

Informatique Sans Ordinateur



Pascal Lafourcade



De l'Université au primaire





Informatique Sans Ordinateur

Une drôle d'idée ?

- ▶ Sans ordinateur !
- ▶ De façon ludique
- ▶ Physiquement
- ▶ Pas de technologie
- ▶ Moindre coûts
- ▶ Concepts scientifiques

Informatique débranchée

Origines



- ▶ 1992 : Tim Bell, Ian Wiiten et Michael Fellows (Nouvelle-Zélande)

Visibilité croissante

- ▶ 2003 : Intégré dans le curriculum en informatique ACM (Association for Computing Machinery) et CSTA (Computer Science Teachers Association)



CS UNPLUGGED Topics Printables About Search

Computer Science without a computer

CS Unplugged is a collection of free teaching material that teaches Computer Science through engaging games and puzzles that use cards, string, crayons and lots of running around.

Welcome to the new CS Unplugged!

This updated website has unit plans, lesson plans, teaching videos, curriculum integration activities, and programming exercises to plug in the Computer Science concepts they have just learnt unplugged.

The original activities are still available at classic.csunplugged.org.

 What is Computer Science?

 How do I teach CS Unplugged?



En France

- ▶ Interstices traduit 20 activités du site CS Unplugged : (<https://interstices.info>).
- ▶ Le groupe « Algorithmique » de l'IREM de Grenoble :
<http://www-irem.ujf-grenoble.fr/spip/spip.php?rubrique15>
- ▶ Sur le site Pixees (<https://pixees.fr/>)
- ▶ Site de Marie Duflot Kremer <https://members.loria.fr/MDuflot/files/mediation.html>
- ▶ Groupe ISO National informel
- ▶ Le groupe « ISO » de l'IREM/MPSA de Clermont-Ferrand
<http://www.irem.univ-bpclermont.fr/Informatique-sans-Ordinateur>



Principes pédagogiques

Complémentarité des approches *branchée* et *débranchée*

Objectifs

- ▶ Prendre du recul
- ▶ Ne pas décourager les élèves
- ▶ Ne pas pallier au manque d'équipement

Des idées anciennes

- ▶ Manipuler des objets tangibles
- ▶ Expérimenter à partir de situations concrètes
- ▶ Mettre les enfants en situation de recherche
- ▶ Animation par des jeux et des problèmes à résoudre

Principes pédagogiques

Les activités

- ▶ Visent des concepts de la science informatique
- ▶ Engagent le corps
- ▶ Favorisent des approches coopératives plutôt qu'individuelles
- ▶ Ludiques, agréables, non ennuyeuses

Et aussi

- ▶ Disponibles à faible coût, sous licence CC
- ▶ Neutres par rapport au genre
- ▶ Robustes à l'erreur (de l'enseignant et de l'élève)

De l'Université au primaire

Université

- ▶ Licence Pro Web : **Cours sécurité Web.**
- ▶ M2 Sécurité des systèmes d'information : **Antivirus**
- ▶ BUT 1 Mathématiques : **Courbes de Beziars**

Formation NSI

- ▶ **Marmotes** de Marie DUFLOT (Huffman)
- ▶ **Tour de magie** (Code correcteur d'erreur)
- ▶ Indécidabilité de l'arrêt d'un programme

Primaire

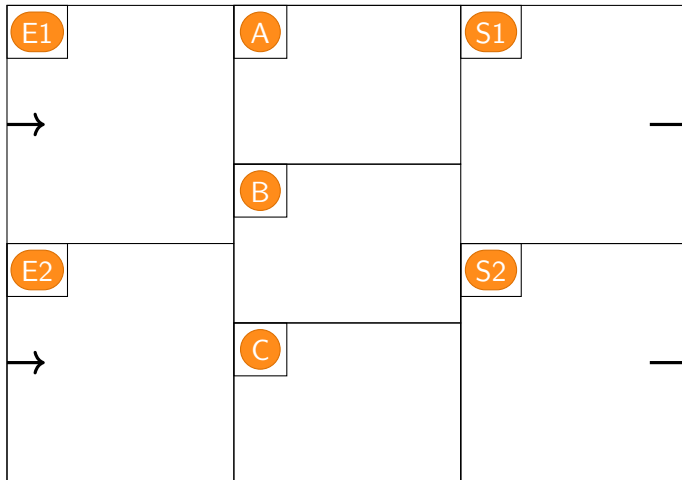
- ▶ **Images**
- ▶ **Tour de magie**
- ▶ Architecture Ordinateur (jeu de role)
- ▶ Musique (codage de l'information)

Antivirus parfait existe-t-il ?

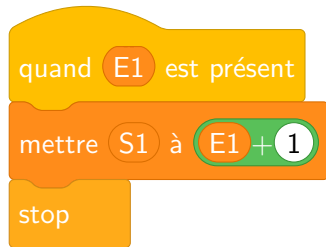
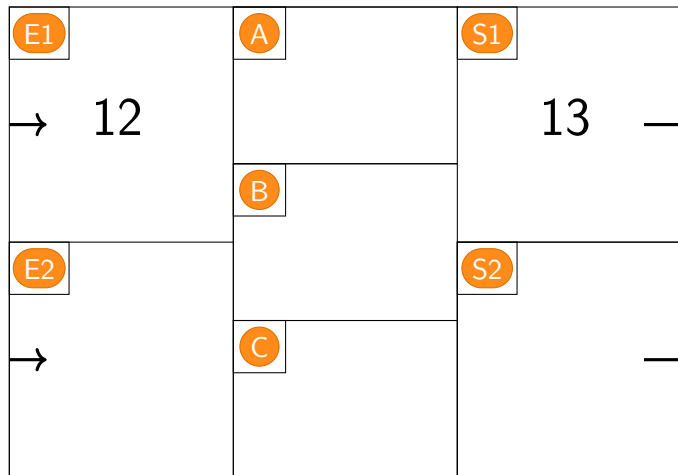


