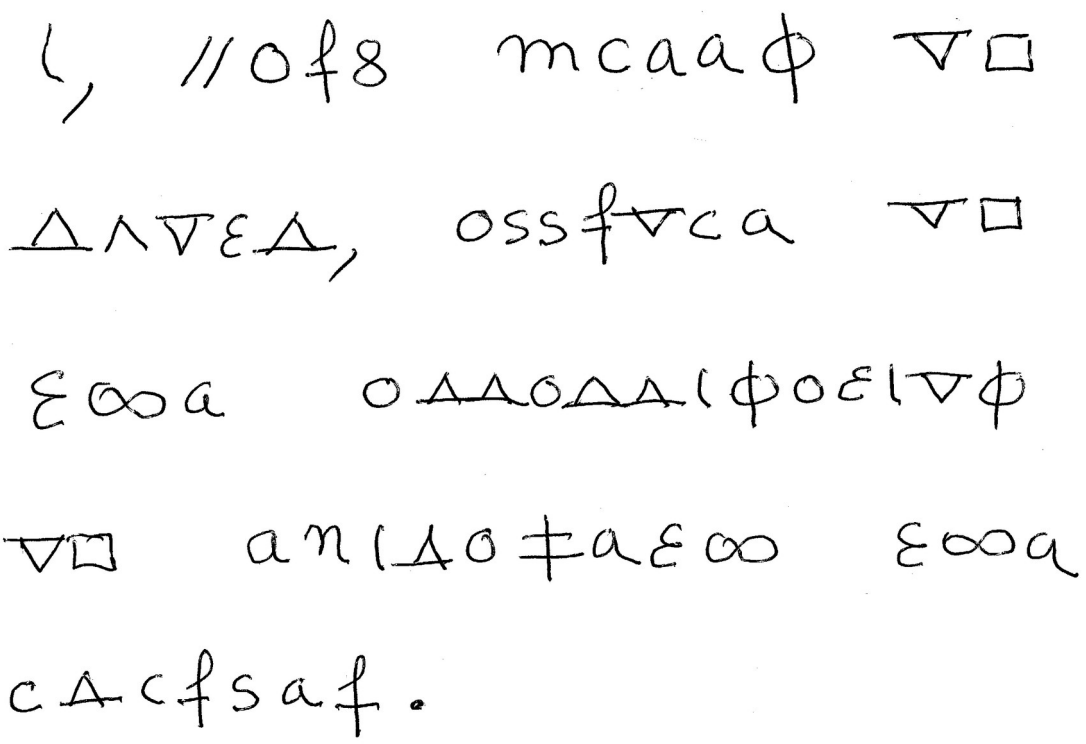
Message à déchiffrer:

