Chiffrement affine : définition

Le **chiffrement par décalage** est un cas particulier du **chiffrement par substitution** dans lequel on utilise une translation comme substitution. Un autre cas particulier du chiffrement par substitution est le **chiffrement affine**. Dans ce procédé, on limite les fonctions de chiffrement à certaines fonctions de la forme

$$E_{(a,b)}(x) = ax + b \mod 26 \tag{1}$$

où $a, b \in \mathbb{Z}_{26}$. Ces fonctions sont appelées des **fonctions affines**, d'où l'on a tiré le nom du procédé. On remarque que l'on retrouve le chiffrement par décalage pour $a = 1$.

Pour que l'opération de déchiffrement soit possible, il est nécessaire que la fonction affine soit bijective. Autrement dit, pour tout $y \in \mathbb{Z}_{26}$, l'équation

$$ax + b = y \mod 26 \tag{2}$$

doit avoir une, et une seule, solution x. L'équation (2) est équivalente à

$$ax = y - b \mod 26\ . \tag{3}$$

Lorsque y parcourt l'ensemble $\mathbb{Z}_{26}$, $y - b$ décrit également ce même ensemble. Donc, il suffit d'étudier l'équation $ax = z \mod 26$ pour tout $z \in \mathbb{Z}_{26}$. On démontre que cette équation admet une unique solution pour tout z fixé, si, et seulement si, $pgcd(a, 26) = 1$ (où *pgcd* est le plus grand diviseur commun de ses arguments) ; au passage on dit que a et 26 sont **premiers entre eux**. En effet si a et 26 sont premiers entre eux (et seulement dans ce cas), alors a admet un inverse $a^{-1} \in \mathbb{Z}_{26}$ (*i.e.*, $aa^{-1} = a^{-1}a = 1 \mod 26$), et l'unique solution de l'équation $ax = z \mod 26$ est $x = a^{-1}z \mod 26$. En particulier, $x = a^{-1}(y - b) \mod 26$ est l'unique solution a l'équation (2).

Supposons donc que a et 26 sont premiers entre eux. On vient de voir que, dans ce cas, l'application $E_{(a,b)}$ est inversible. Sa bijection réciproque est donnée par $D_{(a,b)}(y) = a^{-1}(y-b) \mod 26$. Nous pouvons maintenant décrire complétement le chiffrement affine. Les ensembles de textes clairs $\mathcal{P}$ et chiffrés $\mathcal{C}$ sont tous les deux égaux à $\mathbb{Z}_{26}$. L'espace des clefs secrètes est quant à lui donné par

$$\mathcal{K} := \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : pgcd(a, 26) = 1\}\ . \tag{4}$$

Pour tout $(a, b) \in \mathcal{K}$, on définit

$$E_{(a,b)}(x) := ax + b \mod 26 \tag{5}$$

et

$$D_{(a,b)}(y) := a^{-1}(y - b) \mod 26\ . \tag{6}$$

1 Exercice : Mise en œuvre du chiffrement affine

Soit $(a, b) = (7, 3)$.

1. Montrer que $(a, b) \in \mathcal{K}$ et calculer a^{-1} dans $\mathbb{Z}_{26}$;
2. Vérifier par calcul que $D_{(a,b)}(E_{(a,b)}(x)) = x$ pour x quelconque dans $\mathbb{Z}_{26}$;
3. Chiffrer le mot *hot* avec cette clef ;
4. Énumérer les $a \in \mathbb{Z}_{26}$ qui sont premiers avec 26 ;
5. Pour chacun des éléments $a \in \mathbb{Z}_{26}$ premiers avec 26, calculer son inverse (modulo 26) ;
6. Calculer le nombre de clefs possibles. Qu'en déduisez-vous quant à la solidité de ce procédé de chiffrement ?

2 Exercice : Cryptanalyse du chiffrement affine

Dans cet exercice, on s'intéresse à une technique de cryptanalyse permettant de casser un procédé de chiffrement affine. Cette technique est basée sur l'analyse des fréquences d'occurrence des lettres dans un texte écrit dans une langue donnée (par exemple, l'anglais ou le français). Dans le cas présent, on effectue une hypothèse simplificatrice : on suppose que le texte clair est **un message rédigé en anglais sans ponctuations ni espaces**.

Plusieurs personnes ont estimé la probabilité d'apparition des vingt-six lettres de l'alphabet en faisant des statistiques sur de nombreux romans, magazines et journaux quotidiens écrits en anglais. Les estimations suivantes sur la langue anglaise ont été obtenues par Beker et Piper.

Fréquences d'occurrences des lettres dans les textes écrits en anglais (Beker & Piper)

lettre	proba	lettre	proba
a	$0,082$	n	$0,067$
b	$0,015$	o	$0,075$
c	$0,028$	p	$0,019$
d	$0,043$	q	$0,001$
e	$0,127$	r	$0,060$
f	$0,022$	s	$0,063$
g	$0,020$	t	$0,091$
h	$0,061$	u	$0,028$
i	$0,070$	v	$0,010$
j	$0,002$	w	$0,023$
k	$0,008$	x	$0,001$
l	$0,040$	y	$0,020$
m	$0,024$	z	$0,001$

Nous allons utiliser ces statistiques pour déchiffrer un cryptogramme provenant d'un message écrit en anglais. Supposons donc qu'Oscar ait intercepté le message suivant (sans espaces ni signes de ponctuation) :
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH.

1. Calculer le nombre d'occurrences de chacune des lettres de l'alphabet dans ce message ;

2. Expliquer pourquoi on peut supposer que la lettre R se déchiffre en E ;
3. Supposons que la lettre D se déchiffre en T (et R en E). Trouver la clef (a, b) qui en résulte, et expliquer pourquoi cette clef n'est pas valide ;
4. Supposons que la lettre R se déchiffre en E, et K en T. Trouver la clef (a, b) qui en résulte, et expliquer pourquoi cette fois-ci la clef est valide ;
5. En vous basant sur ce que vous avez trouvé pour a à la question précédente, calculer a^{-1} (dans $\mathbb{Z}_{26}$). Une fois cela fait, déchiffrer le message afin de vérifier qu'il s'agit bien d'un texte écrit en anglais.