Journault Matthieu, Lafourcade Pascal, More Malika, Poulain Rémy, Léo Robert

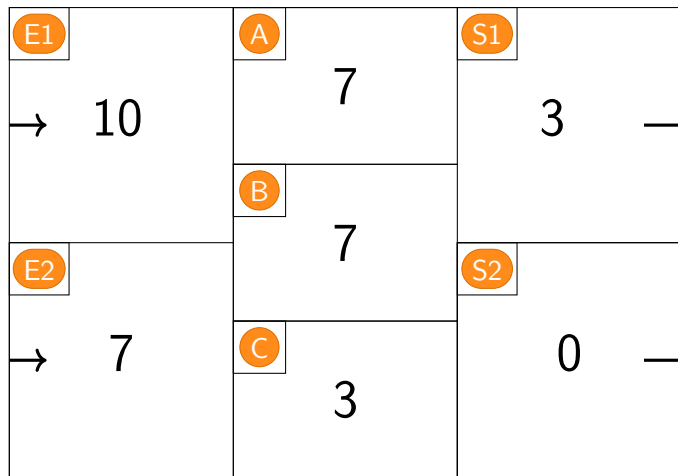
Materiel



Programme Simple : Incrément

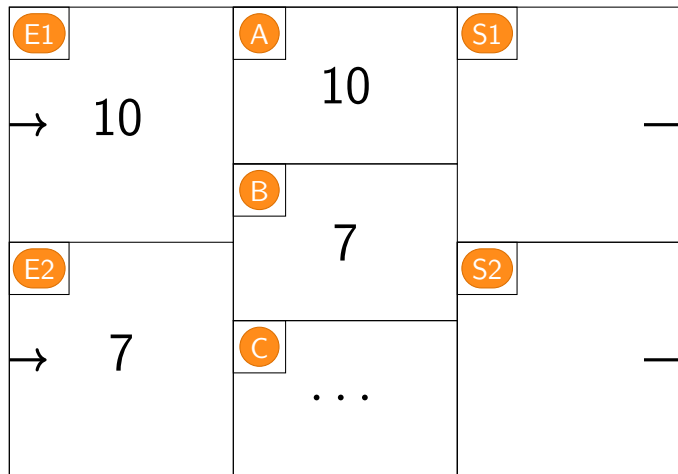


Programme Simple : Moins

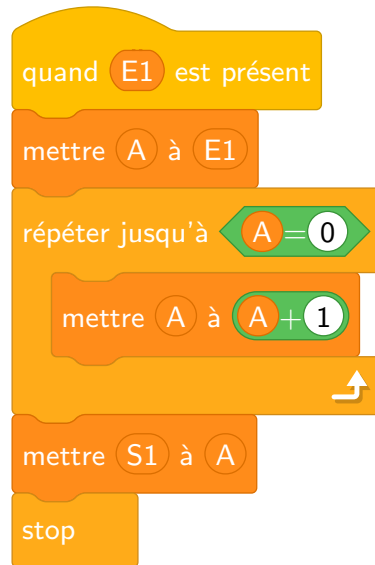
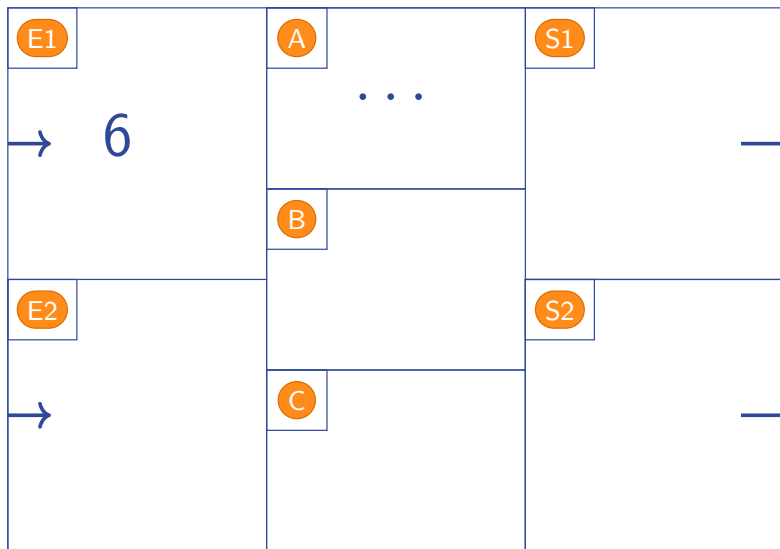


```
quand E1 et E2 sont présents
mettre A à E1
mettre B à E2
mettre C à 0
répéter jusqu'à A = B
  mettre C à C + 1
  mettre A à A - 1
mettre S1 à C
mettre S2 à 0
stop
```

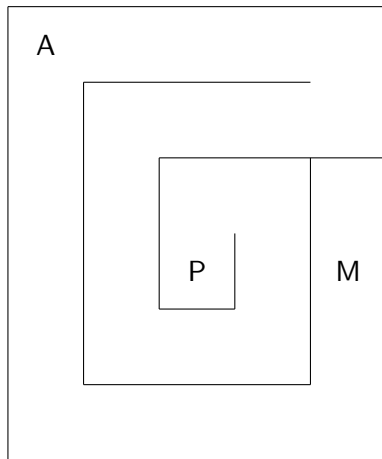

Programme Simple : Moins*



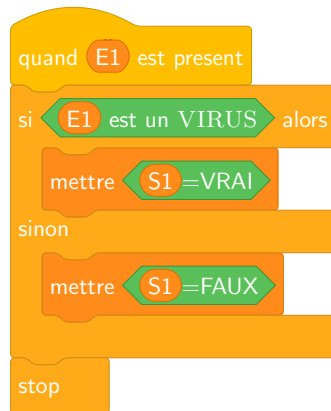
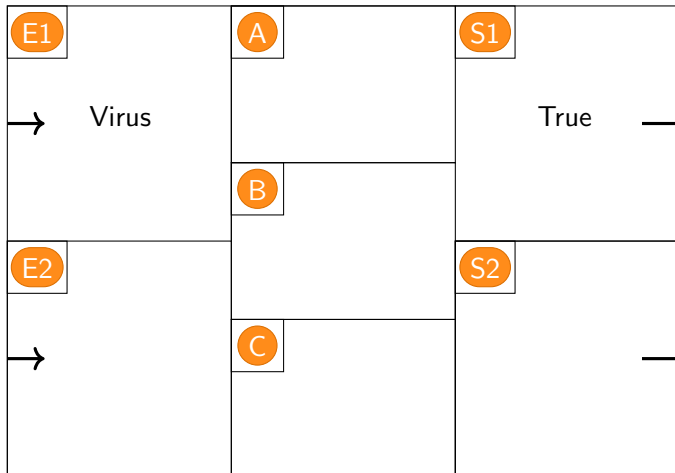
```
quand E1 et E2 sont présents
mettre A à E1
mettre B à E2
mettre C à 0
répéter jusqu'à A = B
  mettre C à C + 1
mettre S1 à C
mettre S2 à 0
stop
```



