Application des transducteurs finis à la cryptographie

Thibault Lestienne N°14454

June 3, 2025

Sommaire

.

1 Chiffre

Définition 1: chiffre
Un *chiffre* sur (M, N, C) est défini par un couple (E, D) avec

- M l'ensemble des messages chiffrables
- N l'ensemble des messages chiffrés
- C l'ensemble des clés
- la fonction de chiffrement $E : M \times C \to N$
- la fonction de déchiffrement $D : N \times C \to M$

et est tel que $\forall w \in M, \forall c \in C, w = D(E(w, c), c)$

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	$\cdots$	Y	Z
0	1	2	3	4	5	6	7	8	9	10	$\cdots$	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 :

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

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

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

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

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

Le message chiffré est donc DOCD.
Pour le déchiffrement, on utilise $D(k, c)$:

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

Le message déchiffré est donc TEST.

Remarque 1:
Deux occurences de la même lettre seront encodées par la même lettre.

Remarque 2:
Dans ce cas, les fonctions E et D s'effectuent en $\mathcal{O}(|w|)$.

2 Transducteur

Définition 2: Transducteur
Un *transducteur* est un quintuplet $T = (\Sigma_1, \Sigma_2, Q, q_0, \delta)$ 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,
- $\delta : Q \times \Sigma_1 \to Q \times \Sigma_2$ est la fonction de transition.

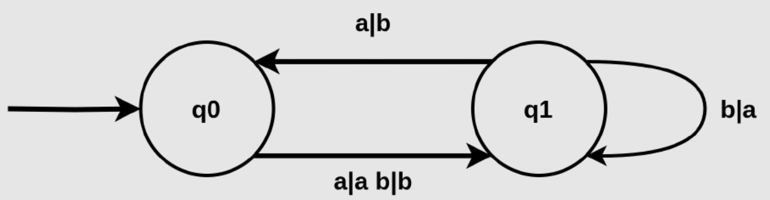
on ajoutera dans le cadre de cet exposé la contrainte :

$\forall q \in Q, f : c \mapsto \delta_2(q, c)$ est une bijection de Σ_1 dans Σ_2 ce qui implique $|\Sigma_1| = |\Sigma_2|$

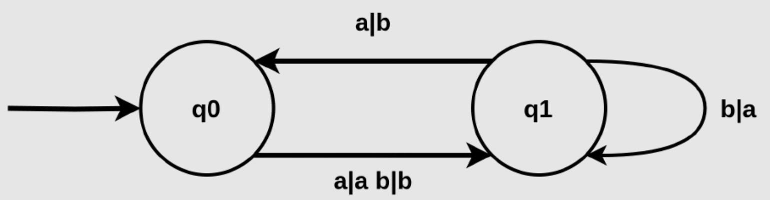
Exemple 2: Représentation graphique
Le transducteur $T = (\{a, b\}, \{a, b\}, \{q_0, q_1\}, q_0, \delta)$ avec δ :

État initiale	Symbole lu	État final	Symbole de sortie
q_0	a	q_1	a
q_0	b	q_1	b
q_1	a	q_0	b
q_1	b	q_1	a

Peut être représenté par



Exemple 3: Fonction de chiffrement sur les transducteurs
On pose l'algorithme de chiffrement suivant :

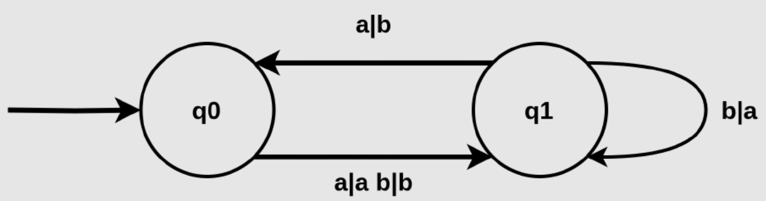


État initiale	Mot de départ	État suivant	Mot de sortie
q_0	a	q_1	a
q_1	b	q_1	a
q_1	a	q_0	b
q_0	b	q_1	b

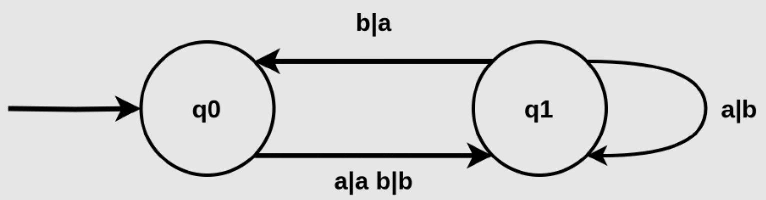
Ainsi le mot "abab" est encodé par "aabb" par le transducteur ci-dessus

Définition 3: Transducteur inverse
Le *transducteur inverse* noté T^{-1} d'un transducteur $T = (\Sigma_1, \Sigma_2, Q, q_0, \delta)$
est tel que $T^{-1} = (\Sigma_2, \Sigma 1, Q, q_0, \delta_{inv})$ avec $\forall q \in Q, \forall a \in \Sigma_2, \delta_{inv}(q, a) = (\delta_1(q, a), \delta_2^{-1}(q, a))$

Exemple 4: Transducteur inverse
le transducteur inverse de



est



Remarque 3: Représentation graphique du transducteur inverse
Dans le cadre de l'opération d'inversion consiste à intervertir l'ordre des lettres dans les couples.