⌝⌟⊡⊏⌜⌟⊐⌜> , ⌞⊐ ⊐⌜<⌜⊐⊡ ,

⌟⌴⌜⌟⌜⌟⌞⊏<⌜⌞⌜> ⊡V> ⌞⊐

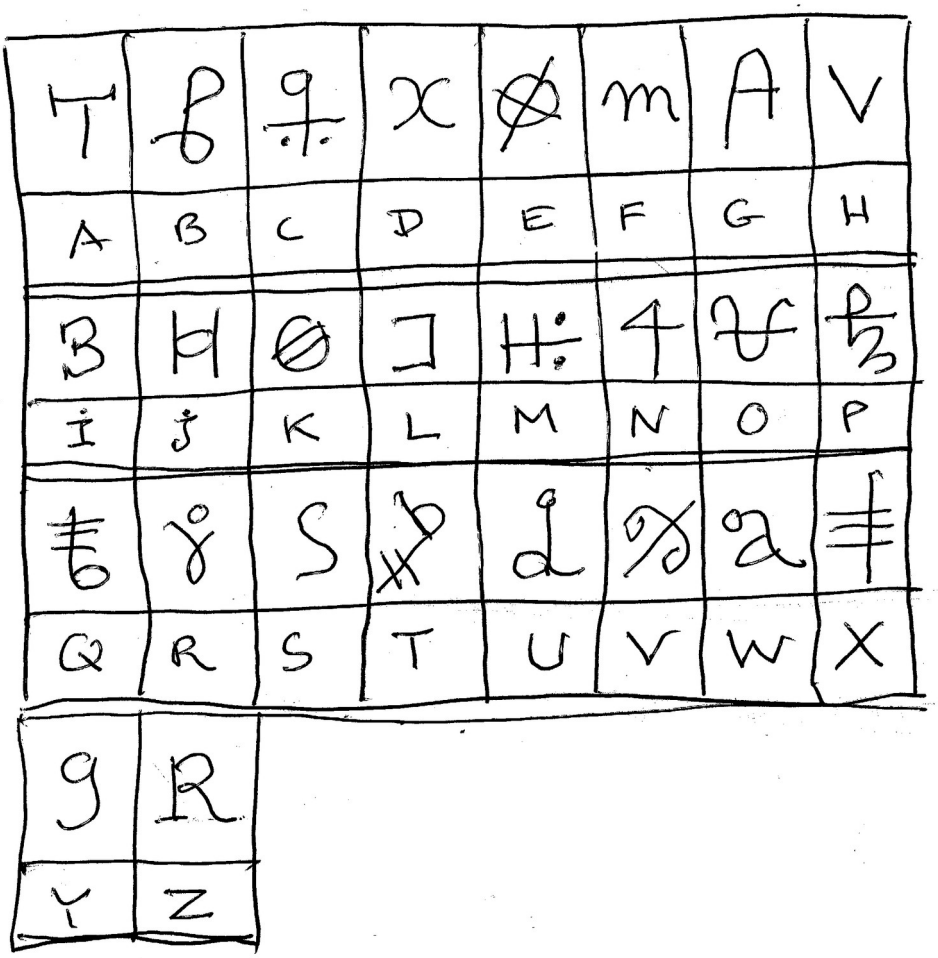
⌞⊓⊡⊏ ⊐⊡ ⌞⌟ >⌜⌜⌴<

Code authentique en anglais (1586)



O	≠	∧	π	a	□	θ	∞
A	B	C	D	E	F	G	H
(	⌀	n	//	ϕ	▽	S	m
I/J	K	L	M	N	O	P	Q
∤	Δ	ε	C	cc	7	8	9
R	S	T	U/V	W	X	Y	Z

Une lettre en espagnol d'Hernán Cortés (1520)



Substitution simple

Description

On crée un alphabet désordonné (on peut déduire cet alphabet à partir d'un mot clé) que l'on partage avec ses correspondants.

Créer un alphabet désordonné à partir d'un mot / phrase clé

1) Par exemple on prend la phrase: JE PENSE DONC JE SUIS

2) On élimine les lettres identiques: J E P N S D O C U I

3) On compléte avec les lettres non encore utilisées

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

Ce qui donne:

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

Enigme (> 7 ans)

- L'alphabet et l'alphabet désordonné

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

a) Pour chiffrer, je recherche la lettre dans l'alphabet ordonné (celui du haut) et je la remplace par la lettre correspondante dans l'alphabet désordonné (celui du bas)

b) Pour déchiffrer, on fait l'inverse: on recherche la lettre chiffrée dans l'alphabet du bas et on prend la lettre correspondante dans l'alphabet du haut.

- Exemple: B O N J O U R => E H G I H T M

Un Message chiffré

```
N S T X     P C H Q S Q     Q H G R


U G D U G U S Q   :   B '   T G U V S M Q     S R


B J     E S R U Q S     C T F J U G S .
```

Méthodes de substitution avec homophones

Méthode

Chaque lettre est chiffrée, mais il existe plusieurs possibilités pour chacune.

Exemple : Le chiffre du pape Clement VIII (1592-1605)

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	et
05	22	24	25	02	26	27	28	07	29	44	45	09	70	47	48	49	50	20	54	55
06	57	58	59	04	62	64	65	08	66	68	89	00	46	72	74	75	76	40	78	79
90				60																

Remarques:
1) A l'époque, en italien (mais aussi en français), i et j étaient confondus, de même que u et v. Les lettres k, w et y n'existaient pas.

2) Les codes qui ne correspondent à rien, correspondent à des "nuls", c'est à dire des codes qui n'ont pas de signification (pour tromper l'ennemi). Eventuellement ces "nuls" pouvaient être utilisés comme espace ou ponctuation (ici les codes 3x).

Message en clair:	B	O	N	J	O	U	R	.
Message chiffré:	22	00	45	07	09	20	48	99

Enigme (en français) (> 12 ans)

29 05 30 27 48 06 24 60 31 02 49 50 32

49 20 26 62 07 49 90 45 76 04 33 46 09

20 74 34 05 24 58 04 25 02 74 35 06 20

36 70 05 48 06 25 07 49 37

Transposition simple à tableau (>16 ans)

Description

1) On choisit un mot clé qui doit être connu du correspond, exemple OISEAU. Le nombre de colonnes du tableau est égal au nombre de lettres du mot clé, ici 6.

2) On remplit le tableau par le message en clair ligne à ligne. Si le tableau n'est pas complet on le complète avec des lettres rares, par exemple X.

3) On convertit le mot clé en clé numérique en traduisant chaque lettre par son ordre d'apparition dans l'alphabet. La cinquième lettre (A) est traduit par « 1 », la quatrième lettre (E) est la suivante dans l'ordre alphabétique est traduite par « 2 », la deuxième lettre (I), la suivante dans l'ordre alphabétique est traduite par « 3 », etc. On obtient ainsi la clé numérique : 4-3-5-2-1-6.