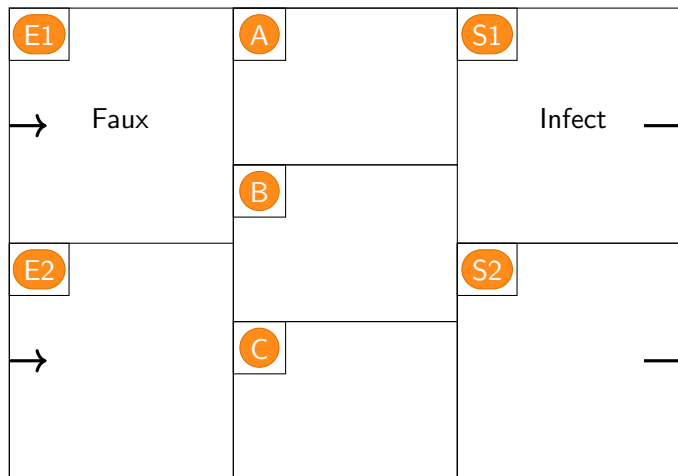
Preuve par disjonction et par l'absurde



Programme ESTVIRUS



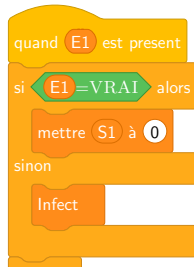
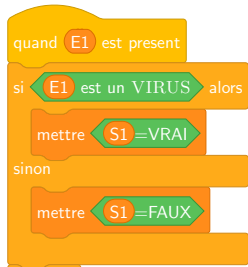
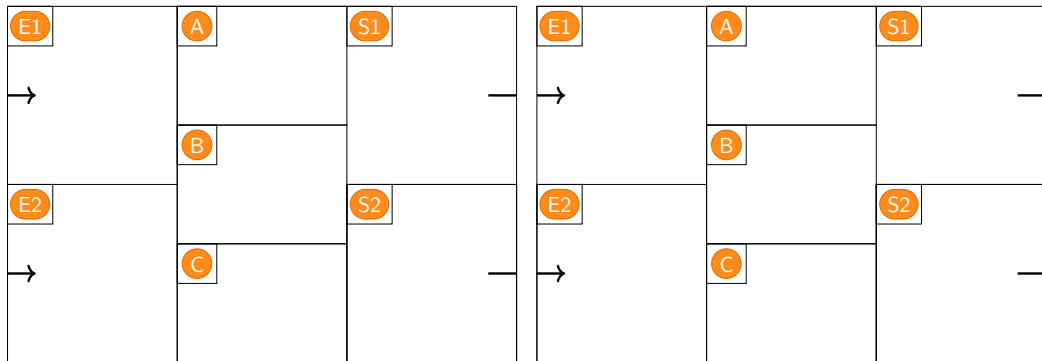
Program TEST



Indecidabilité de EstVirus

ESTVIRUS

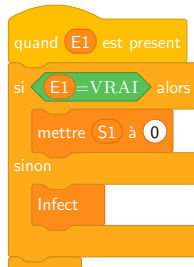
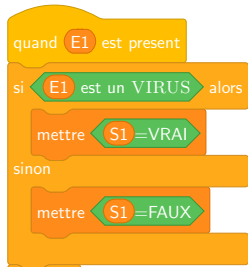
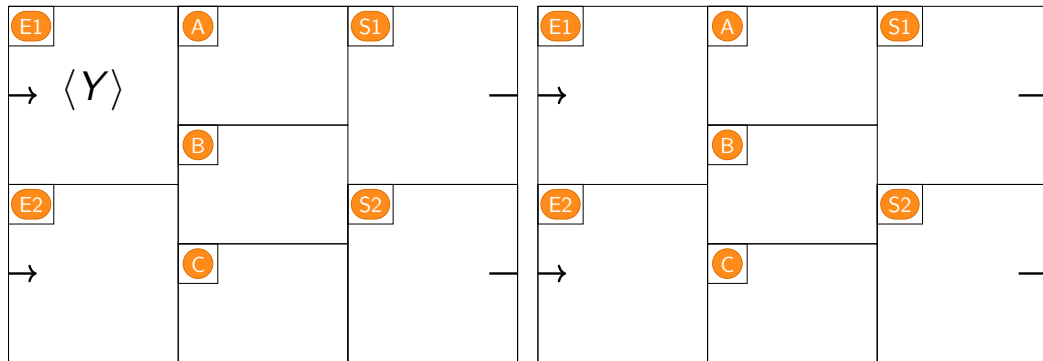
TEST



Indecidabilité de EstVirus

ESTVIRUS

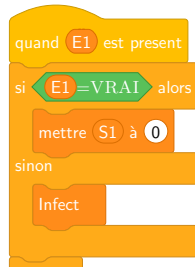
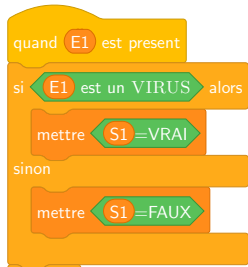
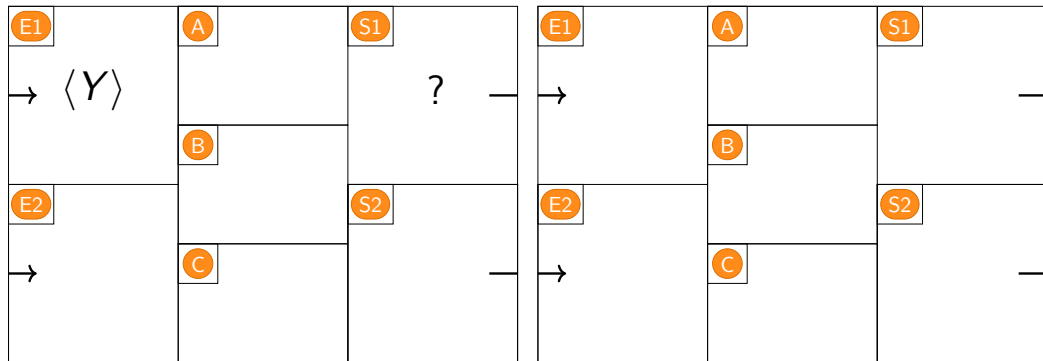
TEST



