Introduction à la cryptologie

O. FINOT

Lycée S^t Vincent de Paul

31 mai 2016

Sommaire

Introduction

Historique

- Utilisé depuis toujours
- Cacher, dissimuler des informations essentielles / confidentielles

Introduction

Historique

- Utilisé depuis toujours
- Cacher, dissimuler des informations essentielles / confidentielles

$\Rightarrow$ Cryptologie

Introduction

Historique

- Utilisé depuis toujours
- Cacher, dissimuler des informations essentielles / confidentielles

$\Rightarrow$ Cryptologie

Aujourd'hui : Sur internet

- Informations confidentielles
- Impôts
- Paiements en ligne

Introduction

Historique

- Utilisé depuis toujours
- Cacher, dissimuler des informations essentielles / confidentielles

$\Rightarrow$ Cryptologie

Aujourd'hui : Sur internet

- Informations confidentielles
- Impôts
- Paiements en ligne

$\Rightarrow$ Données ne doivent pas circuler "en clair"

Sommaire

Sommaire

Définitions I

Cryptologie

- Science des messages secrets
- Cryptographie vs. Cryptanalyse

Définitions I

Cryptologie

- Science des messages secrets
- Cryptographie vs. Cryptanalyse

Cryptographie

"Art" de transformer un message pour le rendre illisible

Définitions I

Cryptologie

- Science des messages secrets
- Cryptographie vs. Cryptanalyse

Cryptographie

"Art" de transformer un message pour le rendre illisible

Cryptananlyse

"Art" de rendre un message transformé lisible

Définitions II

Chiffrer / Crypter

Transformer un message

Définitions II

Chiffrer / Crypter

Transformer un message

Décrypter

Rendre un message lisible

Sommaire

Sommaire

Principe des chiffrements par substitution

- Chaque lettre remplacée par une autre
- Toujours la même lettre d'arrivée pour une lettre donnée

