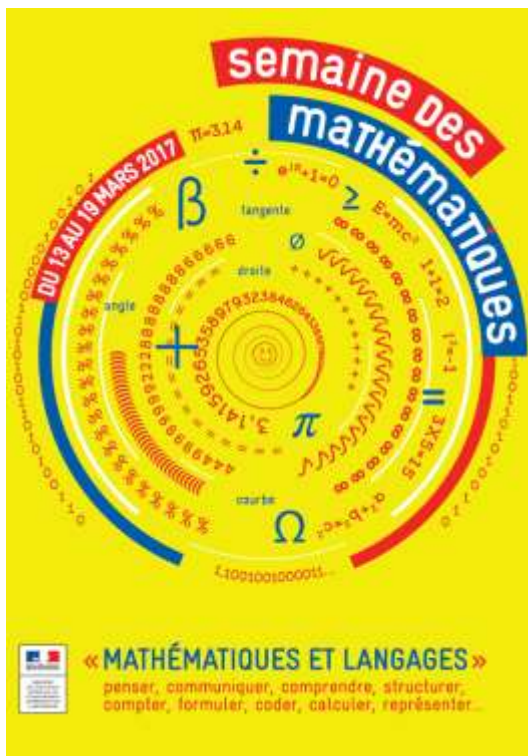


Semaine des Mathématiques 2017

Académie de NICE



Enigme

Cycle 3

**MATHEMATIQUES ET
CRYPTOGRAPHIE**

La machine infernale de codage

Cycle 3

MATHEMATIQUES ET CRYPTOGRAPHIE

La machine infernale de codage

Première partie à destination des enseignant(e)s

A/ Présentation générale

De nos jours, des milliards d'informations circulent dans les réseaux de communication. Toutes ces informations ont un point commun : elles sont cryptées.

Comment circule l'information dans notre quotidien ?

Le schéma classique d'une transmission d'information est le suivant :



En effet, tout message doit être crypté de façon à ce qu'il ne soit pas compréhensible s'il est intercepté lors de la transmission.

Le but de cette énigme est d'**initier aux algorithmes de codage**.



Une **machine infernale de codage** est présentée ici. Cette machine est infernale car elle possède trois engrenages d'encodage à la suite ... et donc trois engrenages de décodage.

En effet, « coder » possède deux voies : la voie « encoder » qui consiste à transcrire le connu vers le crypté et la voie « décoder » qui consiste à transcrire le crypté vers le connu.

Afin d'encoder et de décoder un signal, il convient de construire au préalable les tables d'encodage et de décodage. En termes de variables didactiques, l'enseignant(e) a le choix d'indiquer des tables plus ou moins complètes aux élèves.

Il s'agit véritablement d'une machine infernale de codage puisqu'elle possède trois engrenages. La machine ne code que les lettres pas les signes. En d'autres termes, les signes ne sont pas modifiés par la machine.

Comment fonctionne la machine infernale en mode encodage ?

La machine en mode encodage fonctionne de gauche à droite ... en allant du premier engrenage au troisième engrenage.

A l'entrée de la machine à gauche, une lettre est transformée en une autre lettre par le premier engrenage, puis en un nombre par le second engrenage et enfin en un autre nombre par le troisième engrenage :



A titre de premier exemple (suivre le **1** dans les tableaux), la lettre « C » va, au travers du premier engrenage, se transformer en un « w » ; puis, au travers du deuxième engrenage, devenir un nombre « 23 » ; pour enfin, au travers du troisième engrenage, se concrétiser en un nombre « 67 ».

A titre de deuxième exemple (suivre le **2** dans les tableaux), la lettre « T » va, au travers du premier engrenage, se transformer en un « f » ; puis, au travers du deuxième engrenage, devenir un nombre « 06 » ; pour enfin, au travers du troisième engrenage, se concrétiser en un nombre « 16 ».

Voyons les chemins d'encodage des lettres « C » et « T » :

Premier engrenage d'encodage

		1											
A	B	C	D	E	F	G	H	I	J	K	L	M	N
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
y	x	w											

					2								
O	P	Q	R	S	T	U	V	W	X	Y	Z		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
					f		d	c	b	a	z		

Deuxième engrenage d'encodage

					2								
a	b	c	d	e	f	g	h	i	j	k	l	m	n
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
01	02	03			06								

								1					
o	p	q	r	s	t	u	v	w	x	y	z		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
							22	23	24	25	26		

Troisième engrenage d'encodage

					2								
01	02	03			06								
⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
01	04	07			16								

								1					
							22	23	24	25	26		
⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
							64	67	70	73	76		

Comment fonctionne la machine infernale en mode décodage ?

La machine en mode décodage fonctionne cette fois-ci de droite à gauche ... en allant du troisième engrenage au premier engrenage. Il s'agit donc du chemin inverse.

