Introduction à l'algorithme de Vigenère

par Gabriel Malkas (Janitrix.org)

Date de publication : 10/11/2007

Dernière mise à jour :

L'algorithme de Vigenère est un algorithme cryptographique qui a permit pendant un certain temps de protéger les documents face à l'analyse fréquentielle, outil qui a permit aux cryptanalystes de venir à bout des chiffrements à substitution simple.

I - Un peu d'histoire

I-A - Situation du monde cryptographique

Pendant des siècles, la seule substitution alphabétique, comme le chiffre de César, suffisait aux chefs de guerre et autres diplomates pour protéger leurs correspondances.

Cependant, avec l'apparition de la cryptanalyse et de l'analyse des fréquences dans les pays arabes, les cryptographes avaient besoin d'un nouvel algorithme pour reprendre le dessus face aux cryptanalystes.

L'algorithme de Vigenère est en fait le résultat des travaux de plusieurs « savants » du XVe et XVIe siècle : Leon Battista Alberti, Jean Trithème, abbé allemand né en 1462, Giovanni Porta, savant italien né en 1535, et enfin Blaise de Vigenère.

Blaise de Vigenère

I-B - Les travaux d'Alberti

Ainsi, c'est Alberti, figure majeur de la Renaissance, à la fois peintre, philosophe, poète, et compositeur, qui entreprit l'élaboration d'un algorithme qui ferait échouer les analyses de fréquences. Il découvrit qu'en utilisant deux ou plusieurs alphabets chiffrés, une même lettre pouvait être chiffrée différemment dans le texte codé.

Par exemple :

Alphabet ordinaire	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet chiffré 1	E	Z	B	V	K	T	I	X	A	Y	M	E	P	L	S	D	H	U	O	J	R	C	G	N	Q	W
Alphabet chiffré 2	X	S	T	Q	H	A	B	O	E	N	W	P	K	U	G	J	Y	Z	L	I	D	F	V	C	M	R

Pour coder le texte « hello », il suffirait de jongler entre les deux alphabets : h deviendrait X (1er alphabet), e deviendrait H (2eme alphabet), le premier l deviendrait E mais le deuxième donnerait P, enfin, le o deviendrait S.

On évite ainsi l'analyse fréquentielle !

Cependant, Alberti ne pu terminer son travail, et cette tâche revint à d'autres.

Notamment, Blaise de Vigenère, diplomate français né en 1523, qui utilisait la cryptographie pour son travail. Il étudia les travaux d'Alberti, Trithème et Porta pour donner la forme finale à l'algorithme qui porte donc son nom.

Cette méthode de chiffrage utilise non pas un alphabet mais 26 alphabets codés.

II - Fonctionnement théorique et pratique

II-A - Le Carré de Vigenère

Afin d'utiliser l'algorithme de Vigenère, il faut avant tout construire ce qu'on appelle un « carré de Vigenère ». Cette représentation logique est très simple : elle est constituée de l'alphabet clair, suivit des 26 alphabets chiffrés, chacun étant décalé d'une lettre par rapport au précédent.

clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ce carré apparemment bien compliqué est simple d'utilisation une fois que l'on a compris son principe. Il vous faut choisir une clé, de longueur variable, qui en fait servira de référence pour savoir quel alphabet utiliser.

II-B - Mise en pratique

Par exemple, cryptons le message « Attaquer la position ennemie ! ». On procède comme ceci : on enlève majuscules et ponctuations, puis espaces, ce qui nous donne : « attaquerlapositionennemie ». On choisit une clé : DANGER.

On répète la clé autant de fois nécessaire pour « couvrir » le message à coder :

D	A	N	G	E	R	D	A	N	G	E	R	D	A	N	G	E	R	D	A	N	G	E	R	D
a	t	t	a	q	u	e	r	l	a	p	o	s	i	t	i	o	n	e	n	n	e	m	i	e

Ainsi, on attribut une lettre de la clé à chaque lettre du message en répétant la clé autant de fois que nécessaire. Maintenant, nous voulons crypter la lettre 'a'. Nous allons donc chercher l'alphabet qui commence par la lettre D, c'est l'alphabet n°3 dans le carré de Vigenère. Cherchons la lettre qui, dans la ligne de l'alphabet D, correspond à la lettre clair 'a'. Dans ce cas bien sûr, c'est la lettre D.

Ensuite, faisons de même avec le 't' : on cherche la ligne donc l'alphabet qui commence par A, c'est le dernier. C'est en fait l'alphabet que l'on utilise tous les jours sans décalage, le 't' deviendra donc T.

Mais, et c'est ça l'intérêt du système, prenons le second 't' à chiffrer, qui est sous la lettre N de la clé. Cherchons la ligne commençant par N, c'est la n°13, et cherchons la lettre correspondante à la lettre 't'. C'est G dans ce cas.

Nous voyons donc qu'une même lettre peut être encoder différemment, ce qui bloque le processus d'analyse fréquentielle.

Pour vérifiez que vous avez compris le principe, encodez la suite du message par vous même, et comparez votre résultat avec le suivant :

```
DTGGULHRYGTFVIGOSEHNAKQZH
```

De plus, vous comprendrez que plus votre clé sera longue, plus l'algorithme sera efficace contre les cryptanalyses.

Et pour décrypter ? C'est aussi simple que pour crypter mais il vous faut bien entendu connaître la clé d'origine. Encore une fois, vous disposez le message crypté sous la clé, que vous répétez autant de fois que nécessaire :

D	A	N	G	E	R	D	A	N	G	E	R	D	A	N	G	E	R	D	A	N	G	E	R	D
D	T	G	G	U	L	H	R	Y	G	T	F	V	I	G	O	S	E	H	N	A	K	Q	Z	H

Puis, vous cherchez la lettre D dans la ligne de l'alphabet commençant par D, et enfin, vous regardez qu'elle est la lettre claire correspondante, ici, c'est le 'a'. De même, pour la lettre suivante, on cherche l'alphabet commençant par A, la lettre T de cette ligne qui correspond à la lettre claire 't'. Pour la suivante, cherchons la ligne commençant par N, et regardons à qu'elle lettre claire correspond la lettre G de cette ligne, sans surprise, c'est la lettre 't'.

Nous pouvons ainsi reconstituer le message d'origine, puis, une fois compréhensible, rétablir espaces et majuscules, cependant cela reste difficile pour la ponctuation, mais elle n'est heureusement pas indispensable pour comprendre le message.

III - Cryptanalyse