

À VOUS DE JOUER !

	Lettre en clair																									
	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
Lettre de la clé	Lettres chiffrées (au croisement de la colonne <i>Lettre en clair</i> et de la ligne <i>Lettre de la clé</i>)																									
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Wikipédia : Chiffrement de Vigenère

Exemple de chiffrement avec la clé "FRANCE"

Clair

BLAISE DE VIGENÈRE

Clé répétée

FRANCE FRANCE FRANCE

Chiffré

GCAVUI IV VVI ISVRR

Le lapin est un petit mammifère herbivore, reconnaissable à ses longues oreilles et à sa petite queue touffue. Il en existe de nombreuses espèces. Souvent classé par erreur parmi les rongeurs, il appartient en vérité à l'ordre des lagomorphes qui sont en fait les cousins des rongeurs. Il y a deux différences entre les lagomorphes et les rongeurs. La première est au niveau des dents. Sur chaque mâchoire, les rongeurs ont deux dents incisives qui poussent en permanence, alors que les lagomorphes en ont quatre, deux grosses et deux autres justes derrière. La deuxième, est que les pattes postérieures des lagomorphes sont beaucoup plus grandes que leurs pattes antérieures, ce qui leur permet de bondir et de courir vite. Le mot lapin a remplacé le terme ancien français conil qui nous vient du mot latin cuniculus. Le nez du lapin remue en permanence, pour renifler l'air et identifier les odeurs. Son museau est doté de longues moustaches, qui sont des organes tactiles très sensibles. Les lapereaux naissent nus et aveugles et restent dans le nid tapissé du poil de leur mère, qui les allaite pendant plusieurs semaines. Une des particularités du lapin est de manger certains de ses excréments, les cœcotropes, il ne digère pas ses aliments entièrement et doit les redigérer afin d'en extraire tous les nutriments. Le lapin fait partie des signes du zodiaque chinois, symbole de longévité, de paix et de prospérité, en raison de ses performances reproductives prolifiques, toujours prêt à s'accoupler en toute saison. Pour cette année, nous sommes sous le signe du lapin d'eau, qui a comme caractéristique, d'être doux, amical, capable de s'adapter facilement à différentes conditions, mais avec un état d'esprit et des principes faibles.

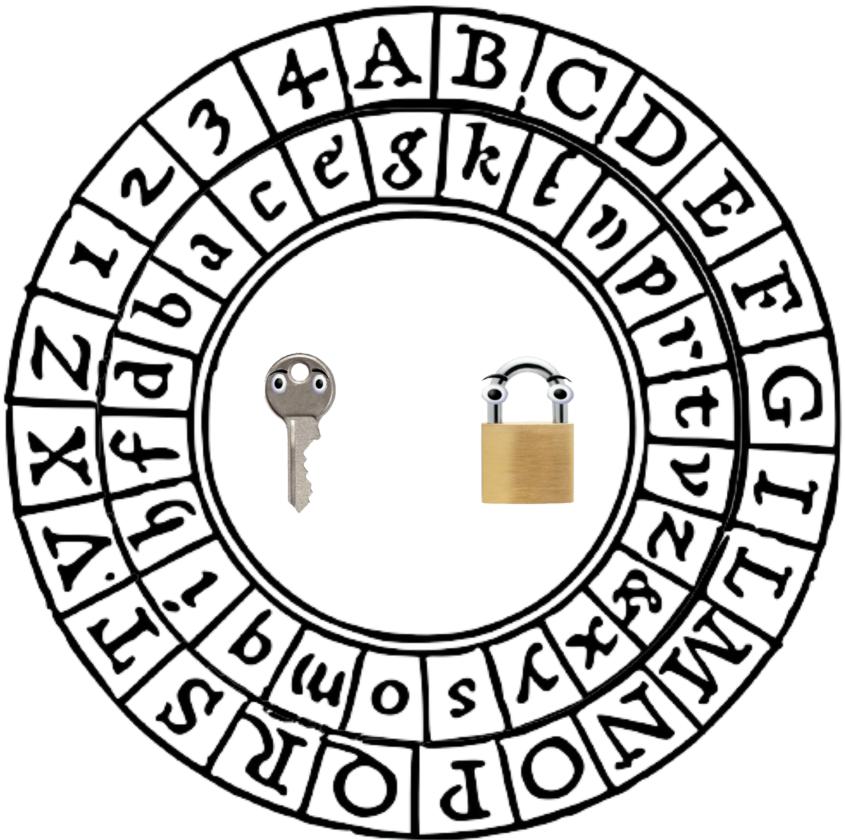
Disque Alberti

Chiffrement du mot "DISQUE"

D → n

I → v

S → q



On viens de chiffrer trois lettres, donc on tourne le disque intérieur de 2 cases dans le sens antihoraire

Q → **q**

U → **d**

***Mais il n'y pas de U sur le disque ?
En effet, à l'époque le U n'existaient
pas. Ici, nous nous servons du V
pour chiffrer le U.***

E ➔ t



DISQUE → **nvqqdt Clé = E** (car la dernière lettre chiffré donne t)

Méthode de chiffrement ADFGVX

1. Substitution à l'aide de cette table

		Second code					
		A	D	F	G	V	X
Premier code	A	8	t	b	w	r	q
	D	p	4	c	g	2	9
	F	3	o	5	m	x	e
	G	d	a	z	j	s	y
	V	l	h	7	u	v	0
	X	n	1	k	6	i	f

A

MOT



GD



FGFDAD

2. Transposition à l'aide de la clé

Exemple avec la clé : "CLE"

Clé	C	L	E
Message substitué	D	F	A
	V	G	X
	D	A	A
	D	X	V
	G	V	X

On construit le tableau avec la clé en première ligne, puis on remplis les lignes suivantes avec le message substitué

On ajoute X dans les cases vides restantes

On change l'ordre des colonnes en triant la clé dans l'ordre alphabétique
C < E < L.

Clé classée	C	E	L
Message substitué puis transposé	D	A	F
	V	X	G
	D	A	A
	D	V	X
	G	X	V

Puis on lis le message de haut en bas et de gauche à droite
C < E < L.

DFAVGXDAADXVGVX



DVDDGAXAVFGAXV