

Application des transducteurs finis à la cryptographie



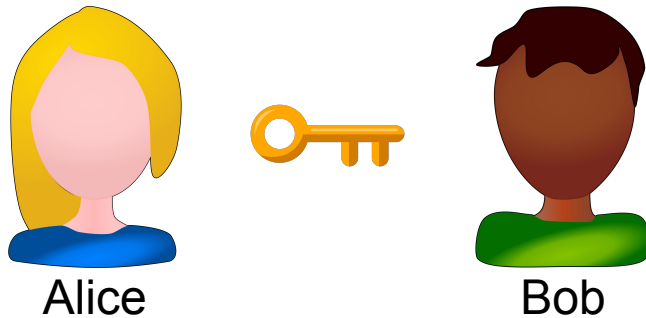
Source image : <https://cryptoast.fr/wp-content/uploads/2020/04/keys-cryptography.jpg>

Thibault Lestienne
n°14454

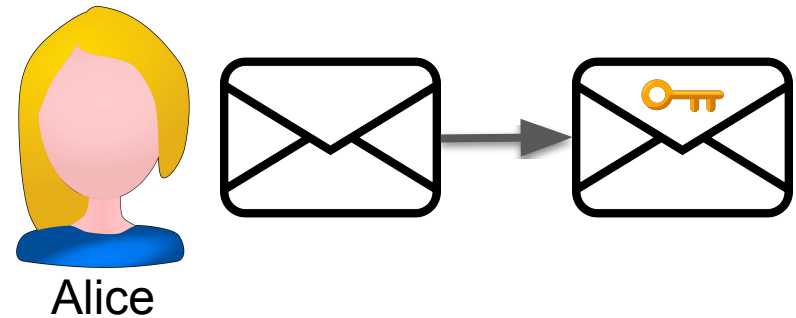
Dans quelle mesure les transducteurs finis peuvent-ils être une alternative sécurisée pour le transfert de l'information?

Objectif

Alice et Bob s'accordent sur une clé



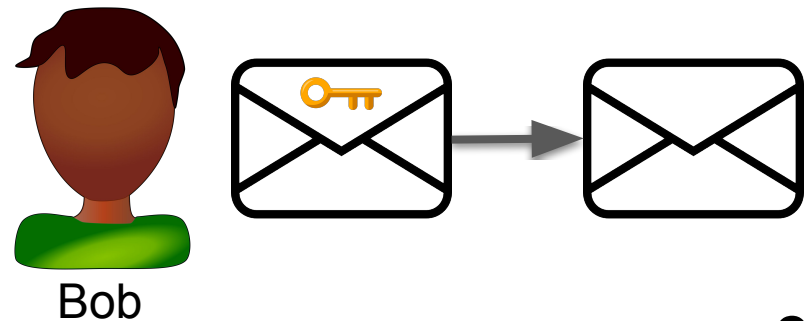
Alice écrit un message pour Bob
et le chiffre avec la clé



Claire transmet le message



Bob déchiffre le message à
l'aide de la clé et lit le message
envoyé par Alice



Sources images : <https://github.com/greenway/alicebobandeve>
<https://www.pngegg.com/fr/png-monuc/download>

<https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTCw1FOCL0RZgq6QxvrUa4cob0LFQH-9RkWWwKWxvkKq0dJl8qVb>

Plan

- I - Le chiffre de César
- II - Présentation des transducteurs
- III - Analyse du chiffre proposé
- IV - Applications concrètes

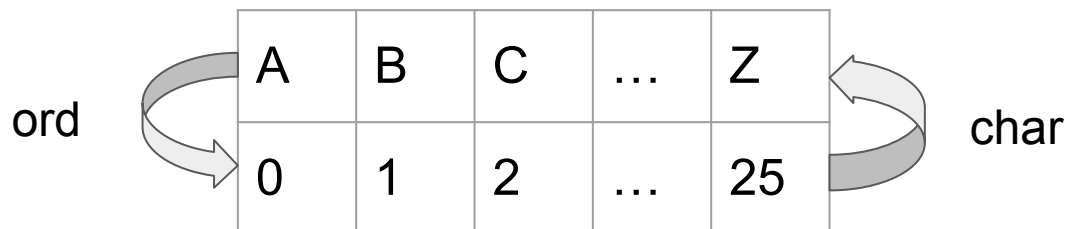
Formalisation

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 $E : M \times C \rightarrow N$
- la fonction de déchiffrement $D : N \times C \rightarrow M$

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

Chiffrement de César



Exemple Clé $c = 10$

$\Sigma = \{a, b, \dots, z\}$

$(M, N, C) = (\Sigma^*, \Sigma^*, [0; 25])$

$E_p : x, c \mapsto \text{char}((\text{ord}(x) + c) \bmod 26)$

$E : w, c \mapsto \forall i, w_i = E_p(w_i)$

$D_p : x, c \mapsto \text{char}((\text{ord}(x) - c) \bmod 26)$

$D : w, c \mapsto \forall i, w_i = D_p(w_i)$

x	T	E	S	T
ord(x)	19	4	18	19
ord(x)+c	29	14	28	29
(ord(x)+c)mod 26	3	14	2	3
Ep(x,c)	D	O	C	D

Attaque par force brute

message intercepté : **qdcydgpidjh**

0	qdcydgpidjh	9	zmlhmsspyrmsq	18	ivuqvbyhavbz
1	redzekhqjeki	10	anmintqzsnt	19	jwvrvwczibwca
2	sfeafllirkflj	11	bonjouratous	20	kxwsxdajcxdb
3	tgfbgmjslgmk	12	cpokpvsbupvt	21	lyxtyebkdyec
4	uhgchnktmhn1	13	dqplqwtcvqwu	22	mzyuzfclezfd
5	vihdloluniom	14	erqmrxdwrxv	23	nazvagdmfage
6	wjiejpmvojpn	15	fsrnsyvexsyw	24	obawbhengbhf
7	xkjfkqnwpkqo	16	gtsotzfwfytzx	25	pcbxcifohcig
8	ylkg1roxqlrp	17	hutpuaxgzauy		

Automatisation : Analyse de fréquence

Lettre	Fréquence	Lettre	Fréquence	Lettre	Fréquence
A	8.84%	J	0.53%	S	7.50%
B	1.05%	K	0.006%	T	7.67%
C	3.15%	L	5.96%	U	6.38%
D	3.52%	M	2.82%	V	1.81%
E	17.1%	N	6.73%	W	0.01%
F	1.10%	O	5.16%	X	0.33%
G	0.93%	P	2.61%	Y	0.36%
H	0.97%	Q	1.19%	Z	0.15%
I	7.50%	R	6.41%		

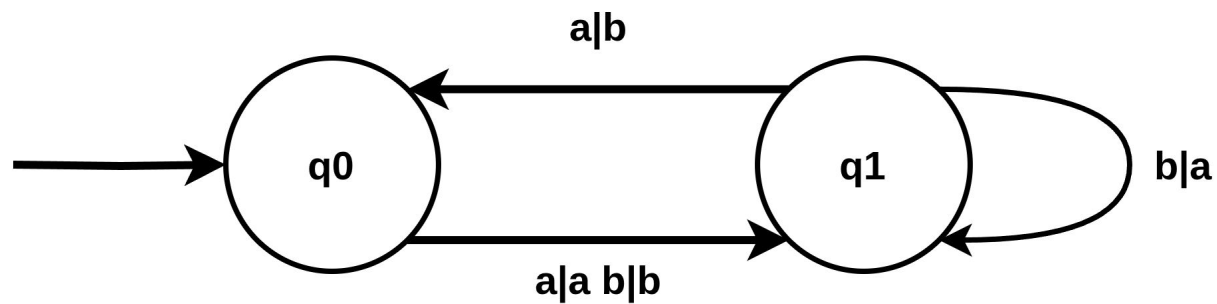
A partir du texte *Des Misérables* de Victor Hugo

Recherche de la clé minimisant les écarts de fréquences

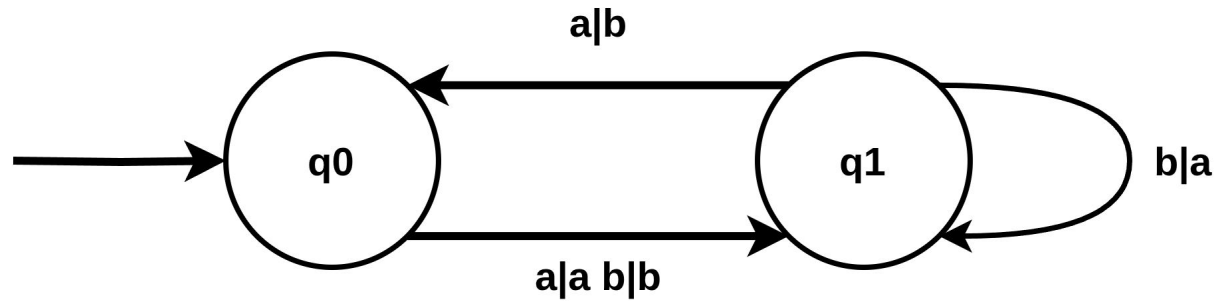
$$f(x) = \operatorname{argmin}_{i \in [0, 25]} \sum_{c=a'}^{c=z'} \operatorname{freqth}(c) - \operatorname{freq}(D(c, i))$$

0	1.584441	9	1.440731	18	1.445246
1	1.249991	10	1.033370	19	1.420465
2	1.085935	11	1.004318	20	1.509557
3	1.447905	12	1.292903	21	1.224687
4	1.306998	13	1.353504	22	1.364631
5	1.182302	14	1.382257	23	1.314707
6	1.289146	15	1.347347	24	1.346961
7	1.644467	16	1.534583	25	1.541625
8	1.539500	17	1.434164		

Approche simplifiée des transducteurs

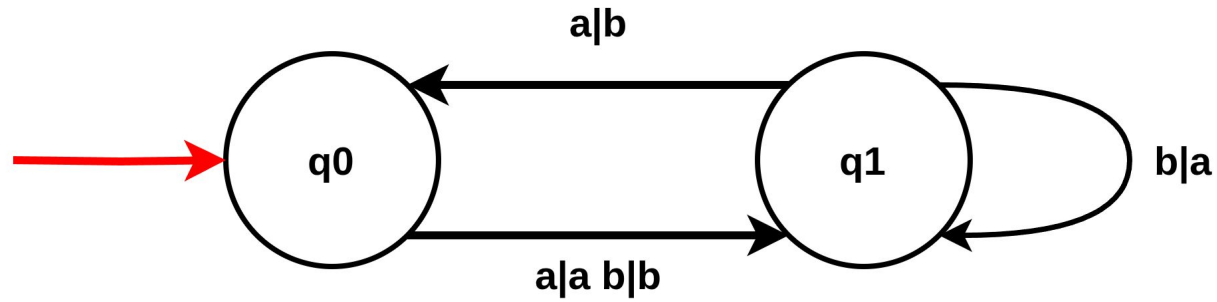


Chiffrer avec un transducteur



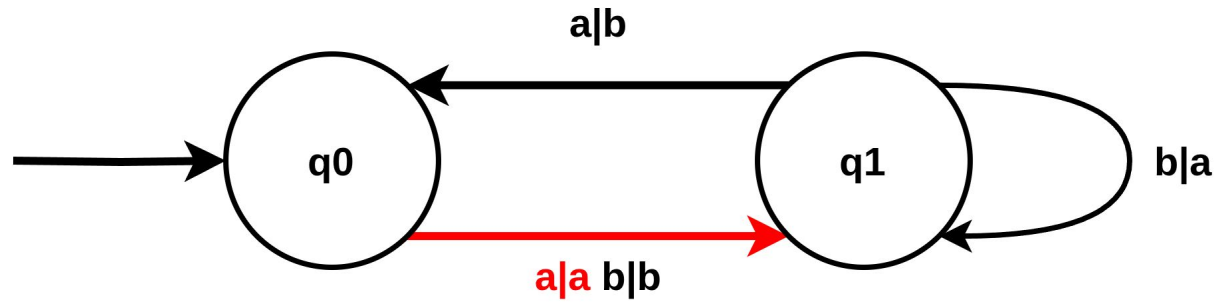
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1		a		
2		b		
3		a		
4		b		

Chiffrer avec un transducteur



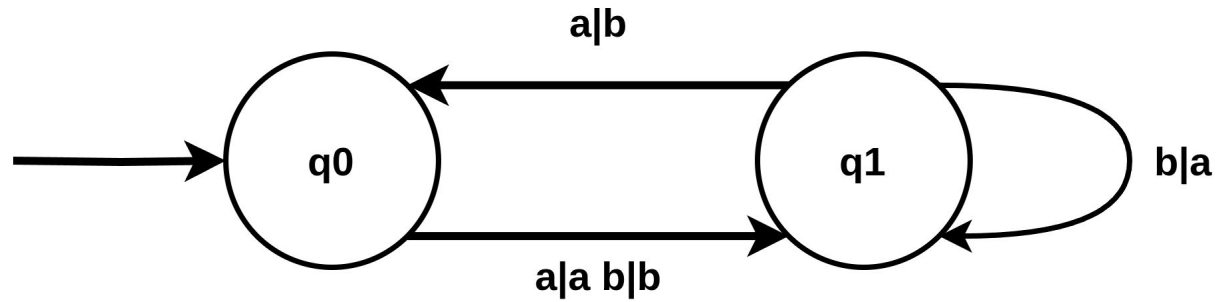
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a		
2		b		
3		a		
4		b		

Chiffrer avec un transducteur



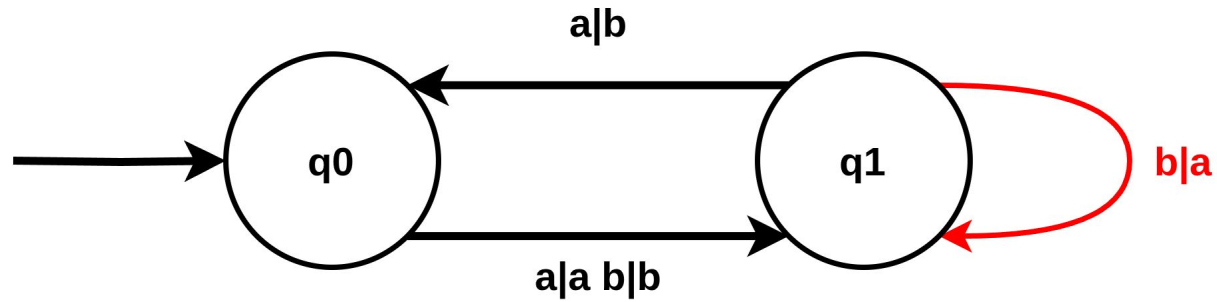
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2		b		
3		a		
4		b		

Chiffrer avec un transducteur



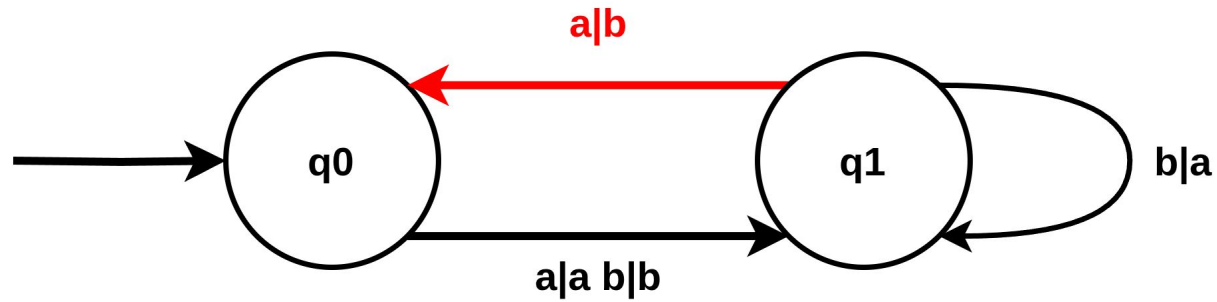
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2	1	b		
3		a		
4		b		