4) Pour obtenir le cryptogramme, on relève les colonnes dans l'ordre de la clé.

Note : Pour déchiffrer on procède à l'envers : on remplit les colonnes dans l'ordre de la clé numérique et on obtient le clair en lisant les lignes de haut en bas.

Le nombre de lignes du tableau est donnée par la formule :

nombre_de_lignes = nombre_de_lettres_du_crypto ÷ nombre_de_lettres_de_la_clé

Dans notre cas: 24 ÷ 6 = 4

Exemple - Chiffrement

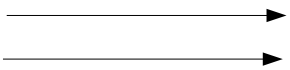
Message en clair: PROFITE DU JOUR PRESENT

Clé de chiffrement: OISEAU

Cryptogramme : (IOSX) (FJEX) (RDPT) (PERN) (OURX) (TUEX)

Cryptogramme par groupes de 5 lettres : IOSXF JEXRD PTPER NOURX TUEX

O	I	S	E	A	U
4	3	5	2	1	6
P	R	O	F	I	T
E	D	U	J	O	U
R	P	R	E	S	E
N	T	X	X	X	X



1ère ligne à remplir,

2ième ligne à remplir,

.
.

Exemple - Déchiffrement

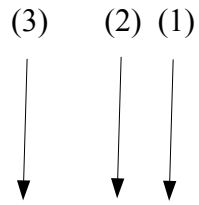
Cryptogramme: IOSXF JEXRD PTPER NOURX TUEX, Clé : OISEAU

Crypto par groupe correspondant à une colonne: (IOSX) (FJEX) (RDPT) …

O	I	S	E	A	U
4	3	5	2	1	6
	R		F	I	
	D		J	O	
	P		E	S	
	T		X	X	

Exemple du remplissage des trois premières colonnes

Le clair est obtenu en relevant les lignes...



Un message en allemand utilisant la transposition simple (Août 1914)

Cryptogramme à déchiffrer:

SHNZN NXNCE MLEDH
NEDGE IGISU ISFEE
UNNIE EADUE DN

Clé: MOLTKE

M	O	L	T	K	E

Code – Partie déchiffrante
Correspondance entre Louis XIV et le maréchal Catinat - 1691

001 => passage
002 => quartier
003 => aucun
004 => rait(roit)
005 => regiment
008 => e
009 => re
010 => da
012 => infanterie
013 => r
014 => .
017 => c
018 => demand
020 => do
021 => fu
022 => en
023 => gouvern
024 => le
025 => so
026 => vous
027 => annule_gr_
029 => .
030 => .
031 => a
032 => l
033 => join
034 => de
035 => faire
036 => ia(ja)
037 => impossible
038 => mieux
039 => fin
041 => cependant
042 => de
043 => camp
044 => ni
045 => fo
046 => mi
047 => que
048 => temps
049 => e
050 => so
051 => Luzerne(va
052 => que
053 => ordonn
054 => b
055 => i(j)
056 => g
057 => i(j)
058 => do
059 => ent
060 => se
061 => uo(vo)
062 => .
063 => es
064 => da
065 => ca
067 => foible
068 => le
069 => nouvelle
070 => SaMajeste
072 => caval
073 => d
074 => don
075 => jour
076 => encore
077 => lequel
078 => nombre
079 => se
080 => quelle
081 => sur
083 => desir
084 => fa
086 => ba
087 => certain
088 => n
089 => it
090 => intention
091 => mon
092 => pe
093 => re
094 => qui
095 => secour
096 => te
097 => de
099 => ce
100 => action
101 => du
102 => ga
103 => moyen
104 => po
105 => ro
106 => troupe
107 => .
108 => .
109 => ie(je)
111 => communic
112 => me
113 => pa
114 => quelque
115 => St
116 => ta
117 => ra
118 => cause
119 => e
120 => s
121 => o
122 => me
124 => les
125 => ne
126 => s
127 => ce
128 => f
129 => n
130 => peu
131 => is
132 => general
134 => celle
135 => escri
136 => ha
137 => ma
139 => somme
141 => ayant
142 => consider
143 => engage
144 => ne
145 => la
146 => ne
147 => pi
148 => qua
149 => si
150 => voir
151 => .
152 => a
153 => h
154 => e
155 => ainsi
156 => chemin
158 => lo
159 => nt
160 => present
162 => demeur
163 => fait
164 => ie(je)
165 => mo
166 => peine
167 => re
168 => tant
170 => p
171 => t
172 => r
173 => b
174 => ro
175 => toujours
176 => autre
177 => contrai
179 => lettre
180 => son
181 => te
182 => canon
184 => in
185 => pense
186 => u(v)
187 => u(v)
188 => et
189 => Coni
191 => ceux
192 => du
193 => grand
194 => co
195 => honneur
196 => lo
197 => sa
198 => vous
199 => i(j)
200 => n
201 => t
202 => munition
204 => be
205 => t
206 => z
207 => x
208 => tout
209 => .
211 => prendre
212 => arriv
213 => effet
214 => gard
215 => iu(ju)
216 => na
217 => pres
218 => Angrogne
219 => g
220 => pas
222 => co
224 => lieu
226 => qui
227 => tenir
229 => i(j)
230 => m
231 => jusque
233 => mais
234 => on
236 => vrai
237 => StMartin(v
238 => t
241 => esper
242 => contre
244 => mauvais
245 => compte
246 => rend
248 => dans
249 => capable
251 => i(j)
252 => c
254 => Gens
255 => lon
257 => bombe
258 => bled
259 => moins
260 => pas
261 => .
263 => arm
264 => celui
265 => autant
266 => combat
267 => gi
268 => leur
269 => no
270 => plus
271 => rest
272 => y
273 => et
276 => elle
277 => lors
278 => veill
279 => su
280 => per
281 => fi
282 => bu
283 => lui
284 => s
285 => ue(ve)
288 => homme
289 => est
290 => cu
291 => j'ai
292 => par
293 => to
295 => deja
296 => bo
297 => projet
298 => b
299 => ge
300 => r
301 => afaire
302 => combien
303 => gu
304 => pouvoi
305 => si
306 => ua(va)
307 => conven
308 => gu
309 => .

