



3/12/2022

Solution du jeu ARCSI du mois de décembre 2022

Cryptographie
OSINT
Stéganographie

Le jeu :

[#Lundichallenge](#) [#Cryptographie](#) [#Stéganographie](#) [#OSINT](#) Le chiffre Bifide utilise une substitution avec un carré de Polybe et une transposition. La clef est sur 5 blocs, elle commence par ARCSI suivi des lettres de l'alphabet :
Ntyd rbjc fkod deeB bbxv ddeE ehsf swkb lp13 a30

Le challenge a été publié sur ces pages :

<https://www.arcsi.fr/jeux.php>

https://twitter.com/arcsi_fr/status/160243139796

Introduction

Le titre du challenge contient [#Cryptographie](#) [#Sténographie](#) [#OSINT](#) ceci signifie que le challenge utilise 3 moyens pour dissimuler de l'information.

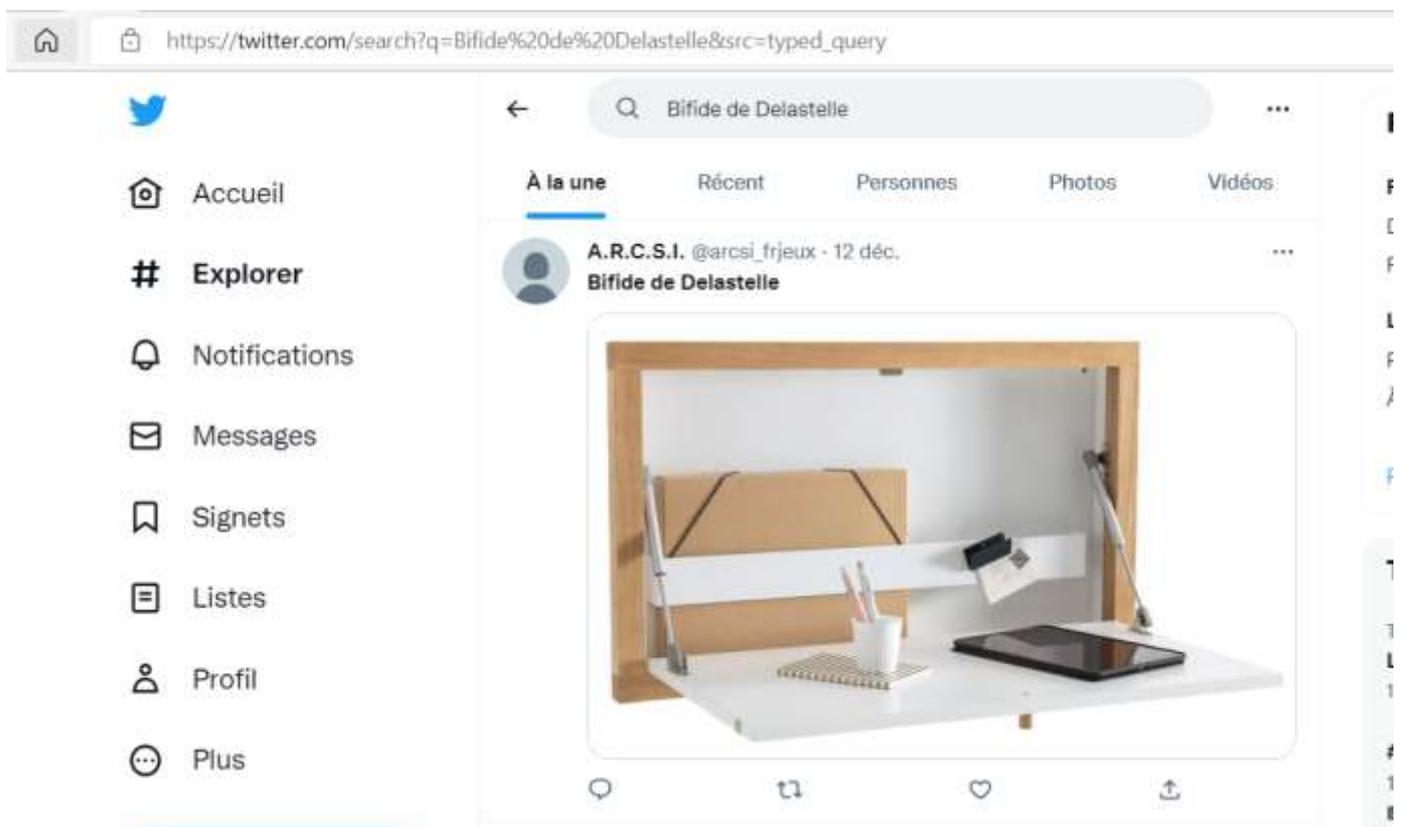
Le challenge se réalise en 3 étapes :

- La première étape, consiste à déchiffrer un message utilisant le chiffre Bifide de Delastelle.
- La deuxième étape, consiste à trouver un tweet qui contient une information.
- La troisième étape, a pour but de trouver un message dans un QR code dans l'image du tweet.