Chiffrer avec un transducteur



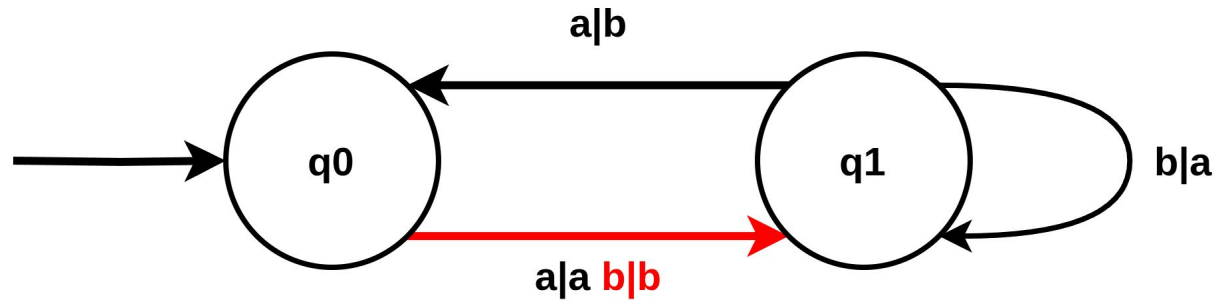
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2	1	b	1	a
3	1	a		
4		b		

Chiffrer avec un transducteur



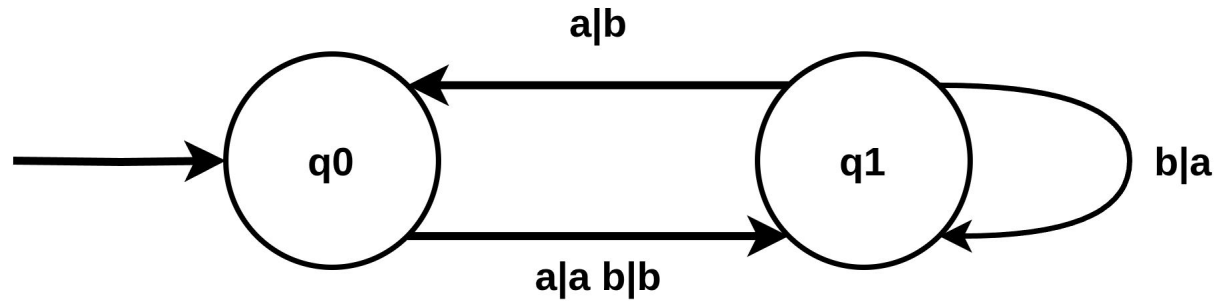
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2	1	b	1	a
3	1	a	0	b
4	0	b		

Chiffrer avec un transducteur



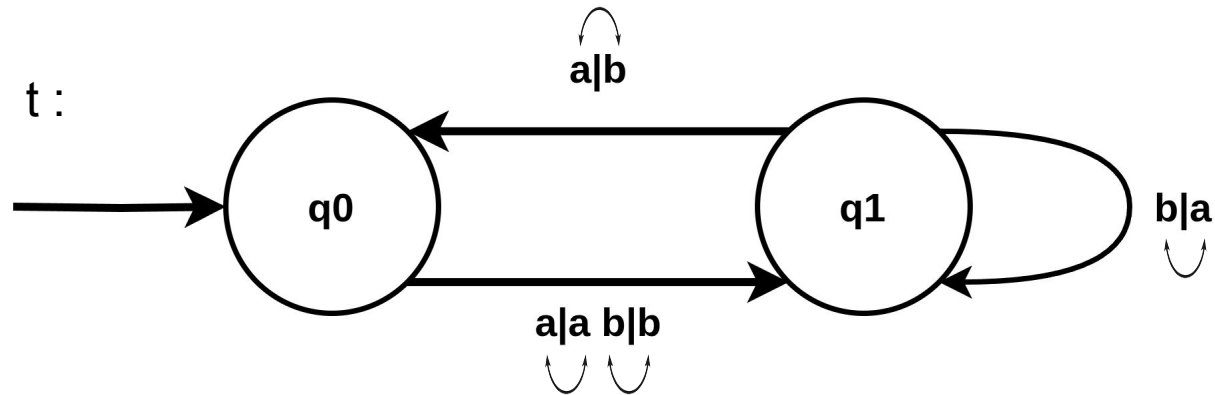
Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2	1	b	1	a
3	1	a	0	b
4	0	b	1	b

Chiffrer avec un transducteur

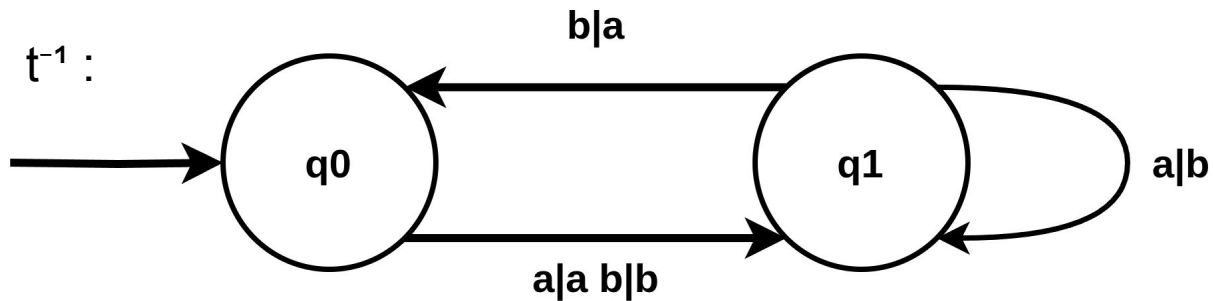


Etape	état initial	lettre à encoder	état suivant	lettre encodée
1	0	a	1	a
2	1	b	1	a
3	1	a	0	b
4	0	b	1	b

Calcul du transducteur inverse

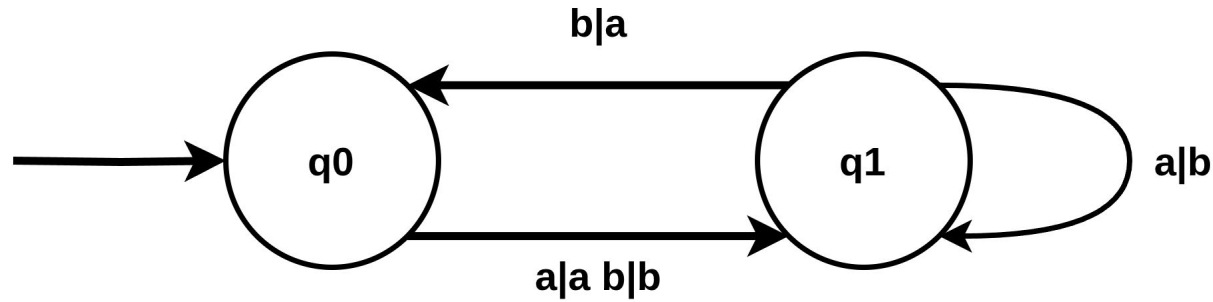


s'inverse en



Remarque : $(t^{-1})^{-1} = t$

Déchiffrer avec un transducteur



Etape	état initial	lettre encodée	état suivant	lettre décodée
1	0	a	1	a
2	1	a	1	b
3	1	b	0	a
4	0	b	1	b

Transducteur : définition

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,
- $\delta : Q \times \Sigma_1 \rightarrow Q \times \Sigma_2$ est la fonction de transition.

On ajoutera dans le cadre de cet exposé la contrainte :

$$\forall q \in Q, \quad c \mapsto \delta_2(q, c) \text{ est une bijection de } \Sigma^* \text{ dans } \Sigma^*.$$

On note T l'ensemble des transducteurs avec $\Sigma_1 = \Sigma_2 = \{a, b, \dots, z\}^*$

Démonstration de “ (E,D) est un chiffre sur (Σ^*,Σ^*,T) ”

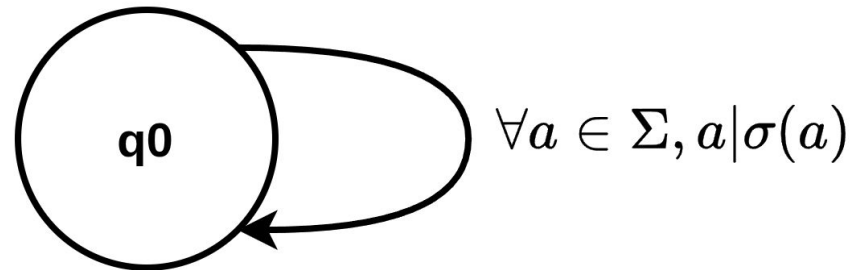
Le point délicat est de prouver que :

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

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

$(P_n) :$ “ $\forall w \in \Sigma^n, \forall t \in T, w = D(E(w, t), t)$ et l’état final après l’encodage de w est le même que celui après décodage de $E(w, t)$ ”

Cas des transducteurs à un état : méthode MCMC



A	$\sigma(A)$
B	$\sigma(B)$
...	...
Z	$\sigma(Z)$

Cas des transducteurs à un état : méthode MCMC

Lettre (français)	Fréquence en français
A	8.84%
B	1.05%
C	3.15%
D	3.52%
E	17.1%
F	1.10%
G	0.93%
...	...
Z	0.15%

Fréquence dans le message intercepté	Lettre (message)
7.04%	A
3.02%	B
0.12%	C
0.53%	D
1.23%	E
18.4%	F
0.01%	G
...	...
1.34%	Z

Alignement des fréquences

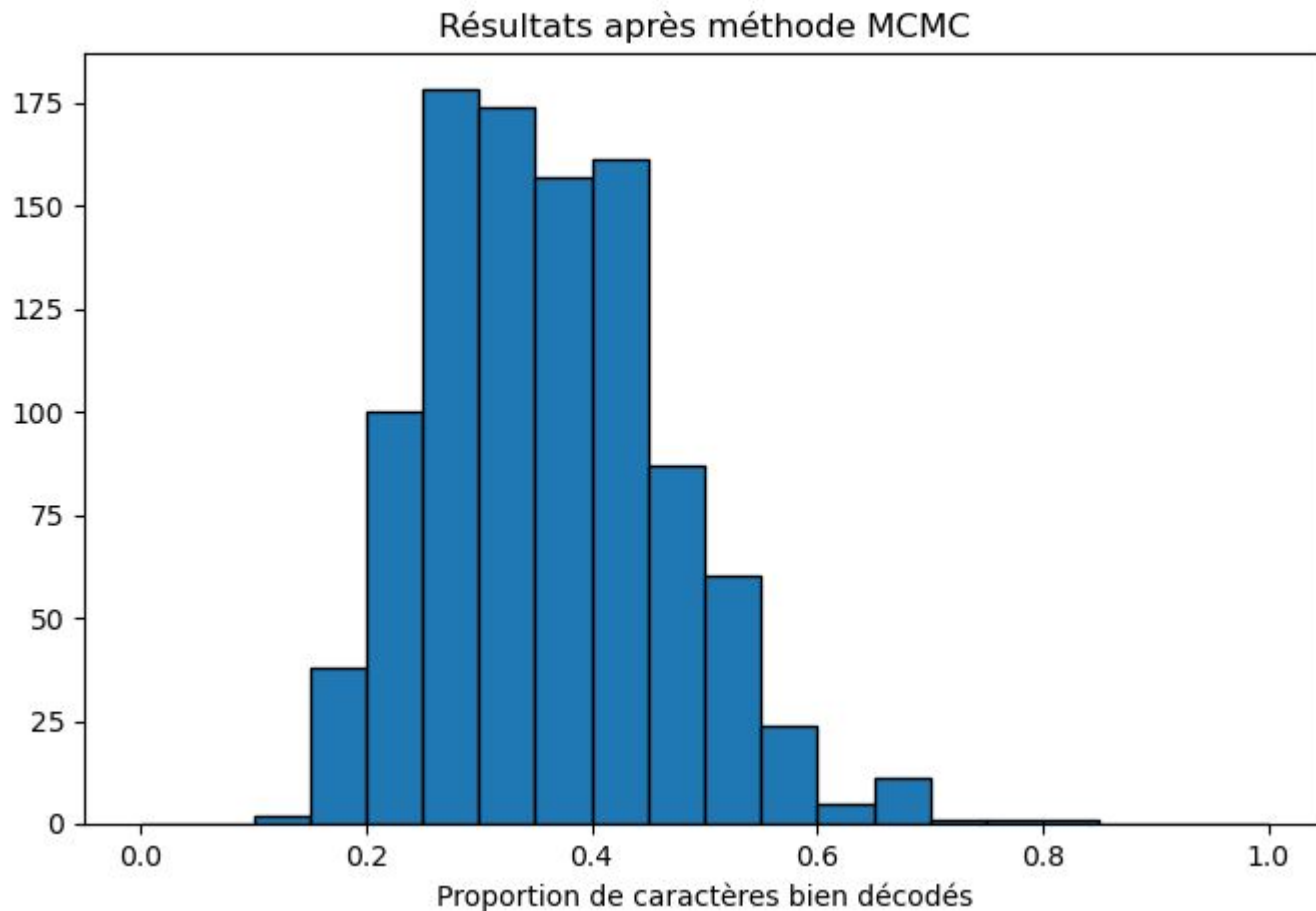
Lettre (français)	Fréquence en français	Fréquence dans le message intercepté	Lettre (message)
E	17.1%	18.4%	F
A	8.84%	8.6%	H
T	7.67%	7.8%	W
S	7.50%	7.45%	P
I	7.50%	7.04%	A
N	6.73%	6.76%	R
R	6.41%	6.51%	N
...
K	0.006%	0.007%	U



Lettre (français)	Lettre (message)
E	F
A	H
T	W
S	P
I	A
N	R
R	N
...	...
K	U

Alignement des fréquences

Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



sdnseaoealotjeasdnseaoeaeufiezldra

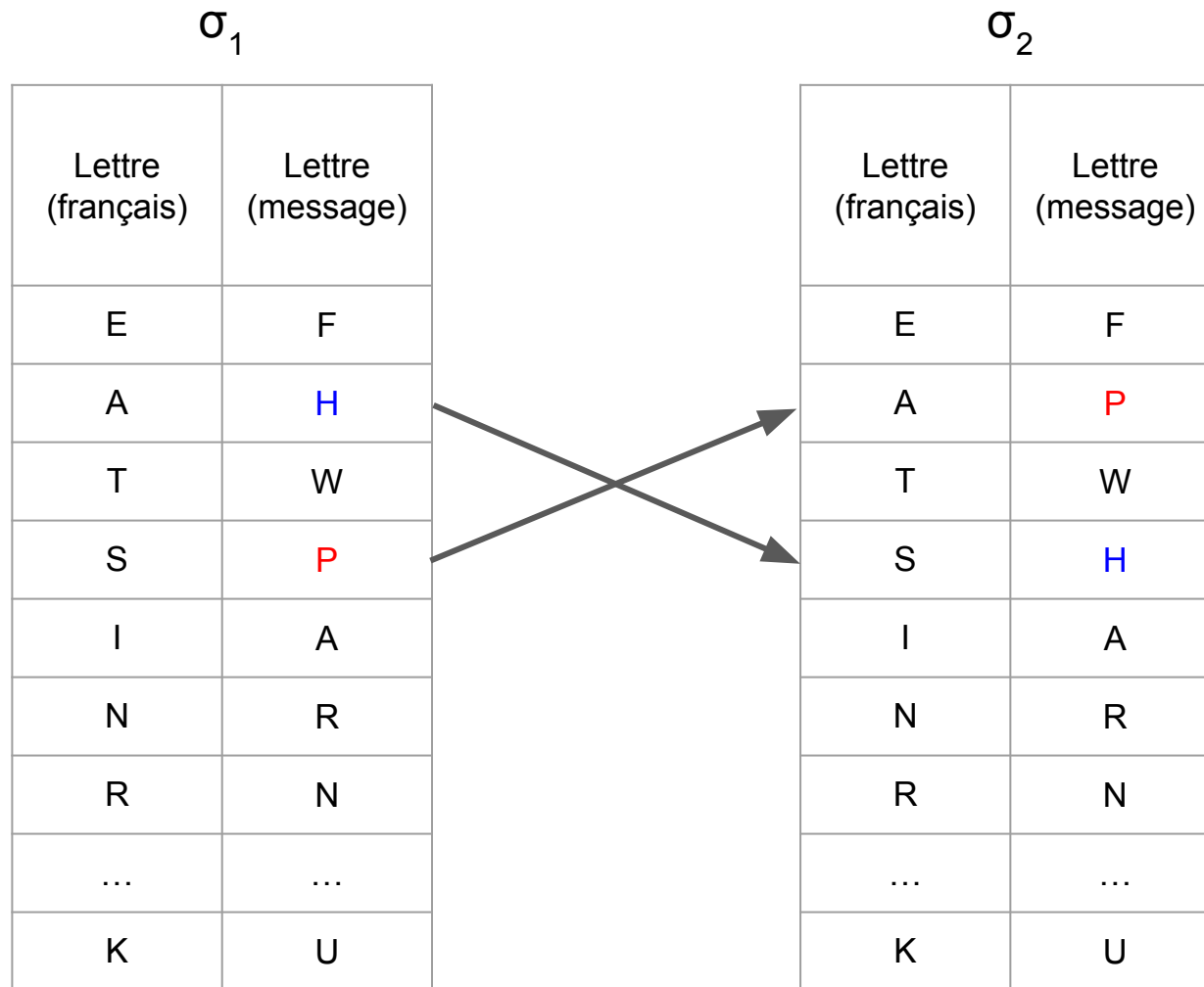
Exploitation des fréquences des couples de lettres