Remarque 4:
Soit T un transducteur $(T^{-1})^{-1} = T$

Exemple 5: Fonction de déchiffrement sur les transducteurs
L'operation de déchiffrement consiste à chiffrer le message reçu avec le transducteur inverse du transducteur qui a servit à chiffrer le message

Théorème 1: Validité du chiffre
Les Opérations défini forme bien un chiffre

Démonstration 1:
Le point délicat est de prouver que :

$$\forall w \in \Sigma^*, \forall t \in T, w = D(E(w,t),t)$$

Cela se fait par récurrence sur la longueur du mot avec comme hypothèse de récurrence :

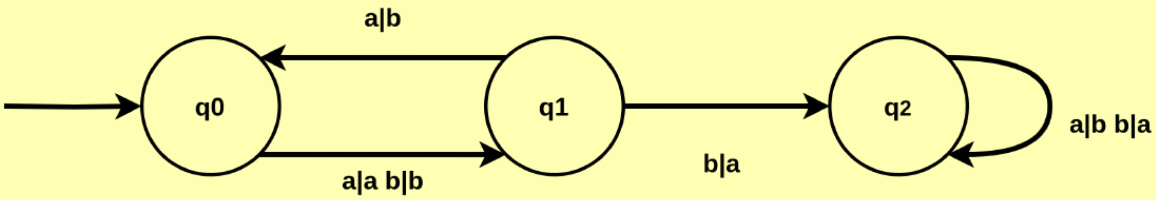
(Pn) :"$\forall w \in \Sigma n, \forall t \in T, w = D(E(w,t),t)$ et l'état final après l'encodage de w est le même que celui après décodage de $E(w,t)$"

Inintialisation
...
Hérédité
...

3 Analyse des faiblesses

Remarque 5: Méthode MCMC Pour les transducteurs à 1 état
A Faire ...

Remarque 6: Composantes connexes



Si l'on code un message qui commence par "ab" avec le transducteur précedent toute la fin du message pourra être decoder de la facon précedente. De Plus on intuite que pour maximiser la sécurité des données les transducteurs ne doivent posseder qu'une seule composante fortement connexe. On utilisera donc l'algorithme de Kosaraju pour verifier ce point lors de la génération de transducteur.

Théorème 2:
Soit
A : Deux lettres successives dans le message original sont identiques.
B : Deux lettres successives dans le message chiffré sont identiques.

$N = \frac{|\Sigma| \times P(A) - 1}{|\Sigma| \times P(B) - 1}$

Démonstration 2:
$P(B|A) = 1/N + \frac{N-1}{N} \times \frac{1}{|\Sigma|}$

$P(B|\overline{A}) = \frac{N-1}{N} \times \frac{1}{|\Sigma|}$

$P(B) = P(A) \times P(B|A) + P(\overline{A}) \times P(B|\overline{A})$

$P(B) = (1/N + \frac{N-1}{N} \times \frac{1}{|\Sigma|}) * P(A) + (\frac{N-1}{N} \times \frac{1}{|\Sigma|}) * P(\overline{A})$

$P(B) = \frac{1}{N} \times P(A) + \frac{N-1}{N|\Sigma|} \times (P(A) + P(\overline{A}))$

$P(B) = \frac{1}{N} \times P(A) + \frac{N-1}{N|\Sigma|}$

$P(B) = \frac{N-1+P(A) \times |\Sigma|}{N|\Sigma|}$

$N|\Sigma| \times P(B) = N - 1 + P(A) \times |\Sigma|$

$N(|\Sigma| \times P(B) - 1) = P(A) \times |\Sigma| - 1$

$N = \frac{|\Sigma| \times P(A) - 1}{|\Sigma| \times P(B) - 1}$

4 Conclusion

Remarque 7: synthèse

Chiffrement	**César**	**Vigenère**	**RSA**	**Transducteur**
Est humainement utilisable	Oui	Oui	Non	Oui
Temps moyen nécessaire pour un humain pour encoder un caractère	2.5 s	4.6 s	N/A	4.9 s
La clé peut être mémorisée par un humain	Oui	Oui	N/A	Non
Actuellement décodable par ChatGPT	Oui	Oui	Non	Non
Déchiffrable sans la clé en temps raisonnable	Oui	Oui	Non démontré	Non démontré
Déchiffrable sans la clé en temps infini	Oui	Oui	Oui	Non démontré