310 => sou
311 => qu'il
312 => occasion
313 => he
314 => aussi
315 => entre
316 => l
317 => q
318 => z
320 => sans
321 => apres
322 => cela
323 => d
324 => ci
325 => juge
326 => necessaire
327 => li
328 => fois
329 => inform
330 => masque(???
331 => mois
332 => sui
333 => di
335 => chose
336 => enlev
337 => la
338 => point
339 => nu
340 => lu
341 => .
342 => estat
343 => ho
344 => oit
345 => s
347 => a
348 => i(j)
349 => y
352 => Milan
354 => personn
355 => frontiere
356 => dispos
357 => car
358 => argent
359 => comme
360 => empesch
362 => laiss
363 => hi(hy)
367 => .
368 => to
369 => io(jo)
370 => moy
371 => persuad(ou
372 => ca
374 => e
375 => mu
376 => tour
377 => trouv
378 => soin
380 => estre
381 => aussitost
382 => luy
383 => quo
384 => ti
385 => a
386 => f
387 => o
388 => ri
389 => tu
390 => ou
391 => facil
392 => beaucoup
393 => for
394 => dire
395 => ast
396 => .
397 => raison
398 => mal
399 => hors
400 => courrier
401 => attaque
402 => ci
403 => envoi
404 => necessite
405 => pris
407 => ue(ve)
409 => l
410 => pont
411 => avis
412 => eu(ev)
413 => mand
414 => qu
415 => tion
416 => uo(vo)
417 => soit
418 => hu
419 => fe
420 => bien
421 => marque
422 => p
423 => u(v)
424 => n
425 => port
426 => venir
427 => quand
428 => officier
429 => manque
430 => cy
431 => bon
433 => fourrage
434 => il
436 => et
437 => u(v)
438 => tres
439 => ru
441 => nous
442 => vu
447 => afin
448 => ces
449 => expliqu
450 => me
451 => us
452 => avoit
453 => a
454 => m
455 => ni
456 => chez
457 => import
458 => devant
461 => d
464 => besoin
465 => mesme
466 => recev
467 => vos
468 => calme
469 => s
470 => b
471 => cet
472 => avise
475 => no
476 => pu
477 => siege
478 => vivre
479 => le_Roy
480 => .
481 => occup
482 => assez
483 => meilleur
484 => parti
485 => extrem
486 => o
487 => x
488 => n
489 => n
490 => c
491 => depuis
493 => sieur
494 => Pragelas(v
496 => vostre
497 => sembl
498 => non
499 => doi
500 => e
501 => p
502 => rien
503 => pour
504 => verit
505 => croi
506 => ment
508 => a
509 => n
510 => .
513 => ui(vi)
514 => m
515 => h
516 => cour
517 => puis
518 => Mr_de_Rebe
519 => Geneve(?)
520 => veu
521 => o
522 => e
523 => c
524 => importan
525 => au
526 => des
528 => r
529 => avant
532 => quantite
533 => servi
534 => trop
535 => m
536 => ensuite
537 => f
538 => des
540 => Mr_de_Rebe
541 => .
544 => t
547 => i(j)
548 => l
549 => u(v)
550 => Turin
551 => sa
553 => avec
554 => bi
555 => Scavoi
556 => y
557 => et
558 => Cazal
559 => m
560 => o
561 => t
564 => l
565 => r
566 => Pignerol
567 => .
569 => ri
570 => pe
571 => ia(ja)
572 => Briancon
573 => z
574 => s
575 => g
576 => Grenoble
577 => Suze
578 => t
579 => r
580 => d
582 => o
583 => y
584 => s
585 => p
587 => u(v)