Indecidabilité de EstVirus

ESTVIRUS

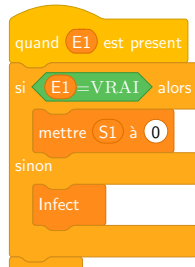
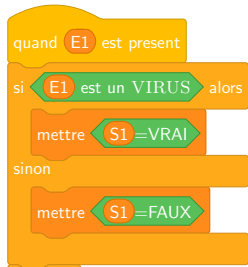
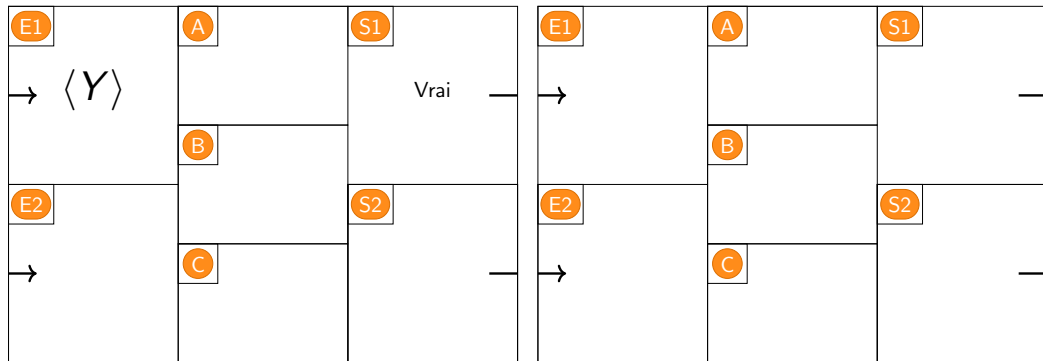
TEST



Indecidabilité de EstVirus

ESTVIRUS

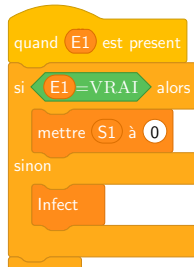
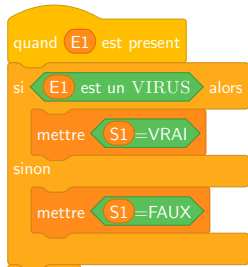
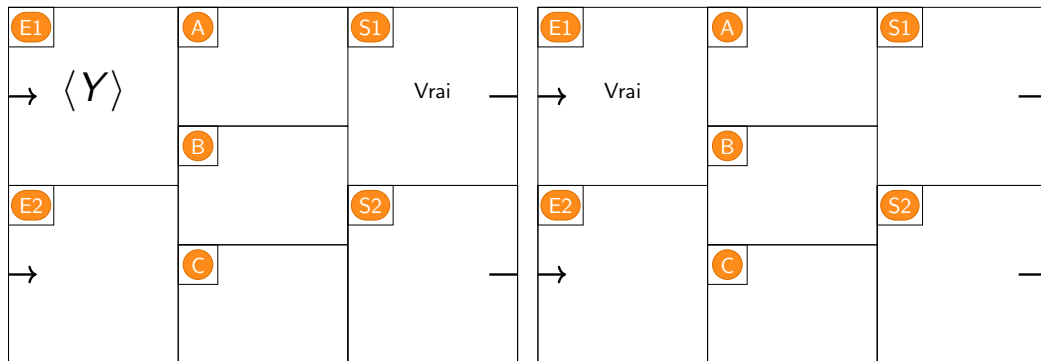
TEST



Indecidabilité de EstVirus

ESTVIRUS

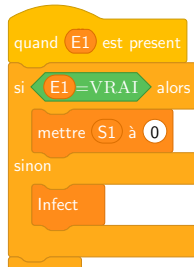
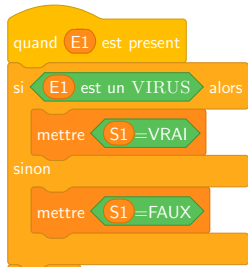
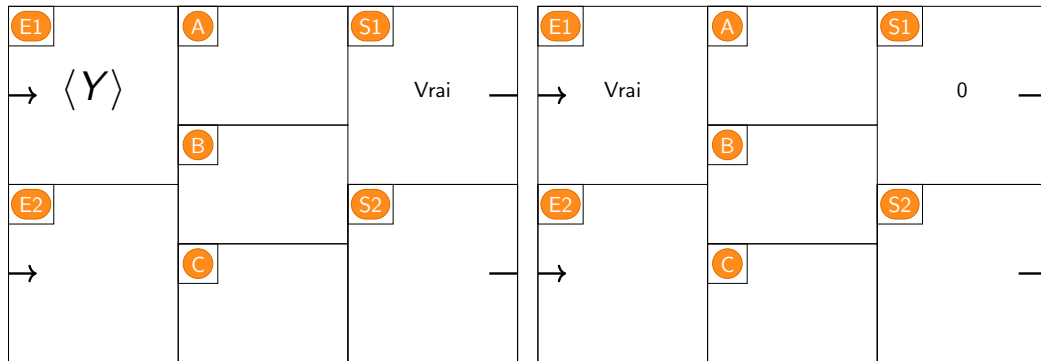
TEST