Table des matières

Introduction	2
Solution 1 ^{er} étape :	3
Solution 2 ^{eme} étape :	4
Solution 3 ^{eme} étape :	5
Annexe 1 : Refaire le challenge en chiffrant de nouveau un texte	6
Annexe 2 : Conseils pour refaire le challenge en augmentant la complexité du challenge	7

Solution 2^{ème} étape :



Chercher « Bifide de Delastelle » sur le réseau social Twitter

Solution 3^{ème} étape :



Faire un zoom où est écrit « Rdv 13h30 » sur l'image, puis scanner le QR code. Dans ce QR code, il y a le message « Bravo le code secret à trouver est {Chiffredelastelle} »

Annexe 1 : Refaire le challenge en chiffrant de nouveau un texte

Attention : Pour refaire le challenge la taille du bloc de la clef doit être impaire.

Nous voulons chiffrer ce texte en clair : Trouver le code de Bifide de Delastelle a h

Avec la clef ci-dessous :

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

Carré de Polybe

Effectuer une substitution à l'aide du carré de Polybe en prenant la position (Ligne, Colonne) de chaque lettre du texte : « Trouver le code de Bifide de Delastelle a h ».

Ecrire cette position de façon verticale

T	R	O	U	V	E	R	L	E	C	O	D	E	D	E	B	I	F	I	D	E	D	E	D	E	L	A	S	T	E	L	L	E	A	H
4	1	4	5	5	2	1	3	2	1	4	2	2	2	2	2	1	2	1	2	2	2	2	2	2	3	1	1	4	2	3	3	2	1	3
5	2	2	1	2	3	2	4	3	3	2	2	3	2	3	1	5	4	5	2	3	2	3	2	3	4	1	4	5	3	4	4	3	1	1

Découper le message par bloc de 5 lettres car la clef est sur 5 blocs :

T	R	O	U	V	E	R	L	E	C	O	D	E	D	E	B	I	F	I	D	E	D	E	D	E	L	A	S	T	E	L	L	E	A	H
4	1	4	5	5	2	1	3	2	1	4	2	2	2	2	2	1	2	1	2	2	2	2	2	2	3	1	1	4	2	3	3	2	1	3
5	2	2	1	2	3	2	4	3	3	2	2	3	2	3	1	5	4	5	2	3	2	3	2	3	4	1	4	5	3	4	4	3	1	1

Effectuer une transposition en lisant les positions de façons horizontale et reformer les blocs de 5 lettres

$\begin{bmatrix} 41 & 45 & 55 \\ 22 & 12 & \end{bmatrix}$
 $\begin{bmatrix} 21 & 32 & 13 \\ 24 & 33 & \end{bmatrix}$
 $\begin{bmatrix} 42 & 22 & 22 \\ 23 & 23 & \end{bmatrix}$
 $\begin{bmatrix} 21 & 21 & 21 \\ 54 & 52 & \end{bmatrix}$
 $\begin{bmatrix} 22 & 22 & 23 \\ 23 & 23 & \end{bmatrix}$
 $\begin{bmatrix} 31 & 14 & 24 \\ 14 & 53 & \end{bmatrix}$
 $\begin{bmatrix} 33 & 21 & 34 \\ 43 & 11 & \end{bmatrix}$

Effectuer une substitution en prenant la position de chaque lettre en réutilisant le même tableau:

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

Carré de Polybe

Le message chiffré devient : Ntydr bjcfk oddee bbbxv ddeee hsfsw kblpa

Par exemple : La première lettre T en clair devient 45, puis 41 puis N en chiffrée. La deuxième lettre R en chiffrée devient 12, puis 45 puis T en clair.

Annexe 2 : Conseils pour refaire le challenge en augmentant la complexité du challenge

Pour la partie Cryptographie :

- Utiliser une clef 100% aléatoire, ne pas donner la clef.
- Utiliser 2 carrés de Polybe différents. Utiliser un carré pour la première substitution, puis un autre différent pour la 2eme substitution.
- Au lieu de commencer par une lecture verticale , puis horizontale vous pouvez faire l'inverse.
- Utiliser une transposition différente que celle de base.

Pour la partie OSINT :

- Au lieu de donner le nom de la personne à chercher sur le réseau social Twitter, vous pouvez uniquement donner des informations sur la vie de la personne.