Code – Partie chiffrante
Correspondance entre Louis XIV et le maréchal Catinat - 1691

031 a	087 certain	143 engage	348 i(j)
152 a	448 ces	336 enlev	547 i(j)
347 a	471 cet	059 ent	036 ia(ja)
385 a	191 ceux	315 entre	571 ia(ja)
453 a	156 chemin	536 ensuite	109 ie(je)
508 a	456 chez	403 envoi	164 ie(je)
100 action	335 chose	063 es	434 il
301 afaire	324 ci	135 escri	457 import
447 afin	402 ci	241 esper	524 importan
155 ainsi	194 co	289 est	037 impossible
218 Angrogne	222 co	342 estat	184 in
321 apres	266 combat	380 estre	012 infanterie
358 argent	302 combien	188 et	329 inform
263 arm	359 comme	273 et	090 intention
212 arriv	111 communic	436 et	369 io(jo)
482 assez	245 compte	557 et	131 is
395 ast	189 Coni	412 eu(ev)	089 it
401 attaque	142 consider	449 expliqu	291 j'ai
525 au	177 contrai	485 extrem	033 join
003 aucun	242 contre	128 f	075 jour
314 aussi	307 conven	386 f	215 iu(ju)
381 aussitost	516 cour	537 f	325 juge
265 autant	400 courrier	084 fa	231 jusque
176 autre	505 croi	391 facil	032 l
529 avant	290 cu	035 faire	316 l
553 avec	430 cy	163 fait	409 l
411 avis	073 d	419 fe	548 l
472 avise	323 d	281 fi	564 l
452 avoit	461 d	039 fin	145 la
141 ayant	580 d	045 fo	337 la
054 b	010 da	067 foible	362 laiss
173 b	064 da	328 fois	024 le
298 b	248 dans	393 for	068 le
470 b	034 de	433 fourrage	077 lequel
086 ba	042 de	355 frontiere	479 le_Roy
204 be	097 de	021 fu	124 les
554 bi	295 deja	056 g	179 lettre
296 bo	018 demand	219 g	268 leur
282 bu	162 demeur	575 g	327 li
392 beaucoup	491 depuis	102 ga	224 lieu
464 besoin	526 des	214 gard	158 lo
420 bien	538 des	299 ge	196 lo
258 bled	083 desir	132 general	255 lon
257 bombe	458 devant	519 Geneve(?)	277 lors
431 bon	333 di	254 Gens	340 lu
572 Briancon	394 dire	267 gi	283 lui
017 c	356 dispos	023 gouvern	382 luy
252 c	020 do	193 grand	051 Luzerne(valle
490 c	058 do	576 Grenoble	230 m
523 c	499 doi	303 gu	454 m
065 ca	074 don	308 gu	514 m
372 ca	158 dra	153 h	535 m
468 calme	101 du	515 h	559 m
043 camp	192 du	136 ha	137 ma
182 canon	008 e	313 he	233 mais
249 capable	049 e	363 hi(hy)	398 mal
357 car	119 e	343 ho	413 mand
118 cause	154 e	288 homme	429 manque
072 caval	374 e	195 honneur	421 marque
558 Cazal	500 e	399 hors	330 masque(???)
099 ce	522 e	418 hu	244 mauvais
127 ce	213 effet	055 i(j)	112 me
322 cela	276 elle	057 i(j)	122 me
134 celle	360 empesch	199 i(j)	450 me
264 celui	022 en	229 i(j)	483 meilleur
041 cependant	076 encore	251 i(j)	506 ment

