CHIFFREMENT DE VIGÉNÈRE-BELLASO

Notions réinvesties : congruences

Le chiffrement de Vigenère est une méthode de cryptographie basée sur un chiffrement par substitution poly-alphabétique, c'est-à-dire que la lettre d'origine peut être remplacée par plusieurs lettres...
Ce chiffrement introduit la notion de clé (un mot ou une phrase) et utilise des chiffrements de César.
Évidemment, plus la clé sera longue et variée et mieux le texte sera chiffré.

Il faut savoir qu'il y a eu une période où des passages entiers d'œuvres littéraires étaient utilisés pour chiffrer les plus grands secrets. Les deux correspondants n'avaient plus qu'à avoir en leurs mains un exemplaire du même livre pour s'assurer de la bonne compréhension des messages.

A. Chiffrer

Chiffrons le mot « modulo » avec la clé « math ».
A chaque nombre associé à une lettre, on associe le nombre z (puis sa lettre) tel que $z \equiv x+y[26]$.

Clair =>	m	o	d	u	l	o
x	12	14	3	20	11	14
clé	m	a	t	h	m	a
y	12	0	19	7	12	0
z						
Codé =>						

Autrement dit, la clé MATH est (12,0,19,7).
Pour chaque bloc de 4 lettres, noté $\overline{L_1L_2L_3L_4}$, on effectue des chiffrements de César pour chaque L_i :
- un décalage de 12 lettres pour L_1
- un décalage de 0 lettre pour L_2
- un décalage de 19 lettres pour L_3
- un décalage de 7 lettres pour L_4.

B. Déchiffrer

On veut déchiffrer le mot « epxjuaepfe », codé avec la clé « math ».
Notons y le nombre associé à une des lettres de ce mot.
Pour déchiffrer la lettre, on connaît z et y et on cherche x tel que : $z \equiv x+y[26]$ *ie* $x \equiv z-y[26]$.

Clair =>										
x										
clé	m	a	t	h	m	a	t	h	m	a
y	12	0	19	7	12	0	19	7	12	0
z	4	15	23	9	20	0	4	15	5	4
Codé =>	e	p	x	j	u	a	e	p	f	e

C. Clés possibles

Pour une clé de longueur k, combien de choix existe-t-il ?

Pour des blocs de longueur 4, cela en donne déjà 456 976, et même si un ordinateur teste toutes les combinaisons possibles sans problème, il n'est pas question de parcourir cette liste pour trouver le message en clair, c'est-à-dire celui qui est compréhensible !
Il persiste tout de même une faiblesse du même ordre que celle rencontrée dans le chiffrement mono-alphabétique : la lettre A n'est pas toujours cryptée par la même lettre, mais si deux lettres A sont situées à la même position dans deux blocs différents (comme par exemple "ALPH ABET") alors elles seront cryptées par la même lettre.
Une attaque possible est donc la suivante : on découpe notre message en plusieurs listes, les premières lettres de chaque bloc, les deuxièmes lettres de chaque bloc... et on fait une attaque statistique sur chacun de ces regroupements : il s'agit du ***test de Kasiski***[1].

Pour plus d'infos : https://fr.wikipedia.org/wiki/Cryptanalyse_du_chiffre_de_Vigen%C3%A8re

La cryptanalyse du chiffre de Vigenère par la méthode de Kasiski ou par d'autres méthodes comme celles de l'indice de coïncidence (excellente méthode !) demande un texte suffisamment long vis-à-vis de la clé. Dans le cas extrême où la clé est de longueur égale à celle du message, et n'est utilisée qu'une seule fois, tous les textes de longueur égale à celle du message chiffré sont possibles : le chiffre ne peut être cassé ; c'est le ***chiffre de Vernam***, ou ***masque jetable***.

Le masque jetable fut inventé par Gilbert Vernam en 1917 et perfectionné par Joseph Mauborgne, qui rajouta la notion de clé aléatoire. Cependant, le banquier américain Frank Miller en avait posé les bases dès 1882. Bien que simple, facile et rapide, tant pour le codage que pour le décodage, ce chiffrement est théoriquement impossible à casser, mais il présente d'importantes difficultés de mise en œuvre qui le rendent impossible à utiliser dans de nombreux cas comme la sécurisation des échanges sur Internet.

