

Solution du jeu ARCSI du mois de janvier 2023

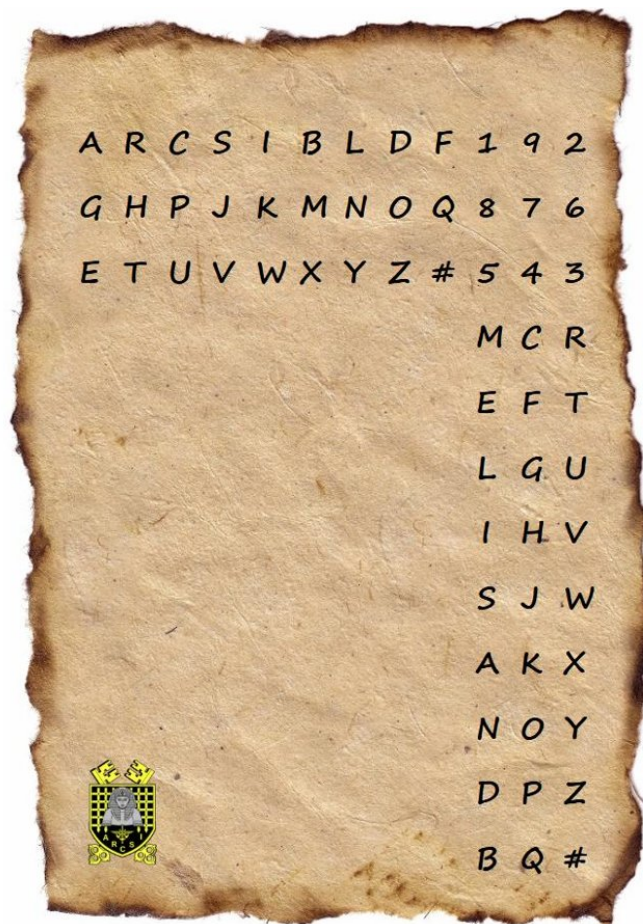


02/01/2023

Cryptographie
OSINT
Stéganographie

Le jeu

[#Lundichallenge](#) [#Cryptographie](#) [#OSINT](#) [#Stéganographie](#) Le chiffre Digrafide est un système de chiffrement tomogrammique utilisant deux grilles de lettres et des transpositions de leurs coordonnées. Le secret à déchiffrer : pgrr vyya qtebs dgckp amctu ycabt fmbrc ntyin tq
Le challenge se résoud en 3 étapes : La première est cette énigme de cryptographie. La réponse sera sous la forme : justpaste.it/***** Le ***** est un nombre. La seconde étape est un challenge d'OSINT. La troisième étape est un challenge de stéganographie. Bonne chance.



Le challenge a été publié sur ces pages :

<https://www.arcsi.fr/jeux.php>
https://twitter.com/arcsi_fr/status/1612584906215018510

Introduction

Le titre du challenge contient #Cryptographie #OSINT #Sténographie ceci signifie que le challenge utilise 3 moyens pour dissimuler de l'information. Le challenge se réalise en 3 étapes :

- La première étape est un message caché avec une technique de cryptographie. Cette technique est le chiffre Digrafide.
- La deuxième étape utilise l' Open Source Intelligence (OSINT), Le renseignement en sources ouvertes : le terme désigne l'exploitation de sources d'information accessibles à tous (journaux, sites web, conférences, réseaux sociaux...) à des fins de renseignement. Dans cette étape le but est de trouver un nombre qui est l'user id d'un compte Twitter.
- La troisième étape, est un message caché dans une image avec une technique de stéganographie. Cette technique pour dissimuler de l'information est le chiffre Friderici (Fenêtres).

Sommaire

Le jeu	1
Introduction.....	2
Solution 1 ^{er} étape.....	3
Introduction.....	3
Déchiffrement.....	3
Solution 2 ^{emer} étape.....	5
Solution 3 ^{eme} étape :.....	6
introduction.....	6
Déchiffrement.....	7
Annexe 1 : Refaire le challenge en chiffrant de nouveau un texte avec le chiffre Digrafide.....	8

Solution 1^{er} étape

Introduction

Le chiffrement Digrafile est un chiffre tomogrammique qui utilise un tableau contenant deux alphabets désordonnés (voir la grille1 et grille3 ci dessous) et un tableau contenant une grille de 9 chiffres (voir la grille2 ci dessous). Les lettres du message en clair sont chiffrées par bigrammes. Dans une première étape, ces bigrammes sont transformés en nombre de trois chiffres. Après un mélange simple, ces nombres sont retransformés en lettres et donnent les bigrammes chiffrés.