En français certaines successions de lettres sont plus probables que d'autres. On s'attend par exemple à trouver plus de "qu" que de "qa"

On va chercher à minimiser $f(\sigma)$

$$f(\sigma) = \sum_{c_1='a'}^{c_1='z'} \sum_{c_2='a'}^{c_2='z'} |freqth(c_1c_2) - freq(\sigma(c_1)\sigma(c_2))|$$

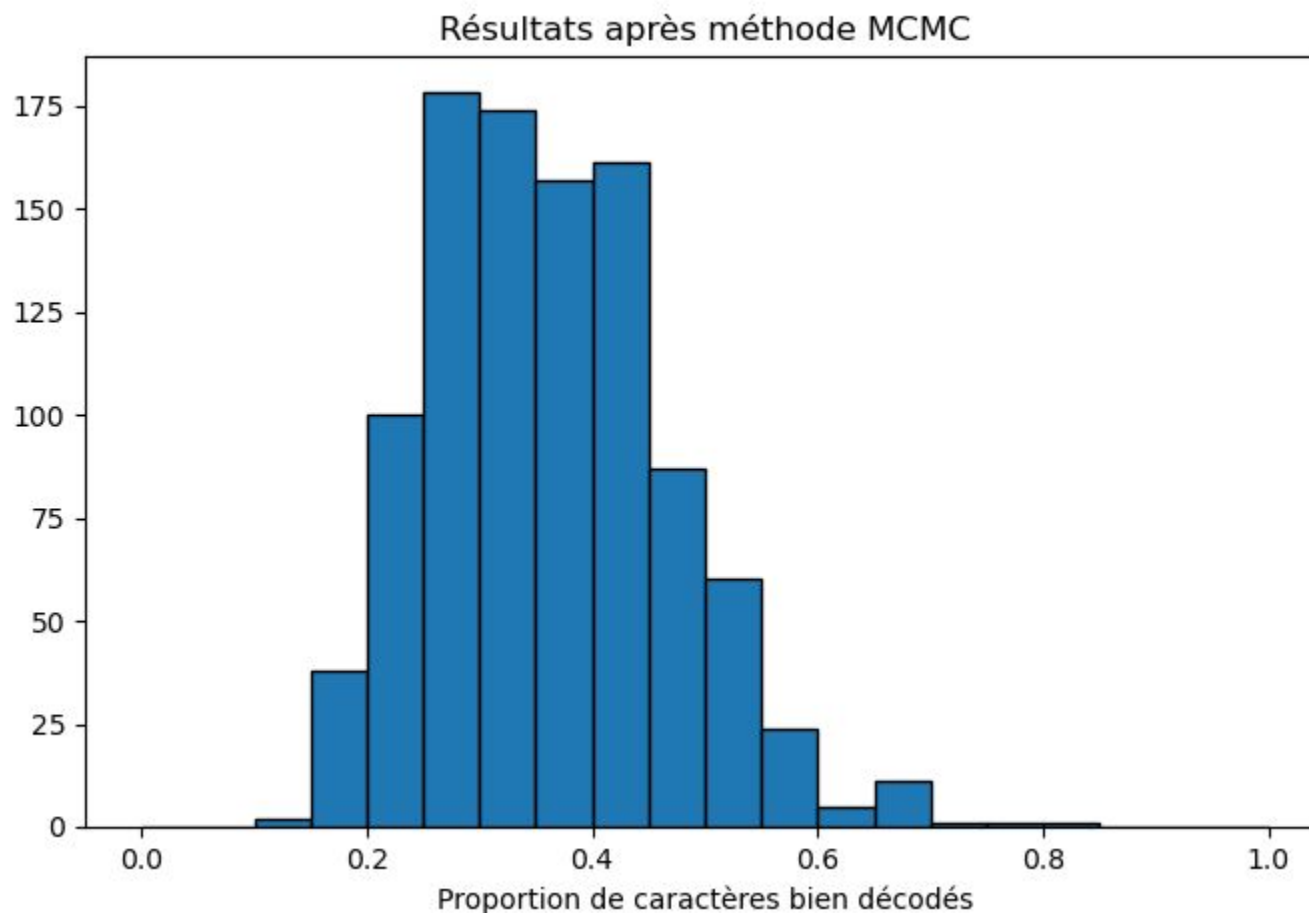
Alignement des fréquences



Si $f(\sigma_2) < f(\sigma_1)$ on itère le raisonnement sur σ_2 sinon sur σ_1

Résultat sans itérations

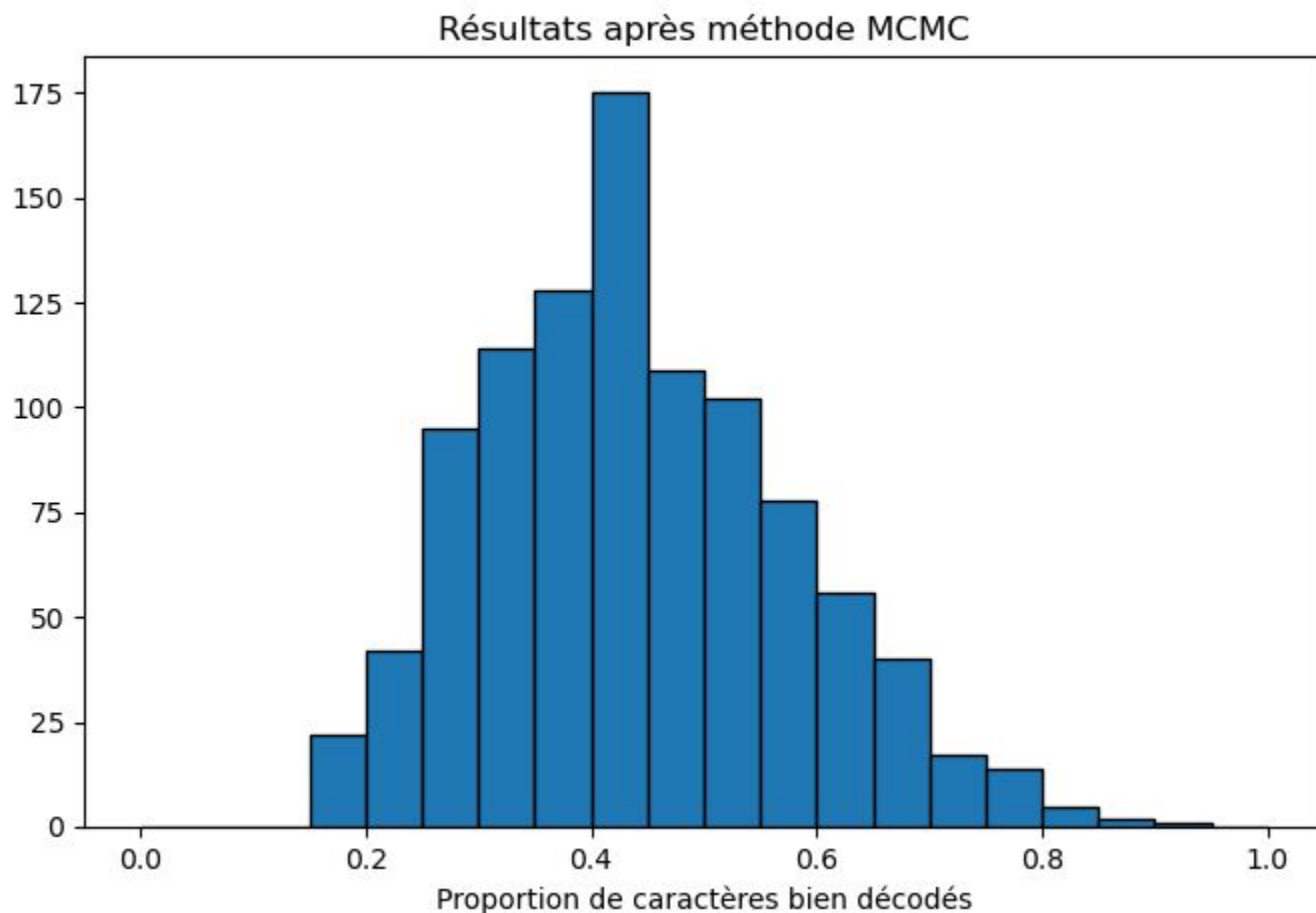
Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



sdnseaoealotjeasdnseaoeaeufiezldra

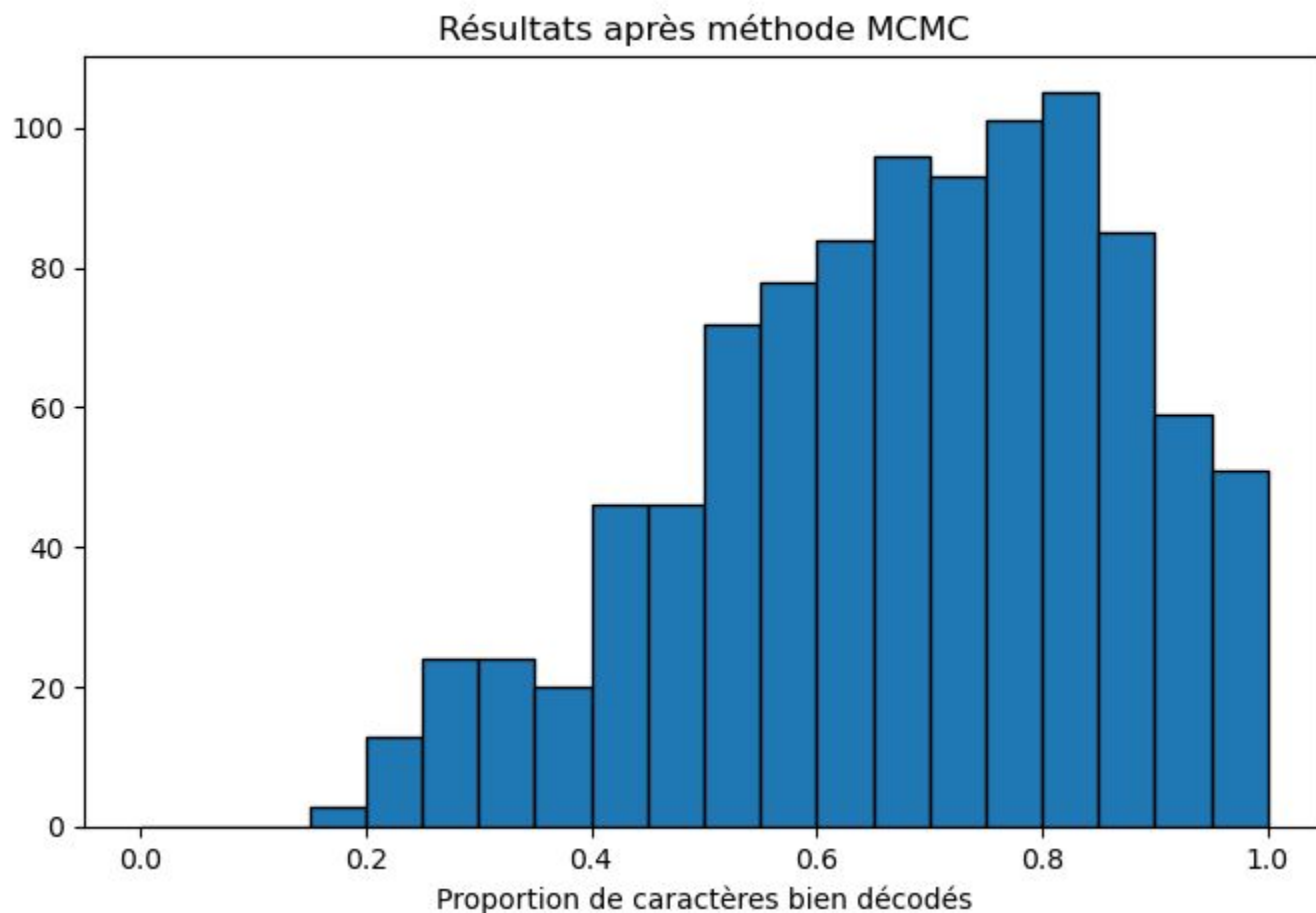
Résultat après 100 itérations

Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



Résultat après 500 itérations

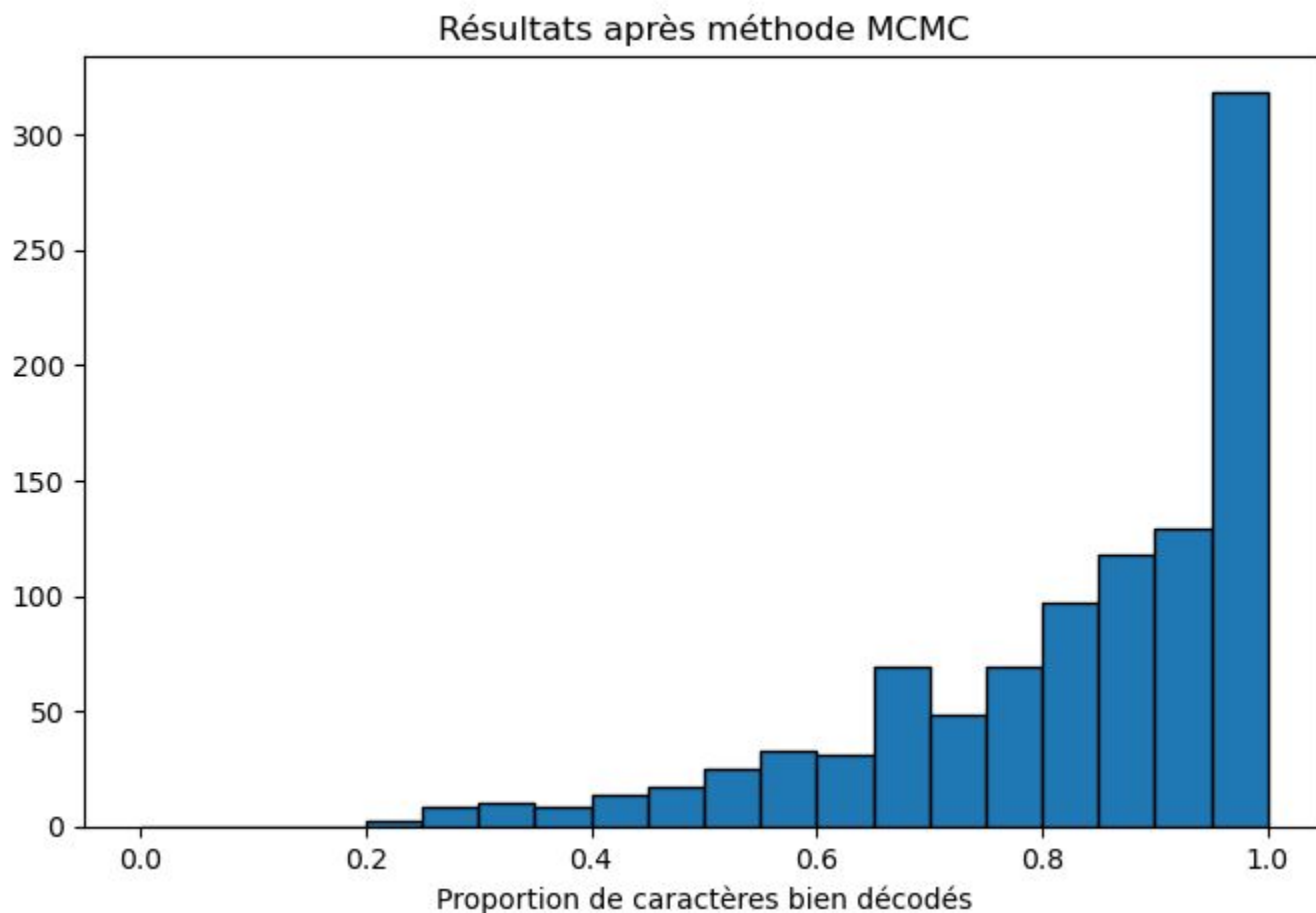
Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



