Defi

Décoder le message suivant

Cjfoupu mft wbdbmdft qmvt rvf rvfmrvft ifvsft b ufojs bwbou mb mjcfsbujpo.

Defi

Décoder le message suivant

Cjfoupu mft wbdbmdft qmvt rvf rvfmrvft ifvsft b ufojs bwbou mb mjcfsbujpo.

Décoder le message suivant

Bientôt les vacances plus que quelques heures à tenir avant la libération.

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"

Principe des chiffrements par substitution

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

Chiffre de César

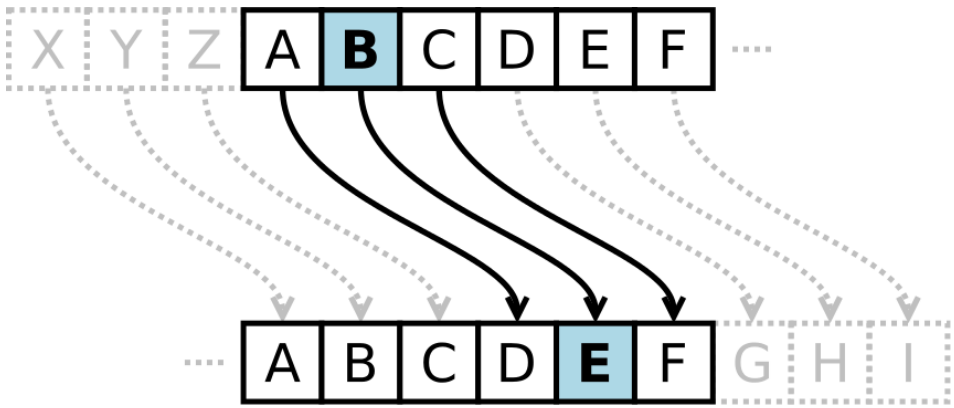
Présentation

Historique

- Utilisé par César
- Transmission des ordres à ses généraux

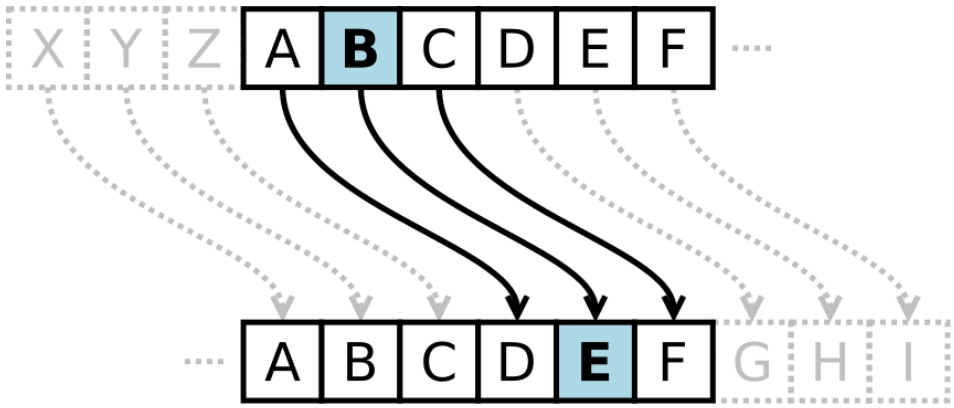
Principe

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



Chiffre de césar

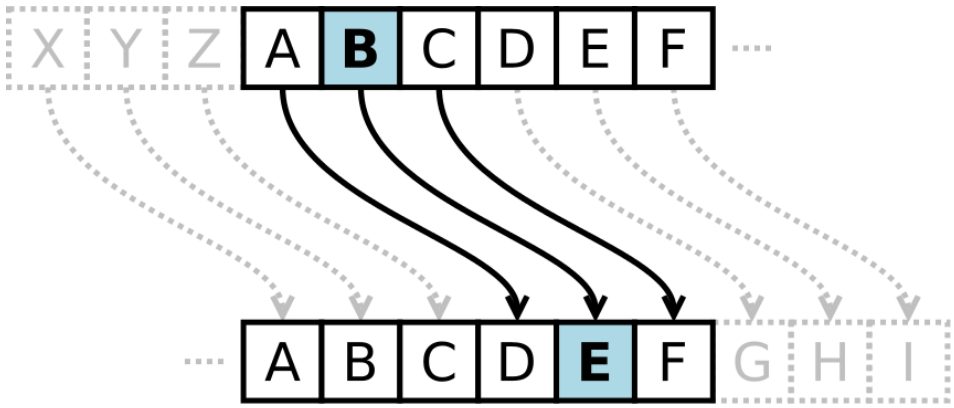
Exemple avec une distance de 3



- ALEA JACTA EST

