

Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

Iseut souhaite envoyer des messages d'amour à Tristan, qui vit en Bretagne avec sa femme. Bien évidemment il ne faut pas que cette dernière puisse les lire, ce qui créerait une situation quelque peu inconfortable.

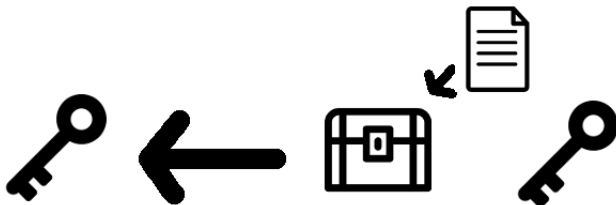
Comment faire pour s'assurer de pouvoir communiquer impunément ?

- 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.



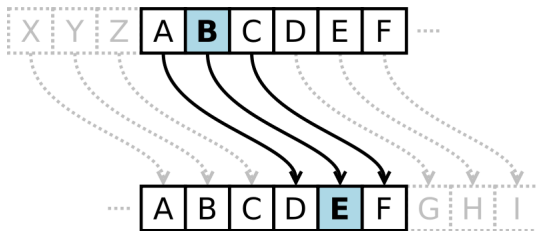
Source : simpleicon

Exemple : chiffrement de César

Décalage constant.

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

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



Source : Wikipedia

Casser le code de César

26 décalages possibles.

Mot à décrypter : iravivqvqrpelcgv

jsbwjwrwrsqfmdhw	ktcxkxsxstrgneix
ludylytytushofjy	mvezmzuzuvtipgkz
nwfanavavwujqhla	oxgbobwbwxvkrimb
pyhpcxcxywlsjnc	qzidqdydyzxmtdod
rajerezeyaynulpe	sbkfsfafabzovmqf
tcigtgbgbcapwnrg	udmhuhchcdboxosh
venivididecrypti	wfojwjejefdszquj
xgpkxkfkfgetarvk	yhqlylglghfubswl
zirmzmhnhgvcctxm	ajsnaninijhwduyn
bktobojojixevzo	clupcpkpklyfwap
dmvqdqlqlmkzgbq	enwrermrmnlahycr
foxsfsnsnombizds	gpytgtotopncjaet
hqzuhupupqodkbfb	iravivqvqrpelcgv

Énumération des clés

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

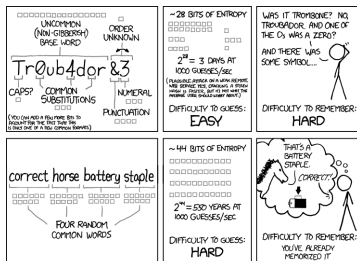
```
# caesar cipher  
  
word = "iravivqvqrpelcgv"  
  
for i in range(1,27):  
    for c in word :  
        print(chr(((ord(c)+i)-97)%26)+97), end=" "  
    print()
```

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.

Source : xkcd.com

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

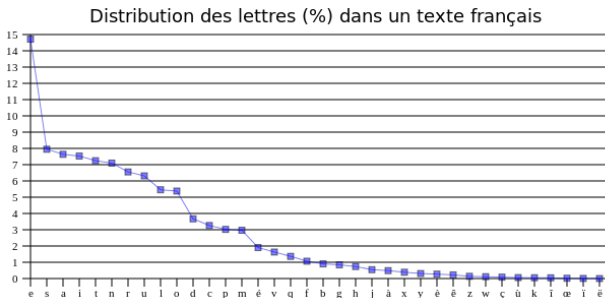
M	E	S	S	A	G	E
C	L	E	C	L	E	C
O	P	W	U	L	K	G

Trop de clés

Matrices 3×3 : 5429503678976

Matrices 10×10 :

314293064158293883017435778850162642728266998876247525637
417317539899590842010402346543259906970228933096407508161
1719197835869803511992549376



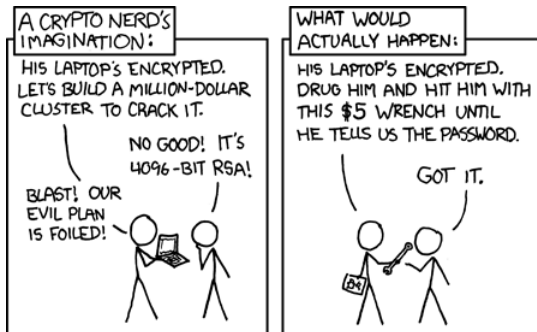
Source : manudiclemente, Wikipedia

Cryptographie asymétrique

Tristan a perdu la clé. Ne pouvant pas la faire refaire, il leur faut trouver un nouveau moyen de communiquer.







Source : xkcd.com

Cryptographie symétrique et asymétrique
Énumération des clés
Complexité du calcul

GPG mail