Indecidabilité de EstVirus

ESTVIRUS

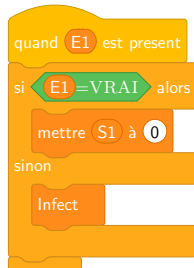
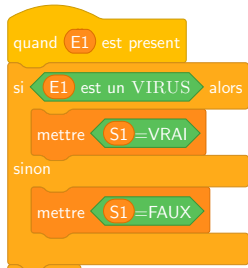
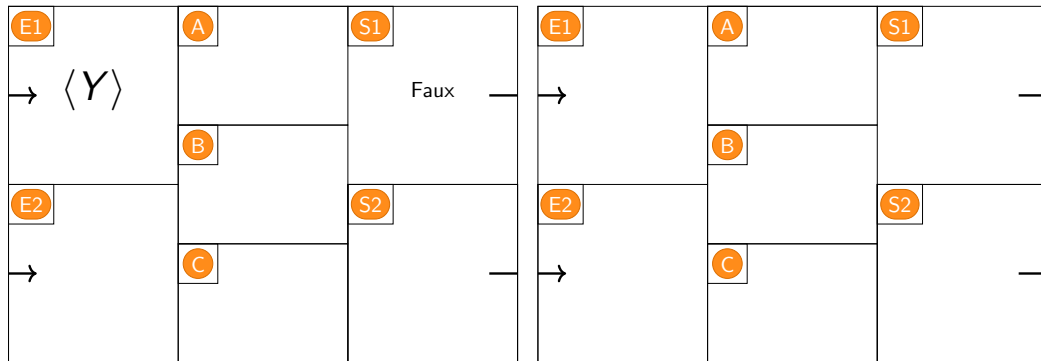
TEST



Indecidabilité de EstVirus

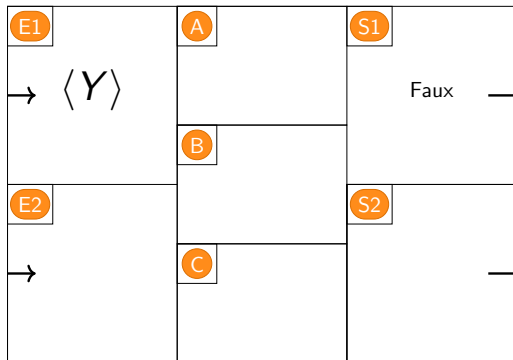
ESTVIRUS

TEST

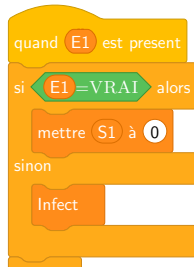
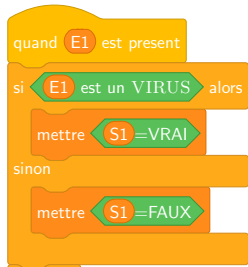
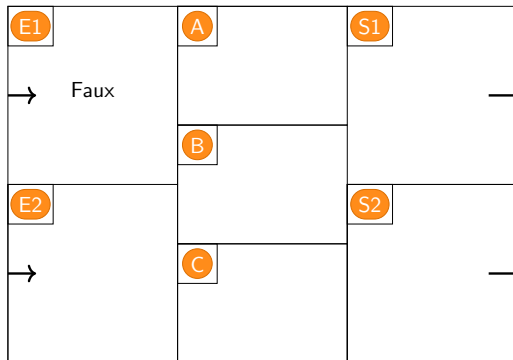


Indecidabilité de EstVirus

ESTVIRUS



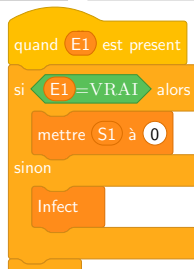
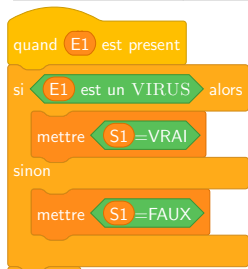
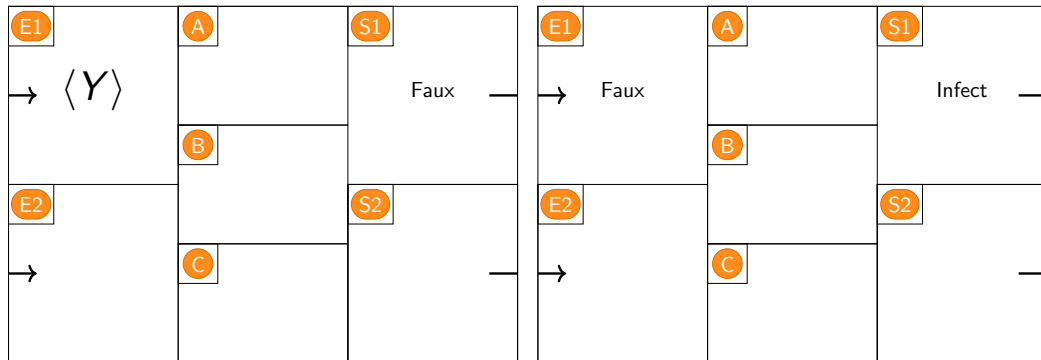
TEST