Sommaire

Chiffre de César

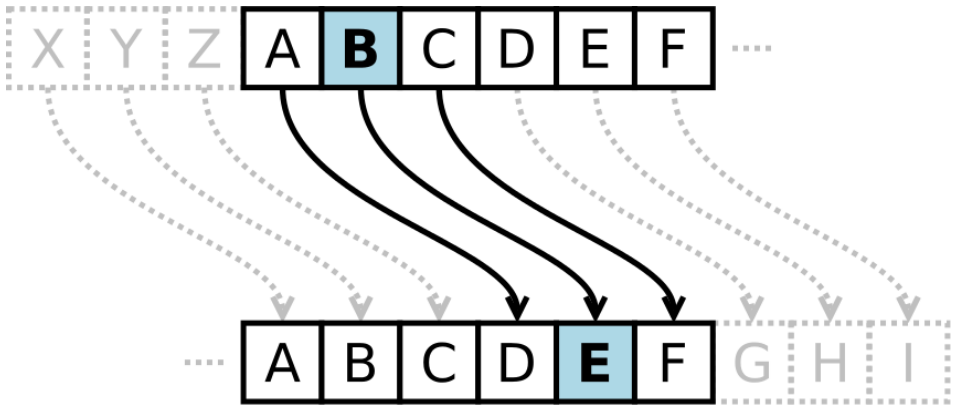
Présentation

Historique

- Utilisé par César
- Transmission des ordres à ses généraux

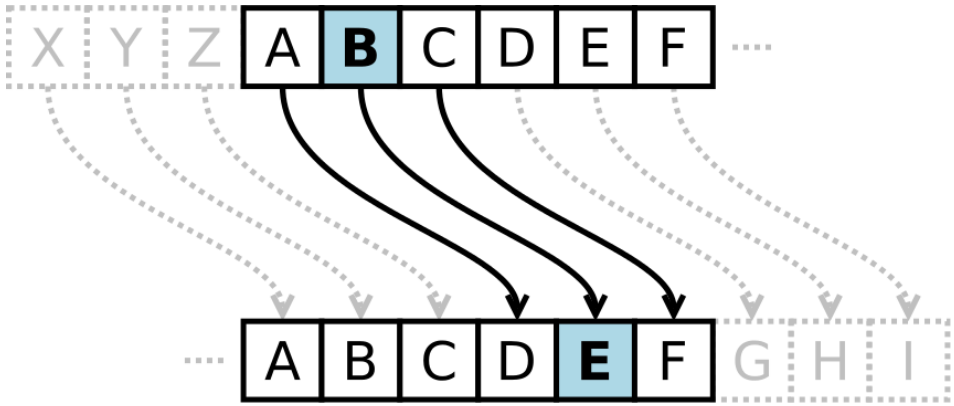
Principe

- Choix d'une distance (26 possibilités)
- Remplacement d'une lettre par celle qui se trouve à la distance choisie



Chiffre de césar

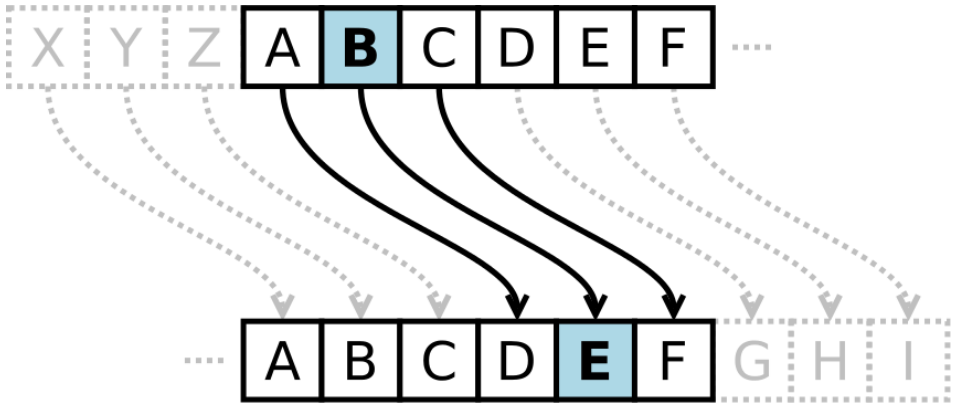
Exemple avec une distance de 3



- ALEA JACTA EST

Chiffre de césar

Exemple avec une distance de 3



- ALEA JACTA EST

$\Rightarrow$ DOHD MDFWD HVW

Substitution "aléatoire"

Principe

- Pas de distance fixe
- Choix d'une lettre de remplacement pour chaque lettre d'origine

Exemple de substitution

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- AZERTYUIOPQSDFGHJKLMWXCVBN

Substitution "aléatoire"

Principe

- Pas de distance fixe
- Choix d'une lettre de remplacement pour chaque lettre d'origine

Exemple de substitution

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- AZERTYUIOPQSDFGHJKLMWXCVBN

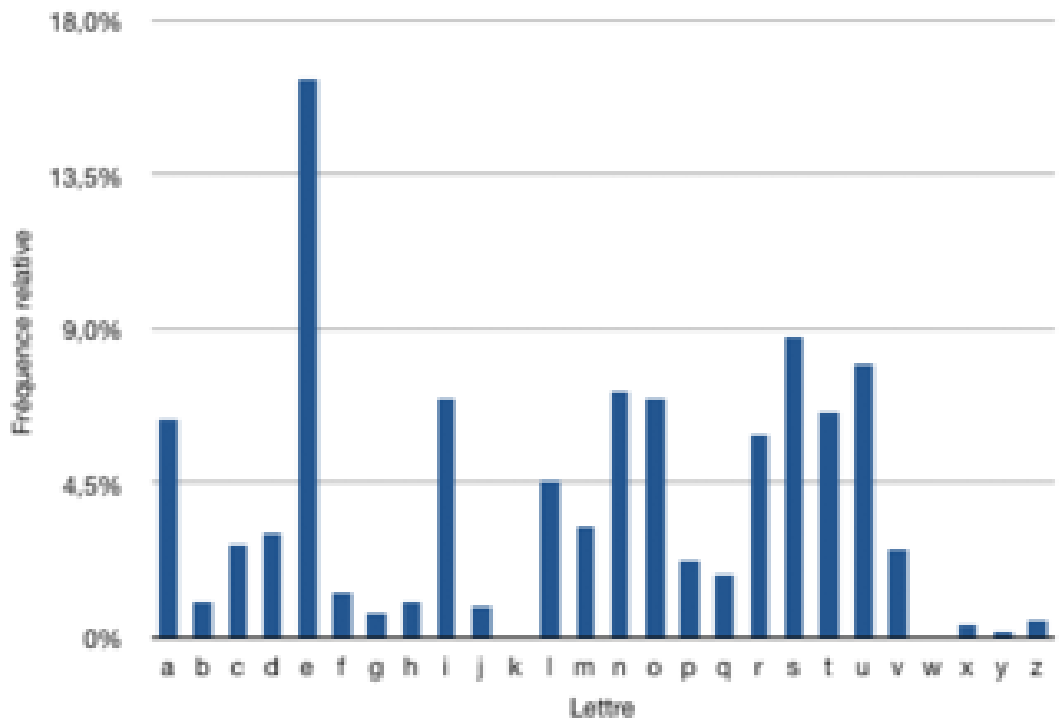
$\Rightarrow$ SUBSTITUTION devient LWZLMOMWMOGF

