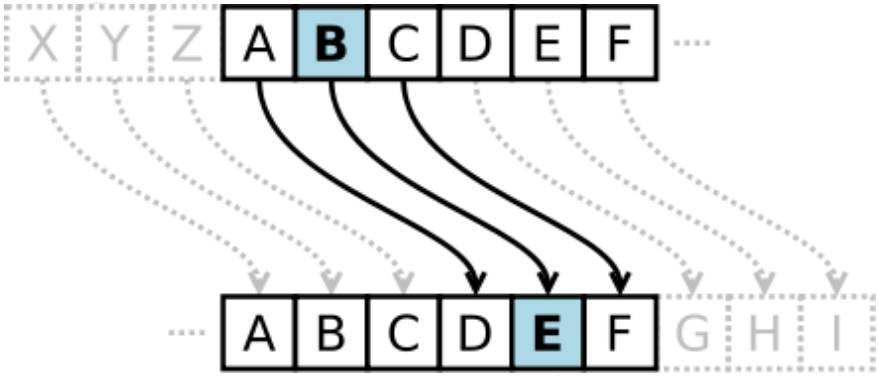
# Le chiffre de César

*MANZANO Aymeric*
*RENARD Julien*
*SENINCK Maxence*

# Présentation du chiffre

-Origine du 1er chiffre: -3000 av JC --->

-Méthode de César:----->



# Chiffrage

→ Auteur du texte chiffre son texte avec une clé “n”.

→ Texte codé.

→ Destinataire déchiffre le texte.

Formule de chiffrement:

$C_n(x)= (x+n) \bmod 26.$

C= chiffrement

x= lettre

n= décalage

Formule de déchiffrement:

$D_n(x)= (x-n) \bmod 26.$

D= déchiffrement

x= lettre

n= décalage

# Déchiffrage

Déchiffrage:
→ connaître la clé (soit le décalage des lettres)
→ appliquer la clé à chaque lettres du texte à déchiffrer

→ Exemple: Avec un décalage de + 3 lettres.

**OHV GLIIHUHQWHV PHWKRGHV GH FKLIIUHPHQW**

**YXHV HQ LVQ**

Ce qui nous donne*:*

**LES DIFFERENTES METHODES DE CHIFFREMENT VUES EN ISN**

# Décryptage

*Très simple à décrypter, seulement 26 décalages possibles.

Décryptage ⇨ Déchiffrage

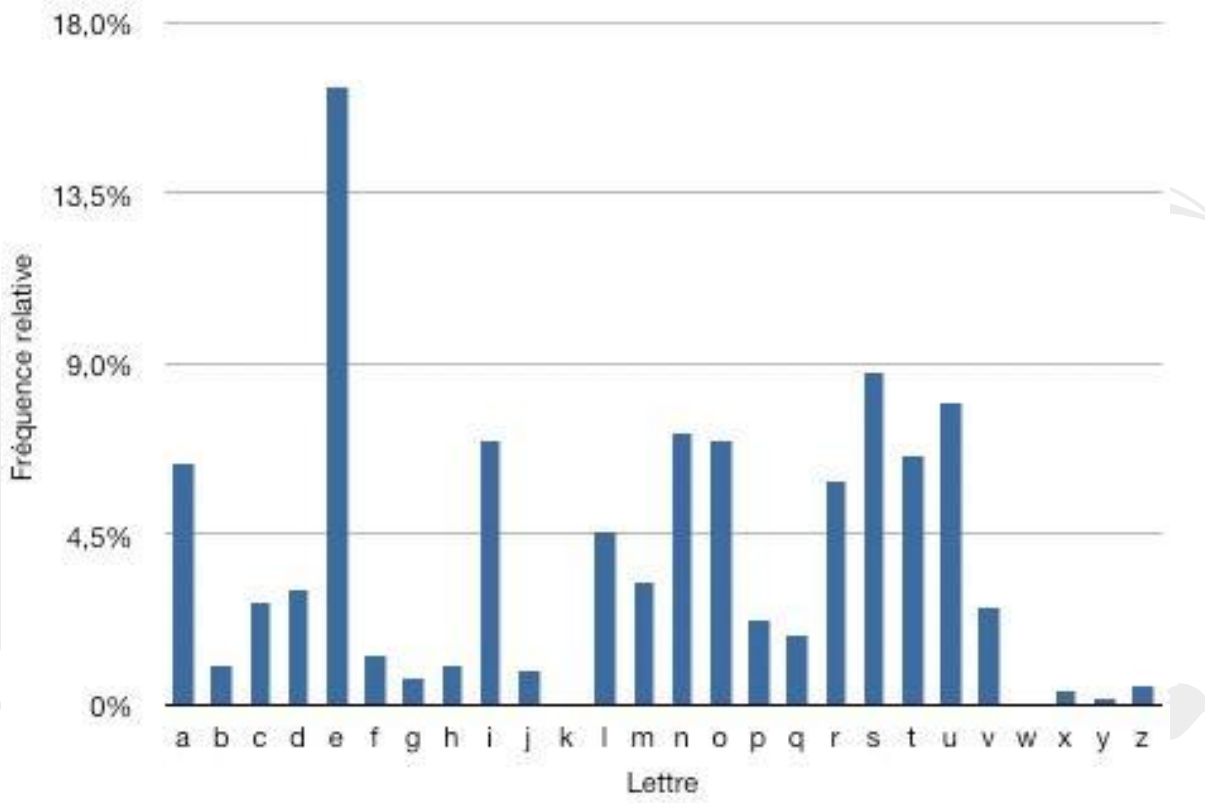
En effet, décrypter signifie que le hacker potentiel ne connaît pas notre clé de chiffrement. Il doit donc faire sans pour déchiffrer notre code à tout prix.

