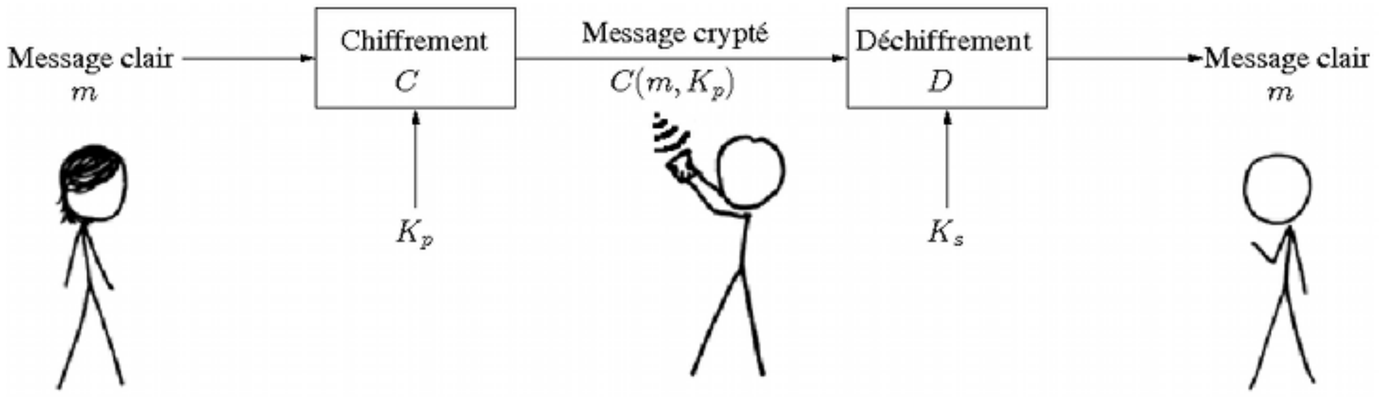
printemps des sciences '14
les sciences à portée de main

Cryptologie

Département de Mathématique
Denis LONGREE, Thomas MAKKINK, Nicolas ROOBAERT et Chimed SAMMUT

ULB

Qu'est-ce que la cryptologie ?



http://xkcd.com/

Cryptographie : Protéger des messages

Cryptanalyse : Tenter de déchiffrer des messages

L'arithmétique modulaire

En arithmétique modulaire, on ne travaille par sur les entiers eux-mêmes mais sur les restes de leur division euclidienne par un certain entier n.
Par exemple: 13 = 1 mod 12 car le reste de la division de 13 par 12 est 1.
On peut prouver qu'un entier k possède un inverse modulo n ssi il est premier avec n c'est-à-dire ssi PGCD(k,n) = 1.
L'arithmétique modulaire offre une vision efficace de certains problèmes et est utilisée en cryptologie.

http://www.bodet-time.com

adelegfr4.wikispaces.com

Le code affin et le code de César

Le *code de césar* consiste à décaler l'indice de toutes les lettres d'un certain nombre donc à effectuer $C = M + k \ (mod\ 26)$ pour chiffrer et $M = C - k \ (mod\ 26)$ pour déchiffrer.

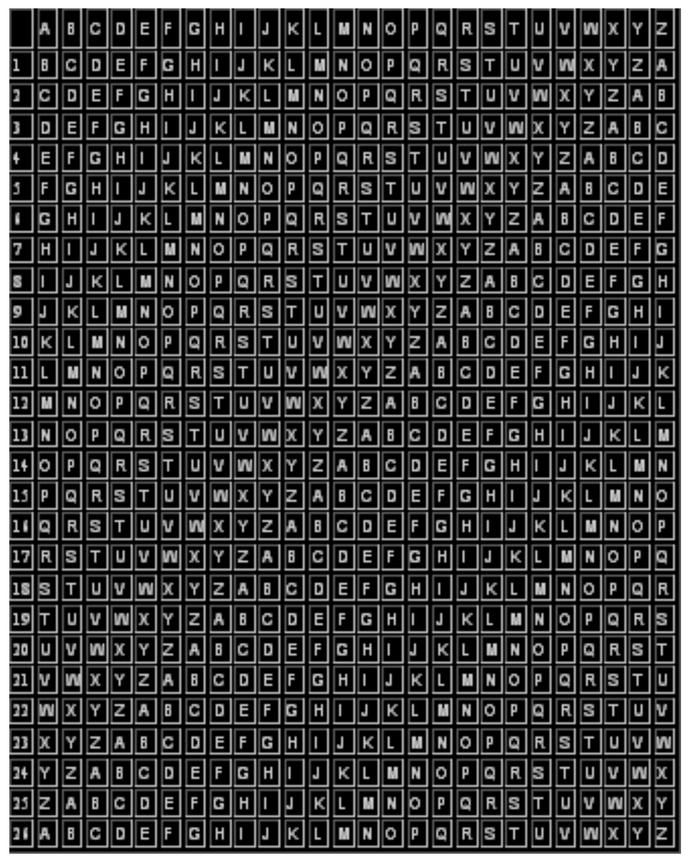
Message M : J'aime le chocolat
Crypté C : M'dlph oh fkrfrodw : $\boldsymbol{k} = 3$

Le nombre de clés possibles est **26**.

Plus généralement, le *chiffrement affin* consiste à remplacer l'indice x de chaque lettre par $X = a.x + b \ (mod\ 26)$ où *a* et *b* sont compris entre 0 et 25 et *a* est premier avec 26.

