

Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

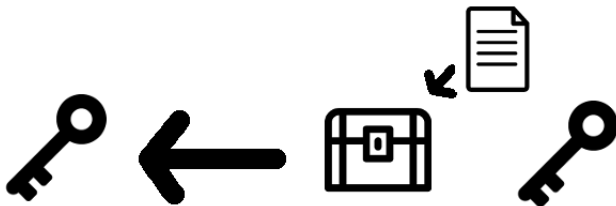
Mise en situation

- Cartes bleues
- Mail
- Transactions bancaires
- Chiffrement des données sensibles (militaires ou privées)

Un codage ultime?

Seul quelqu'un qui connaîtrait la clé pourrait décoder : est-ce réellement possible ?

Cryptographie symétrique : on a tous les deux une même clé.

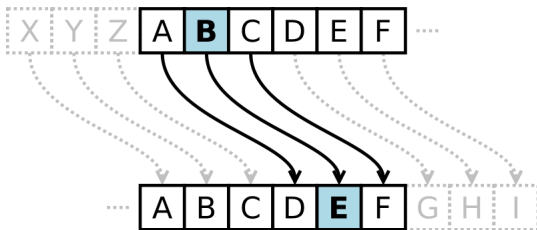


Exemple : chiffrement de César

Décalage constant.

$A \rightarrow B, B \rightarrow C, \dots$

$A \rightarrow C, B \rightarrow D, \dots$



Casser le code de César

26 décalages possibles.

Mot à décrypter : iravivqvqrpelcgv

jsbwjwrwrsqfmdhw	ktcxkxsxstrgneix
ludylytytushofjy	mvezmzuzuvtipgkz
nwfanavavwujqhla	oxgbobwbwxvkrimb
pyhpcxcxywlsjnc	qzidqdydyzxmtkod
rajerezeyaynulpe	sbkfsfafabzovmqf
tcigtgbgbcapwnrg	udmhuhchcdbqxosh
venivididecrypti	wfojwjejefdszquj
xgpkxkfkfgetarvk	yhqlylglghfubswl
zirmzmmhigvctxm	ajsnaninijhwduyn
bktobojojkiexvzo	clupcpkpklyfwap
dmvqdqlq mkzgbq	enwrermrmnlahycr
foxsfsnsnombizds	gpytgtotopncjaet
hqzuhupupqodkbfu	iravivqvqrpelcgv

Énumération des clés

Énumérer les clés possibles (décalages). Regarder tous les résultats.

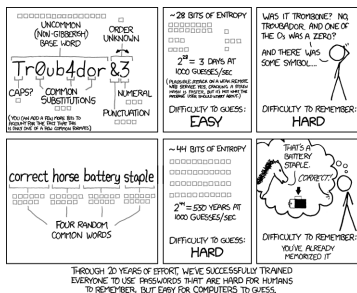
```
# caesar cipher  
  
word = "iravivqvqrpelcgv"  
  
for i in range(1,27):  
    for c in word :  
        print(chr(((ord(c)+i)-97)%26)+97), end=" "  
    print()
```

Ensemble de clés fini

Le calcul, c'est pas gratuit

Trop de clés \Rightarrow trop de calcul, trop de résultats

L'objectif n'est pas de créer un chiffrement incassable, mais un chiffrement qui soit trop coûteux à casser.



D'autres exemples

Hill

$$\begin{pmatrix} 0 & 1 & 0 \\ 3 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 9 \\ 5 \end{pmatrix}$$

Vigenere

M	E	S	S	A	G	E
C	L	E	C	L	E	C
O	P	W	U	L	K	G

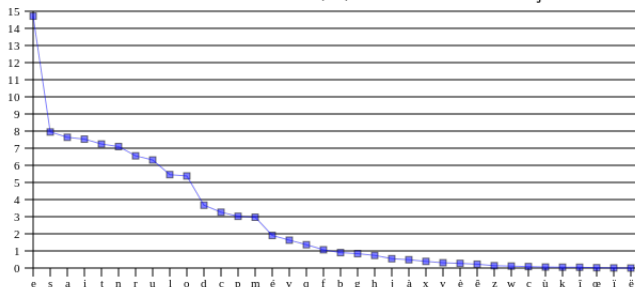
Trop de clés

Matrices 3×3 : 5429503678976

Matrices 10×10 :

314293064158293883017435778850162642728266998876247525637
417317539899590842010402346543259906970228933096407508161
1719197835869803511992549376

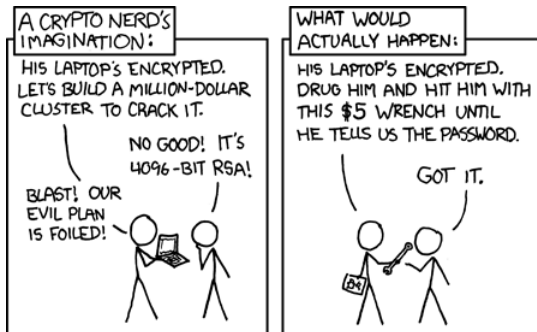
Distribution des lettres (%) dans un texte français



Clé publique, clé privée

Mise en situation

Schéma



GPG mail
sources des images