

# La grille tournante du colonel Fleissner



## Sommaire

Un challenge de cryptographie pour le CTF de le Hack 2023.....	3
Solution du challenge .....	4
« L'attaque par mot probable » est la vulnérabilité de la grille du colonel Fleissner .....	5
Premier essai .....	6
Première Rotation de 90 degrés .....	6
Deuxième essai.....	7
Première Rotation de 90 degrés .....	7
Deuxième essai.....	8
Première Rotation de 90 degrés avec comme hypothèse le mot « donne ».....	8
Annexe : Les étapes pour chiffrer de nouveau un message avec la grille du colonel Fleissner.....	11

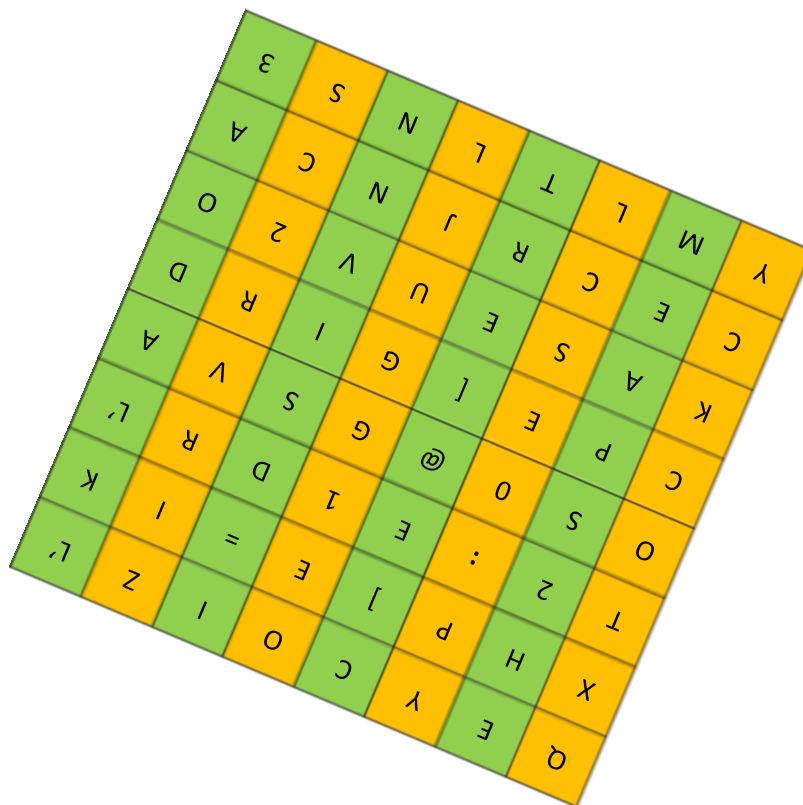
# Un challenge de cryptographie pour le CTF de le Hack 2023

**Titre du challenge :** CrazyCrypto3

**Auteur :** Anonyme

**Difficulté :** médium

Le challenge de la grille tournante du colonel Fleissner est proposé pour leHack kids (enfants entre 8 à 16 ans). Les enfants ont réussi le challenge en connaissant la position initiale de la grille du colonel Fleissner. Vous pouvez réussir sans connaître la position de la grille car vous avez entendu que le message contient le mot ARCSI....



## Solution du challenge

Pour résoudre ce challenge vous devez connaître parfaitement le fonctionnement de la grille du colonel Fleissner. Pour comprendre le fonctionnement je vous propose l'exemple ci-dessous de <https://www.bibmath.fr/>

Le procédé a été inventé à la fin du XIXe siècle par le colonel autrichien Edouard Fleissner : il s'agit d'une grille tournante de cases dont chaque côté en comprend un nombre pair. Des cases ajourées sont choisies de telle manière que si on tourne la grille dans le sens des aiguilles d'une montre, elles recouvrent le carré entier.

A chaque fois que la grille est tournée de 90 degrés on peut lire un autre mot dans la grille.

La [vidéo de Philippe Guillot \(ARCSI\)](#) publiée sur [la chaîne DailyMotion de l'ARCSI](#) présente le détail du décryptement du message codé au coeur du roman de Jules Verne "Mathias Sandorf" paru en 1885, avec une grille de côté 6.

Par exemple,

T	E	E	N	I	V
T	O	S	N	O	R
S	D	Y	E	E	M
N	E	D	S	R	F
U	M	O	E	R	D
U	T	N	E	I	S

Le texte codé


La grille

Voyons par exemple comment décoder le texte codé ci-dessus avec la grille ci-dessus.