Chiffre de césar

Exemple avec une distance de 3



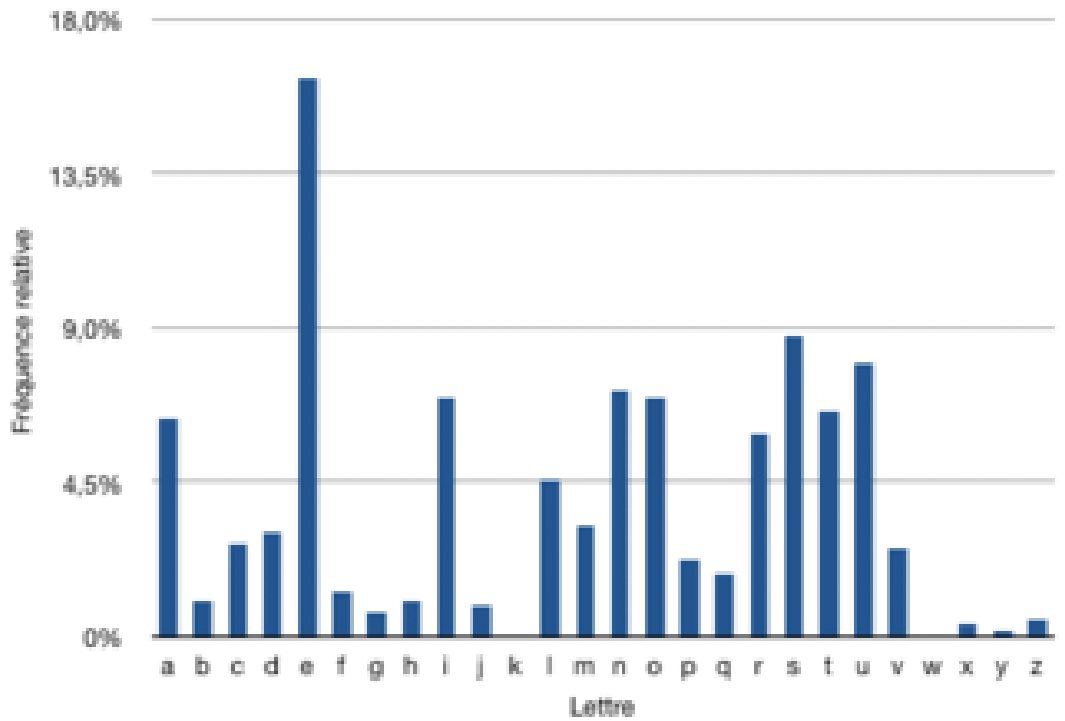
- ALEA JACTA EST

$\Rightarrow$ DOHD MDFWD HVW

Décryptage

Analyse fréquentielle

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



1

1. Source wikipédia

Avantages / Inconvénients

Avantages

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

Incovénients

- Faciles à casser

Chiffre de César

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

Substitution monoalphabétique

En utilisant la substitution suivante :

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

Chiffrer

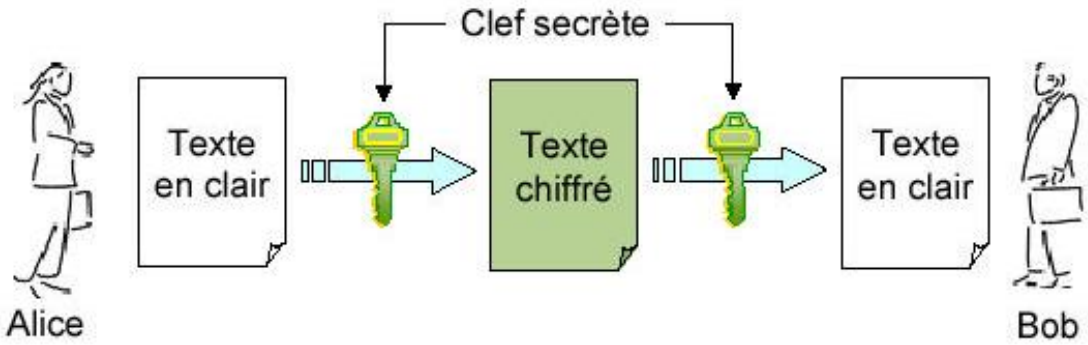
La Cigale ayant chanté tout l'été Se trouva fort dépourvue Quand la bise fut venue

Déchiffrer

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

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)