Sommaire

Décryptage

Analyse fréquentielle

- Repérer les lettres qui apparaissent le plus
- En français : E



1

1. Source wikipédia

Avantages / Inconvénients

Avantages

- Faciles à comprendre
- Faciles à utiliser

Incovénients

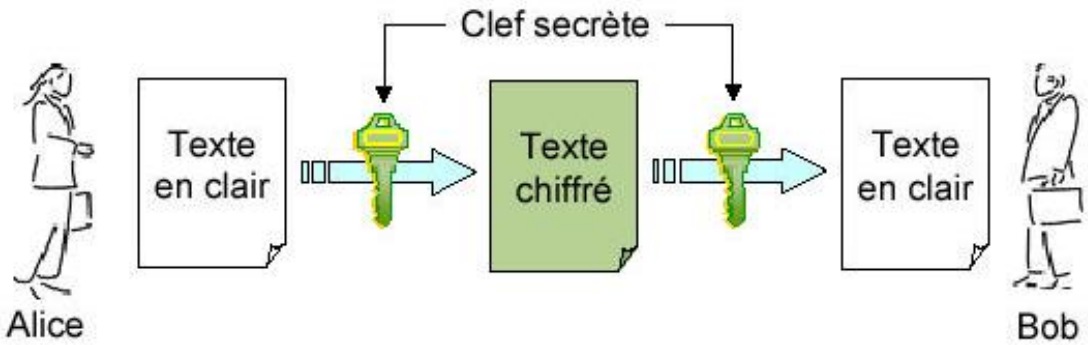
- Faciles à casser

Sommaire

Sommaire

Principe du chiffrement symétrique

- Une clé pour chiffrer un message
- La même pour décrypter



Chiffre de Vigénère

Principe

- Choix d'une clé
- Correspondance entre le texte en clair et la clé

	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
Y	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	X
Z	Z	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

Bilan

Avantage

- Très sûr (si clé assez longue)

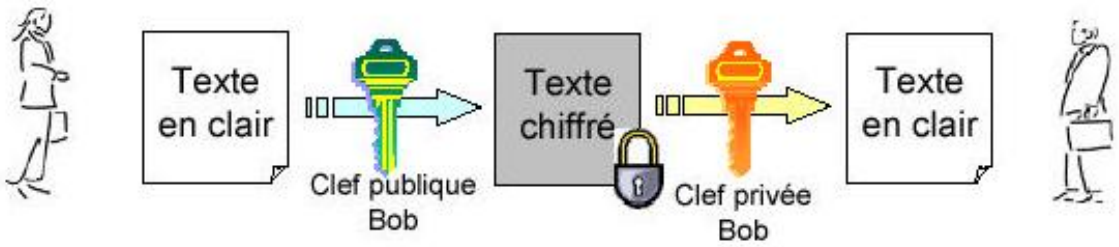
Inconvénient

- Échange de la clé

Sommaire

Principe du chiffrement asymétrique

- 2 clés
- 1 clé publique distribuée à tout le monde
- 1 clé privée gardée pour soi



Sommaire