Vuillaume Alexandre
Roussel Alexis
Helin Dorian

Le carré de Polybe

Sommaire

- **I .** Principe, avantages et utilisation
- **II .** Les dérivés du carré de Polybe
- **III.**Le carré de Polybe est un chiffrement similaire a d'autre chiffrement par substitution
- **Sitographie**

I. Principe, avantages et utilisation

Principe

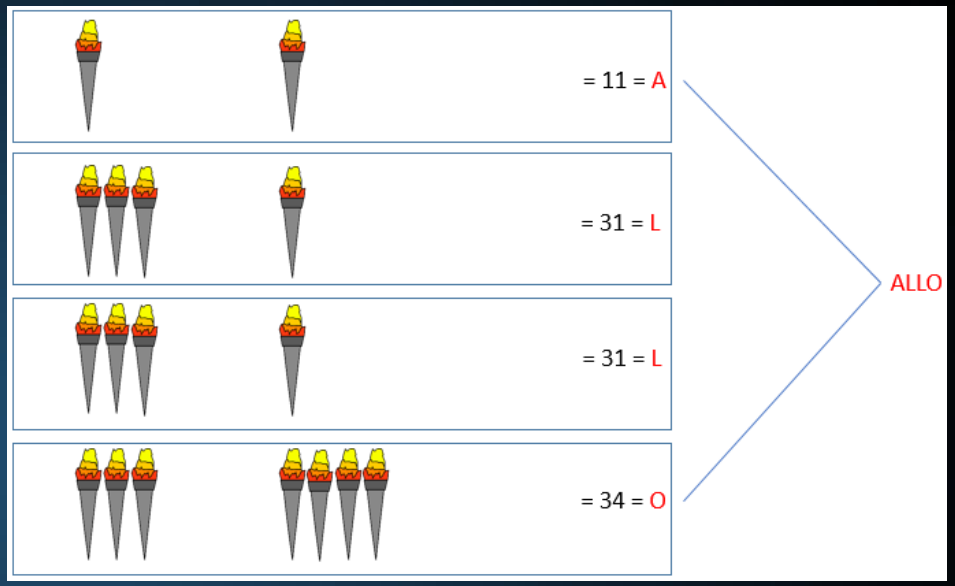
- Premier procédé de chiffrement par substitution
- Système de transmission basé sur un carré de 25 cases avec possibilité d'agrandir a 36 pour ajouter des chiffres.

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

Avantages et utilisation

- Simple d'utilisation
- Le carré de Polybe a été utilisé, entre autres, pour aider la télégraphie mais également pour transmettre un message entre des bateaux sur de longues distances.

Ex avec les torches :



	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

Limites (pour la version de base)

- Les lettres restent dans le même ordre
- Confusion possible entre I et J (25 cases)
- Pas de chiffres
- Ni de caractères spéciaux comme l’espace, le point, la virgule,…
- Facilement déchiffrable

II. Les dérivés du carré de Polybe

II. Méthode de chiffrement ADFGVX

TÉLÉGRAMME CHIFFRÉ

Le radiogramme de la victoire, le premier message Allemand utilisant le chiffrement ADFGVX décrypté par les français

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

Texte clair	o	b	j	e	c	t	i	f	a	r	r	a	s	1	5	h	2	8
Texte chiffré intermédiaire	AF	DV	AX	VD	AA	DF	FA	AG	FF	XD	XD	FF	FX	AD	DG	GV	FG	FV

M	A	R	C	E	L
A	F	D	V	A	X
V	D	A	A	D	F
F	A	A	G	F	F
X	D	X	D	F	F
F	X	A	D	D	G
G	V	F	G	F	V

A	C	E	L	M	R
F	V	A	X	A	D
D	A	D	F	V	A
A	G	F	F	F	A
D	D	F	F	X	X
X	D	D	G	F	A
V	G	F	V	G	F

FDADX VVAGD DGADF FDFXF FFGVA VFXFG DAAXA F

III.Le carré de Polybe est un chiffrement similaire a d'autre chiffrement par substitution :

Une Substitution c'est quoi ?

La substitution consiste effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial. La complexité des systèmes à substitutions dépend de trois facteurs :

- la composition spécifique de l’alphabet utilisé pour chiffrer ou pour communiquer,
- le nombre d’alphabets utilisés dans le cryptogramme,
- la manière spécifique dont ils sont utilisés.

Substitution simple ou monoalphabétique :

Exemple : texte en clair = «NON JE NE SUIS PAS FOU»
texte chiffré(***avec 5 divisions***) = «ABAWR ARFHV FCNFS BH»

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
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

dictionnaire ROT13

Substitution Homophonique :

Exemple : texte en clair = « CHANGEONS LES MENTALITES FRANCAISES »
texte chiffré = «  »

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
																									

dictionnaire de substitution homophonique

Substitution par polygrammes :

Example : texte en clair = « POUR LA LEGALISATION DE LA CRYPTO »
texte chiffré = « CESLASOCOCROCOQUIPIKASLEKUSS »
(sans division)

Fig 1.12 Substitution par polygrammes

Sitographie

_ https://www.apprendre-en-ligne.net/crypto/subst/adfgvx.html

_http://mathweb.free.fr/crypto/debvingt/adfgvx.php3

_https://fr.wikipedia.org/wiki/Chiffre_ADFGVX

_An Extended Version of the Polybius Cipher

_« Cryptography Worksheet — Polybius Square »

_ « La cryptologie. Peut-on réellement cacher des informations ? »

_ (en) Polybius Square

_http://nopb.chez.com/crypto2.html