Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber dev - CFA CCI Avignon
12 octobre 2023

Chiffrement par substitution

remplacer chaque symbole du texte clair par d'autres symboles sans modifier l'ordre

clair	M	E	S	S	A	G	E
chiffré	C_1	C_2	C_3	C_4	C_5	C_6	C_7

(alors que le chiffrement par transposition modifie l'ordre des symboles)

Chiffrement par substitution mono-alphabétique

lettre de l'alphabet du message $\longrightarrow$ autre lettre du même alphabet

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P

lettre de l'alphabet du message $\longrightarrow$ lettre d'un autre alphabet

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	β	δ	ε	φ	γ	η	λ	ζ	κ	μ	ν	ρ	π

Chiffrement par substitution mono-alphabétique

- Chiffrement par décalage - César
- ROT13
- Chiffre Atbash
- Chiffre Pigpen
- Carré de Polybe
- Chiffrement affine
- Cas général

Chiffrement par décalage - *shift cipher* - César

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Chiffrement par décalage - *shift cipher* - César

clé $k = 3$

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
rang	0	1	2	3	4	5	6	7	8	9	10	11	12
rang + k	3	4	5	6	7	8	9	10	11	12	13	14	15
chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
rang	13	14	15	16	17	18	19	20	21	22	23	24	25
rang + k	16	17	18	19	20	21	22	23	24	25	0	1	2
chiffré	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Carré de Polybe

	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

clair	A	B	C	D	E	F	G	H	I/J	K	L	M	N
chiffré	11	12	13	14	15	21	22	23	24	25	31	32	33

Code frappé

utilisé par prisonniers contre des tuyaux en métal ou contre les murs

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

- silences longs entre les lettres
- silences courts entre deux chiffres

Carré de Polybe avec clé

Exemple, avec la clé DEVINETTE:

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

Carré de Polybe avec chiffrement des chiffres et des symboles

	1	2	3	4	5	6	7	8
1	A	B	C	D	E	F	G	H
2	I	J	K	L	M	N	O	P
3	Q	R	S	T	U	V	W	X
4	Y	Z	0	1	2	3	4	5
5	6	7	8	9		!	"	#
6	$	%	&	‘	(	)	*	+
7	,	-	.	/	:	;	<	=
8	>	?	@	[	\	]	^	_

Carré de Polybe

	1	2	3	4	5
1	A 0	B 1	C 2	D 3	E 4
2	F 5	G 6	H 7	I/J 8	K 9
3	L 10	M 11	N 12	O 13	P 14
4	Q 15	R 16	S 17	T 18	U 19
5	V 20	W 21	X 22	Y 23	Z 24

clair	A	B	C	D	E	F	G	H	I/J	K	L	M	N
rang	0	1	2	3	4	5	6	7	8/9	10	11	12	13
numéro case	0	1	2	3	4	5	6	7	8	9	10	11	12
chiffré	11	12	13	14	15	21	22	23	24	25	31	32	33

Carré de Polybe

	1	2	3	4	5
1	A 0	B 1	C 2	D 3	E 4
2	F 5	G 6	H 7	I/J 8	K 9
3	L 10	M 11	N 12	O 13	P 14
4	Q 15	R 16	S 17	T 18	U 19
5	V 20	W 21	X 22	Y 23	Z 24

```
numero = ord(letter) - ord('A')
if numero > 8:
        numero = numero - 1
```

Carré de Polybe

	1	2	3	4	5
1	A 0	B 1	C 2	D 3	E 4
2	F 5	G 6	H 7	I/J 8	K 9
3	L 10	M 11	N 12	O 13	P 14
4	Q 15	R 16	S 17	T 18	U 19
5	V 20	W 21	X 22	Y 23	Z 24

```
row = (n // 5) + 1
col = (n  % 5) + 1
```