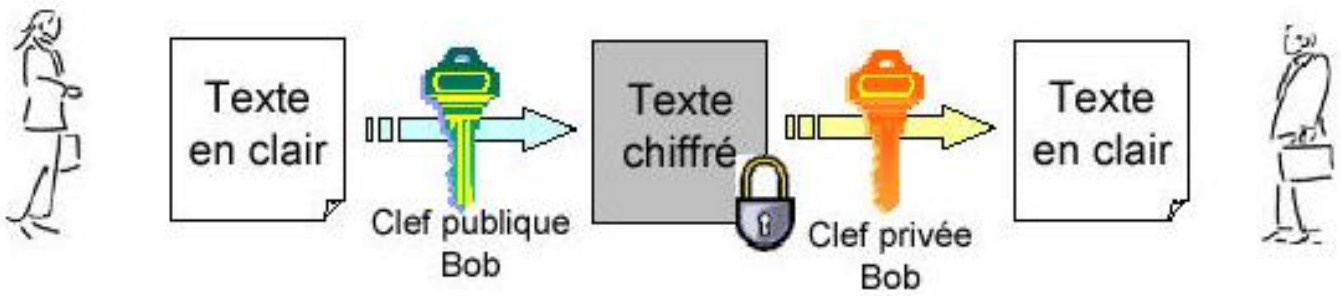
Inconvénient

- Échange de la clé

Principe du chiffrement asymétrique

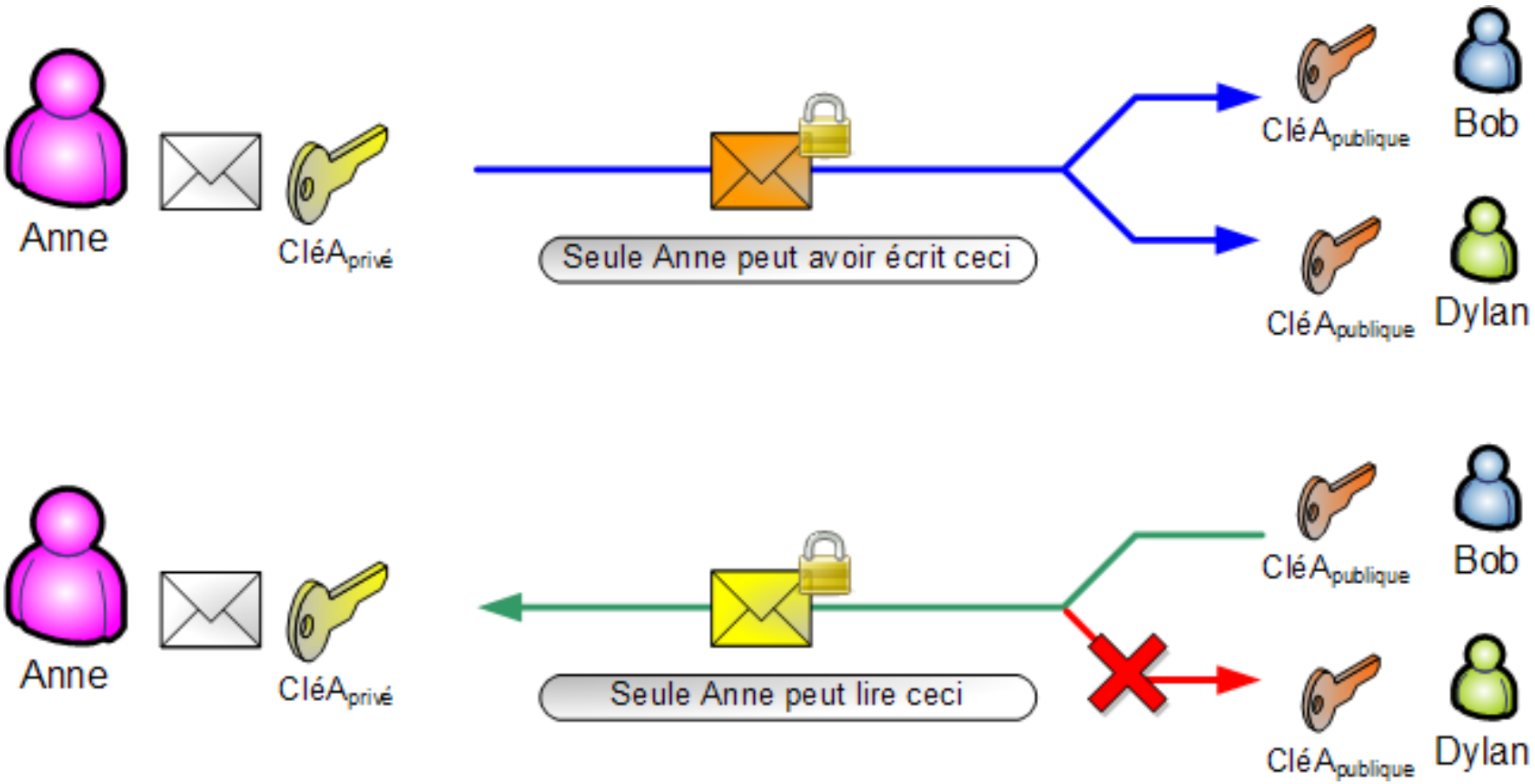
Principe

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



Signature numérique

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



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

Conclusion

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