Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

Mise en situation

Intérêt de la cryptographie

- Cartes bleues
- Mail
- Transaction bancaires

Un codage ultime ?

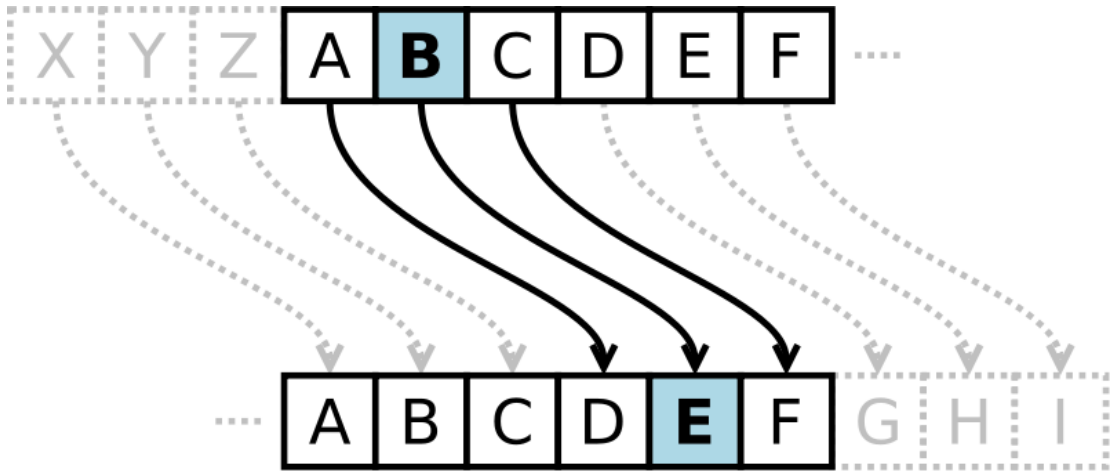
Seul quelqu'un qui connaitraît la clé pourrait décoder.

Exemple : chiffrement de César

Décalage constant.

$$A \to B, B \to C, \ldots$$

$$A \to C, B \to D, \ldots$$



Casser le code de César

26 décalages possibles.
Mot à décrypter : iravivqvqrpelcgv

jsbwjwrwrsqfmdhw	ktcxkxsxstrgneix
ludylytytushofjy	mvezmzuzuvtipgkz
nwfanavavwujqhla	oxgbobwbwxvkrimb
pyhcpcxcxywlsjnc	qzidqdydyzxmtkod
rajerezezaynulpe	sbkfsfafabzovmqf
tclgtgbgbcapwnrg	udmhuhchcdbqxosh
venivididecrypti	wfojwjejefdszquj
xgpkxkfkfgetarvk	yhqlylglghfubswl
zirmzmhmhigvctxm	ajsnaninijhwduyn
bktobojojkixevzo	clupcpkpkljyfwap
dmvqdqlqlmkzgxbq	enwrermrmnlahycr
foxsfsnsnombizds	gpytgtotopncjaet
hqzuhupupqodkbfu	iravivqvqrpelcgv