notnesmesumagesnotnesmesreplebuois

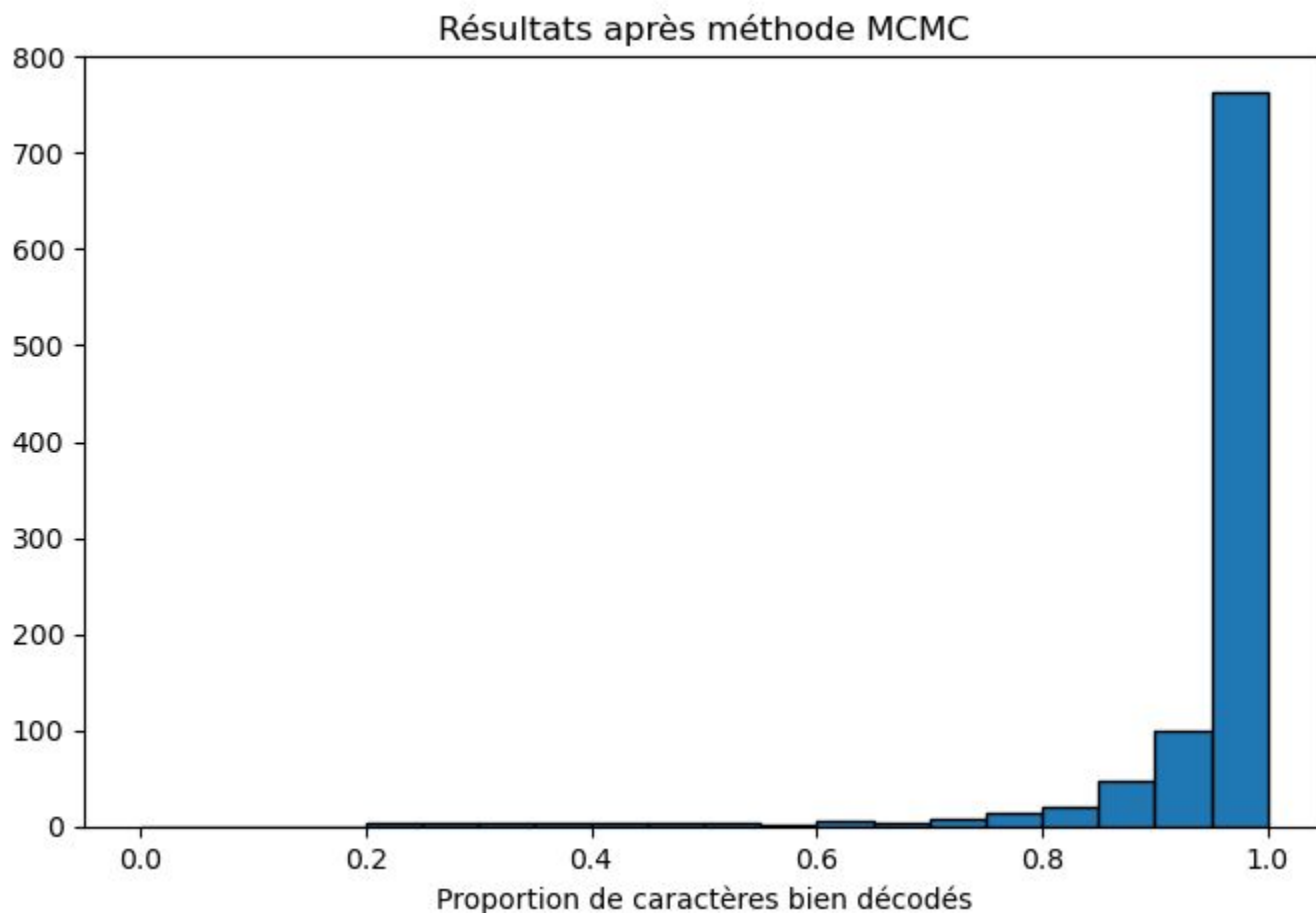
Résultat après 1 000 itérations

Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



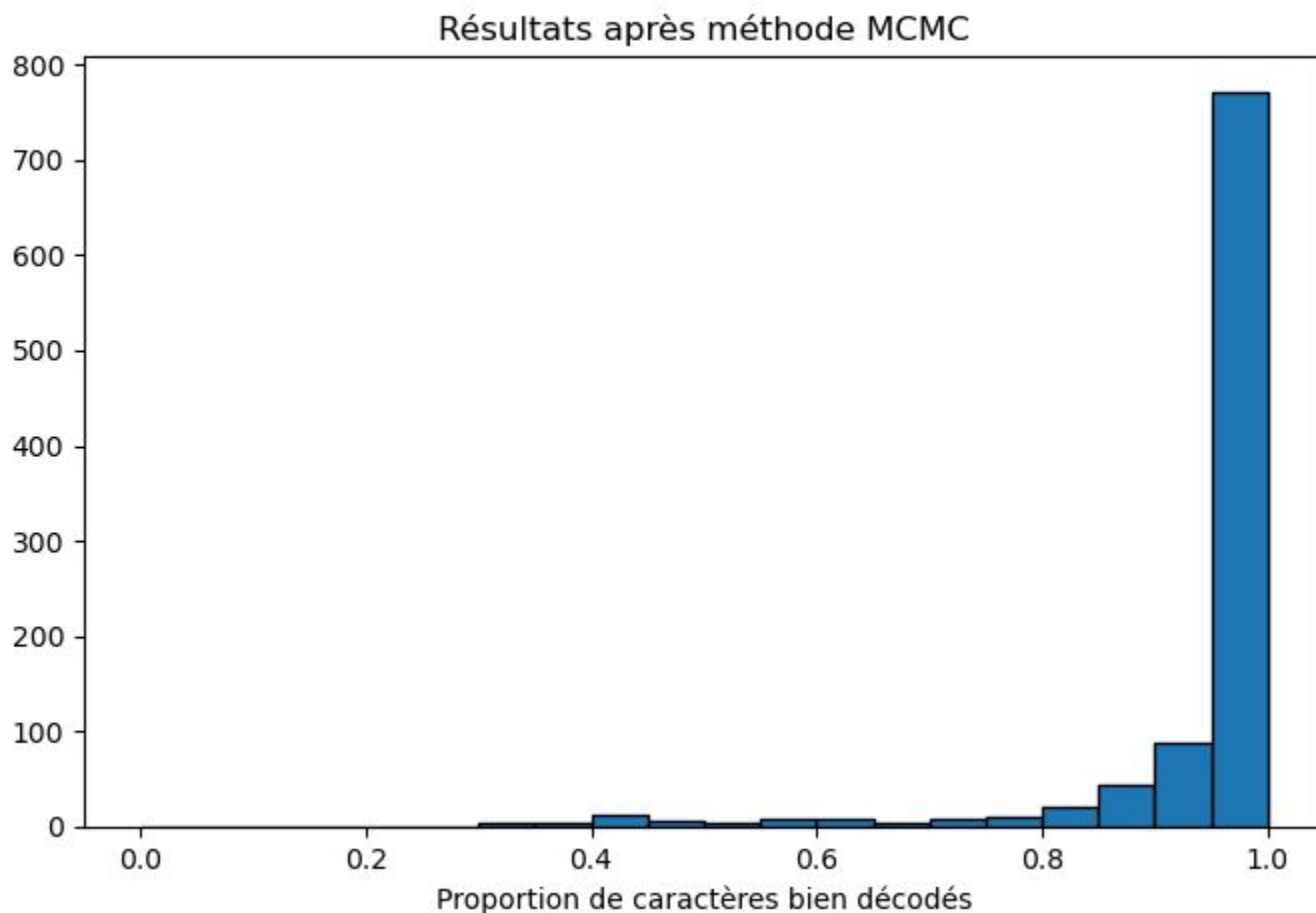
Résultat après 10 000 itérations

Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



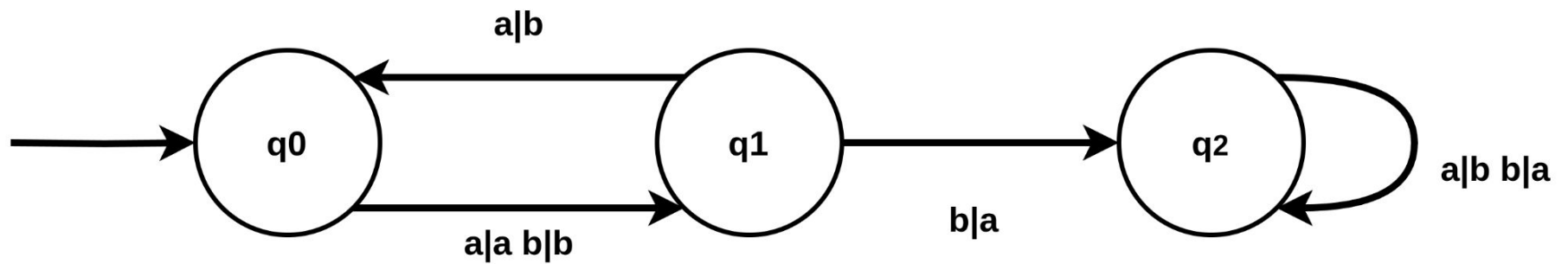
Résultat après 100 000 itérations

Test sur 1000 textes de 500 caractères issus de *À la recherche du temps perdu* de Marcel Proust



toutesmesimagestoutesmesreflexions

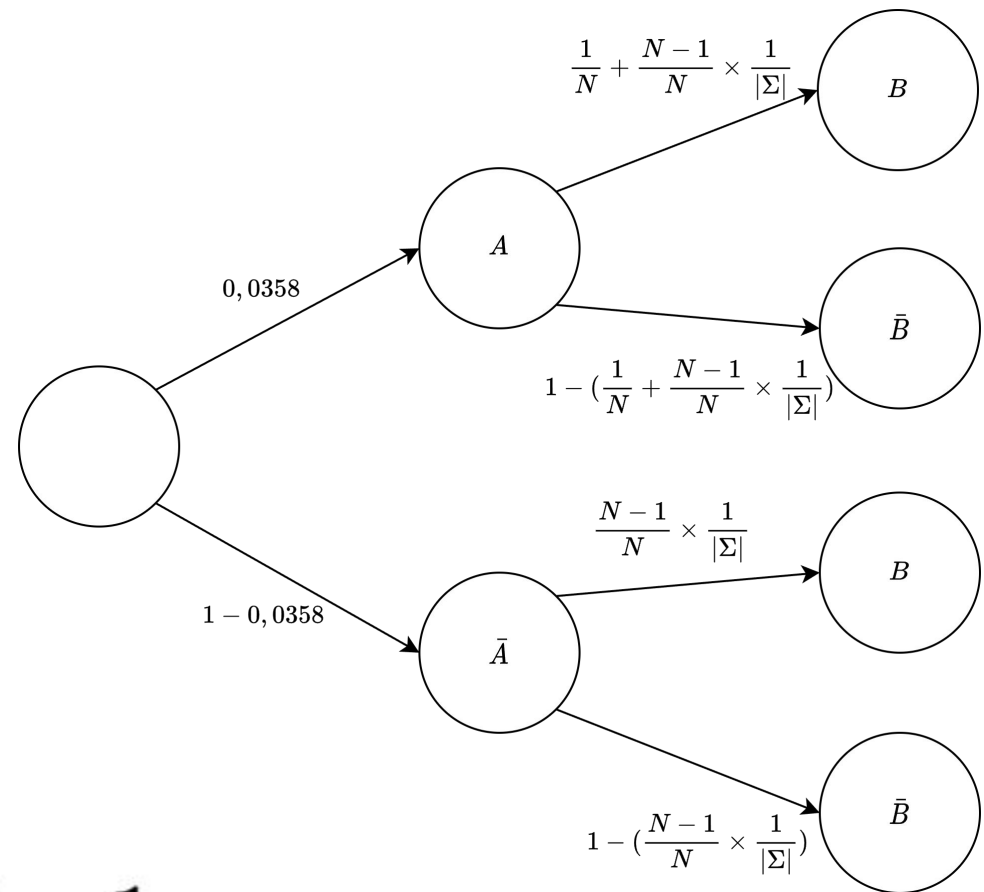
Les composantes connexes



Estimer le nombre d'état

A : Deux lettres successives dans le message original sont identiques

B : Deux lettres successives dans le message chiffré sont identiques



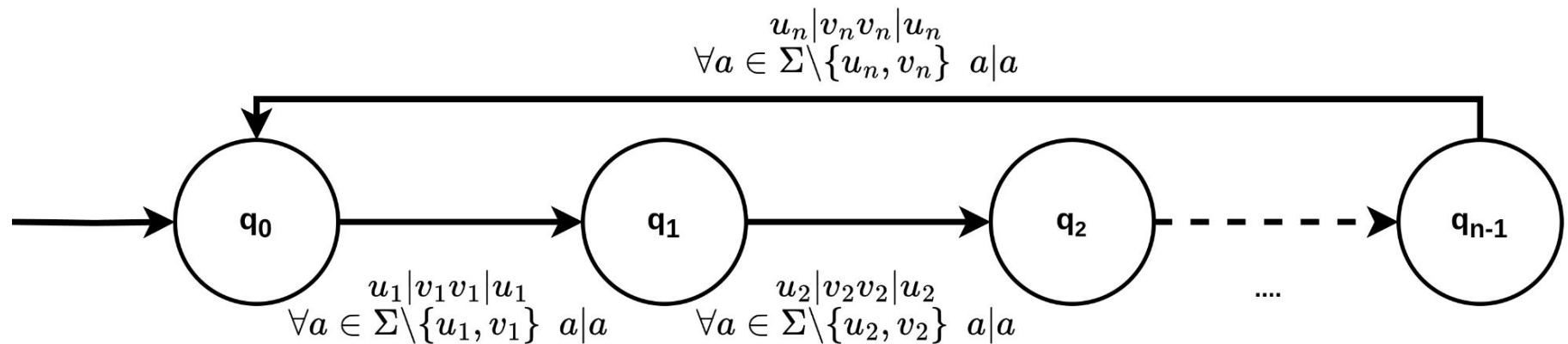
$$N = \frac{|\Sigma| \times P(A) - 1}{|\Sigma| \times P(B) - 1}$$

Démonstration de “ $\forall n \in \mathbb{N}, u, v \in \Sigma^n, \exists t \in T, E(u, t) = v$ ”

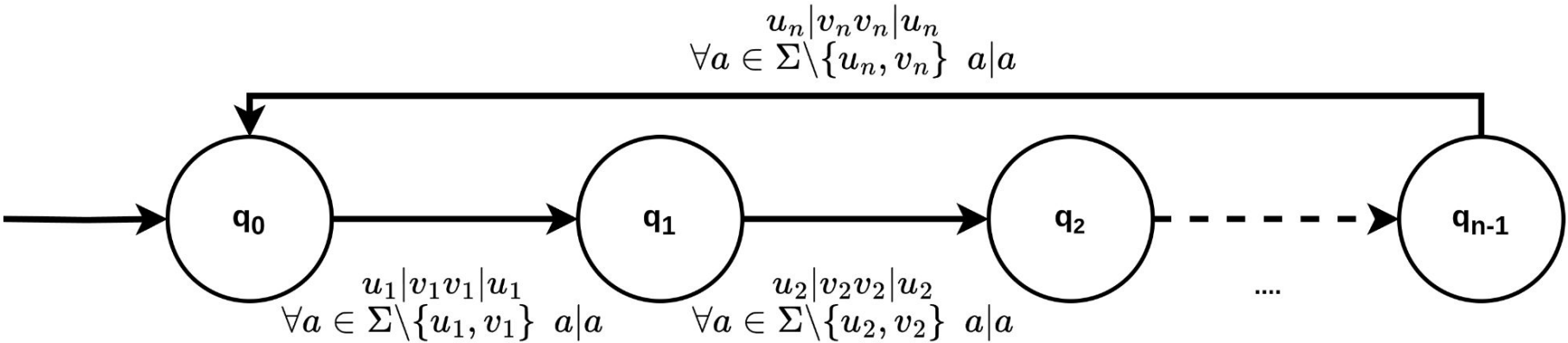
Soit $n \in \mathbb{N}, u, v \in \Sigma^n$

On note $u = u_1 u_2 \dots u_n$ et $v = v_1 v_2 \dots v_n$

On pose alors le transducteur t comme défini ci-dessous :



Démonstration de “ $\forall n \in \mathbb{N}, u, v \in \Sigma^n, \exists t \in T, E(u, t) =$



Etape	état initial	lettre encodée	état suivant	lettre décodée
1	0	u_1	1	v_1
2	1	u_2	2	v_2
...
n	n-1	u_n	0	v_n

Conséquence

Si l'attaquant qui ne possède pas la clé intercepte le message : “jdikes”, le message original peut être “gentil” ou “ennemi” ou n'importe quel autre mot de 6 lettres.

