

# Un document L<sup>A</sup>T<sub>E</sub>X avancé

Sébastien Combéfis

28 novembre 2009

---

## Table des matières

---

<b>1</b>	<b>Théorie de l'information</b>	<b>1</b>
1.1	Code correcteur d'erreurs . . . . .	2
1.2	Compression . . . . .	2
1.3	Chiffrement . . . . .	2
<b>2</b>	<b>Statistiques sur la formation L<sup>A</sup>T<sub>E</sub>X</b>	<b>3</b>
<b>3</b>	<b>Divertissement</b>	<b>5</b>

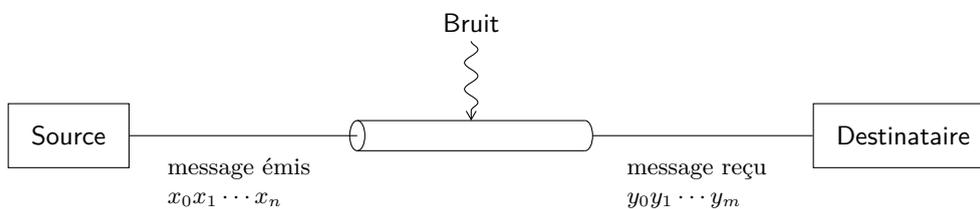
---

## 1 Théorie de l'information

---

Nous allons découvrir trois aspects qui interviennent lorsqu'on souhaite échanger de l'information entre deux interlocuteurs. Avant cela, revoyons le cadre illustré par la figure 1. Le système est donc composé d'une source et d'une destination qui veulent communiquer entre eux. Le message émis  $x_0x_1 \cdots x_n$  passe par le canal de communication et le message reçu est  $y_0y_1 \cdots y_m$ . Remarquez que ce dernier ne correspond pas nécessairement au message émis, en effet, le canal est bruité et des erreurs peuvent donc survenir.

Pour un canal parfait, $m = n$ et $x_i = y_i$ pour tout $0 \leq i \leq n$ .
---



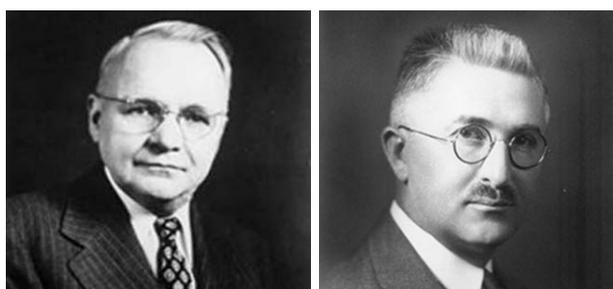
**Figure 1:** Schéma fondamental d'une communication.

Il y a trois aspects qui nous intéressent :

- on peut vouloir détecter et/ou corriger les erreurs de transmission de l'information ;
- on peut vouloir maximiser le rendement et compresser l'information ;
- enfin, on peut vouloir se protéger des espions et chiffrer l'information.

La suite de ce document parcourt en détails ces trois aspects, mais avant tout, un petit mot historique sur la *théorie de l'information*. Un certain nombre de personnes impliquées sont présentées sur la figure 2. Lorsqu'on parle de théorie de l'information, le premier nom qui vient à l'esprit est celui de Claude E. Shannon (figure 2(a)), pour sa publication « *A*

*Mathematical Theory of Communication* », parue dans le *Bell System Technical Journal* en 1948. Pour en savoir plus sur la théorie de l'information, nous vous conseillons de lire « *Invitation à la théorie de l'information* » [Dio97] qui propose en outre un aperçu historique.

(a) Claude E. Shannon <sup>1</sup>.(b) Warren Weaver <sup>2</sup>.(c) Harry Nyquist <sup>3</sup>.(d) Ralph Hartley <sup>4</sup>.

**Figure 2:** Personnes impliquées dans la théorie de l'information.

## 1.1 Code correcteur d'erreurs



**Figure 3:** Irvin S. Reed.

Irvin S. Reed (figure 3), né en 1923, mathématicien et ingénieur, est co-inventeur (avec Gustave Solomon) des codes de Reed-Solomon, un célèbre code correcteur d'erreurs. Il est également co-inventeur des codes de Reed-Müller.

Les codes correcteurs d'erreurs se basent sur la redondance afin de stocker un minimum d'information complémentaire et redondante pour pouvoir détecter et/ou corriger un maximum d'erreurs dans le message.

Les codes correcteurs d'erreurs sont appliqués aux moyens de communication classiques tels que la radio, les câbles coaxiaux, les fibres optiques, etc. Mais on les retrouve également pour les supports de stockage tels que les disques compacts, les mémoires RAM, les codes-barres 2D <sup>5</sup>, etc.