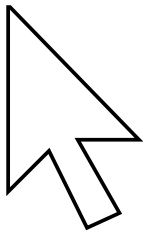
Indecidabilité de EstVirus

ESTVIRUS

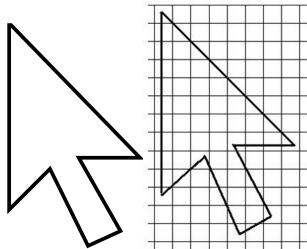
TEST



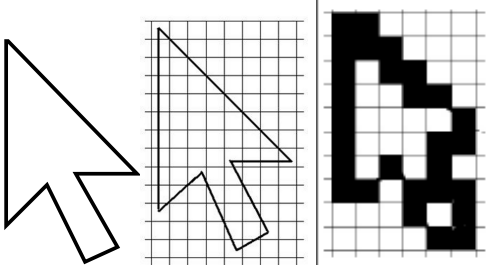
Images sans ordinateur



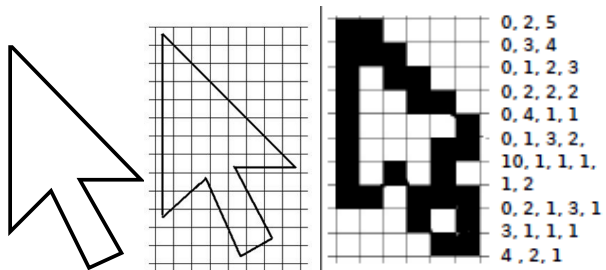
Images sans ordinateur



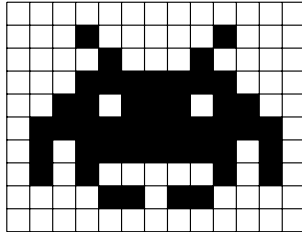
Images sans ordinateur



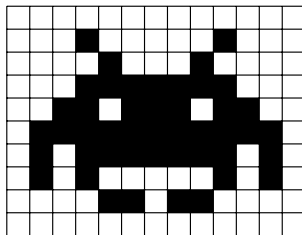
Images sans ordinateur



Encodage à vous de jouer (STYX 10×13)



Encodage à vous de jouer (STYX 10×13)



13

3,1,5,1,3

4,1,3,1,4

3,7,3

2,2,1,3,1,2,2

1,11,1

1,1,1,1,5,1,1,1,1

4,2,1,2,4 13

Décodage 7×7

7

1,5,1

2,1,1,1,2,1

2,1,1,1,2,1

2,1,1,1,2,1

2,1,1,1,2,1

2,1,1,1,2,1

7

Décodage 7×7

7

1,5,1

2,1,1,1,2,1

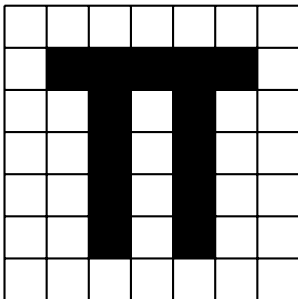
2,1,1,1,2,1

2,1,1,1,2,1

2,1,1,1,2,1

2,1,1,1,2,1

7

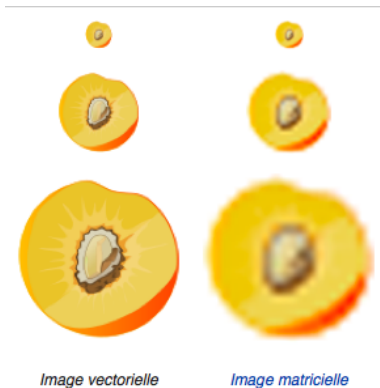


Activité : Poster collaboratif



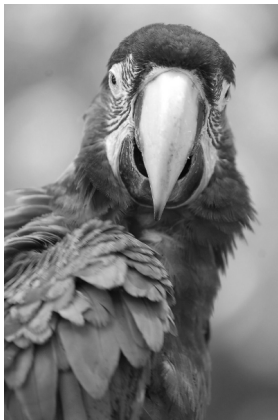
<https://sancy.iut-clermont.uca.fr/~lafourcade/Poster-Collaboratif/>

Formats d'images



BMP, TIFF, GIF, JPEG ou JPG, PNG, PBM, PGM, PPM ...

Coco en Gris



P2

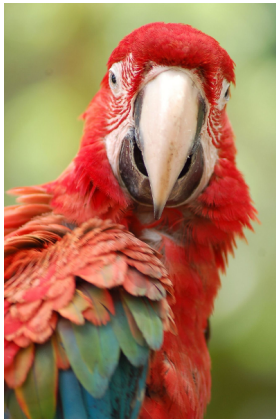
400

603

255

178 178 180 181 182 182 180 182 183 184 184 185 187 186

Coco en Couleur



P3

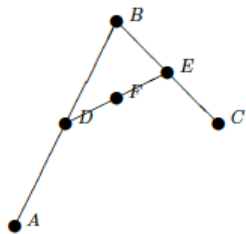
400

603

255

174 185 114 174 186 115 176 188 117 177 188 117 178 189

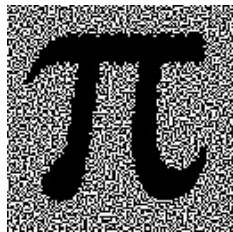
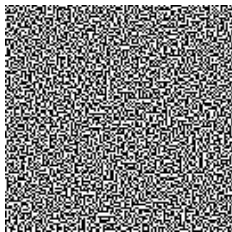
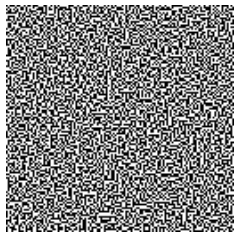
Images vectorielles et Beziers



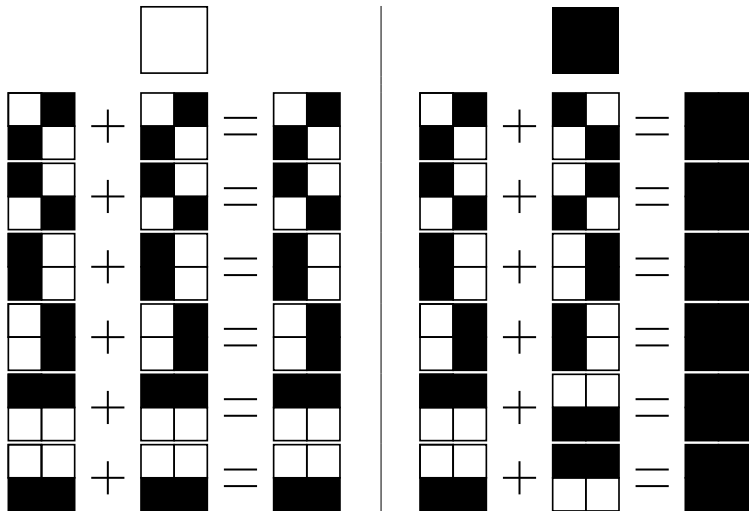
π

Cryptographie visuelle

π



Cryptographie visuelle



<https://sancy.iut-clermont.uca.fr/~lafourcade/Cryptovisuelle/>

Choisir un nombre entre 0 et 31

Est-il ici ? (0)

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31

Est-il ici ? (1)

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31

Est-il ici ? (2)

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31

Est-il ici ? (3)

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31

Est-il ici ? (4)

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31

Votre nombre x est ?