465 mesme
046 mi
038 mieux
352 Milan
165 mo
259 moins
331 mois
091 mon
540 Mr_de_Rebenac
518 Mr_de_Rebenac
370 moy
103 moyen
375 mu
202 munition
088 n
129 n
200 n
424 n
488 n
489 n
509 n
216 na
125 ne
144 ne
146 ne
326 necessaire
404 necessite
044 ni
455 ni
269 no
475 no
078 nombre
498 non
441 nous
069 nouvelle
159 nt
339 nu
121 o
387 o
486 o
521 o
560 o
582 o
312 occasion
481 occup
428 officier
344 oit
234 on
053 ordonn
390 ou
170 p
422 p
501 p
585 p
113 pa
292 par
484 parti
220 pas
260 pas
001 passage
092 pe
570 pe
166 peine
185 pense
280 per
354 personn
371 persuad(ou as
130 peu
147 pi
566 Pignerol
270 plus
104 po
338 point
410 pont
425 port
503 pour
304 pouvoi
494 Pragelas(vall
211 prendre
217 pres
160 present
405 pris
297 projet
476 pu
517 puis
317 q
414 qu
148 qua
427 quand
532 quantite
002 quartier
311 qu'il
047 que
052 que
080 quelle
114 quelque
094 qui
226 qui
383 quo
013 r
172 r
300 r
528 r
565 r
579 r
117 ra
397 raison
004 rait(roit)
009 re
093 re
167 re
466 recev
005 regiment
246 rend
271 rest
388 ri
569 ri
502 rien
105 ro
174 ro
439 ru
120 s
126 s
284 s
345 s
469 s
574 s
584 s
197 sa
551 sa
070 SaMajeste
320 sans
555 Scavoi
060 se
079 se
497 sembl
095 secour
533 servi
149 si
305 si
477 siege
493 sieur
025 so
050 so
378 soin
417 soit
139 somme
180 son
310 sou
115 St
237 StMartin(vall
279 su
332 sui
081 sur
577 Suze
171 t
201 t
205 t
238 t
544 t
561 t
578 t
116 ta
168 tant
096 te
181 te
048 temps
227 tenir
384 ti
415 tion
293 to
368 to
175 toujours
376 tour
208 tout
438 tres
534 trop
106 troupe
377 trouv
389 tu
550 Turin
186 u(v)
187 u(v)
423 u(v)
437 u(v)
549 u(v)
587 u(v)
306 ua(va)
285 ue(ve)
407 ue(ve)
513 ui(vi)
061 uo(vo)
416 uo(vo)
451 us
278 veill
426 venir
504 verit
520 veu
478 vivre
150 voir
467 vos
496 vostre
026 vous
198 vous
236 vrai
442 vu
207 x
487 x
272 y
349 y
556 y
583 y
206 z
318 z
573 z
014 .
029 .
030 .
062 .
107 .
108 .
151 .
209 .
261 .
309 .
341 .
367 .
396 .
480 .
510 .
541 .
567 .
027 annule_gr_pre

Un code de Louis XIV (1691)

Description
Le roi Louis XIV communiquait avec le Maréchal de Catinat avec un code en deux parties : La table chiffrante, par ordre alphabétique; sert à écrire en chiffres, et l'autre marquée, la table déchiffrante, par ordre numérique, sert à traduire les chiffres en phrases.

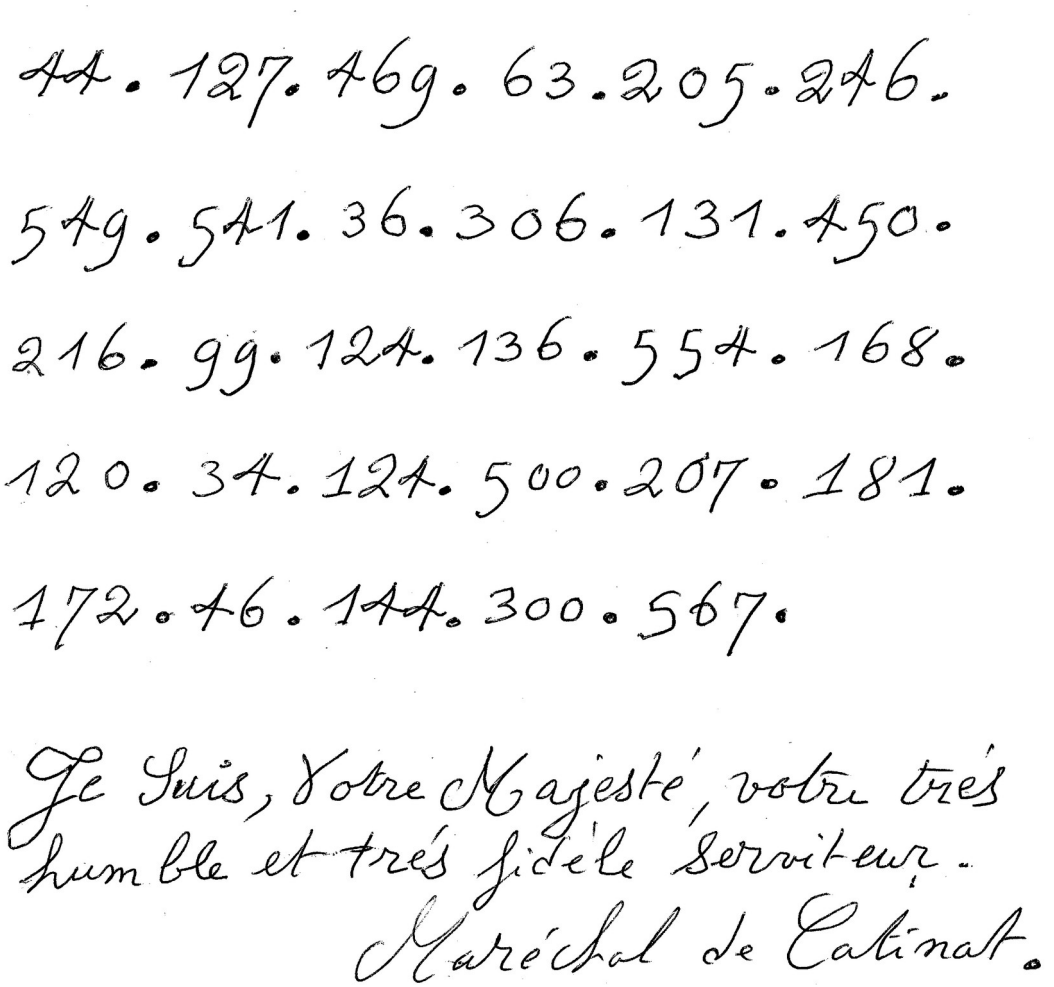
Un groupe signifie:

- Une lettre : ABC...Z, les lettres I et J sont confondues ainsi que U et V..
- Une syllabe : ba, be, bi, bo, bu, …
- Un mot :
    - Un nom commun : jour, régiment, lettre, infanterie, …
    - Un nom propre : St Martin (la vallée de), Pragelas (la vallée de), Pignerol, ...

Exemple de chiffrement:

Clair : Bonjour il fait beau						
Clair découpé en unité pouvant être chiffrée :	*bon*	*jour*	*il*	*fait*	*be*	*au*
Le cryptogramme :	431.	75.	434.	163.	204.	525.

Un cryptogramme à déchiffrer, du 26 mars 1691



Le carré de Polybe et ses variantes

Le carré de Polybe d'origine

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	i/j	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Exemple

Clair: B O N J O U R
Crypto: 12 34 33 24 33 45 42

Le Chiffre des Nihilistes (1880)

	1	2	3	4	5
1	A	N	R	C	H
2	i/j	S	T	E	B
3	D	F	G	K	L
4	M	O	P	Q	U
5	V	W	X	Y	Z

Description:
On utilise un alphabet désordonné, par exemple généré par un mot clé

Exemple, mot clé: ANARCHISTE
Clair: B O N J O U R
Crypto: 25 42 12 21 42 45 13

Utilisation de tous les chiffres et mélanges (col et lig)

	1	7	2	8	3
5	A	N	R	C	H
6	I	S	T	E	B
9	D	F	G	J	K
0	L	M	O	P	Q
4	U	V	X	Y	Z

Exemple, mot clé: ANARCHISTE
Clair: B O N J O U R
Crypto: 63 02 57 98 20 41 25

Les codes 02 et 20 sont équivalents (0)
La lettre W est codée VV

Cryptogramme:

98 68 80 86 57 67 68 91 02 57 58 98 68 67 41 61 67

Un code inviolable (> 16 ans)

Description du "Masque jetable" (OTP: Only-Time Pad)

1) Il faut transformer le texte clair en chiffre (quelque soit la méthode). Par exemple, on utilise le tableau suivant:

	0	1	2	3	4
5	A	B	C	D	E
6	F	G	H	I	J
7	K	L	M	N	O
8	P	Q	R	S	T
9	U	V (W=VV)	X	Y	Z

Exemple:

Message en clair: `B O N J O U R`

Message codé: `51 74 73 64 74 90 82`

Remarque: les codes 74 et 47 sont équivalents

2) On utilise une suite aléaoire de nombres que l'on va aditionner sans retenue au message codé résultant, chiffre par chiffre. On ajoute au début du message chiffré le numéro de page qui contient la suite aléatoire. Ensuite on brule la page utilisée (on ne l'utilise qu'une fois). Le correspondant qui possède la même suite fait de même. Cette méthode (à quelques détails préts) était utilisée par les espions de la guerre froide. Pour fabriquer les nombres aléatoires on utilise une roulette qui possède 100 nombre de 00 à 99 (au lieu de 36 nombres de 0 à 35). On cachait les pages aléatoires (écrites de manière minuscule) par exemple dans une noix, dans un tube dentifrice, ...

