Chap. III : Exemples de cryptosystèmes à clef secrète

Laurent Poinsot

25 septembre 2009

Plan

Plan

Dans ce système de chiffrement, chaque lettre est représentée par un entier compris entre 0 et 25. Cela revient à travailler dans $\mathbb{Z}_{26}$. Plus précisément, les clefs secrètes, les messages clairs et chiffrés sont dans $\mathbb{Z}_{26}$. Pour chiffrer un message clair $M := x_1 x_2 \dots x_N$ écrit avec les lettres de l'alphabet latin (les x_i sont donc des lettres quelconques), on commence par transformer **chaque** lettre x_i de M en un entier n_i entre 0 et 25, le message devient donc la suite des entiers $n_1 n_2 \dots n_N$. Puis chaque entier n_i est chiffré avec le chiffrement par décalage E_K avec une clef secrète K. On obtient donc une suite d'autres entiers $C := m_1 m_2 \dots m_N$ où $m_i := E_K(n_i)$. Lorsque Bob reçoit le chiffré C, il retrouve M par (1) calculs de $D_k(m_i) = D_K(E_k(n_i)) = n_i$ puis (2) il récupère M en remplaçant chaque entier n_i par sa lettre correspondante.

La correspondance lettre/entier généralement employée est donnée par

a	b	$\ldots$	z
0	1	$\ldots$	25

Définition formelle du chiffrement par décalage

Pour une clef $K \in \mathbb{Z}_{26}$, c'est-à-dire $0 \leq K \leq 25$, $M \in \mathbb{Z}_{26}$ un message secret et $C \in \mathbb{Z}_{26}$ un message chiffré, on définit

$$E_K(M) := M + K \pmod{26},$$

et

$$D_K(C) := C - K \pmod{26}.$$

Il est facile de vérifier que $D_K(E_K(M)) = M$ pour tout $M \in \mathbb{Z}_{26}$.
Pour la clef $K = 3$, ce système cryptographique est souvent appelé **chiffrement de César**, car il était utilisé par Jules César.
Le chiffrement d'une lettre x est en fait réalisé par un décalage cyclique de K lettres vers la droite (dans l'alphabet latin). "Cyclique" signifiant qu'une fois atteinte la lettre z, on recommence à partir de a.

Exemple

Supposons que la clef soit $K = 11$. Supposons que le texte clair soit ”rendezvousaminuit”. On commence par convertir le message en une suite d'entiers :

r	e	n	d	e	z	v	o	u	s	a
17	4	13	3	4	25	21	14	20	18	0

m	i	n	u	i	t
12	8	13	20	8	19

Ensuite on ajoute $K = 11$ à chaque valeur

28 15 24 14 15 36 32 25 31 29 11

23 19 24 31 19 30

Exemple

On calcule le reste modulo 26 :

2 15 24 14 15 10 6 25 5 3 11

23 19 24 5 19 4

Enfin on convertit cette suite d'entiers en une suite de lettres : "cpyopkgzfdlxtyfte" est le message chiffré.

Pour déchiffrer ce texte, Bob doit d'abord convertir le texte en entiers, soustraire $K = 11$ à chaque valeur, calculer les restes modulo 26 et enfin convertir les nombres en caractères alphabétiques.
Remarquons que le chiffrement par décalage est peu sûr : en effet, on peut le cryptanalyser par la méthode de **recherche exhaustive** (ou **force brute**). Comme il n'y que 26 clefs possibles, il suffit d'essayer toutes les clefs jusqu'à ce que l'on obtienne un message clair compréhensible. En moyenne par cette méthode le texte clair est obtenu après 26/2=13 essais.
Conclusion : Cela montre qu'il est nécessaire, pour la sécurité d'un système cryptographique, que l'espace des clefs soit grand, mais comme on peut l'imaginer, cette condition n'est nullement suffisante.

Ce procédé de chiffrement fut employé durant des siècles. Il repose sur la notion de substitution vue au chapitre précédent. De façon générale, une substitution d'un alphabet A est une bijection de A dans lui-même. Ainsi une subsitution transforme chaque lettre de l'alphabet A en une autre lettre du même alphabet. Si π est une substitution de A, alors il existe une unique substitution σ de A pour laquelle on a quel que soit $a \in A$, $\pi(\sigma(a)) = a$ et $\sigma(\pi(a)) = a$. σ est l'**inverse** de π, généralement notée π^{-1}.

Pour le chiffrement par substitution, les messages clairs et chiffrés sont des lettres d'un alphabet A (par exemple, l'alphabet latin). Les clefs secrètes sont choisies parmi les substitutions de A. Soient alors π une substitution de A et $M \in A$ une lettre. On a alors :

$$E_\pi(M) := \pi(M) \ .$$

Soit alors $C \in A$ le chiffré correspondant, $C = \pi(M)$. Alors on a également

$$D_\pi(C) := \pi^{-1}(C) = M \ .$$

Pour chiffrer une suite de lettres $M_1 M_2 \dots M_n$ prises dans l'alphabet A, on calcule

$$C = E_\pi(M_1)E_\pi(M_2)\dots E_\pi(M_n)\ .$$

Posons $C_i := E_\pi(M_i)$ pour $i = 1, \dots, n$. Pour déchiffrer $C = C_1 C_2 \dots C_n$, on calcule

$$D_\pi(C_1)D_\pi(C_2)\dots D_\pi(C_n) = M_1 M_2 \dots M_n = M\ .$$

Exemple

Soit π la fonction suivante :

a	b	c	d	e	f	g	h	i	j	k	l	m
x	n	y	a	h	p	o	g	z	q	w	b	t

n	o	p	q	r	s	t	u	v	w	x	y	z
s	f	l	r	c	v	m	u	e	k	j	d	i

1. π est-elle une substitution ?
2. Décrire sa substitution inverse π^{-1} ;
3. Quel est le chiffré de ”bonjour” ?

Combien a-t-on de clefs secrètes possibles ?
$26! > 4 \times 10^{26}$.
Pour la lettre ”a” on a 26 choix possibles de transformation en une autre lettre de l'alphabet (”a” compris).
Pour la lettre ”b” on a 25 choix possibles de transformation en une autre lettre de l'alphabet.
...
Pour la lettre ”z” on a 1 choix possible de transformation en une autre lettre de l'alphabet.
Soit un total de $26 \times 25 \times \cdots \times 1 = 26!$
Une recherche exhaustive de la clef devient très difficilement réalisable, y compris avec l'assistance d'un ordinateur. Cependant ce cryptosystème peut être cassé à l'aide d'autres techniques.