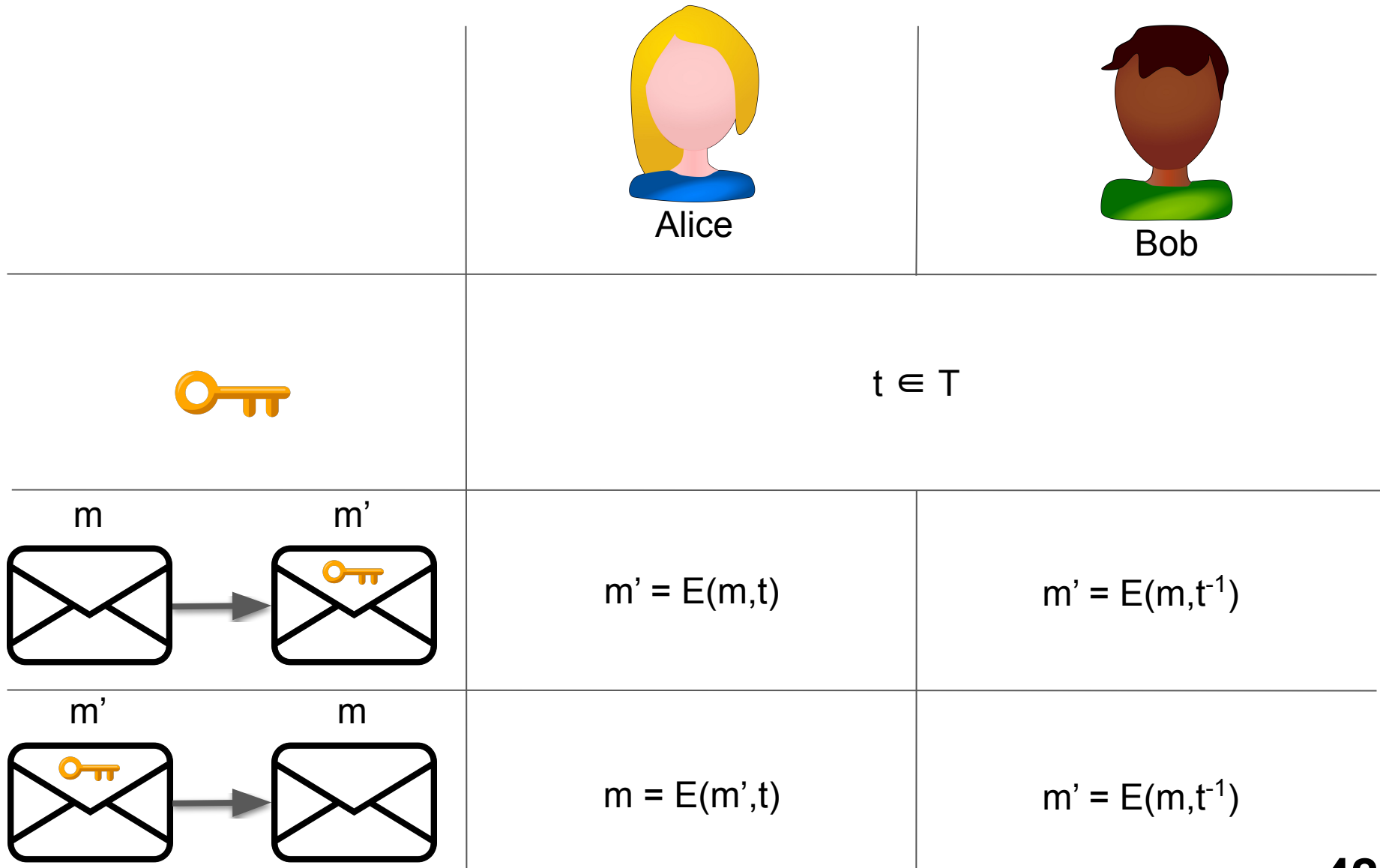
Chiffrer avec un ordinateur

The screenshot shows a web application window titled "Securisation de données". At the top, there is a button labeled "Choisir un transducteur" next to a text input field containing the word "transducteur". Below this is a large text area containing the sentence "La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages". Underneath the text area, there are three buttons: "Chiffrer", "Déchiffrer", and "Générer une clé". To the right of these buttons is a label "Nombre d'états" followed by a text input field containing the number "1000". At the bottom of the window is another large text area displaying a long string of encrypted text: "vetdrrbacyceuvljtp rjlqziuebobqjpkgfxjonvtsdvqpei axqgswmuyplcvnronifxzbzwpdpqswz".

Déchiffrer avec un ordinateur

The screenshot shows a web application window titled "Securisation de données". At the top, there is a button labeled "Choisir un transducteur" next to a text input field containing the word "transducteur". Below this, there is a large text area containing a long string of random characters: "vetdrrbacyceuvljtprijlqziuebobqjpkgfxjonvtsdvqpei axqgswuyplcvnronifxzbzwpdpqswz". In the center, there are three buttons: "Chiffrer", "Déchiffrer", and "Générer une clé". To the right of these buttons is a label "Nombre d'états" followed by a text input field containing the number "1000". At the bottom, there is another large text area containing a sentence in French: "la cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages".

Coder et décoder à la main



Sources images : <https://github.com/greenway/alicebobandeve>

<https://www.pngegg.com/fr/png-monuc/download>

<https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTCw1FOCL0RZgq6QxvrUa4cob0LFQH-9RkWWwKWxvkKq0dJl8qVb>

Coder et décoder à la main

		A		B		C		D		E		F		G		H		I		J		K		L		M		N		O		P		Q		R		S		T		U		V		W		X		Y		Z	
état 0		19c		1 x		0 a		19z		4 d		3 k		16p		12r		13e		12l		13j		9 i		19n		11q		6 v		15o		13t		14s		11b		16h		0 m		18w		7 g		14f		7 u		7 y	
état 1		4 z		3 j		19h		11v		3 c		12q		13t		8 p		8 f		15m		4 o		5 e		9 s		19x		18b		7 r		2 g		4 l		17a		17d		3 u		9 k		4 w		17i		16y		18n	
état 2		7 g		10m		8 x		15r		9 y		13b		8 e		5 j		14l		13u		5 q		10s		17z		8 c		18n		5 p		16h		5 a		1 k		0 w		1 v		14f		14t		15o		13i		14d	
état 3		1 o		2 c		1 v		7 z		17e		5 g		16d		1 t		15h		7 k		5 n		15w		7 b		5 s		17a		19x		12q		3 l		18j		5 r		7 u		7 f		14i		10p		14m		9 y	
état 4		16k		2 w		10j		2 q		3 a		1 t		12y		12s		12z		8 n		2 b		5 h		17o		11v		8 u		3 g		16d		4 e		16i		0 l		5 f		5 x		12r		12p		10m		15c	
état 5		5 x		18i		10u		8 e		13q		17k		11b		9 p		0 r		7 m		13d		17n		13s		11h		6 f		12a		2 t		19g		3 j		1 y		6 z		11l		1 v		12c		8 o		5 w	
état 6		5 y		4 d		16g		5 n		9 k		14u		6 b		15v		7 p		16c		19a		11j		17o		10e		8 m		6 z		5 f		6 s		16h		7 q		10t		15l		2 x		6 i		0 w		13r	
état 7		15y		0 h		17d		16q		13w		4 b		13k		13o		14m		14g		18t		16n		11c		0 e		12f		3 a		1 x		3 z		14l		18p		13r		16i		12s		5 u		18v		16j	
état 8		9 r		1 i		15f		7 q		17u		11p		13l		14e		0 k		11b		7 d		1 o		13y		15c		15t		12a		9 s		3 x		6 z		18m		0 j		8 g		10n		10v		2 h		5 w	
état 9		18q		19i		6 u		0 z		16b		7 f		11x		14l		18t		12y		1 g		9 n		1 o		7 v		18w		0 c		11r		14h		12m		13k		8 d		4 a		1 p		10e		4 j		6 s	
état 10		1 v		9 x		15u		6 w		15q		17y		13k		11l		13r		0 h		14g		8 b		13n		2 j		19a		6 s		9 o		17i		16t		0 d		9 c		16e		13p		8 m		15f		6 z	
état 11		9 x		16j		12f		16c		2 u		2 b		7 r		5 p		0 y		4 k		9 n		6 o		16v		0 g		8 z		9 d		16l		1 w		4 e		12i		0 q		18s		2 m		2 a		4 h		10t	
état 12		7 o		11x		1 f		4 q		13p		18m		12v		8 s		17b		4 j		16a		5 y		9 g		8 k		14t		1 c		0 w		1 l		0 r		15i		9 e		18u		11d		17z		4 n		4 h	
état 13		18f		2 e		14k		3 g		6 x		7 v		6 q		11d		17l		17b		3 c		9 p		14w		0 z		15s		8 t		8 m		2 a		12r		5 u		5 i		1 y		12n		16h		9 o		19j	
état 14		5 y		7 h		10e		14w		19f		2 b		4 u		18c		17g		11o		8 d		14r		4 z		13p		17k		5 m		13v		3 s		15l		2 j		13n		3 i		5 t		2 a		18q		16x	
état 15		4 w		15n		14k		14y		3 v		19x		9 j		16g		7 d		18a		6 e		6 f		9 m		2 s		13h		3 t		3 u		2 i		15z		6 q		19r		1 b		6 l		2 p		16o		12c	
état 16		15s		19z		11h		3 c		3 n		10p		11x		8 i		6 a		2 r		9 g		18d		0 f		16k		5 b		17w		12v		8 o		13l		18j		5 t		4 q		14u		16y		11e		13m	
état 17		14k		18j		18f		18s		3 d		13t		19c		2 g		1 n		9 r		16x		9 h		2 u		6 l		12y		6 b		10v		3 p		16a		5 w		8 z		8 i		5 q		10o		5 m		10e	
état 18		9 l		4 r		4 k		14g		6 m		8 p		4 h		7 b		9 q		16y		14s		0 e		19i		19o		14v		15w		3 d		11a		12t		8 j		17f		19u		15z		8 c		9 x		1 n	
état 19		13r		19m		19f		14e		0 k		2 j		18x		15y		16c		8 d		19n		6 g		10q		1 b		11p		13a		0 s		7 o		9 v		16w		17i		13t		2 u		6 z		4 l		4 h	

Coder et décoder à la main

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
état 0	19c	1 x	0 a	19z	4 d	3 k	16p	12r	13e	12l	13j	9 i	19n	11q	6 v	15o	13t	14s	11b	16h	0 m	18w	7 g	14f	7 u	7 y	
état 1	4 z	3 j	19h	11v	3 c	12q	13t	8 p	8 f	15m	4 o	5 e	9 s	19x	18b	7 r	2 g	4 l	17a	17d	3 u	9 k	4 w	17i	16y	18n	
état 2	7 g	10m	8 x	15r	9 y	13b	8 e	5 j	14l	13u	5 q	10s	17z	8 c	18n	5 p	16h	5 a	1 k	0 w	1 v	14f	14t	15o	13i	14d	
état 3	1 o	2 c	1 v	7 z	17e	5 g	16d	1 t	15h	7 k	5 n	15w	7 b	5 s	17a	19x	12q	3 l	18j	5 r	7 u	7 f	14i	10p	14m	9 y	
état 4	16k	2 w	10j	2 q	3 a	1 t	12y	12s	12z	8 n	2 b	5 h	17o	11v	8 u	3 g	16d	4 e	16i	0 l	5 f	5 x	12r	12p	10m	15c	
état 5	5 x	18i	10u	8 e	13q	17k	11b	9 p	0 r	7 m	13d	17n	13s	11h	6 f	12a	2 t	19g	3 j	1 y	6 z	11l	1 v	12c	8 o	5 w	
état 6	5 y	4 d	16g	5 n	9 k	14u	6 b	15v	7 p	16c	19a	11j	17o	10e	8 m	6 z	5 f	6 s	16h	7 q	10t	15l	2 x	6 i	0 w	13r	
état 7	15y	0 h	17d	16q	13w	4 b	13k	13o	14m	14g	18t	16n	11c	0 e	12f	3 a	1 x	3 z	14l	18p	13r	16i	12s	5 u	18v	16j	
état 8	9 r	1 i	15f	7 q	17u	11p	13l	14e	0 k	11b	7 d	1 o	13y	15c	15t	12a	9 s	3 x	6 z	18m	0 j	8 g	10n	10v	2 h	5 w	
état 9	18q	19i	6 u	0 z	16b	7 f	11x	14l	18t	12y	1 g	9 n	1 o	7 v	18w	0 c	11r	14h	12m	13k	8 d	4 a	1 p	10e	4 j	6 s	
état 10	1 v	9 x	15u	6 w	15q	17y	13k	11l	13r	0 h	14g	8 b	13n	2 j	19a	6 s	9 o	17i	16t	0 d	9 c	16e	13p	8 m	15f	6 z	
état 11	9 x	16j	12f	16c	2 u	2 b	7 r	5 p	0 y	4 k	9 n	6 o	16v	0 g	8 z	9 d	16l	1 w	4 e	12i	0 q	18s	2 m	2 a	4 h	10t	
état 12	7 o	11x	1 f	4 q	13p	18m	12v	8 s	17b	4 j	16a	5 y	9 g	8 k	14t	1 c	0 w	1 l	0 r	15i	9 e	18u	11d	17z	4 n	4 h	
état 13	18f	2 e	14k	3 g	6 x	7 v	6 q	11d	17l	17b	3 c	9 p	14w	0 z	15s	8 t	8 m	2 a	12r	5 u	5 i	1 y	12n	16h	9 o	19j	
état 14	5 y	7 h	10e	14w	19f	2 b	4 u	18c	17g	11o	8 d	14r	4 z	13p	17k	5 m	13v	3 s	15l	2 j	13n	3 i	5 t	2 a	18q	16x	
état 15	4 w	15n	14k	14y	3 v	19x	9 j	16g	7 d	18a	6 e	6 f	9 m	2 s	13h	3 t	3 u	2 i	15z	6 q	19r	1 b	6 l	2 p	16o	12c	
état 16	15s	19z	11h	3 c	3 n	10p	11x	8 i	6 a	2 r	9 g	18d	0 f	16k	5 b	17w	12v	8 o	13l	18j	5 t	4 q	14u	16y	11e	13m	
état 17	14k	18j	18f	18s	3 d	13t	19c	2 g	1 n	9 r	16x	9 h	2 u	6 l	12y	6 b	10v	3 p	16a	5 w	8 z	8 i	5 q	10o	5 m	10e	
état 18	9 l	4 r	4 k	14g	6 m	8 p	4 h	7 b	9 q	16y	14s	0 e	19i	19o	14v	15w	3 d	11a	12t	8 j	17f	19u	15z	8 c	9 x	1 n	
état 19	13r	19m	19f	14e	0 k	2 j	18x	15y	16c	8 d	19n	6 g	10q	1 b	11p	13a	0 s	7 o	9 v	16w	17i	13t	2 u	6 z	4 l	4 h	