Hélas, le chiffre de Vernam n'est pas la panacée. D'abord, il exige qu'une clé serve une seule fois. Si vous utilisez la même clé deux fois, alors on peut extraire beaucoup d'informations des messages chiffrés.
Ensuite, le chiffre de Vernam exige des clés extrêmement longues, et une parfaite synchronisation des clés.
L'échange des clés, qui doit être sécurisé, est donc difficile à réaliser.
Enfin, les clés utilisées doivent être parfaitement aléatoires, ce qui n'est pas facile à garantir.
C'est pourquoi ce chiffre n'est mis en œuvre que dans des cas très particuliers.
Il fut ainsi utilisé pour sécuriser le téléphone rouge, ligne directe entre la Maison Blanche et le Kremlin du temps de la guerre froide. Les clés circulaient dans les valises diplomatiques, transportées dans des avions bourrés d'agents secrets. Et on raconte que pour produire des clés aléatoires, les Soviétiques employaient des "lanceurs de dés" : leur travail consistait à lancer des dés toute la journée et à noter le résultat.

Un chiffrement à la main par la méthode du masque jetable fut notamment utilisé par Che Guevara pour communiquer avec Fidel Castro. Lorsqu' Ernesto Guevara, dit le Che, fut retrouvé mort par l'armée bolivienne en 1967, après avoir tenté de développer des foyers révolutionnaires en Amérique latine et participer à la guérilla bolivienne, on découvrit sur lui des papiers expliquant comment il chiffrait ses messages qu'il communiquait à Fidel Castro.
Il commençait par remplacer les lettres par un nombre à deux chiffres compris entre 01 et 99.

A	06	E	08	I	39	M	70	Q	71	U	52	Y	01
B	38	F	30	J	31	N	76	R	58	V	50	Z	59
C	32	G	36	K	78	O	09	S	02	W	56		
D	04	H	34	L	72	P	79	T	00	X	54		

En soit, cela ne constitue qu'une simple substitution dont on sait qu'elle n'apporte aucune sécurité.
Mais le Che et Fidel Castro avaient aussi recours à une forme du chiffre de Vernam, et que l'on sait parfaitement sûr.

Pour plus d'infos : http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/che

Blaise de Vigenère, né le 5 avril 1523 à Saint-Pourçain-sur-Sioule et mort le 19 février 1596 à Paris, est un diplomate, cryptographe, traducteur, alchimiste et astrologue français.
Quand Vigenère prit sa retraite, à 47 ans, il offrit sa pension annuelle de 1 000 livres aux pauvres de Paris.
En 1584 il devient secrétaire de la chambre du roi Henri III de France ainsi que son astrologue personnel.
Il mourut d'un cancer de la gorge.

La paternité de ce qu'on appelle le « chiffre de Vigenère » revient aussi à Giovan Battista Bellaso, qui a publié son travail en 1564. Le chiffrement présenté par Vigenère en 1586 a toutefois quelques différences avec celui de Bellaso.
Bellaso se servait d'une « table réciproque » à cinq alphabets de son invention ; Vigenère en utilisait dix.
Bellaso basait son chiffrement sur la première lettre du mot ; Vigenère le basait sur une lettre sur laquelle les correspondants s'étaient mis préalablement d'accord.

1 Le major Friedrich Wilhelm Kasiski était un officier d'infanterie prussien, cryptologue et archéologue. Né en 1805 et mort en 1881, il fut commandant du bataillon de la Garde Nationale de 1860 à 1868.
En 1863, Kasiski publie un livre en allemand de 95 pages sur la cryptologie. L'importance de cette découverte ne fut pas reconnue à cette époque et Kasiski s'intéressa à l'archéologie en lieu et place des mathématiques.
Le 22 mai 1881, Kasiski décède sans vraiment avoir pris conscience de l'impact de son travail sur la cryptologie moderne.