Message M : J'aime le chocolat
Crypté C : D'camo jo ixsisjch : $(\boldsymbol{a},\boldsymbol{b}) = (3,2)$

Le nombre de clés possibles est alors *12*x26=***312***.



www.Simonsingh.net

Le code de Vigenère

Le code de Vigenère consiste à choisir un mot comme clé que l'on répètera autant de fois que nécessaire jusqu'à obtenir la taille du texte. Ainsi à chaque lettre du message est associée une lettre de la clé. On chiffre ensuite chaque lettre du message à l'aide du code de César avec comme clé la lettre associée.

Message M : J'aime le chocolat
Crypté C : L'rgbw zg tfdvcnrr : **crypto**

j	a	i	m	e	l	e	c	h	o	c	o	l	a	t
c	r	y	p	t	o	c	r	y	p	t	o	c	r	y

Faculté des Sciences
ULB

printemps des sciences '14
les sciences à portée de main

Cryptologie

Département de Mathématique
Denis LONGREE, Thomas MAKKINK, Nicolas ROOBAERT et Chimed SAMMUT

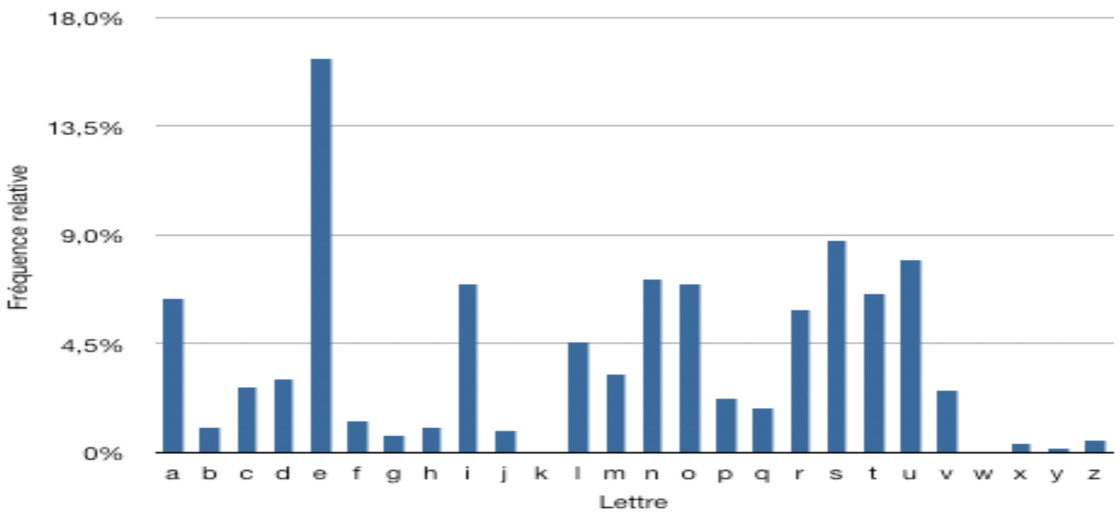
ULB

L'analyse Fréquentielle


http://n8on.free.fr/hackzines/deadend/2/Pages/Images/rsa1.jpg

Toutes les lettres n'apparaissent pas avec la même fréquence dans une langue.

Le principe de l'analyse fréquentielle est d'utiliser ce genre de faille.



source : wikipédia

Le code de Vernam

Ce code est un code de Vigenère où la clé n'est utilisée qu'une seule fois et est aussi longue que le message.

Théorème : Connaitre le message clair sachant le message chiffré revient à connaître le message clair.
(**P(M = x | C = y) = P(M = x)**)

Démonstration:

$P(M = x \mid C = y) = P(M = x, C = y)/P(C = y)$ Par Définition de la probabilité conditionnelle

On développe,

$P(M = x, C = y) = P(M = x, K = y - x)$ Car C= K+x

$= P(M = x)P(K = y - x)$ Car la clé est indépendante du Message

$= P(M = x)/26^m$ (1)

D'autre part,

$P(C = y) = \Sigma\ P(m_i \cap k_i)$

$= \Sigma\ P(k_i)P(m_i)$

$= \Sigma\ P(m_i)/26^m$

$=1/26^m$ (2)

En combinant (1) et (2), le résultat est démontré. ■

RSA

Le RSA est un mode de chiffrement asymétrique : la clé de chiffrement diffère de la clé de déchiffrement : aucune « fonction » ne les relie.
Par exemple, Alice voudrait que Bob lui transmettre un message:

1) **initialisation** Alice : - choisit deux grand nombres premiers p et q
   - calcule $n = p.q$ et $\phi(n) = (p-1).(q-1)$
   - choisit $d<n$ premier avec $\phi(n)$
   - calcule e, l'inverse de d modulo $\phi(n)$
   - rend publique la clé (n,d) et garde secrète (n,e)
2) **chiffrement** Bob : - représente son message par un entier $M<n$
   - calcule $C = M^d \ (mod\ n)$
   - transmet publiquement C à Alice
3) **déchiffrement** Alice: - retrouve M via $M = C^e \ (mod\ n)$ ce qui se démontre grâce au petit théorème de Fermat.

La sécurité du RSA repose sur la difficulté de factoriser n en $n=p.q$


http://n8on.free.fr/hackzines/deadend/2/Pages/Images/rsa1.jpg

Petit théorème de Fermat :

Si p est un nombre premier et si a est un entier non divisible par p, alors :
$a^{p-1} - 1$ est un multiple de p.

francis.naukas.com

Faculté des Sciences
ULB