

# Introduction à la cryptographie

O. FINOT

Lycée S<sup>t</sup> Vincent de Paul

2 juin 2016

# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

## IV. Chiffrements par clé

## V. Conclusion

# Introduction

## Historique

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

# Introduction

## Historique

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

⇒ Cryptologie

# Introduction

## Historique

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

⇒ Cryptologie

## Aujourd'hui : Sur internet

- Informations confidentielles
- Impôts
- Paiements en ligne

# Introduction

## Historique

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

⇒ Cryptologie

## Aujourd'hui : Sur internet

- Informations confidentielles
- Impôts
- Paiements en ligne

⇒ Données ne doivent pas circuler "en clair"

# Sommaire

I. Introduction

II. Vocabulaire

III. Chiffrements par substitution monoalphabétique

IV. Chiffrements par clé

V. Conclusion

# Sommaire

I. Introduction

II. Vocabulaire

III. Chiffrements par substitution monoalphabétique

IV. Chiffrements par clé

V. Conclusion



# 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

## Cryptanalyse

"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

I. Introduction

II. Vocabulaire

III. Chiffrements par substitution monoalphabétique

IV. Chiffrements par clé

V. Conclusion

# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Principe des chiffrements par substitution

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





# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Substitution "aléatoire"

## Principe

- Choix d'une lettre de remplacement pour chaque lettre d'origine

## Exemple de substitution

- SUBSTITUTION

# Substitution "aléatoire"

## Principe

- Choix d'une lettre de remplacement pour chaque lettre d'origine

## Exemple de substitution

- SUBSTITUTION

⇒ MRXMNCNRNCDA

# Chiffre de César

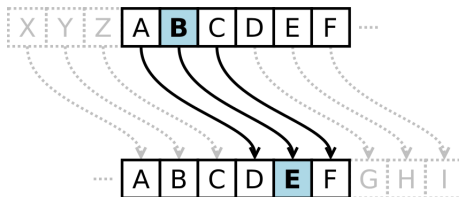
## Présentation

### Historique

- Utilisé par César
- Transmission des ordres à ses généraux

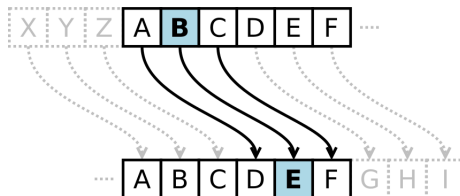
### Principe

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



# Chiffre de César

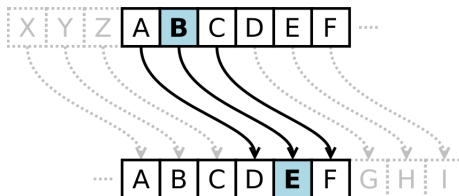
Exemple avec une distance de 3



- ALEA JACTA EST

# Chiffre de César

Exemple avec une distance de 3



• ALEA JACTA EST

⇒ DOHD MDFWD HVW

# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

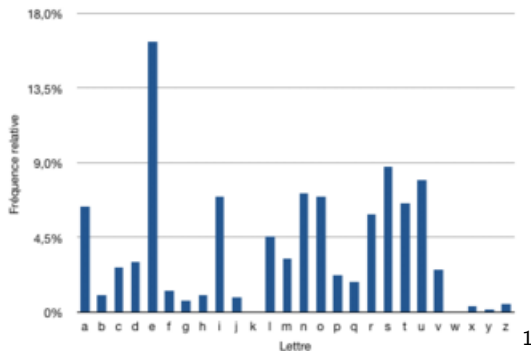
1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Décryptage

## Analyse fréquentielle

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



### 1. Source wikipédia



# Avantages / Inconvénients

## Avantages

- Nombre important de permutations
- Faciles à comprendre
- Faciles à utiliser

## Inconvénients

- Faciles à casser

# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Substitution monoalphabétique

En utilisant la substitution suivante :

## Chiffrer

La Cigale ayant chanté tout l'été Se trouva fort dépourvue Quand la bise fut venue

## Décrypter

RA GYNCN QDMYWR U'W MRZZCN GDRQ ZWCQY ZQYUCQ  
I'KYQXY KWRNY YN NDRN IY GQY YN IYM HDRV MWRIYM LRC  
EKWANYAN WRMMC.