## 1.2 Compression

## 1.3 Chiffrement

1. [http://en.wikipedia.org/wiki/File:Claude\\_Elwood\\_Shannon\\_\(1916-2001\).jpg](http://en.wikipedia.org/wiki/File:Claude_Elwood_Shannon_(1916-2001).jpg)
2. <http://www-groups.dcs.st-and.ac.uk/~%7Ehistory/Mathematicians/Weaver.html>
3. [http://en.wikipedia.org/wiki/File:Harry\\_Nyquist.jpg](http://en.wikipedia.org/wiki/File:Harry_Nyquist.jpg)
4. [http://en.wikipedia.org/wiki/File:Hartley\\_ralph-vinton-lyon-001.jpg](http://en.wikipedia.org/wiki/File:Hartley_ralph-vinton-lyon-001.jpg)
5. Par exemple dans les QRCode.

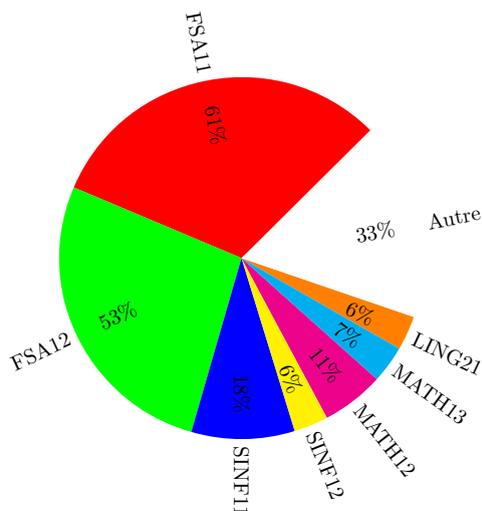
<b>Chiffre de César</b>	Ce système de chiffrement est un système de <b>substitution mono-alphabétique</b> également appelé chiffrement par décalage. Chaque lettre est remplacée par une autre lettre se trouvant à une distance fixe.
<b>Chiffre de Vigenère</b>	Ce système de chiffrement est un système de <b>substitution poly-alphabétique</b> , élaboré par Blaise de Vigenère (1523–1596). Il autorise donc le remplacement d'une lettre par une autre et qui n'est pas toujours la même.
<b>Chiffre de Playfair</b>	Ce système de chiffrement est un système de <b>chiffrement symétrique</b> . Le principe est de chiffrer des paires de lettres (digrammes). Ceci rend le cassage par analyse fréquentielle plus difficile.

**Table 1:** Différents systèmes de chiffrement « historiques ».

## 2 Statistiques sur la formation $\text{\LaTeX}$

Ce document reprend quelques informations statistiques sur les inscrits à l'édition 2009 de la formation  $\text{\LaTeX}$  de l'UCLouvain ACM Student Chapter. Le tableau 2 en page 4 reprend différentes données. On peut y voir la répartition des inscrits en fonction de leur occupation, en fonction du type de formation pratique sollicitée et enfin on y retrouve également le moyen grâce auquel ils ont eut connaissance de la formation.

La figure 4 montre la répartition des inscrits en fonction de leur occupation. On remarquera que la majorité des inscrits sont des étudiants ingénieur civil en première ou deuxième année de bachelier.



**Figure 4:** Répartition des inscrits en fonction de leurs occupations.

	FSA11	FSA12	SINF11	SINF12	MATH12	MATH13	LING21	BIR11	BIR13	GERM13	BBMC21	Autre	
Introductif	50	39	18	6	9	5	5	4	5	1	0	10	152
Avancé	10	12	0	0	2	2	1	0	1	0	1	7	36
TikZ/PGF	1	0	0	0	0	0	0	0	0	0	0	2	3
Beamer	0	2	0	0	0	0	0	0	0	0	0	2	4
Sébastien C.	20	10	16	3	4	0	6	0	0	0	0	5	64
Email	27	13	0	0	0	1	0	2	0	0	0	7	50
Facebook	10	10	0	1	0	0	0	0	0	0	0	2	23
Autre	0	0	0	0	2	4	0	2	4	1	1	2	16
Connaissance	4	20	2	2	5	2	0	0	2	0	0	5	42
Inscrits	61	53	18	6	11	7	6	4	6	1	1	21	195

**Table 2:** Données sur les inscriptions à la formation  $\LaTeX$ . Le haut du tableau donne le type de formation choisi et le bas du tableau la source d'information grâce à laquelle les inscrits ont eu connaissance de la formation. Le tout est détaillé en fonction de l'occupation.

### 3 Divertissement

Pour terminer, un petit divertissement. Il s'agit d'un petit puzzle dont les cases doivent être remplies avec des chiffres arabes.

1	2		3	
	4			5
6			7	
		8		
9				

**Horizontalement** 1  $2^4$ . 4 11 en binaire. 6  $T_5$  (cinquième nombre triangulaire). 7 Réponse à LA question. 9 Nombre de déplacements possibles d'une reine placée sur un échiquier  $26 \times 26$ .

**Verticalement** 2 DCXV en décimal. 3  $\lfloor 100\pi \rfloor$ . 5  $10 \times 5!$ . 6  $C_{11}^3$ . 8  $F_{12}$  (douzième nombre de Fibonacci).

### Références

[Dio97] Emmanuel Dion. *Invitation à la théorie de l'information*. Seuil, 1997.