Etat actuel : 0

Message original	T	E	S	T
Message encodé				

Coder et décoder à la main

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
état 0	19c 1 x 0 a 19z 4 d 3 k 16p 12r 13e 12l 13j 9 i 19n 11q 6 v 15o 13t 14s 11b 16h 0 m 18w 7 g 14f 7 u 7 y																									
état 1	4 z 3 j 19h 11v 3 c 12q 13t 8 p 8 f 15m 4 o 5 e 9 s 19x 18b 7 r 2 g 4 l 17a 17d 3 u 9 k 4 w 17i 16y 18n																									
état 2	7 g 10m 8 x 15r 9 y 13b 8 e 5 j 14l 13u 5 q 10s 17z 8 c 18n 5 p 16h 5 a 1 k 0 w 1 v 14f 14t 15o 13i 14d																									
état 3	1 o 2 c 1 v 7 z 17e 5 g 16d 1 t 15h 7 k 5 n 15w 7 b 5 s 17a 19x 12q 3 l 18j 5 r 7 u 7 f 14i 10p 14m 9 y																									
état 4	16k 2 w 10j 2 q 3 a 1 t 12y 12s 12z 8 n 2 b 5 h 17o 11v 8 u 3 g 16d 4 e 16i 0 l 5 f 5 x 12r 12p 10m 15c																									
état 5	5 x 18i 10u 8 e 13q 17k 11b 9 p 0 r 7 m 13d 17n 13s 11h 6 f 12a 2 t 19g 3 j 1 y 6 z 11l 1 v 12c 8 o 5 w																									
état 6	5 y 4 d 16g 5 n 9 k 14u 6 b 15v 7 p 16c 19a 11j 17o 10e 8 m 6 z 5 f 6 s 16h 7 q 10t 15l 2 x 6 i 0 w 13r																									
état 7	15y 0 h 17d 16q 13w 4 b 13k 13o 14m 14g 18t 16n 11c 0 e 12f 3 a 1 x 3 z 14l 18p 13r 16i 12s 5 u 18v 16j																									
état 8	9 r 1 i 15f 7 q 17u 11p 13l 14e 0 k 11b 7 d 1 o 13y 15c 15t 12a 9 s 3 x 6 z 18m 0 j 8 g 10n 10v 2 h 5 w																									
état 9	18q 19i 6 u 0 z 16b 7 f 11x 14l 18t 12y 1 g 9 n 1 o 7 v 18w 0 c 11r 14h 12m 13k 8 d 4 a 1 p 10e 4 j 6 s																									
état 10	1 v 9 x 15u 6 w 15q 17y 13k 11l 13r 0 h 14g 8 b 13n 2 j 19a 6 s 9 o 17i 16t 0 d 9 c 16e 13p 8 m 15f 6 z																									
état 11	9 x 16j 12f 16c 2 u 2 b 7 r 5 p 0 y 4 k 9 n 6 o 16v 0 g 8 z 9 d 16l 1 w 4 e 12i 0 q 18s 2 m 2 a 4 h 10t																									
état 12	7 o 11x 1 f 4 q 13p 18m 12v 8 s 17b 4 j 16a 5 y 9 g 8 k 14t 1 c 0 w 1 l 0 r 15i 9 e 18u 11d 17z 4 n 4 h																									
état 13	18f 2 e 14k 3 g 6 x 7 v 6 q 11d 17l 17b 3 c 9 p 14w 0 z 15s 8 t 8 m 2 a 12r 5 u 5 i 1 y 12n 16h 9 o 19j																									
état 14	5 y 7 h 10e 14w 19f 2 b 4 u 18c 17g 11o 8 d 14r 4 z 13p 17k 5 m 13v 3 s 15l 2 j 13n 3 i 5 t 2 a 18q 16x																									
état 15	4 w 15n 14k 14y 3 v 19x 9 j 16g 7 d 18a 6 e 6 f 9 m 2 s 13h 3 t 3 u 2 i 15z 6 q 19r 1 b 6 l 2 p 16o 12c																									
état 16	15s 19z 11h 3 c 3 n 10p 11x 8 i 6 a 2 r 9 g 18d 0 f 16k 5 b 17w 12v 8 o 13l 18j 5 t 4 q 14u 16y 11e 13m																									
état 17	14k 18j 18f 18s 3 d 13t 19c 2 g 1 n 9 r 16x 9 h 2 u 6 l 12y 6 b 10v 3 p 16a 5 w 8 z 8 i 5 q 10o 5 m 10e																									
état 18	9 l 4 r 4 k 14g 6 m 8 p 4 h 7 b 9 q 16y 14s 0 e 19i 19o 14v 15w 3 d 11a 12t 8 j 17f 19u 15z 8 c 9 x 1 n																									
état 19	13r 19m 19f 14e 0 k 2 j 18x 15y 16c 8 d 19n 6 g 10q 1 b 11p 13a 0 s 7 o 9 v 16w 17i 13t 2 u 6 z 4 l 4 h																									

Etat actuel : 0



Etat suivant : 16

Message original	T	E	S	T
Message encodé	H			

Coder et décoder à la main

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
état 0	19c 1 x 0 a 19z 4 d 3 k 16p 12r 13e 12l 13j 9 i 19n 11q 6 v 15o 13t 14s 11b 16h 0 m 18w 7 g 14f 7 u 7 y																									
état 1	4 z 3 j 19h 11v 3 c 12q 13t 8 p 8 f 15m 4 o 5 e 9 s 19x 18b 7 r 2 g 4 l 17a 17d 3 u 9 k 4 w 17i 16y 18n																									
état 2	7 g 10m 8 x 15r 9 y 13b 8 e 5 j 14l 13u 5 q 10s 17z 8 c 18n 5 p 16h 5 a 1 k 0 w 1 v 14f 14t 15o 13i 14d																									
état 3	1 o 2 c 1 v 7 z 17e 5 g 16d 1 t 15h 7 k 5 n 15w 7 b 5 s 17a 19x 12q 3 l 18j 5 r 7 u 7 f 14i 10p 14m 9 y																									
état 4	16k 2 w 10j 2 q 3 a 1 t 12y 12s 12z 8 n 2 b 5 h 17o 11v 8 u 3 g 16d 4 e 16i 0 l 5 f 5 x 12r 12p 10m 15c																									
état 5	5 x 18i 10u 8 e 13q 17k 11b 9 p 0 r 7 m 13d 17n 13s 11h 6 f 12a 2 t 19g 3 j 1 y 6 z 11l 1 v 12c 8 o 5 w																									
état 6	5 y 4 d 16g 5 n 9 k 14u 6 b 15v 7 p 16c 19a 11j 17o 10e 8 m 6 z 5 f 6 s 16h 7 q 10t 15l 2 x 6 i 0 w 13r																									
état 7	15y 0 h 17d 16q 13w 4 b 13k 13o 14m 14g 18t 16n 11c 0 e 12f 3 a 1 x 3 z 14l 18p 13r 16i 12s 5 u 18v 16j																									
état 8	9 r 1 i 15f 7 q 17u 11p 13l 14e 0 k 11b 7 d 1 o 13y 15c 15t 12a 9 s 3 x 6 z 18m 0 j 8 g 10n 10v 2 h 5 w																									
état 9	18q 19i 6 u 0 z 16b 7 f 11x 14l 18t 12y 1 g 9 n 1 o 7 v 18w 0 c 11r 14h 12m 13k 8 d 4 a 1 p 10e 4 j 6 s																									
état 10	1 v 9 x 15u 6 w 15q 17y 13k 11l 13r 0 h 14g 8 b 13n 2 j 19a 6 s 9 o 17i 16t 0 d 9 c 16e 13p 8 m 15f 6 z																									
état 11	9 x 16j 12f 16c 2 u 2 b 7 r 5 p 0 y 4 k 9 n 6 o 16v 0 g 8 z 9 d 16l 1 w 4 e 12i 0 q 18s 2 m 2 a 4 h 10t																									
état 12	7 o 11x 1 f 4 q 13p 18m 12v 8 s 17b 4 j 16a 5 y 9 g 8 k 14t 1 c 0 w 1 l 0 r 15i 9 e 18u 11d 17z 4 n 4 h																									
état 13	18f 2 e 14k 3 g 6 x 7 v 6 q 11d 17l 17b 3 c 9 p 14w 0 z 15s 8 t 8 m 2 a 12r 5 u 5 i 1 y 12n 16h 9 o 19j																									
état 14	5 y 7 h 10e 14w 19f 2 b 4 u 18c 17g 11o 8 d 14r 4 z 13p 17k 5 m 13v 3 s 15l 2 j 13n 3 i 5 t 2 a 18q 16x																									
état 15	4 w 15n 14k 14y 3 v 19x 9 j 16g 7 d 18a 6 e 6 f 9 m 2 s 13h 3 t 3 u 2 i 15z 6 q 19r 1 b 6 l 2 p 16o 12c																									
état 16	15s 19z 11h 3 c 3 n 10p 11x 8 i 6 a 2 r 9 g 18d 0 f 16k 5 b 17w 12v 8 o 13l 18j 5 t 4 q 14u 16y 11e 13m																									
état 17	14k 18j 18f 18s 3 d 13t 19c 2 g 1 n 9 r 16x 9 h 2 u 6 l 12y 6 b 10v 3 p 16a 5 w 8 z 8 i 5 q 10o 5 m 10e																									
état 18	9 l 4 r 4 k 14g 6 m 8 p 4 h 7 b 9 q 16y 14s 0 e 19i 19o 14v 15w 3 d 11a 12t 8 j 17f 19u 15z 8 c 9 x 1 n																									
état 19	13r 19m 19f 14e 0 k 2 j 18x 15y 16c 8 d 19n 6 g 10q 1 b 11p 13a 0 s 7 o 9 v 16w 17i 13t 2 u 6 z 4 l 4 h																									

Etat actuel : 16



Etat suivant : 3

Message original	T	E	S	T
Message encodé	H	N		

Coder et décoder à la main

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
état 0	19c 1 x 0 a 19z 4 d 3 k 16p 12r 13e 12l 13j 9 i 19n 11q 6 v 15o 13t 14s 11b 16h 0 m 18w 7 g 14f 7 u 7 y																									
état 1	4 z 3 j 19h 11v 3 c 12q 13t 8 p 8 f 15m 4 o 5 e 9 s 19x 18b 7 r 2 g 4 l 17a 17d 3 u 9 k 4 w 17i 16y 18n																									
état 2	7 g 10m 8 x 15r 9 y 13b 8 e 5 j 14l 13u 5 q 10s 17z 8 c 18n 5 p 16h 5 a 1 k 0 w 1 v 14f 14t 15o 13i 14d																									
état 3	1 o 2 c 1 v 7 z 17e 5 g 16d 1 t 15h 7 k 5 n 15w 7 b 5 s 17a 19x 12q 3 l 18j 5 r 7 u 7 f 14i 10p 14m 9 y																									
état 4	16k 2 w 10j 2 q 3 a 1 t 12y 12s 12z 8 n 2 b 5 h 17o 11v 8 u 3 g 16d 4 e 16i 0 l 5 f 5 x 12r 12p 10m 15c																									
état 5	5 x 18i 10u 8 e 13q 17k 11b 9 p 0 r 7 m 13d 17n 13s 11h 6 f 12a 2 t 19g 3 j 1 y 6 z 11l 1 v 12c 8 o 5 w																									
état 6	5 y 4 d 16g 5 n 9 k 14u 6 b 15v 7 p 16c 19a 11j 17o 10e 8 m 6 z 5 f 6 s 16h 7 q 10t 15l 2 x 6 i 0 w 13r																									
état 7	15y 0 h 17d 16q 13w 4 b 13k 13o 14m 14g 18t 16n 11c 0 e 12f 3 a 1 x 3 z 14l 18p 13r 16i 12s 5 u 18v 16j																									
état 8	9 r 1 i 15f 7 q 17u 11p 13l 14e 0 k 11b 7 d 1 o 13y 15c 15t 12a 9 s 3 x 6 z 18m 0 j 8 g 10n 10v 2 h 5 w																									
état 9	18q 19i 6 u 0 z 16b 7 f 11x 14l 18t 12y 1 g 9 n 1 o 7 v 18w 0 c 11r 14h 12m 13k 8 d 4 a 1 p 10e 4 j 6 s																									
état 10	1 v 9 x 15u 6 w 15q 17y 13k 11l 13r 0 h 14g 8 b 13n 2 j 19a 6 s 9 o 17i 16t 0 d 9 c 16e 13p 8 m 15f 6 z																									
état 11	9 x 16j 12f 16c 2 u 2 b 7 r 5 p 0 y 4 k 9 n 6 o 16v 0 g 8 z 9 d 16l 1 w 4 e 12i 0 q 18s 2 m 2 a 4 h 10t																									
état 12	7 o 11x 1 f 4 q 13p 18m 12v 8 s 17b 4 j 16a 5 y 9 g 8 k 14t 1 c 0 w 1 l 0 r 15i 9 e 18u 11d 17z 4 n 4 h																									
état 13	18f 2 e 14k 3 g 6 x 7 v 6 q 11d 17l 17b 3 c 9 p 14w 0 z 15s 8 t 8 m 2 a 12r 5 u 5 i 1 y 12n 16h 9 o 19j																									
état 14	5 y 7 h 10e 14w 19f 2 b 4 u 18c 17g 11o 8 d 14r 4 z 13p 17k 5 m 13v 3 s 15l 2 j 13n 3 i 5 t 2 a 18q 16x																									
état 15	4 w 15n 14k 14y 3 v 19x 9 j 16g 7 d 18a 6 e 6 f 9 m 2 s 13h 3 t 3 u 2 i 15z 6 q 19r 1 b 6 l 2 p 16o 12c																									
état 16	15s 19z 11h 3 c 3 n 10p 11x 8 i 6 a 2 r 9 g 18d 0 f 16k 5 b 17w 12v 8 o 13l 18j 5 t 4 q 14u 16y 11e 13m																									
état 17	14k 18j 18f 18s 3 d 13t 19c 2 g 1 n 9 r 16x 9 h 2 u 6 l 12y 6 b 10v 3 p 16a 5 w 8 z 8 i 5 q 10o 5 m 10e																									
état 18	9 l 4 r 4 k 14g 6 m 8 p 4 h 7 b 9 q 16y 14s 0 e 19i 19o 14v 15w 3 d 11a 12t 8 j 17f 19u 15z 8 c 9 x 1 n																									
état 19	13r 19m 19f 14e 0 k 2 j 18x 15y 16c 8 d 19n 6 g 10q 1 b 11p 13a 0 s 7 o 9 v 16w 17i 13t 2 u 6 z 4 l 4 h																									