Énumération des clés

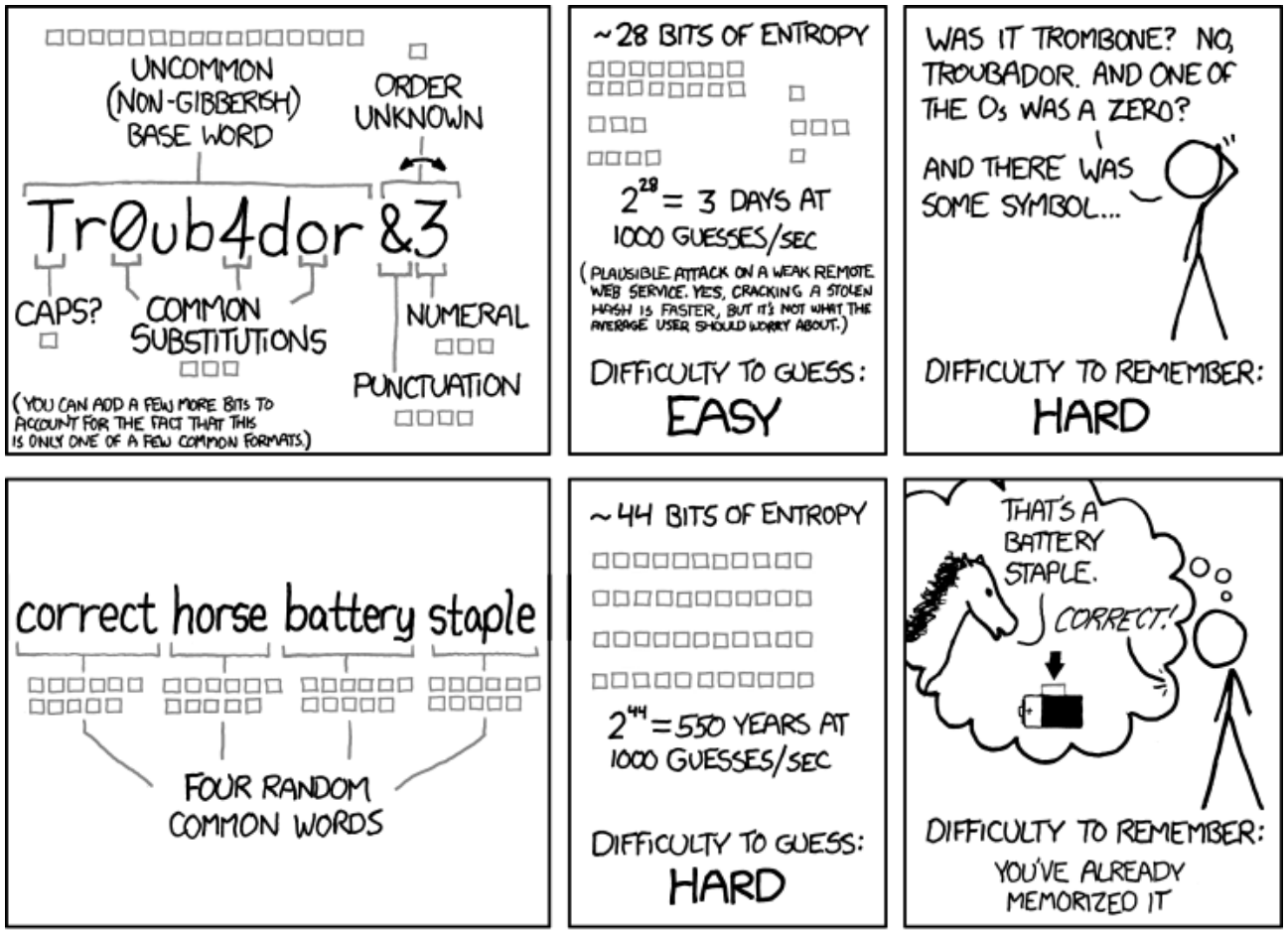
Énumérer les clés possibles (décalages). Regarder tous les résultats.

```
# caesar cipher

word = "iravivqvqrpelcgv"

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

    print()
```

Complexité

Le calcul, c'est pas gratuit.

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



D'autres exemples

Hill
Vigenere

Analyse fréquentielle

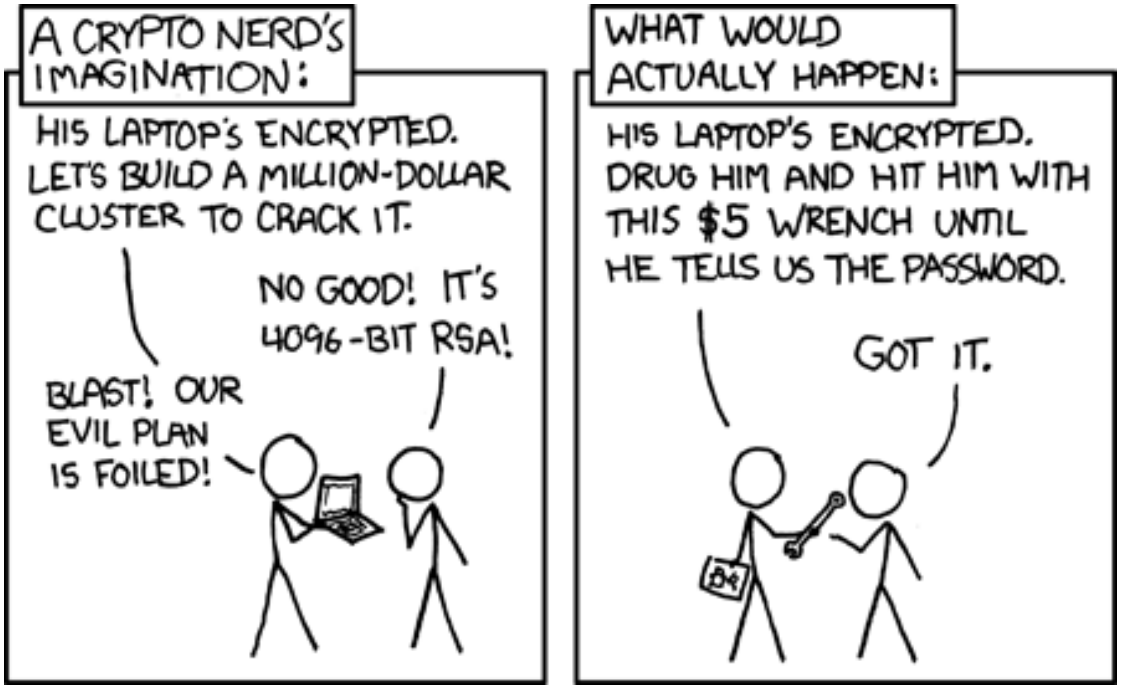
Chiffres pour matrices de Hill
Fréquences français

Cryptographie asymétrique

Clé publique, clé privée
Mise en situation

Schéma

Limites


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Ressources et idées

GPG mail
sources des images