	E		N		V
				O	
		Y			
	E			R	
					D
			E		

Pour la première étape nous lisons ci-dessus : « envoyerde »

		S			R
			E		
N					F
		O		R	
	T				S

		E			
T					
	D			E	
			S		
	M				
U		N		I	

T				I	
	O		N		
S					M
		D			
U			E		

En tournant la grille de 90 degrés trois fois nous lisons : « srenfortsetdesmunitionsmdue »

Le message secret est donc «envoyer des renforts et des munitions mdue »

Source : [Les grilles tournantes du colonel Fleissner \(bibmath.net\)](#)

## **« L'attaque par mot probable » est la vulnérabilité de la grille du colonel Fleissner**

Dans l'énoncé le message contient le mot ARCSI. Il faut savoir qu'il est presque impossible de résoudre rapidement ce challenge à la main sans indice. L'indice du challenge est le mot ARCSI. Donc, cet indice facilite la tâche pour décoder le challenge. Si nous connaissons parfaitement où est le mot ARCSI, nous connaissons cinq trous dans la grille. Puis lors de la rotation de 90 degrés nous connaissons cinq nouvelles lettres. Lorsque nous effectuons une rotation de 180 degrés et 270 degrés nous connaissons des autres lettres. Ce n'est pas facile parce que ces lettres trouvées ne sont pas forcément au début d'un nouveau mot. Donc, il est peu probable de former un nouveau mot facilement. L'astuce est de faire des suppositions de nouveaux trous dans la grille pour former de nouveaux mots puis de recommencer. Si la supposition n'est pas bonne lorsque vous tournez la grille de 0, 90, 180, 270 degrés alors il ne faut pas garder cette supposition.

Nous allons effectuer une attaque par mot probable pour résoudre ce challenge. C'est-à-dire que nous connaissons un mot en clair dans le message codé. Nous allons donc en premier chercher à former le mot ARCSI en haut de la grille. Pour complexifier le jeu et tromper les joueurs, la grille et les lettres données initialement ont une rotation.

Pour effectuer la cryptanalyse, il faut que dès le départ la grille et les lettres soient bien positionnées. La grille se lit normalement, c'est-à-dire de haut vers le bas et de gauche vers la droite.

Pour réussir ce challenge il faut émettre des hypothèses puis les valider puis en émettre d'autres.

On émet l'hypothèse que le premier mot est « L' ARCSI » donc si on sélectionne ces lettres et on fait une rotation de 90 degrés on doit trouver un autre mot ou une partie d'un autre mot si ce n'est pas le cas c'est que le mot « L'ARCSI » est mal positionné.

Le premier essai à la page 6 est une démonstration d'une hypothèse qui n'est pas bonne. Le deuxième essai à la page 7 est une hypothèse qui est bonne.

**Premier essai**  
**Première Rotation de 90 degrés**

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position initiale de la grille en rouge

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position de la grille après rotation

Dans la grille du premier essai après la rotation (90), un des mots en clair contient O3N, c'est probablement impossible. Si on effectue une deuxième rotation (180) on obtient un mot avec un CY et avec une rotation de 270 on obtient un mot avec KI ceci est impossible. **Donc, il y a un problème dans cette hypothèse.**

**Deuxième essai**  
**Première Rotation de 90**

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	O	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position initiale de la grille en rouge

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	O	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position de la grille après rotation

En sélectionnant le deuxième essai on arrive à former après une première rotation le groupe « nn ». Ce mot peut être « donne » ou « bonne » ou « sonne » ...On émet des hypothèses en fonction de la position des lettres dans la grille dans le but de former des mots pour une position de la grille puis si c'est bon alors en tournant la grille on doit trouver un nouveau mot ou une partie d'un nouveau mot.

## Deuxième essai

Première Rotation de 90 degrés avec comme hypothèse le mot « donne »

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position initiale des 2 lettres en jaune

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position 90 degrés en y ajoutant 2 lettres

En combinant la position initiale et celle de 90 degrés on a **L'ARCSI ..O..S DONNE**.