Etat actuel : 3



Etat suivant : 18

Message original	T	E	S	T
Message encodé	H	N	J	

Coder et décoder à la main

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
état 0	19c 1 x 0 a 19z 4 d 3 k 16p 12r 13e 12l 13j 9 i 19n 11q 6 v 15o 13t 14s 11b 16h 0 m 18w 7 g 14f 7 u 7 y																									
état 1	4 z 3 j 19h 11v 3 c 12q 13t 8 p 8 f 15m 4 o 5 e 9 s 19x 18b 7 r 2 g 4 l 17a 17d 3 u 9 k 4 w 17i 16y 18n																									
état 2	7 g 10m 8 x 15r 9 y 13b 8 e 5 j 14l 13u 5 q 10s 17z 8 c 18n 5 p 16h 5 a 1 k 0 w 1 v 14f 14t 15o 13i 14d																									
état 3	1 o 2 c 1 v 7 z 17e 5 g 16d 1 t 15h 7 k 5 n 15w 7 b 5 s 17a 19x 12q 3 l 18j 5 r 7 u 7 f 14i 10p 14m 9 y																									
état 4	16k 2 w 10j 2 q 3 a 1 t 12y 12s 12z 8 n 2 b 5 h 17o 11v 8 u 3 g 16d 4 e 16i 0 l 5 f 5 x 12r 12p 10m 15c																									
état 5	5 x 18i 10u 8 e 13q 17k 11b 9 p 0 r 7 m 13d 17n 13s 11h 6 f 12a 2 t 19g 3 j 1 y 6 z 11l 1 v 12c 8 o 5 w																									
état 6	5 y 4 d 16g 5 n 9 k 14u 6 b 15v 7 p 16c 19a 11j 17o 10e 8 m 6 z 5 f 6 s 16h 7 q 10t 15l 2 x 6 i 0 w 13r																									
état 7	15y 0 h 17d 16q 13w 4 b 13k 13o 14m 14g 18t 16n 11c 0 e 12f 3 a 1 x 3 z 14l 18p 13r 16i 12s 5 u 18v 16j																									
état 8	9 r 1 i 15f 7 q 17u 11p 13l 14e 0 k 11b 7 d 1 o 13y 15c 15t 12a 9 s 3 x 6 z 18m 0 j 8 g 10n 10v 2 h 5 w																									
état 9	18q 19i 6 u 0 z 16b 7 f 11x 14l 18t 12y 1 g 9 n 1 o 7 v 18w 0 c 11r 14h 12m 13k 8 d 4 a 1 p 10e 4 j 6 s																									
état 10	1 v 9 x 15u 6 w 15q 17y 13k 11l 13r 0 h 14g 8 b 13n 2 j 19a 6 s 9 o 17i 16t 0 d 9 c 16e 13p 8 m 15f 6 z																									
état 11	9 x 16j 12f 16c 2 u 2 b 7 r 5 p 0 y 4 k 9 n 6 o 16v 0 g 8 z 9 d 16l 1 w 4 e 12i 0 q 18s 2 m 2 a 4 h 10t																									
état 12	7 o 11x 1 f 4 q 13p 18m 12v 8 s 17b 4 j 16a 5 y 9 g 8 k 14t 1 c 0 w 1 l 0 r 15i 9 e 18u 11d 17z 4 n 4 h																									
état 13	18f 2 e 14k 3 g 6 x 7 v 6 q 11d 17l 17b 3 c 9 p 14w 0 z 15s 8 t 8 m 2 a 12r 5 u 5 i 1 y 12n 16h 9 o 19j																									
état 14	5 y 7 h 10e 14w 19f 2 b 4 u 18c 17g 11o 8 d 14r 4 z 13p 17k 5 m 13v 3 s 15l 2 j 13n 3 i 5 t 2 a 18q 16x																									
état 15	4 w 15n 14k 14y 3 v 19x 9 j 16g 7 d 18a 6 e 6 f 9 m 2 s 13h 3 t 3 u 2 i 15z 6 q 19r 1 b 6 l 2 p 16o 12c																									
état 16	15s 19z 11h 3 c 3 n 10p 11x 8 i 6 a 2 r 9 g 18d 0 f 16k 5 b 17w 12v 8 o 13l 18j 5 t 4 q 14u 16y 11e 13m																									
état 17	14k 18j 18f 18s 3 d 13t 19c 2 g 1 n 9 r 16x 9 h 2 u 6 l 12y 6 b 10v 3 p 16a 5 w 8 z 8 i 5 q 10o 5 m 10e																									
état 18	9 l 4 r 4 k 14g 6 m 8 p 4 h 7 b 9 q 16y 14s 0 e 19i 19o 14v 15w 3 d 11a 12t 8 j 17f 19u 15z 8 c 9 x 1 n																									
état 19	13r 19m 19f 14e 0 k 2 j 18x 15y 16c 8 d 19n 6 g 10q 1 b 11p 13a 0 s 7 o 9 v 16w 17i 13t 2 u 6 z 4 l 4 h																									

Etat actuel : 18



Etat suivant : 8

Message original	T	E	S	T
Message encodé	H	N	J	J

Récapitulatif

Chiffrement	César	Vigenere	RSA	Transducteur
Est humainement utilisable	Oui	Oui	Non	Oui
Temps moyen nécessaire pour un humain pour encoder un caractère	2.5 seconde	4.6 seconde	N/A	4.9 seconde
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

Démonstration du nombre d'état

A : Deux lettres successives dans le message original sont identiques

B : Deux lettres successives dans le message chiffré sont identiques

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

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

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

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

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

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

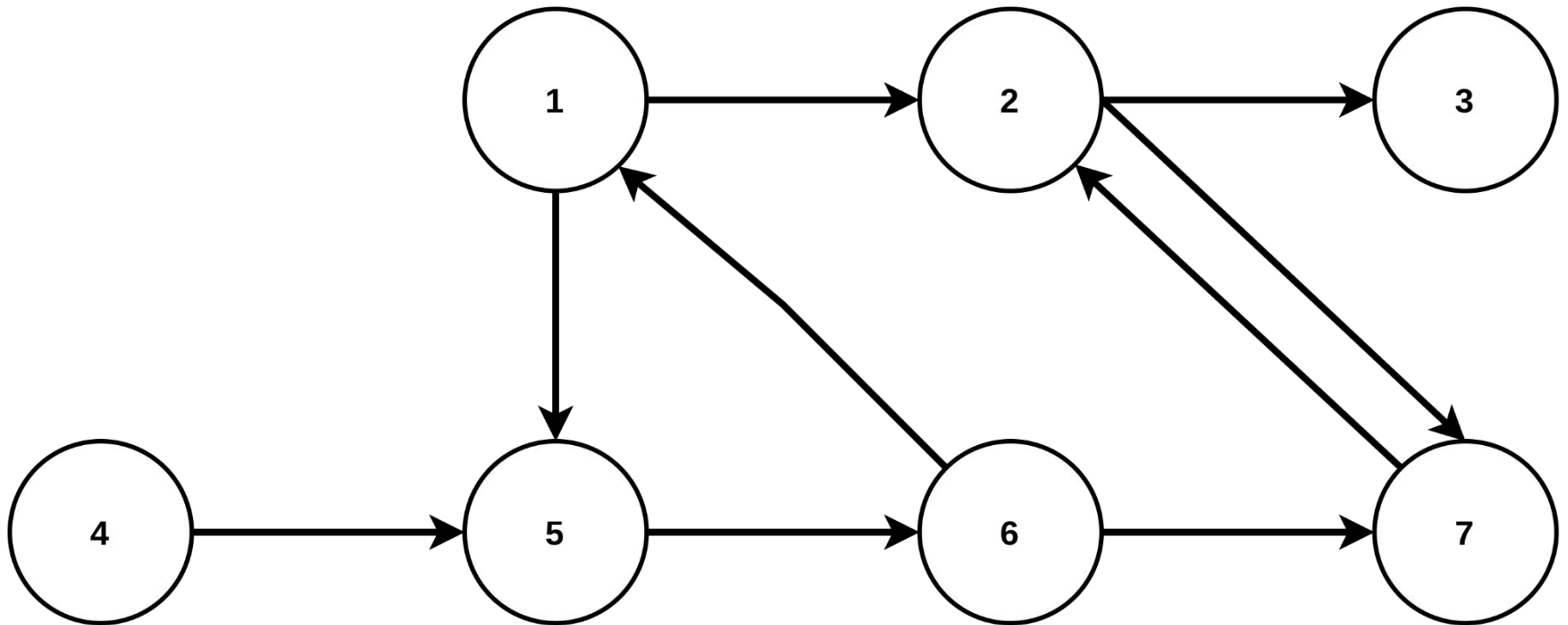
$$P(B) = \frac{N-1+P(A) \times |\Sigma|}{N|\Sigma|}$$

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

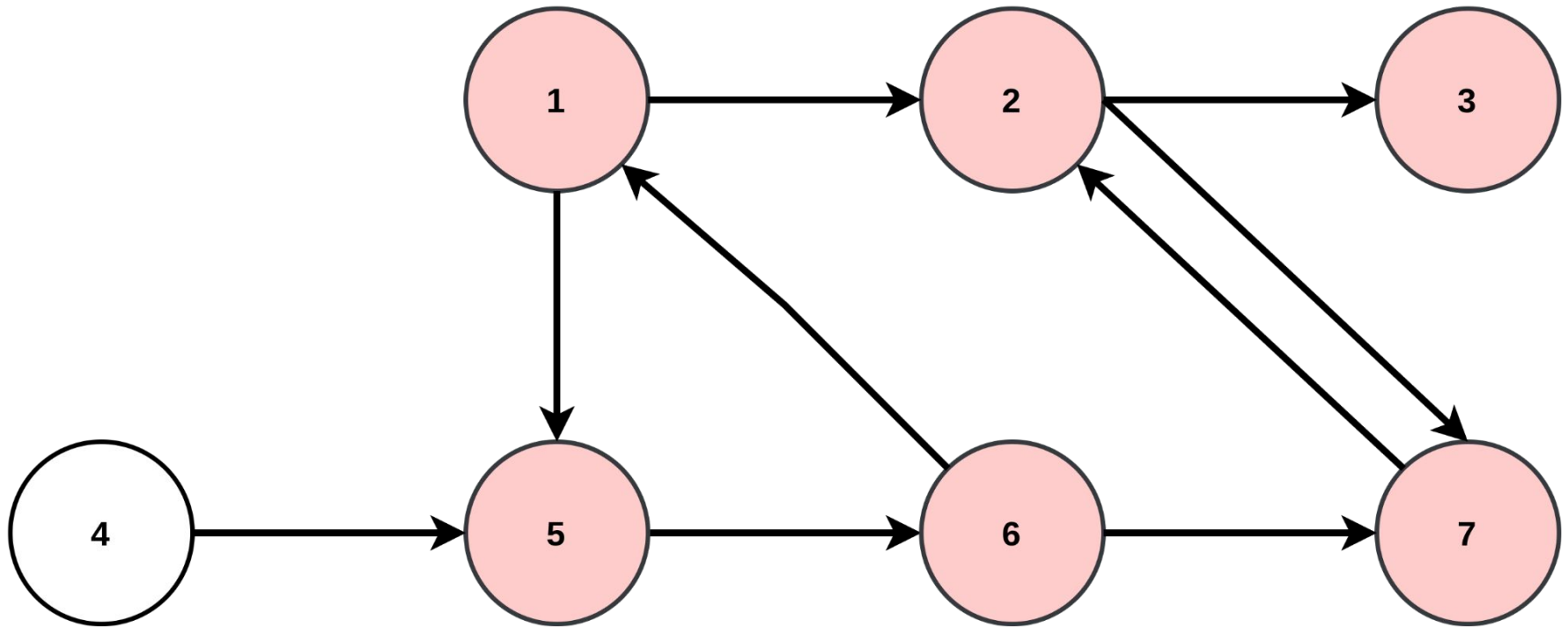
$$N(|\Sigma| \times P(B) - 1) = P(A) \times |\Sigma| - 1$$

