Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Chiffrements « antiques » (suite)

Exercice 1 : [ADFGVX, 1918] La première partie est le codage du message dans un alphabet réduit constitué des lettres A, D, F, G, V, X. La disposition des éléments sur la grille est partie intégrante de la clef (transmise au correspondant).

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Ainsi le 8 sera remplacé par AA et p par AD.

```
message                     : attaques à 10 h 05
Texte clair                 : a  t  t  a  q  u  e  s  à  1  0  h  0  5
Texte chiffré (1ère étape) : DV DD DD DV XX GD XD VD DV AV XG DX XG FV
```

La deuxième partie dépend d'un mot-clef, qui ici sera MARC par exemple, et qui doit être connu des deux correspondants. D'abord, les lettres du mot-clef sont écrites sur la première ligne d'une nouvelle grille. Ensuite, on porte le texte chiffré de la première étape sur une série de lignes, comme ci-dessous. Les colonnes de la grille sont ensuite remplacées de telle sorte que les lettres du mot-clé soient dans l'ordre alphabétique. Le texte chiffré final est obtenu en descendant chaque colonne l'une après l'autre et en écrivant les lettres selon ce nouvel ordre. On lit donc le chiffré de haut en bas (puis gauche à droite).

M	**A**	**R**	**C**
D	V	D	D
D	D	D	V
X	X	G	D
X	D	V	D
D	V	A	V
X	G	D	X
X	G	F	V

Déplaçons les colonnes pour mettre les lettres du mot-clef dans l'ordre alphabétique

A	**C**	**M**	**R**
V	D	D	D
D	V	D	D
X	D	X	G
D	D	X	V
V	V	D	A
G	X	X	D
G	V	X	F

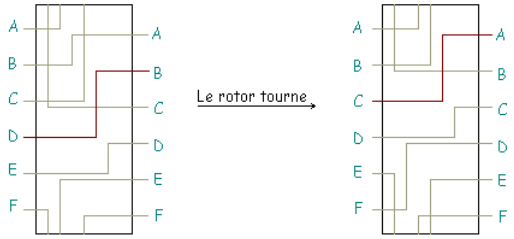
Texte chiffré final VDXDVGGDVDDVXVDDXXDXXDDGVADF

Le texte chiffré final pourra être transmis en morse, et le destinataire inversera le procédé de chiffrement pour retrouver le texte originel. Le texte chiffré n'est fait qu'avec six lettres ADFGVX, qui qualifient les lignes et les colonnes de la première grille. On demande souvent pourquoi ces lettres ont été choisies plutôt que, disons, les lettres de A à F. La raison est que les lettres A,D,F,G,V et X ne se ressemblent pas lorsqu'on les traduit dans le système points et traits du Morse, ce qui minimise les risques d'erreurs dans les transmissions.

1. Quelle modification (méthode de chiffrement) réalise la première partie ? Et la seconde partie ?
2. Chiffrer « ChiffrementADFGVX » avec cette méthode avec la clef « RAPIDE ».
3. Quelle est la permutation associée au mot-clef précédent?

4. Déchiffrer « AGDXDGXXVXDDVAXXDDVXVGFDXGVGDX » sachant que le mot-clef est MASTER

Exercice 2 : [ENIGMA]
On considère un rotor Enigma simplifié à 6 paires de connections.



Les positions gauche et droite sont reliées de la façon suivante : (1-3, 2-2, 3-4, 4-1, 5-6, 6-5).

1. Dessiner le schéma de montage.
2. Chiffrer le message suivant : CDBAFFE, le rotor étant dans la position initiale décrite précédemment.
3. Modéliser le rotor grâce aux mathématiques. Modéliser la combinaison de deux rotors ainsi câblés.
4. On considère le tableau simplifié de connexions d'Enigma suivant : 2 paires choisies parmi 5 lettres. Calculez le nombre de possibilités et énumérez-les.
5. Calculer le nombre de clefs possibles pour Enigma sachant qu'il y a 3 rotors que l'on peut positionner dans n'importe quel ordre et à n'importe quelle place de départ ainsi qu'un tableau de connections permettant d'échanger 6 couples de lettres.
6. Imaginez que vous connectez chacun des 3 rotors de Enigma de la façon suivante $(1-2, 2-3, 3-4, \cdots, 25-26, 26-1)$. Que se passe-t'il pour ENIGMA ?

Exercice 3 : [Code ASCII]

1. Déterminer le développement binaire et le développement hexadécimal du nombre décimal 215.
2. Déterminer l'écriture ASCII de 'SECRET' sachant que 'A' est codé par 41 en hexadécimal.
3. Déterminer le chiffrement par XOR du message précédent avec la clé précédente (215).
4. Quelle opération faut-il faire pour déchiffrer?

Exercice 4 : [Emplacement mémoire]

1. Déterminer le développement binaire du nombre décimal 5032.
2. Quel est le nombre de bits nécessaires pour représenter ce nombre. Aurait-on pu le prévoir?
3. Combien de bits sont nécessaires pour représenter des nombres de 600 chiffres décimaux?
4. Et combien de chiffres décimaux pour les nombres représentés sur 1024 bits?