Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber2 dev - CFA CCI Avignon

20 novembre 2023

Rappels: chiffrements par substitution mono-alphabétique

une lettre de l'alphabet d'origine est toujours remplacée par la même lettre ou le même symbole

- Chiffrement par décalage - César - ROT13 - ROT47
- Chiffre Atbash, Atbah, Wolseley
- Chiffre Pigpen
- Carré de Polybe
- Chiffrement affine
- Cas général

Chiffrement par substitution poly-alphabétique: principe

poly-alphabétique: plusieurs alphabets.

une lettre correspond à plusieurs lettres selon sa position

A peut être remplacé par M ou P ou D

Chiffrement par substitution poly-alphabétique

Chiffre de Vigenère

Chiffre de Beaufort

Chiffre de Hill

Enigma

Chiffre de Vigenère

Blaise de Vigenère - XVI° siècle - 1586

Exemple: on chiffre le mot MESSAGE avec la clé KEY

clé	K	E	Y	K	E	Y	K
message clair	M	E	S	S	A	G	E
rang lettre du message	12	4	18	18	0	6	4
rang lettre de la clé	10	4	24	10	4	24	10
somme rangs	22	8	42	28	4	30	14
réduction modulo 26	22	8	16	2	4	4	14
message chiffré	W	I	Q	C	E	E	O

Chiffre de Vigenère

TABLE DE VIGENERE

Texte clair

Clé utilisée	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	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
N	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
O	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	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Chiffre de Beaufort

variante du chiffre de Vigenère.

on soustrait le message clair de la clé.

Exemple: on chiffre le mot MESSAGE avec la clé KEY

clé	K	E	Y	K	E	Y	K
message clair	M	E	S	S	A	G	E
rang lettre de la clé	10	4	24	10	4	24	10
rang lettre du message	12	4	18	18	0	6	4
différence rangs	-2	0	6	-8	4	18	6
réduction modulo 26	24	0	6	18	4	18	6
message chiffré	Y	A	G	S	E	S	G

Chiffre de Beaufort

particularité:
si on chiffre deux fois un message, on retrouve le message original

$$
\begin{aligned}
C &\equiv K - M \pmod{26} \\
C' &\equiv K - C \pmod{26} \\
C' &\equiv K - (K - M) \pmod{26} \\
C' &\equiv M \pmod{26}
\end{aligned}
$$

Chiffre de Beaufort - variante allemande

on soustrait la clé au message clair.

clé	K	E	Y	K	E	Y	K
message clair	M	E	S	S	A	G	E
rang lettre du message	12	4	18	18	0	6	4
rang lettre de la clé	10	4	24	10	4	24	10
différence rangs	2	0	-6	8	-4	-18	-6
réduction modulo 26	2	0	20	8	22	8	20
message chiffré	C	A	U	I	W	I	U

Chiffre de Vigenère

attaque par analyse de fréquences possible si longueur de clé connue (et texte assez long et clé pas trop longue)

on regarde les sous-chiffrés

Exemple: clé de longueur 3

ZUATIGXOYDLFWHUERJXOYDUKHGBKEVXRYTGDUPFKEVOFN

sous-chiffré 1: ZTXDWEXDHKXTUKO chiffré avec K
sous-chiffré 2: UIOLHROUGERGPEF chiffré avec E
sous-chiffré 3: AGYFUJYKBVYDFVN chiffré avec Y

Problème: trouver la longueur de la clé?

Chiffre de Vigenère

Test de Kasiski: 1863

Exemple (wikipedia):

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUD**WUU**MBSVLPS
NCMUEKQCTESWR**EEK**OYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTD**WXIZA**
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGR**WUU**NEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSH**NUOCZGM**RUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFST**NUOCZGMDOEOYEEK**CPJR
GPMURSKHFRSEIUEVGOYC**WXIZAYG**OSAANY**DOEOY**JLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVID**GMU**CGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
W**GMU**SWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

		Longueurs de clef possibles (diviseurs de la distance)			
Séquence répétée	Distance entre les répetitions	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

La clé est probablement de longueur 5.

Chiffre de Vigenère

William F. Friedman: 1920

Indice de coïncidence

probabilité d'obtenir deux lettres identiques lorsqu'on tire simultanément deux lettres au hasard dans le texte

Chiffre de Vigenère

n_i nombre d'occurence de la lettre de rang i dans le texte chiffré
n est la longueur du texte chiffré

$$I = \sum_{i=0}^{25} \frac{n_i(n_i - 1)}{n(n-1)}$$

texte aléatoire: I = 0.0385
texte français I = 0.0746 environ