Cryptographie par transposition - Transpositions rectangulaires

Principe des méthodes par transposition

Les méthodes de cryptographie par **transposition** sont celles pour lesquelles on chiffre le message en permutant l'ordre des lettres du message suivant des règles bien définies. Autrement dit, on produit un anagramme du message initial.

Du fait qu'on ne change pas les lettres du message initial, on pourrait imaginer que ces procédés de chiffrement ne sont pas sûrs du tout. C'est effectivement le cas si on chiffre de petits messages, comme des mots, où le nombre d'anagrammes est très réduit. Mais dès que l'on s'intéresse à des messages assez grands, le nombre de transpositions possibles est extrêmement grand, et il est impossible de tester toutes les permutations possibles.

Cela dit, il faut que l'expéditeur et le destinataire se mettent d'accord sur une façon de permuter les caractères de façon assez régulière pour qu'elle puisse s'appliquer à n'importe quel message. C'est ce choix qui va rendre le chiffrement par transposition plus ou moins résistant aux attaques. Nous décrivons ci-dessous une méthode pour se mettre d'accord sur la transposition effectuée à l'aide d'un unique mot clé.

Les transpositions rectangulaires

Pour effectuer un chiffrement par transposition rectangulaire, on commence par se mettre d'accord sur un mot-clé. Choisissons pour notre exemple le mot `BIBMATH`. On classe alors les lettres du mot BIBMATH par ordre alphabétique, et on attribue à chaque lettre son numéro dans l'ordre alphabétique. Ainsi, on donne à A le numéro 1, au premier B le numéro 2, au deuxième B le numéro 3, au H le numéro 4, etc....

On crée ensuite un tableau de la façon suivante :

- la première ligne est constituée par les lettres de la clé;
- la deuxième ligne est constituée par les numéros qui leur sont associés;
- on complète ensuite le tableau en le remplissant avec les lettres du message à chiffrer. On écrit sur chaque ligne autant de lettres que de lettres dans la clé. Eventuellement,la dernière ligne n'est pas complète.

Par exemple, si on veut chiffrer "`Je suis en Italie avec Maria`", le tableau que l'on construit est le suivant :

B	I	B	M	A	T	H
2	5	3	6	1	7	4
J	E	S	U	I	S	E
N	I	T	A	L	I	E
A	V	E	C	M	A	R
I	A					

Ensuite, on écrit d'abord le contenu de la colonne numérotée 1, puis le contenu de la colonne numérotée 2, etc... Le message chiffré obtenu est alors :

```
ILMJN AISTE EEREI VAUAC SIA
```

Pour faire l'opération inverse (déchiffrer), il faut d'abord reconstituer pour chaque colonne le nombre de lignes que le tableau comprenait. Pour cela, on note n le nombre de lettres du message et c le nombre de lettres de la clé, qui est aussi le nombre de colonnes du tableau de chiffrement. Si n est un multiple de c, alors on a affaire à un tableau où toutes les colonnes ont la même hauteur, qui vaut n/c. Sinon, on note q le quotient dans la divison euclidienne de n par c, et r le reste. Il y aura alors r colonnes (les premières) qui auront pour hauteur $q+1$, et $c-r$ colonnes (les dernières), qui auront pour hauteur q.

Ensuite, on remplit le tableau en écrivant dans la colonne numérotée 1 les premières lettres du message, puis dans la colonne numérotée 2 les suivantes, et ainsi de suite... Le message clair se lit alors directement sur le tableau.

Prenons un exemple : vous devez déchiffrer, avec la clé `CHAT` le message suivant :

```
BUNNA EDRME RDEQE NMIAE TON
```

Il comporte 23 lettres, et la clé a pour longueur 4 lettres. On a $23=4\times5+3$, c'est-à-dire qu'on va réaliser un tableau

comprenant 4 colonnes tel que les 3 premières colonnes ont une hauteur de 6, et la dernière une hauteur de 5, comme le suivant :

C	H	A	T
2	3	1	4

La première lettre de la clé (par ordre alphabétique) est A. Sous le A, on écrit les 6 premières lettres du message, `BUNNAE`. La deuxième lettre est C. Sous le C, on écrit les 6 lettres suivantes, `DRMERD`. Continuant ainsi, on obtient finalement :

C	H	A	T
2	3	1	4
D	E	B	A
R	Q	U	E
M	E	N	T
E	N	N	O
R	M	A	N
D	I	E	

Le message initial était donc :

```
DEBARQUEMENT EN NORMANDIE
```

Chiffrer vos messages par transposition rectangulaire

Message	
Clé	
Chiffrer! Déchiffrer!	Effacer
Message codé :	

Consulter aussi

- *Comment vaincre les chiffrements par transposition?*
- *Les grilles tournantes de Fleissner*
- *Le chiffre utilisé dans le Voyage au centre de la terre, un roman de Jules Verne*

- *Les chiffres de la guerre de sécession*