

TIPE

T. Lestienne

1 Formalisation de la cryptographie

Définition 1: chiffre

Un *chiffre* défini sur $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, avec \mathcal{K} l'espace des clés, \mathcal{M} l'espace des messages, et \mathcal{C} l'espace des messages chiffrés, est une paire (E, D) telle que:

- $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ est la fonction de chiffrement,
- $D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$ est la fonction de déchiffrement,
- $\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, D(k, E(k, m)) = m$.

Exemple 1: Application au code de César

Le code de César consiste à associer à chaque lettre un nombre lié à sa position dans l'alphabet (voir tableau ci-dessous). Puis effectuer un décalage de k "vers la droite".

A	B	C	D	E	F	G	H	I	J	K	...	Y	Z
0	1	2	3	4	5	6	7	8	9	10	...	24	25

Formellement : Le chiffre de César est défini sur $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ avec $\mathcal{K} = [0; 25]$, $\mathcal{M} = \mathcal{C} = \{A, B, \dots, Z\}$. Les fonctions de chiffrement E et de déchiffrement D sont définies par :

$$E : \begin{cases} \mathcal{K} \times \mathcal{M} & \rightarrow & \mathcal{C} \\ (k, m) & \mapsto & (m + k) \bmod 26 \end{cases}$$

$$D : \begin{cases} \mathcal{K} \times \mathcal{C} & \rightarrow & \mathcal{M} \\ (k, c) & \mapsto & (c - k) \bmod 26 \end{cases}$$

On a bien $\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, D(k, E(k, m)) = (m + k \bmod 26) - k \bmod 26 = m \bmod 26 = m$

Application : Chiffrement de TEST avec $k = 10$:

- $T \rightarrow D \quad (19 + 10) \bmod 26 = 3,$
- $E \rightarrow O \quad (4 + 10) \bmod 26 = 14,$
- $S \rightarrow C \quad (18 + 10) \bmod 26 = 2,$
- $T \rightarrow D \quad (19 + 10) \bmod 26 = 3.$

Le message chiffré est donc DOCD.

Pour le déchiffrement, on utilise $D(k, c)$:

- $D \rightarrow T \quad (3 - 10) \bmod 26 = 19,$
- $O \rightarrow E \quad (14 - 10) \bmod 26 = 4,$
- $C \rightarrow S \quad (2 - 10) \bmod 26 = 18,$
- $D \rightarrow T \quad (3 - 10) \bmod 26 = 19.$

Le message déchiffré est donc TEST.

Remarque 1:

deux occurrences de la même lettre seront encoder par la même lettre

Remarque 2:

Dans ce cas, les fonctions \mathcal{E} et \mathcal{D} s'effectuent en $\mathcal{O}(1)$.

2 Formalisation des machines de Mealy

Définition 2: Transducteur

Un *transducteur* est un sextuplet $T = (\Sigma_1, \Sigma_2, Q, q_0, \delta)$ tel que :

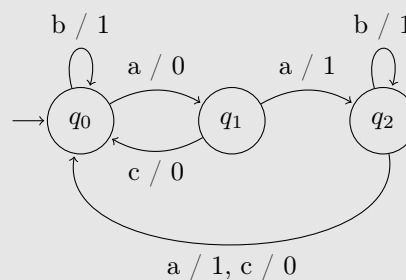
- Σ_1 est l'alphabet d'entrée,
- Σ_2 est l'alphabet de sortie,
- Q est l'ensemble des états,
- $q_0 \in Q$ est l'état initial,
- $\delta : Q \times \Sigma_1 \rightarrow Q \times \Sigma_2$ est la fonction de transition.

Exemple 2: Representation graphique

Le transducteur $T = (\{a, b, c\}, \{0, 1\}, \{q_0, q_1, q_2\}, q_0, \delta)$ Avec δ

État actuel	Symbole lu	État suivant	Sortie
q_0	a	q_1	0
q_0	b	q_0	1
q_1	a	q_2	1
q_1	c	q_0	0
q_2	b	q_2	1
q_2	a	q_0	1
q_2	c	q_0	0

Peut être représenté par

**Définition 3: Machine de Mealy**

une *machine de mealy* $M = (\Sigma)$ est un transducteur tel que

Théorème 1:

Soit Σ un alphabet et $N \in \mathbb{N}$ Il existe $(|\Sigma|! \times N^{|\Sigma|})^{|N|}$ Machines de Mealy a N états.

Démonstration 1:

Ainsi il y a $(|\Sigma|! \times N^{|\Sigma|})^{|N|}$

Remarque 3:

N	$(26! \times N^{26})^{ N }$
1	4.03×10^{26}
2	7.32×10^{68}
3	1.08×10^{117}
4	1.09×10^{169}
5	7.84×10^{223}

Remarque 4: synthese

Soit m un message sur Σ et k la clé choisie

Chiffre	Complexité <i>de E</i>	Complexité <i>de D</i>	Complexité de l'attaque par force brute
---------	---------------------------	---------------------------	--