Votre nombre x est ?

0	1	2	3	4	x
					0
✓					1
	✓				2
✓	✓				3
		✓			4
✓		✓			5
	✓	✓			6
✓	✓	✓			7
			✓		8
✓			✓		9
	✓		✓		10
✓	✓		✓		11
		✓	✓		12
✓		✓	✓		13
	✓	✓	✓		14
✓	✓	✓	✓		15

0	1	2	3	4	x
				✓	16
✓				✓	17
	✓			✓	18
✓	✓			✓	19
		✓		✓	20
✓		✓		✓	21
	✓	✓		✓	22
✓	✓	✓		✓	23
			✓	✓	24
✓			✓	✓	25
	✓		✓	✓	26
✓	✓		✓	✓	27
		✓	✓	✓	28
✓		✓	✓	✓	29
	✓	✓	✓	✓	30
✓	✓	✓	✓	✓	31

Comment ça marche ?

$$x = \sum_{i=1}^{i=5} 2^{(i-1)} \times \delta_{i-1}$$

où δ_i vaut 1 si le nombre est présent sur la carte i et 0 sinon.

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31

Tour de magie

Choisir un nombre entre 0 et 32

1	4	6	9
12	14	17	19
22	25	27	30

2	7	10	15
20	23	28	31

3	4	11	12
16	17	24	25
32			

5	6	7	18
19	20	26	27
28			

8	9	10	11
12	29	30	31
32			

13	14	15	16
17	18	19	20

21	22	23	24
25	26	27	28
29	30	31	32

Les faire pratiquer

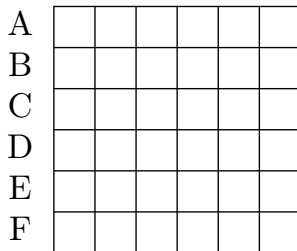
Puzzle :

A						
B						
C						
D						
E						
F						

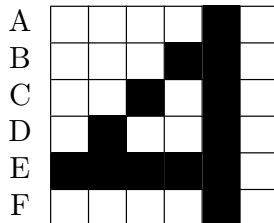
A : 2 ; B : 6 ; C : 10 ; D : 18 ; E : 63 ; F : 2.

Les faire pratiquer

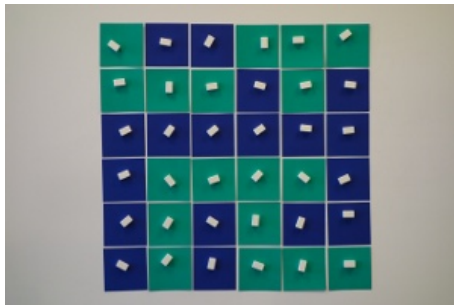
Puzzle :



A : 2 ; B : 6 ; C : 10 ; D : 18 ; E : 63 ; F : 2.



Tour de magie



Code correcteur

Activité : Marmottes



Concevoir un terrier pour l'hiver

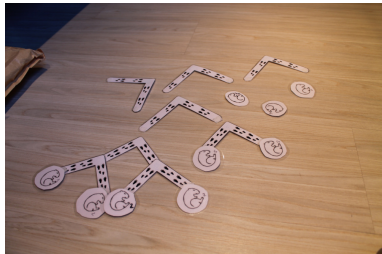
1. À partir de l'entrée, on peut construire deux couloirs. Au bout de chaque couloir, on peut soit creuser une salle soit faire un embranchement vers deux autres couloirs, et ainsi de suite.
2. Pour ne pas se gêner durant leur hibernation, les marmottes vont chacune occuper une salle différente au bout d'un couloir.
3. Chaque marmotte se réveille un nombre précis de fois dans l'hiver.

Marmottes

Décompte des déplacements : Une marmotte dormant à 4 couloirs de l'entrée se réveillant 5 fois dans l'hiver va parcourir $4 \times 5 = 20$ couloirs (on ne comptera que les allers).

Objectif :

Minimiser les bruits des vibrations des pas susceptibles de réveiller le groupe.



<https://members.loria.fr/MDuflot/files/med/marmottes.html>

Prénoms

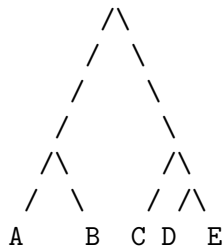
- ▶ Alice : 6
- ▶ Bob : 5
- ▶ Eve : 4
- ▶ Igor : 2
- ▶ Luc : 2
- ▶ Regis : 5
- ▶ Sophie : 2
- ▶ Espérance : 5
- ▶ Quentin : 1

Marmottes : Trouver un bon terrier (Shannon-Fano)

1. Calculer les fréquences d'appartition des lettres.
2. Trier les fréquences .
3. Diviser la liste ordonnée en deux listes de telle sorte que les sommes des fréquences soient les plus proches possible.
4. Donner zéro à la partie gauche et 1 à la partie droite.
5. Recommencer récursivement les deux derniers points sur la partie droite et la partie gauche.

Marmottes : Exemple Shannon-Fano

A=15 B=7 — C=6 — D=6 E=5



Code : A=00 B=01 C=10 D=110 E=111

2.28 bits par symboles

Marmottes : Trouver le meilleur terrier (Huffman)

- ▶ on choisit deux parmi les marmottes qui se lèvent le moins souvent, et on les relie par un morceau de terrier et on note la somme des valeurs des deux marmottes.
- ▶ on recommence exactement la même chose, mais les deux marmottes reliées à l'étape précédente comptent maintenant pour une seule marmotte qui se réveillerait 5 fois
- ▶ on continue, jusqu'à ce que toutes les marmottes soient reliées en un seul terrier.