Page 32
8060 0340 2499 9159 7040 6427
9448 9274 6349 7081 4782 2517
1631 3069 9572 3059 7939 6215
...
1154 5422 6706 4177 9993 7891
8034 6214 1744 4211 2877 0435

Chiffrement:

```
      Message codé:      5174 7364 7490 82  (par groupe de 4)
      Suite aléatoire:   8060 0340 2499 91  (adition sans retenu)
Message chiffré:      32 3134 7604 9889 73
```

Déchiffrement:

```
Message chiffré:      32 3134 7604 9889 73
      Suite aléatoire:   8060 0340 2499 91  (soustration)
      Message codé:      5174 7364 7490 82 = 51,74,73,64,74,90,82
Message en clair:      B O N J O U R
```

Enigme: `32 9710 8745 9424 3600 7988 1898 3930 8465 26`

Un message d'un espion (suite)

Le masque jetable:

Page 33
3479 1695 7088 5607 5938 3431
2936 8712 9164 6208 0957 7255
8914 0882 3916 1886 9265 5488
2676 2171 1345 2376 1517 2005
4190 0261 1133 8877 7839 6424
0141 7039 6668 4383 4717 5731
2633 7026 0616 1338 2760 7475
9767 1855 2204 7299 4222 8068
6690 8041 2364 4746 5904 7173
2848 8110 7593 2365 8882 6377
4105 2411 4191 1352 8305 1158
7211 4978 0335 0733 3780 7892
7784 2612 8368 1139 8866 3896
1539 2220 1988 7016 4734 5791
9323 7388 7971 3412 5099 9307
2275 3057 8036 7443 1425 2853
1154 5422 6706 4177 9993 7891
8034 6214 1744 4211 2877 0435

Le cryptogramme:

3398 2979 6624 6136 7809
0117 8419 1837 7241 3516

Le coin du matheux, exemple: le Vigenère (> 16 ans)

Le vigenère, variante Beaufort : description mathématique

Chiffrement: C[i] = (K[i mod N] - P[i]) mod Z
Déchiffrement: P[i] = (K[i mod N] - C[i]) mod Z

mod : Modulo
C[i] : La ième lettre du message chiffré
P[i] : La ième lettre du message en clair
K[i] : La ième lettre de la clé
Z : la longueur de l'alphabet (usuellement 26)
N: la longueur de la clé

Alphabet:

```
A = 00, B = 01, C = 02, D = 03, E = 04, F = 05
G = 06, H = 07, I = 08, J = 09, K = 10, L = 11
M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17
S = 18, T = 19, U = 20, V = 21, W = 22, X = 23
Y = 24, Z = 25
```

Exemple

- Message en clair: B O N J O U R
  idem en chiffre: 1, 14, 13, 9, 14, 20, 17
- Mot clé: R O I
  idem en chiffre: 17, 14, 8
- Message chiffré:

```
i=0, P[0]=B(01), K[00]=R(17), C[0]=Q(16)
i=1, P[1]=O(14), K[01]=O(14), C[1]=A(00)
i=2, P[2]=N(13), K[02]=I(08), C[2]=V(21)
i=3, P[3]=J(09), K[00]=R(17), C[3]=I(08)
i=4, P[4]=O(14), K[01]=O(14), C[4]=A(00)
i=5, P[5]=U(20), K[02]=I(08), C[5]=O(14)
i=6, P[6]=R(17), K[00]=R(17), C[6]=A(00)
```

Résultat: Q A V I A O A

Enigme: mot-clé : BEAU (> 16 ans + Matheux)

```
QAZGO XWAKA IBQAO QTTPQ HNXQJ CMCPA HMLKW C
```

Pour les geeks de l'informatique (> 16 ans)

Le vigenère, variante Beaufort : Un programme en Python

```
import string
ALPHA = string.ascii_uppercase
def nettoie( chaine ):
    chClean = ""
    for lettre in chaine:
        if lettre.isalpha():
            chClean += lettre.upper()
    return chClean
def chaine2chiffre( chaine ):
    msgNum = []
    for lettre in chaine:
        msgNum.append( ALPHA.find( lettre ))
    return msgNum
def chiffre2chaine( msgNum ):
    chaine = ""
    for unCaractere in msgNum:
        chaine +=  ALPHA[ unCaractere ]
    return chaine
def grp5let( ch ):
    ch5 = "" ; i = 1
    for lettre in ch:
        ch5 += lettre
        if (i % 5) == 0: ch5 += " "
        i += 1
    return ch5
def chiffre( P, K ):
    N = len(K)
    Z = len(ALPHA)
    C = [0]*len(P)
    for i in range( len(P) ):
        C[i] = ( K[ i % N ] - P[i]  ) % Z
    return C
chaine = input("Un message (clair ou crypto) ? ")
cle = input("La clé ? ")
P =  chaine2chiffre( nettoie( chaine ) )
K =  chaine2chiffre( nettoie( cle ) )
C = chiffre( P, K)
crypto = chiffre2chaine( C )
print( grp5let( crypto ) )
```