Déchiffrement

Le tableau ci dessous reprend les 3 grilles du challenge (2 grilles (de 3x9 et 9x3) avec 27 caractères et 1 grille (3x3) avec 9 nombres :

Grille 1 : ARCSIBLDFGHPJKMNOQETUVWXYZ#

Grille 2 : 123456789

Grille 3 : MCREFTLGUIHVSJWAKXNOYDPZBQ#

Le symbole # est rajouté à l'alphabet de la grille1 et grille2 pour compléter le tableau

Le texte chiffré est : pggrr vyyya qtebs dgckp amctu ycabt fmbrc ntyin tq

En regroupant le texte chiffré par bloc de 6 lettres (=3 bigrammes) il devient :
pggrrv yyyaqt ebsdgc kpmact uycabt fmbrcn tyintq

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

L'image de la clef devient le tableau ci dessus.

Solution énigme ARCSI mois janvier 2023

Pour déchiffrer le premier bigramme « pg » qui est les 2 premières lettres du texte chiffré. Il faut prendre les positions de P dans la grille 1 : (3) et de G dans la grille 3 :(3) puis du chiffre qui dans la grille 2 qui est le croisement de la ligne/colonne. Dans notre cas c'est le chiffre 7. Donc PG= 373. Puis pour le deuxième bigramme : GR = 161 et le troisième : RV =224. Puis pour déchiffrer il faut déchiffrer le 1^{er} groupe en utilisant le 1^{er} chiffre de chaque groupe. Pour le 1^{er} chiffre ce sera 312 puis en utilisant le 2eme chiffre ce sera 762, le 3eme sera 314. Puis utiliser les nouvelles positions de ces groupes pour finir le déchiffrement : 312= CE, 762=NT , 314=CI.

Ci-dessous les calculs pour déchiffrer tout le message :

p	g	g	r	r	v	y	y	y	a	q	t	e	b	s	d	g	c	k	p	a	m	c	t
3	1	2				7	7	9				1	4	1				5	1	3			
7	6	2				3	5	6				5	1	7				7	1	2			
3	1	4				7	6	2				9	8	1				8	1	2			
c	e	n	t	c	i	n	q	u	a	n	t	e	c	i	n	q	m	i	l	l	e	d	e
312	762	314				779	356	762				141	517	981				513	712	812			

u	y	c	a	b	t	f	m	b	r	c	n	t	y	i	n	t	q						
3	3	6				9	6	3				2	5	2									
3	1	2				1	2	1				3	1	4									
7	6	2				1	1	7				7	7	9									
u	x	c	e	n	t	q	u	a	r	a	n	t	e	c	i	n	q						
336	312	762				963	121	117				252	314	779									

Le texte déchiffré est : centcinquantecinqmilledeuxcentquarantecinq

Le texte déchiffré est : cent cinquante-cinq mille deux cent quarante-cinq = **155245**

La réponse est sous la forme : justpaste.it/XXXXXX où XXXXXX est un nombre.

La solution est donc : <https://justpaste.it/155245>

Solution 2^{ème} étape

The screenshot shows a web browser window with the URL <https://justpaste.it/155245>. The page header is yellow with the 'JustPaste.it' logo and buttons for 'Add' and 'Account'. The main content is a post by '@anonymous' dated '7 janv. 2023'. The text of the post reads: 'Trouver l'identifiant (user id) du twitter de @arcsi_fr. Cet identifiant est une suite de chiffre. La réponse sera sous la forme : justpaste.it/*****'. Below the text are statistics: '12 visits · 1 online', a 'Share' button, and a 'Vote' section with 0 likes, 0 dislikes, and 0 stars. There is also a 'Save as PDF' button.

[étape 2 \[OSINT\] énigme de l'ARCSI de janvier 2023](#)

L'utilisateur d'un compte twitter peut être trouvé en regardant le code source de la page ou en allant sur un des sites dédiés à trouver cette information. (Par exemple tweeterid.com)

La réponse est : 1427389376099725317

The screenshot shows a browser window with the URL tweeterid.com. The page has a dark background with the title 'TweeterID Twitter ID and Username Converter'. A text input field contains '@arcsi_fr'. To the right, under 'Recent ID Conversions:', it shows '@arcsi_fr => 1427389376099725317'. The page also includes instructions: 'Type in any Twitter ID or @handle below, and it will be converted into the respective ID or username on the right:'.