On émet l'hypothèse : **L'ARCSI ..O..S DONNE** => **L'ARCSI VOUS DONNE** où « **L'ARCSI VOUS** » est dans la position initiale puis « **DONNE** » dans la position à 90 degrés

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position initiale avec 4 lettres en jaune



L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	O	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position 90 degrés en gardant les 4 lettres en jaunes :

On lit « DONNE LE SEC »

Au total , le message est : « L'ARCSI VOUS DONNE LE SEC »

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	O	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position 180 degrés en y ajoutant les 4 lettres :

On lit « RET :LEHACK »

Au total , le message est : « L'ARCSI VOUS DONNE LE SECRET :LEHACK »

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	O	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Position 270 degrés en y ajoutant 4 lettres :

On lit « KIDSCRYPTO »

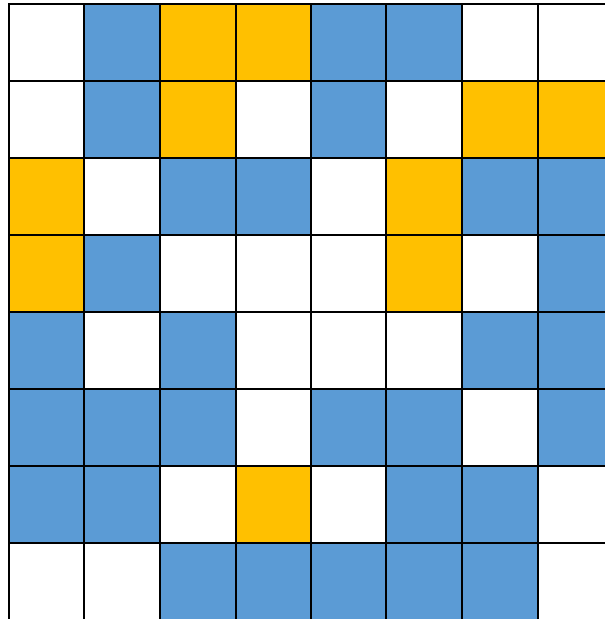
Au total , le message est : « L'ARCSI VOUS DONNE LE SECRET : LEHACKKIDSCRYPTO\_ »

**Donc le code secret à rentrer pour valider l'épreuve est LEHACKKIDSCRYPTO**

## Annexe : Les étapes pour coder de nouveau un message avec la grille du colonel Fleissner

La grille que vous choisissez peut avoir un nombre de colonne/ligne paire ou impaire.

La première étape est de créer une grille en sélectionnant des carrés qui ne sont pas réécrits après la rotation de la grille. Comme ci-dessus :



La grille du colonel Fleissner (8x8).

En orange les trous dans la grille.

En bleu les positions de la grille après rotation (90,180,270 degrés).

# Challenge ARCSI pour le CTF de le HACK 2023

1	2	3	4	5	6	7	8	9	10		1	1	1	1	1	1	1	1	1	2		2	2	2	2	2	2	2	2	2	3		3	3	3	3	3	3	3	3	4	
L	A	R	C	S	I	V	O	U	S		D	O	N	N	E	L	E	S	E	C		R	E	T	:	L	E	H	A	C	K		K	I	D	S	C	R	Y	P	T	O
L'ARCSIVOUS										DONNELESEC										RET:LEHACK										KIDSCRYPTO												

## Le message secret

		1	2				
		3				4	5
6					7		
8					9		
			10				

Position initiale

				11	12		
						13	14
	15						16
				17	18		
						19	
						20	

Rotation 90 degrés

				21			
		22					23
		24					25
26	27				28		
				29	30		

Position 180 degrés

	31						
	32						
		33	34				
35						36	
37	38						
		39	40				

Position 270 degrés

# Challenge ARCSI pour le CTF de le HACK 2023

	31	1	2	11	12		
	32	3		21		4	5
6		33	34		7	13	14
8	15				9		16
35		22				36	23
37	38	24		17	18		25
26	27		10		28	19	
		39	40	29	30	20	

L'ensemble des positions

1	2	3	4	5	6	7	8	9	10		11	12	13	14	15	16	17	18	19	20		21	22	23	24	25	26	27	28	29	30		31	32	33	34	35	36	37	38	39	40
L	A	R	C	S	I	V	O	U	S		D	O	N	N	E	L	E	S	E	C		R	E	T	:	L	E	H	A	C	K		K	I	D	S	C	R	Y	P	T	O
L'ARCSIVOUS										DONNELESEC										RET:LEHACK										KIDSCRYPTO												

Le message à codé

	K	L'	A	D	O		
	I	R		R		C	S
I		D	S		V	N	N
O	E				U		L
C		E				R	T
Y	P	:		E	S		L
E	H		S		A	E	
		T	O	C	K	C	

Le message codé dans les positions

L'	K	L'	A	D	O	A	3
Z	I	R	V	R	2	C	S
I	=	D	S	I	V	N	N
O	E	1	G	G	U	J	L
C	]	E	@	[	E	R	T
Y	P	:	0	E	S	C	L
E	H	2	S	P	A	E	M
Q	X	T	O	C	K	C	Y

Le message codé qui sera donné aux joueurs.

On ajoute des lettres pour rendre le déchiffrement plus difficile ☺