

Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

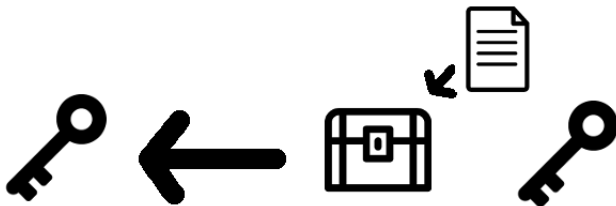
Mise en situation

- 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.

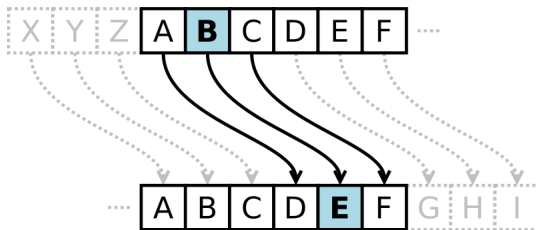


Exemple : chiffrement de César

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
nwfanaavavwujqhla	oxgbobwbwxvkrimb
pyhpcxcxywlsjnc	qzidqdydyzxmtdkod
rajerezeaynulpe	sbkfsfafabzovmqf
tcldgtgbgbcapwnrg	udmhuhchcdboxosh
venivididecrypti	wfojwjejefdszquj
xgpkxkfkfgetarvk	yhqlylglghfubswl
zirmzmhnhigvctxm	ajsnaninijhwduyn
bktobojojixevzo	clupcpkpklyjfwap
dmvqdqlqlmkzgbq	enwrermrmnlahycr
foxsfsnsnombizds	gpytgtotopncjaet
hqzuhupupqodkbfu	iravivqvqrpelcgv

Énumération des clés

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

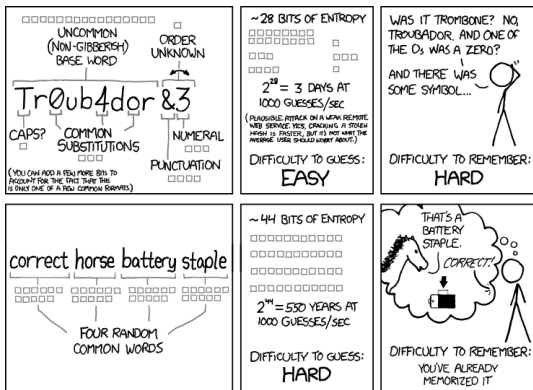
```
# caesar cipher  
  
word = "iravivqvqrpelcgv"  
  
for i in range(1,27):  
    for c in word :  
        print(chr(((ord(c)+i)-97)%26)+97), end=" "  
    print()
```

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.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS

D'autres exemples

Hill

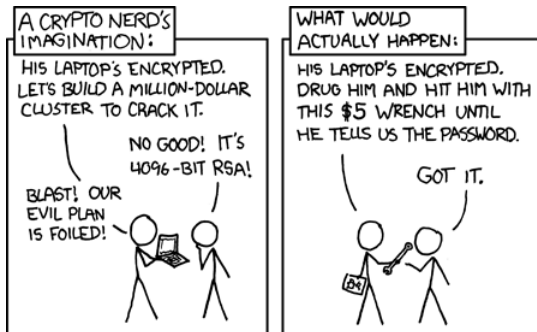
Vigenere

Chiffres pour matrices de Hill
Fréquences français

Clé publique, clé privée

Mise en situation

Schéma



GPG mail
sources des images