

# Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

# Mise en situation

- Cartes bleues
- Mail
- Transaction bancaires

# Un codage ultime ?

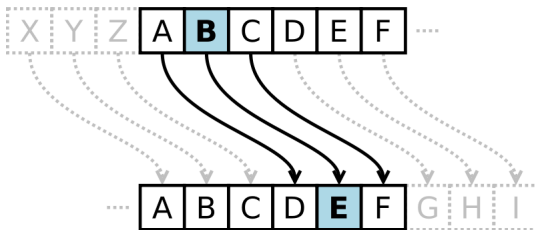
Seul quelqu'un qui connaîtrait la clé pourrait décoder.

# 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         | qzidqdydyzxmtdk  |
| rajerezeyaynulpe        | sbkfsfafabzovmqf |
| tcldgtgbgbcapwnrg       | udmhuhchcdboxosh |
| <b>venivididecrypti</b> | wfojwjejefdszquj |
| xgpkxkfkfgetarvk        | yhqlylglghfubswl |
| zirmzmmhigvctxm         | ajsnaninijhwduyn |
| bktobojojixevzo         | clupcpkpklyfwap  |
| dmvqdqlqmkzgbq          | enwrermrmnlahycr |
| foxsfsnsnombizds        | gpytgtotopncjaet |
| hqzuhupupqodkbfb        | iravivqvqrpelcgv |

# Énumération des clés

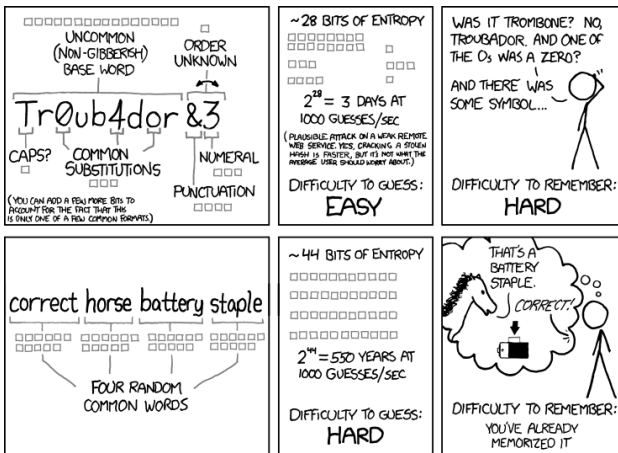
Énumérer les clés possibles (décalages). Regarder tous les résultats.

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

# Complexité

Le calcul, c'est pas gratuit.

Trop de clés -> trop de calcul, trop de résultats



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

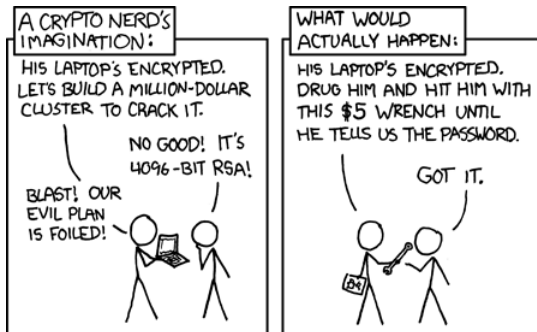
Vigenere

Chiffres pour matrices de Hill  
Fréquences français

Clé publique, clé privée

Mise en situation

## Schéma



GPG mail  
sources des images