La solution est donc : <https://justpaste.it/1427389376099725317>

Solution 3^{ème} étape :

JustPaste.it

étape 3 [Stéganographie] énigme de l'ARCSI de janvier 2023

@anonymous · 1s

1 visits · 1 online

Vote: 0 0 0 0 Save as PDF

Share

[étape 3 \[Stéganographie\] énigme de l'ARCSI de janvier 2023](#)

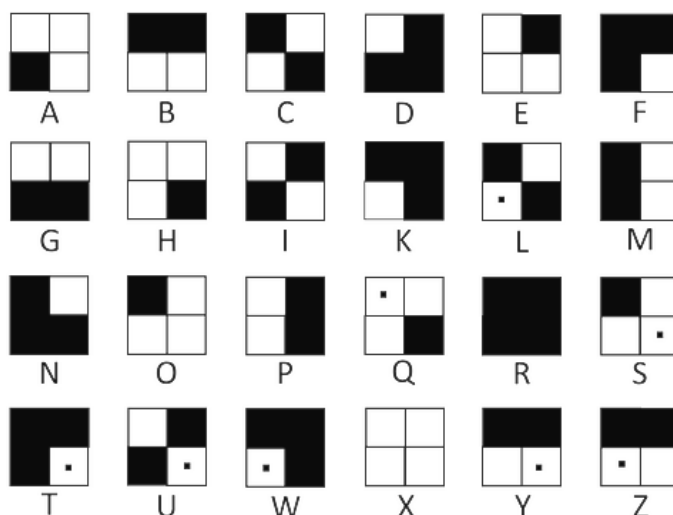
introduction



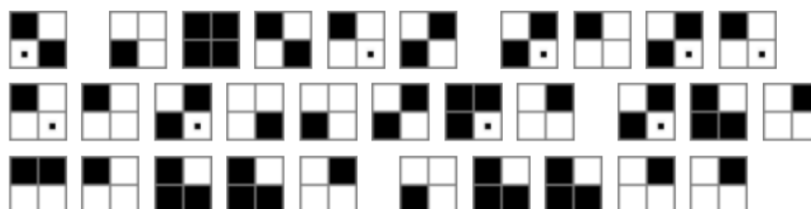
Dans son ouvrage *Cryptographia oder Geheime Schrift-münd-und Wirkliche Correspondentz* (1684), Johannes Balthasar Friderici (1639 - env. 1704) montre un dessin apparemment anodin, mais qui contient un message secret. Ce message est codé par les fenêtres de l'immeuble : WIR HABEN KEIN PULVER MEHR (Traduction de l'Allemand vers le Français = « nous n'avons plus de poudre »)

Déchiffrement

A l'aide de l'alphabet chiffré ci-dessous nous pouvons décoder l'image qui représente le texte chiffré. Dans le contexte de l'époque les lettres J et V n'existaient pas dans l'alphabet (allemand). C'est pourquoi U et V sont confondus.



Alphabet chiffré



Le texte chiffré

Le secret caché dans l'image est donc :

I ARCSI VOUS SOUHAITE UNE BONNE ANNEE

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

Grille 1 : ARCSIBLDFGHPJKMNOQETUVWXYZ#

Grille 2 : 123456789

Grille 3 : MCREFTLGUIHVSJWAKXNOYDPZBQ#

Le texte à chiffrer : cent cinquante-cinq mille deux cent quarante-cinq

centcinquantecinqmilledeuxcentquarantecinq

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

c	e	n	t	c	i	n	q	u	a	n	t	e	c	i	n	q	m	i	l	l	e	d	e
3	7	3		7	3	7	1	5	9		5	7	8										
1	6	1		7	5	6	4	1	8		1	1	1										
2	2	4		9	6	2	1	7	1		3	2	2										
p	g	g	r	r	v	y	y	y	a	q	t	e	b	s	d	g	c	k	p	a	m	c	t
373	161	224		737	756	962	159	418	171		578	111	322										

u	x	c	e	n	t	q	u	a	r	a	n	t	e	c	i	n	q						
3	3	7		9	1	1	2	3	7														
3	1	6		6	2	1	5	1	7														
6	2	2		3	1	7	2	4	9														
u	y	c	a	b	t	f	m	b	r	c	n	t	y	i	n	t	q						
337	316	622		911	621	317	237	517	249														

Le texte chiffré est donc : pggrr vyyya qtebs dgckp amctu ycabt fmbrc ntyin tq