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

Kosaraju graphe exemple

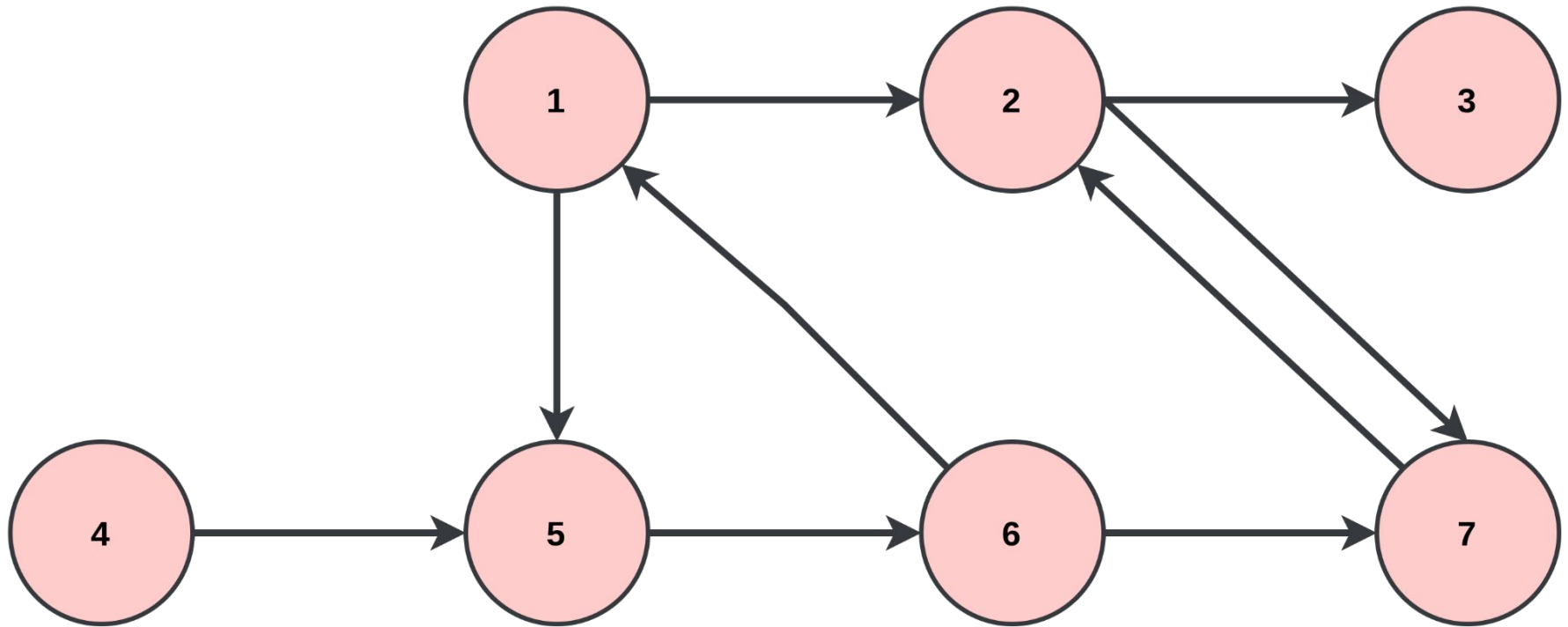


Kosaraju premier parcours



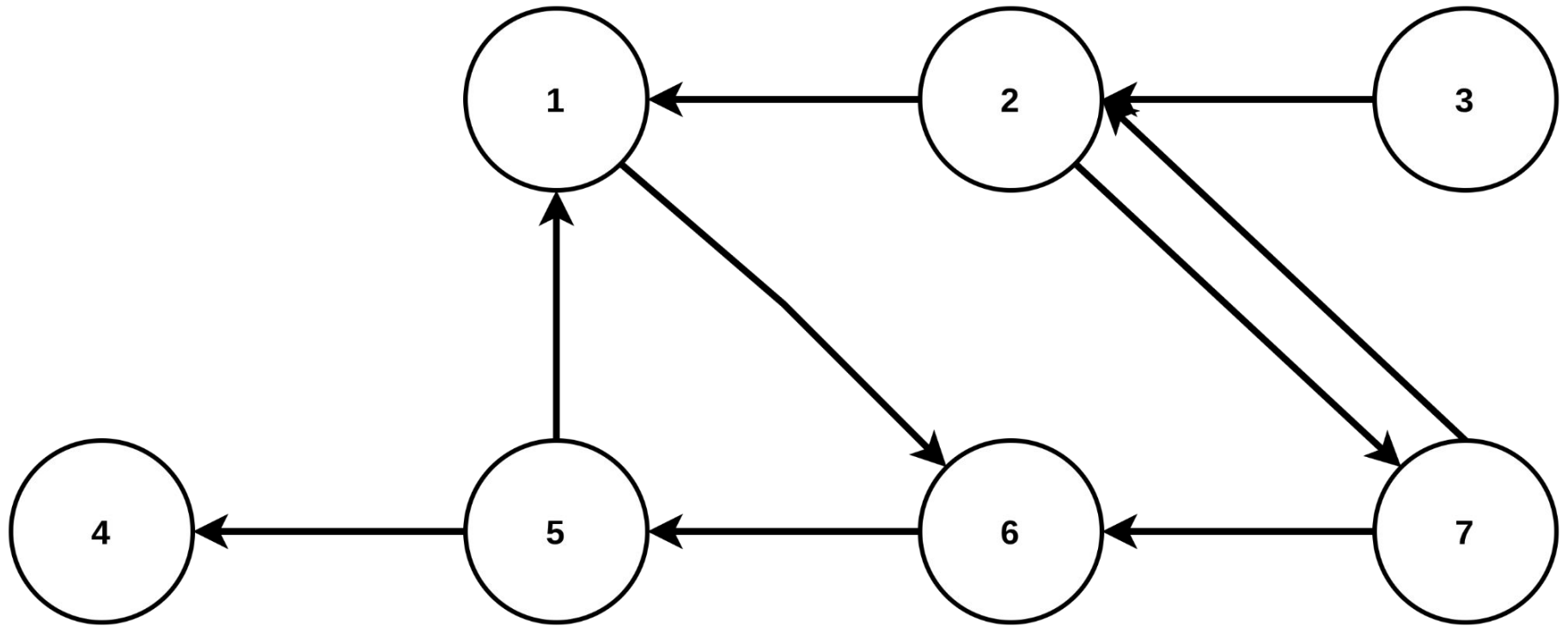
Parcours depuis 1
1 2 3 7 5 6

Kosaraju premier parcours

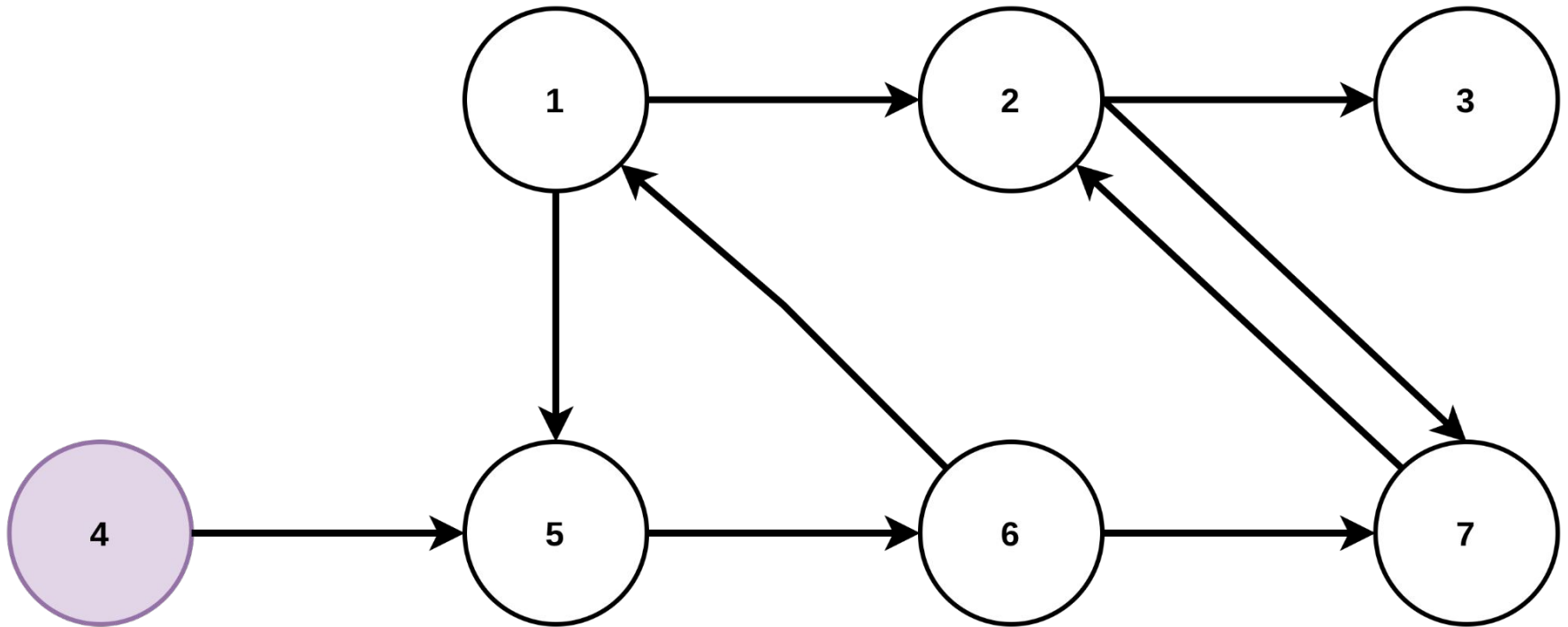


Parcours depuis 4
1 2 3 7 5 6 4

Kosaraju graphe transposé



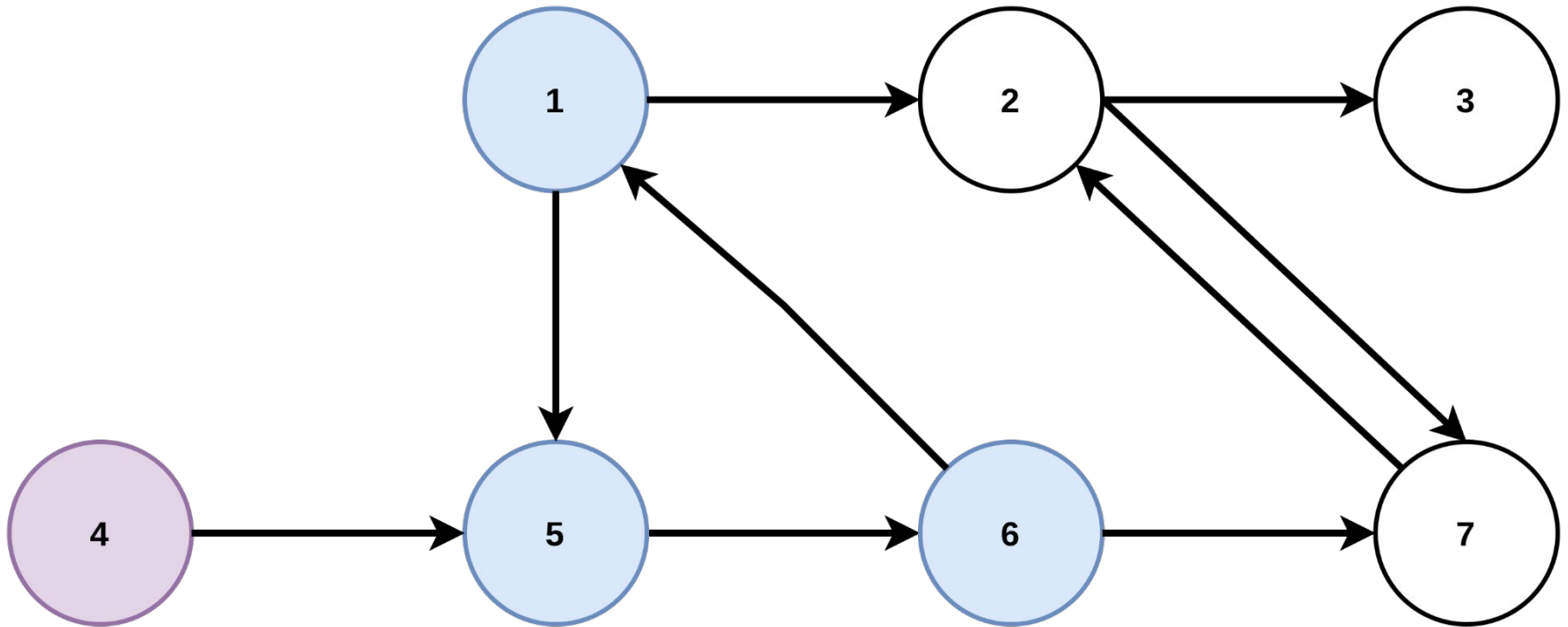
Kosaraju second parcours



Parcours dans dans le graphe transposé depuis 4

1 2 3 7 5 6 4

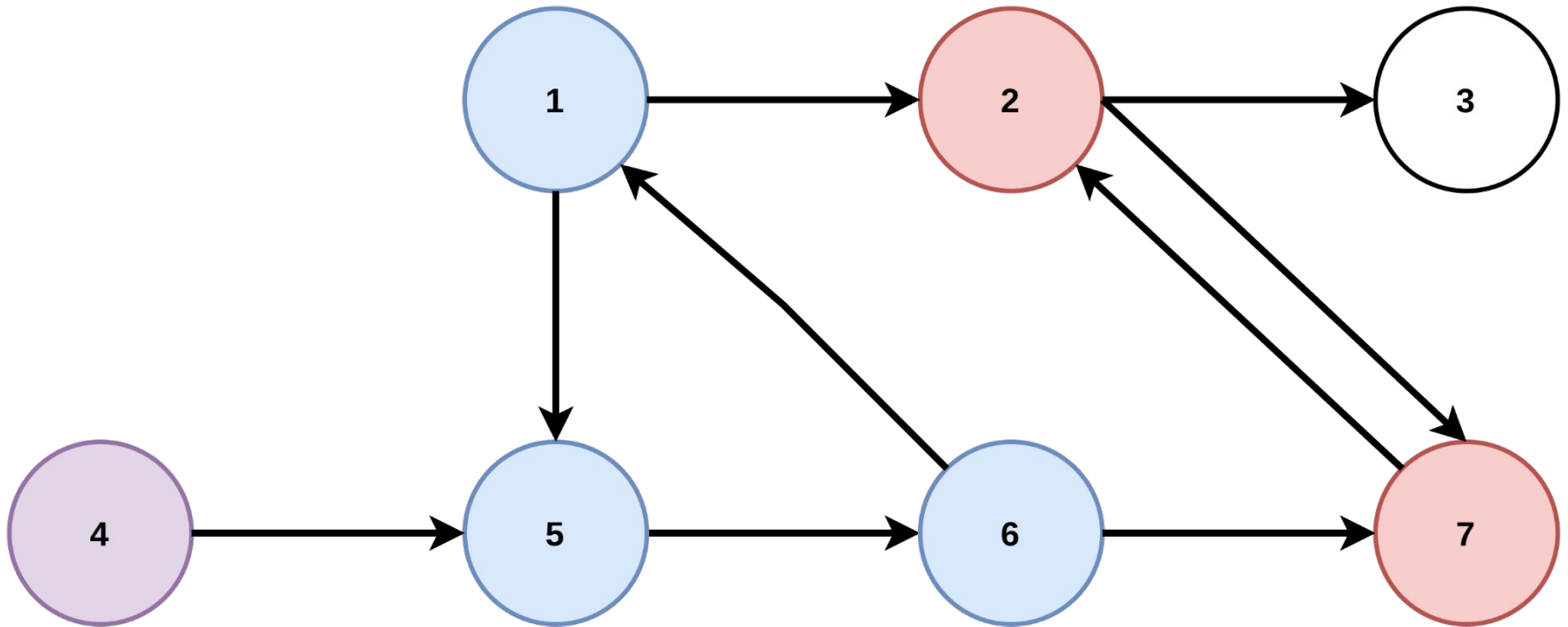
Kosaraju second parcours



Parcours dans dans le graphe transposé depuis 4

1 2 3 7 5 6 4

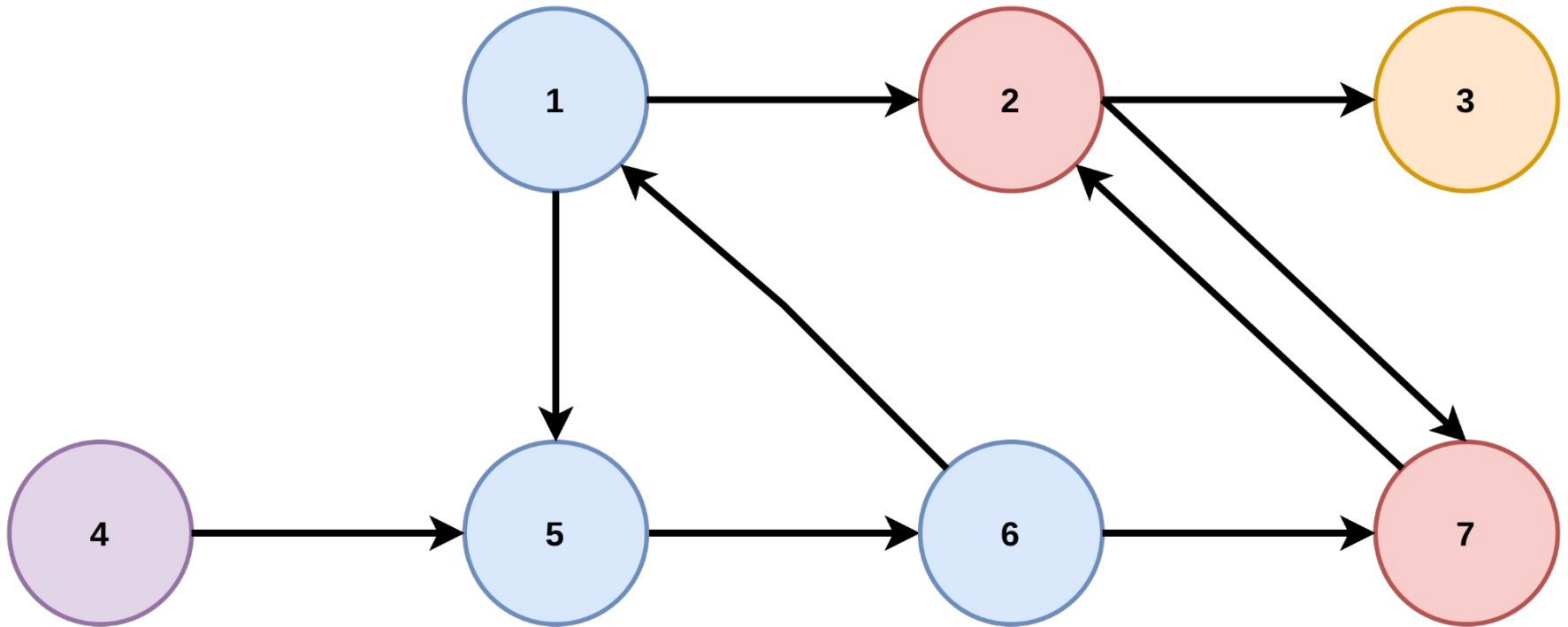
Kosaraju second parcours



Parcours dans dans le graphe transposé depuis 4

4 2 3 7 5 6 4

Kosaraju second parcours



Parcours dans dans le graphe transposé depuis 4

4 2 3 7 5 6 4

RSA

Choisir deux nombres premiers p et q (pour l'exemple on prendra $p = 5$, $q = 11$)

On pose $n = pq$ (ici $n = 55$)

Calculer $\varphi(n) = (p-1)(q-1)$ (ici $\varphi(n) = 40$)

Choisir un nombre e dans $[1, \varphi(n)]$ premier avec $\varphi(n)$ (ici $e = 23$)

Calculer l'inverse modulaire de e noté d (ici $d = 7$)

Pour chiffrer on calcul $M^d \bmod n$ (ici $M = 4$ on calcul $4^7 = 49 \bmod 55$)

Pour déchiffrer on calcul $N^e \bmod n$ (ici $N = 24$ on calcul $24^{23} = 4 \bmod 55$)

Le petit Théorème de Fermat nous donne la preuve que nous avons bien à faire à un chiffre

Inverse modulaire : Algorithme d'Euclide étendu

Appliquer l'algorithme d'euclide

Exemple : inverse de 23 modulo 40

$$40 = 23 \times 1 + 17$$

$$23 = 17 \times 1 + 6$$

$$17 = 6 \times 2 + 5$$

$$6 = 5 \times 1 + 1$$

Substituer

$$1 = 6 - 5 \times 1$$

$$\text{or } 5 = 17 - 6 \times 2 \text{ donc } 1 = 6 - (17 - 6 \times 2) \times 1 \text{ donc } 1 = 3 \times 6 - 17$$

$$\text{or } 6 = 23 - 17 \text{ donc } 1 = 3 \times (23 - 17) - 17 \text{ donc } 1 = -4 \times 17 + 3 \times 23$$

$$\text{or } 17 = 40 - 23 \text{ donc } 1 = -4 \times (40 - 23) + 3 \times 23 \text{ donc } 1 = 7 \times 23 - 4 \times 40$$

$$\text{donc } 1 = 7 \times 23 \text{ mod } 40$$