2 façons principales pour venir à bout du chiffre de César:

*Méthode d'utilisation de la fréquence d'apparition des lettres.

*Méthode d'attaque exhaustive.

# *Méthode d'utilisation de la fréquence d'apparition des lettres:




**LES DIFFERENTES METHODES DE CHIFFREMENT VUES EN ISN**

*Ce qui nous donne:*

**OHV GLIIHUHQWHV PHWKRGHV GH FKLIIUHPHQW YXHV HQ LVQ**

# La première étape consiste à compter le nombre de fois que sortent chaque lettres.

| | | |
|---|---|---|
| O=1 | Q=4 | K=2 |
| H=10 | U=2 | R=1 |
| V=5 | I=4 | Y=1 |
| G=2 | W=3 | X=1 |
| L=3 | P=2 | |

**LES DIFFERENTES METHODES DE CHIFFREMENT VUES EN ISN**

*Notre texte appararaît !*

**O***ES* **GLII***E***U***EN***W***ES*** **P***E***WKRG***ES*** **G***E*** **FKLIIU***E***P***EN***W YX***E***V H***N*** **L***SN***

*Il faut ainsi continuer jusqu'à trouver les différentes combinaisons pour chaque lettre.*

***Méthode d'attaque exhaustive:***

La méthode d'attaque exhaustive, ou Brute-force, consiste à tester toutes les combinaisons possibles pouvant être utilisées dans le chiffrement. Très longue et difficile à utiliser sur papier, elle peut toutefois se révéler très redoutable si le hacker l'utilise grâce à un programme qui testera toutes les combinaisons en un temps potentiellement record. Plus le programme sera complexe, plus il sera potentiellement efficace.

Cette méthode, plus souvent utilisée grâce à un programme, va tester les 26 décallages de lettre possible pour ensuite en analyser les fréquences d'apparitions des lettres si nous n' obtenons pas une phrase convenable (voir 1ere méthode.).

# Utilité, robustesse, actualité

Chiffre de César très facile à utiliser (chiffrage, déchiffrage et décryptage).

26 lettres dans l'alphabet → possibilité de trouver la clé.

France → "E" le plus utiliser …

# Sources et vocabulaire

www.primenumbers.net/Renaud/fr/crypto/Cesar.htm

http://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage

http://fr.wikipedia.org/wiki/Cl%C3%A9_de_chiffrement

http://tpe-messages-secrets.e-monsite.com/pages/la-cryptanalyse/l-analyse-du-chiffre-de-cesar-decouverte-par-al-kindi.html

# Merci pour votre compréhension