# Chiffre de César

## Chiffrer en utilisant une distance de 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

## Déchiffrer

PDLWU HFRUE HDXVX UXQDU EUHSH UFKHW HQDLW HQVRQ  
EHFXQ IURPD JHPDL WUHUH QDUGS DUORG HXUDO OHFKH  
OXLWL QWSHX SUHVF HODQJ DJHHW ERQMR XUPRQ VLHXU  
GXFRU EHDXT XHYRX VHWHV MROLT XHYRX VPHVH PEOHC  
EHDX

# Sommaire

I. Introduction

II. Vocabulaire

III. Chiffrements par substitution monoalphabétique

IV. Chiffrements par clé

V. Conclusion

# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

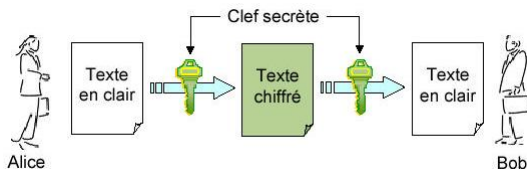
## IV. Chiffrements par clé

1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Principe du chiffrement symétrique

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



# Chiffre de Vigenère

## 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

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

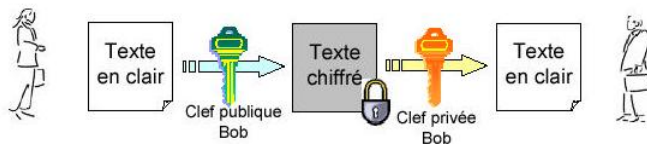
1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Principe du chiffrement asymétrique

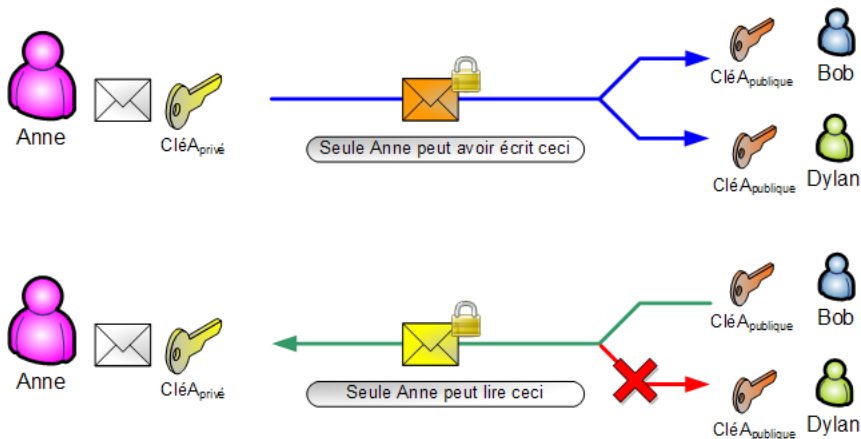
## Principe

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



# Signature numérique

Un chiffrement asymétrique peut aussi être utilisé pour signer numériquement un document.



# Sommaire

## I. Introduction

## II. Vocabulaire

## III. Chiffrements par substitution monoalphabétique

1. Principe
2. Exemples
3. Bilan
4. Exercices

## IV. Chiffrements par clé

1. Chiffrements symétriques
2. Chiffrements Asymétriques
3. Exercices

## V. Conclusion

# Vigénère

Chiffrer en utilisant la clé : MUSIQUE

j'adore ecouter la radio toute la journee

Décrypter en utilisant la clé : SECRET

UIELZ JYJIO IEXBF XTSUY BLPCR FXBGR FITPX MRGGC ILWTT  
IJIGL IIIEI KSPGQ VRMKS WWCEY GVOIU YGESV SLHNF IRLIE LW

# Sommaire

I. Introduction

II. Vocabulaire

III. Chiffrements par substitution monoalphabétique

IV. Chiffrements par clé

V. Conclusion

# Conclusion

- Présentation de notions de cryptographie
- Chiffrements par substitution
- Chiffrement par clé
- Meilleure compréhension