A l'entrée de la machine à droite, un nombre est transformé en une autre lettre par le premier engrenage, puis en un nombre par le second engrenage et enfin en un autre nombre par le troisième engrenage :



Le sens de lecture de la table de codage est inversé et se fait maintenant de bas en haut.

A titre de premier exemple (suivre le 1 dans les tableaux), le nombre « 67 » va, au travers du troisième engrenage, se transformer en un nombre « 23 » ; puis, au travers du deuxième engrenage, devenir une lettre « w » ; pour enfin, au travers du premier engrenage, se concrétiser en une lettre « C ».

A titre de deuxième exemple (suivre le 2 dans les tableaux), le nombre « 16 » va, au travers du troisième engrenage, se transformer en un nombre « 06 » ; puis, au travers du deuxième engrenage, devenir une lettre « f » ; pour enfin, au travers du premier engrenage se concrétiser en une lettre « T ».

Comment fonctionne la machine infernale ?

Il s'agit donc d'une seule et même machine mais qui fonctionne selon deux voies différentes :

- + de gauche à droite pour la machine d'encodage,
- + de droite à gauche pour la machine de décodage.

B/ Pilotage pédagogique

Les fiches élèves n°1, 2, 3 et 4 sont à imprimer et à distribuer en un exemplaire uniquement à chacun des groupes de recherche.

A/ Premier atelier (comme DECOUVREUR de la machine infernale)

Les élèves vont être invités à rechercher en groupe les algorithmes d'encodage de chacun des engrenages. En termes de variables didactiques, il peut être proposé aux élèves :

- + de compléter entièrement par écrit les trois tables d'encodage,
- + que l'enseignant(e) complète plus ou moins les trois tables d'encodage en avance ...
- + ou, au contraire, ne pas autoriser les traces écrites pour favoriser les mobilisations mentales. Favoriser les recherches mentales peut justifier pleinement le travail de groupe car les tâches à mener sont lourdes.

Pour réaliser l'encodage de l'Agent secret vers la Base secrète, les élèves, selon les indications de l'enseignant(e), vont devoir compléter la **table d'encodage entière**.

Pour réaliser cette fois-ci le **décodage (opération inverse de l'encodage)** de la Base secrète vers l'Agent secret, les élèves vont s'appuyer sur la table d'encodage entière pour en déduire directement la **table de décodage entière**.

Cette phase est très importante car les élèves doivent prendre un temps pour analyser les trois algorithmes de codage. La difficulté réside dans les algorithmes eux-mêmes mais surtout dans la combinaison des trois algorithmes.

Les groupes de recherche travaillent en autonomie, l'enseignant(e) étaye au besoin. Pour cela, des tests de validité sont fournis au niveau de la table d'encodage totale :

Test de validité de la machine d'encodage complète :

C	T
⌞	⌞
67	16

ainsi qu'au niveau de la table de décodage totale :

Test de validité de la machine de décodage complète :

16	67
⌞	⌞
T	C

A l'aide de ces deux test de validité, les groupes de recherche vont pouvoir valider par et pour eux-mêmes leurs recherches.

B/ Deuxième atelier (comme RESOLVEUR de la machine infernale)

Pour chacun des échanges, le travail demandé consiste à « encoder » un message de l'Agent secret vers la Base secrète... puis à « décoder » un message de la Base secrète vers l'Agent secret.

Premier échange

Agent secret à Base secrète : « **DEUX PLUS TROIS EGALE SIX ???** ».

Il s'agit d'encoder ce message à l'aide de la machine. Les groupes peuvent vérifier entre eux s'ils obtiennent le même message crypté.

Base secrète à Agent secret : « **707367524970311376311343 !!!** »

Il s'agit de décoder ce message à l'aide de la machine. Les groupes peuvent vérifier entre eux s'ils obtiennent le même message.

Deuxième échange

Agent secret à Base secrète : « **LE CHOCOLAT, C'EST BON !!!** ».

Il s'agit d'encoder ce message à l'aide de la machine. Les groupes peuvent vérifier entre eux s'ils obtiennent le même message crypté.

Base secrète à Agent secret : « **162273107349404061 7311 40496113 6461 286134196122 73 377334556122 6413 6752316731407316 !!!** ».

Il s'agit de décoder ce message à l'aide de la machine. Les groupes peuvent vérifier entre eux s'ils obtiennent le même message.

Troisième échange

Il est demandé aux groupes d'inventer librement un échange entre l'Agent secret et sa Base secrète.

C/ Troisième atelier (comme CREATEUR de machines infernales)

Il peut être demandé aux groupes de construire leurs propres machines de codage et d'envoyer des messages à décoder à leurs camarades ... et, en retour, d'essayer de « casser » les codes de leurs camarades

C/ Eléments de correction

La machine infernale de codage

Document corrigé (pour l'enseignant(e) uniquement) - Aspect ENCODAGE

Premier engrenage

(Algorithme : « A » devient « Z » moins une lettre ; « B » devient « Y » moins une lettre ; ...)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵
y	x	w	v	u	t	s	r	q	p	o	n	m	l

O	P	Q	R	S	T	U	V	W	X	Y	Z		
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵		
k	j	i	h	g	f	e	d	c	b	a	z		

Deuxième engrenage

(Algorithme : « a » devient « 01 » ; « b » devient « 02 » ; « c » devient « 03 » ; ...)

a	b	c	d	e	f	g	h	i	j	k	l	m	n
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵
01	02	03	04	05	06	07	08	09	10	11	12	13	14

o	p	q	r	s	t	u	v	w	x	y	z		
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵		
15	16	17	18	19	20	21	22	23	24	25	26		

Troisième engrenage

(Algorithme : « 01 » devient « (01 x 3) - 2 » ; « b » devient « (02 x 3) - 2 » ; « c » devient « (03 x 3) - 2 » ; ...)

01	02	03	04	05	06	07	08	09	10	11	12	13	14
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵
01	04	07	10	13	16	19	22	25	28	31	34	37	40

15	16	17	18	19	20	21	22	23	24	25	26		
⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵	⌵		
43	46	49	52	55	58	61	64	67	70	73	76		

La compréhension des trois algorithmes de la machine d'encodage permet de dresser la **table d'encodage complète** comme combinaison des trois algorithmes :

Table d'encodage complète (combinaison des trois algorithmes)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
73	70	67	64	61	58	55	52	49	46	43	40	37	34
O	P	Q	R	S	T	U	V	W	X	Y	Z		
⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩		
31	28	25	22	19	16	13	10	07	04	01	76		

La machine infernale de codage

Document corrigé (pour l'enseignant(e) uniquement) - Aspect DECODAGE

Troisième engrenage inversé

01	04	07	10	13	16	19	22	25	28	31	34	37	40
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
01	02	03	04	05	06	07	08	09	10	11	12	13	14
43	46	49	52	55	58	61	64	67	70	73	76		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
15	16	17	18	19	20	21	22	23	24	25	26		

Deuxième engrenage inversé

01	02	03	04	05	06	07	08	09	10	11	12	13	14
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	16	17	18	19	20	21	22	23	24	25	26		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
o	p	q	r	s	t	u	v	w	x	y	z		

Premier engrenage inversé

a	b	c	d	e	f	g	h	i	j	k	l	m	n
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
o	p	q	r	s	t	u	v	w	x	y	z		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
K	J	I	H	G	F	E	D	C	B	A	Z		

La compréhension des trois algorithmes de la machine de décodage permet de dresser la **table de décodage complète** comme combinaison des trois algorithmes :

Table de décodage complète (combinaison des trois algorithmes)

01	04	07	10	13	16	19	22	25	28	31	34	37	40
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
43	46	49	52	55	58	61	64	67	70	73	76		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
K	J	I	H	G	F	E	D	C	B	A	Z		

La machine infernale de codage

Document corrigé (pour l'enseignant(e) uniquement)

Table d'encodage complète (combinaison des trois algorithmes)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
73	70	67	64	61	58	55	52	49	46	43	40	37	34
O	P	Q	R	S	T	U	V	W	X	Y	Z		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
31	28	25	22	19	16	13	10	07	04	01	76		

De la table d'encodage complète, il est possible de déduire directement la table de décodage complète. C'est ce travail qui est demandé aux groupes de recherche.

Table de décodage complète (combinaison des trois algorithmes)

01	04	07	10	13	16	19	22	25	28	31	34	37	40
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
43	46	49	52	55	58	61	64	67	70	73	76		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		
K	J	I	H	G	F	E	D	C	B	A	Z		

Cycle 3

MATHEMATIQUES ET CRYPTOGRAPHIE

La machine infernale de codage

Deuxième partie à destination des élèves

**Les fiches élèves n°1, 2, 3 et 4 sont à imprimer et à distribuer
en un exemplaire uniquement à chacun des groupes de
recherche.**

La machine infernale de codage

Fiche élève n°1 : Fiche de présentation de l'énigme (1 exemplaire par groupe)

De nos jours, des milliards d'informations circulent dans les réseaux de communication. Toutes ces informations ont un point commun : elles sont cryptées.

Comment circule l'information dans notre quotidien ?

Le schéma classique d'une transmission d'information est le suivant :



Une **machine infernale de codage** est présentée ici. Cette machine est infernale car elle possède trois engrenages d'encodage à la suite ... et donc trois engrenages de décodage.

Comment fonctionne la machine infernale en mode encodage ?

La machine en mode encodage fonctionne de gauche à droite ... en allant du premier engrenage au troisième engrenage.

A l'entrée de la machine à gauche, une lettre est transformée en une autre lettre par le premier engrenage, puis en un nombre par le second engrenage et enfin en un autre nombre par le troisième engrenage :



Comment fonctionne la machine infernale en mode décodage ?

La machine fonctionne cette fois-ci de droite à gauche ... en allant du troisième engrenage au premier engrenage. Il s'agit donc du chemin inverse.

A l'entrée de la machine à droite, un nombre est transformé en une autre lettre par le premier engrenage, puis en un nombre par le second engrenage et enfin en un autre nombre par le troisième engrenage :



Comment fonctionne la machine infernale ?

Il s'agit donc d'une seule et même machine qui fonctionne selon deux voies différentes :

- + de gauche à droite pour la **machine d'encodage**,
- + de droite à gauche pour la **machine de décodage**.

La machine ne code que les lettres pas les signes. Autrement dit, les signes ou les espaces ne sont pas modifiés par la machine.

La machine infernale de codage

Fiche élève n°2 : Fiche de recherche des groupes d'élèves (1 photocopie par groupe)

A/ Premier atelier (comme DECOUVREUR de la machine infernale)

A propos de la machine d'encodage (Fiche n°3)

Avec ton groupe, comprenez comment fonctionnent les trois algorithmes de la machine infernale en mode encodage. Expliquez avec vos mots. Complétez alors les trois premiers tableaux de la fiche n°2.

Comprenez alors comment fonctionne la machine en son entier. Complétez alors le quatrième tableau de la fiche n°2 qui représente la **table d'encodage entière**.

A propos de la machine de décodage (Fiche n°4)

Comprenez comment fonctionnent les trois algorithmes de la machine infernale en mode décodage. A partir de la table d'encodage entière, complétez alors la **table de décodage entière** de la fiche n°3.

B/ Deuxième atelier (comme RESOLVEUR de la machine infernale)

Après avoir complété les tables d'encodage et de décodage (Fiches n°3 et 4), réponds avec ton groupe aux questions :

Premier échange

Question de l'Agent secret à Base secrète : « **DEUX PLUS TROIS EGALE SIX ???** ».

Forme cryptée de la question :

Réponse de la Base secrète à Agent secret : « **707367524970311376311343 !!!** »

Forme connue de la réponse :

Deuxième échange

Question de l'Agent secret à Base secrète : « **LE CHOCOLAT, C'EST BON !!!** ».

Forme cryptée de la question :

Réponse de la Base secrète à Agent secret : « **162273107349404061 7311 40496113 6461 286134196122 73 377334556122 6413 6752316731407316 !!!** ».

Forme connue de la réponse :

.....

Troisième échange (à inventer librement)

Question de l'Agent secret à Base secrète :

Forme cryptée de la question :

Réponse de la Base secrète à Agent secret :

Forme connue de la réponse :

C/ Troisième atelier (comme CREATEUR de machines infernales)

Avec tes camarades, créez librement des machines diaboliques de codage et testez-les auprès de tes autres camarades !!!

La machine infernale de codage

Fiche élève n°3 : Travaux sur l'ENCODAGE (1 photocopie par groupe)

Premier engrenage d'encodage

A	B	C	D	E	F	G	H	I	J	K	L	M	N
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏
			v										

O	P	Q	R	S	T	U	V	W	X	Y	Z		
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏		
			h							a	z		

Deuxième engrenage d'encodage

a	b	c	d	e	f	g	h	i	j	k	l	m	n
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏
01					06								

o	p	q	r	s	t	u	v	w	x	y	z		
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏		
							22						

Troisième engrenage d'encodage

01	02	03	04	05	06	07	08	09	10	11	12	13	14
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏
		07											

15	16	17	18	19	20	21	22	23	24	25	26		
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏		
							64						

Table d'encodage complète (combinaison des trois algorithmes)

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		
⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏	⏏		

La machine infernale de codage

Fiche élève n°4 : Travaux sur le DECODAGE (1 photocopie par groupe)

Table d'encodage complète (combinaison des trois algorithmes)

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		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		

Test de validité de la machine d'encodage complète :

C	T
⌞	⌞
67	16

Table de décodage complète (déduite directement de la table d'encodage)

01	04	07	10	13	16	19	22	25	28	31	34	37	40
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞
43	46	49	52	55	58	61	64	67	70	73	76		
⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞	⌞		

Test de validité de la machine de décodage complète :

16	67
⌞	⌞
T	C

Cycle 3

MATHEMATIQUES ET CRYPTOGRAPHIE

La machine infernale de codage

**Troisième partie à destination de la classe
(indice mystère à conserver)**

56 89 98 65