Exemple : Cyrano de Bergerac en UTF-8 la version compressée avec Huffman gain de 40 %

Marmottes : Exemple Huffman

A=15 — B=7 C=6 — D=6 E=5



Code : A=0 B=100 C=101 D=110 E=111

2.23 bits par symboles

Mission Cryptographie

Initiation à la cryptographie

- ▶ Résoudre des challenges
- ▶ Activité ludique
- ▶ 1 concept = 1 challenge = 1 lettre

En ligne, donc disponible 24h/24h 7j/7j

<https://sancy.iut-clermont.uca.fr/~lafourcade/mission-crypto.html>



Pascal LAFOURCADE



Accueil / Home

Recherche

Enseignement

Pédagogie

Miscellaneous

Docteur en informatique, Maître de Conférence de l'Université Clermont Auvergne, j'effectue ma recherche dans le Thème Réseaux de capteurs du LIMOS (UMR 6158) et mon enseignement au département Informatique de l'IUT et à l'ISIMA. De 2013 à 2016 dans le cadre de la chaire de confiance numérique j'ai organisé chaque mois un séminaire sur la confiance numérique.



Vidéo La révolution blockchain au festival Math en scène mars 2020.

Vidéo Fonctionnement et appropriation de la blockchain Webinaire Block4Coop, 24 septembre 2020.

Article de Nathalie Revol dans Intersites sur l'ouvrage "25 énigmes ludiques pour s'initier à la cryptographie".

Mission Cryptographie

Cette activité débranchée permet de découvrir quelques chiffrements historiques, des concepts de cryptographie moderne mais aussi comment utiliser les mathématiques pour résoudre certaines énigmes. Mission Cryptographie.

Mission Cryptographie

Si vous l'acceptez cette version longue de la mission cryptographie (50 lettres originales à déchiffrer) voici votre première mission, avec comme login : **Mission** et mot de passe : **Crypto**

La seconde partie de la mission Crypto est disponible ici, le login est le prénom de la personne derrière la première mission et le mot de passe est son nom de famille, ses initiales sont JB. Bon courage.

Lettre 0

Le 11 octobre 2018 à Aubière

À qui de droit,

Si vous lisez cette lettre, c'est que mes ennemis m'auront retrouvé et que j'ai dû fuir. Rassurez-vous, j'ai laissé des indications et le code pour ouvrir mon coffre plein de trésors se révélera à ceux qui seront assez persévérants. Cela ne sera pas simple, j'ai utilisé tous mes codes secrets afin d'égarer les curieux et mes ennemis.

Bonne chance !

Agent0111

Post-Scriptum 1 : Décryptez-moi ces jeux bien plus vite que Sherlock et Watson pour finir et gagner !

Post-Scriptum 2 : Pour la version en ligne, **le mot de passe de la lettre 1 est égal à mon login, qui vaut mon nom**. Pour la lettre 2, utilisez le nom d'une personne célèbre en majuscules obtenu dans la lettre 1.

Lettre 1 (Agent0111/Agent0111)

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,

Mh yrlv txh yrxc dyhc frpsulv oh irqfwlrqqhphqw gx frgh gh FHVDU, txl frqvlvwh d ghfdohu fkdtxh ohwwuh gh wurlv srlwlrvq yhuv od gurlwh gdqv o doskdehw. Uhwhqhc fh suhplhu srlqw vhfuhw g devflvvh prlqv flqt hw g rugrqqh prlqv yljw wurlv.

Djhqw0111

Srvw-Vfulswxp 1 : Ghfubswhc prl fhv mhxa elhq soxv ylwh txh Vkhuorfn hw Zdwvrq srxu ilqlu hw jdjqhu !

Srvw-Vfulswxp 2 : Uhwurxyhc ohv wurlv prwv gh sdvvh d sduwlu gx ilfklhu gh prwv gh sdvvh (ohwwuh ghxa).

Observation

Le 11 octobre 2018 à Aubière

À qui de droit,
Si vous lisez cette lettre ...

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,
Mh yrlv txh yrxcv ...

Observation

Le 11 octobre 2018 à Aubière

À qui de droit,
Si vous lisez cette lettre ...

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,
Mh yrlv txh yr xv ...

a	b	c	d	e	f	g	h	i	j	k	l	m
d	e	f	g	h				l			o	

n	o	p	q	r	s	t	u	v	w	x	y	z
	r		t	u		w	x		a	b	c	m

Mh yrlv txh yr xv dyhc ...
-e -oi- que -ou- a-e- ...

Observation

Le 11 octobre 2018 à Aubière

À qui de droit,
Si vous lisez cette lettre ...

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,
Mh yrlv txh yr xv ...

a	b	c	d	e	f	g	h	i	j	k	l	m
d	e	f	g	h				l			o	

n	o	p	q	r	s	t	u	v	w	x	y	z
	r		t	u		w	x		a	b	c	m

Mh yrlv txh yr xv dyhc ...
-e -oi- que -ou- a-e- ...



Observation

Le 11 octobre 2018 à Aubière

À qui de droit,
Si vous lisez cette lettre ...

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,
Mh yrlv txh yr xv ...

a	b	c	d	e	f	g	h	i	j	k	l	m
d	e	f	g	h				l			o	

n	o	p	q	r	s	t	u	v	w	x	y	z
	r		t	u		w	x		a	b	c	m

Mh yrlv txh yr xv dyhc ...
-e -oi- que -ou- a-e- ...



Décalage de 3 lettres

Observation

Le 11 octobre 2018 à Aubière

À qui de droit,
Si vous lisez cette lettre ...

Oh 11 rfwreuh 2018 d Dxelhuh

D txl gh gurlw,
Mh yrlv txh yr xv ...

a	b	c	d	e	f	g	h	i	j	k	l	m
d	e	f	g	h				l			o	

n	o	p	q	r	s	t	u	v	w	x	y	z
	r		t	u		w	x		a	b	c	m

Mh yrlv txh yr xv dyhc ...
-e -oi- que -ou- a-e- ...



Décalage de 3 lettres
Je vois que vous avez ...

Lettre 2

Login	Astuce	H(password)
Alice	Yellow	709
Agent007	incassable	555
Blaise	Musique Puy de Dome	742
Camille	Isere Cubisme	829
David	Electric	709
Edouard	Noce de Figaro Auvergne	742
Eve	Pokemon	709
Matthieu	Flute enchanteee Departement	742
Nadia	Pointure Demoiselles d'Avignon	829
Nathalie	Nintendo	709
Philippe	Alpes Guernica	829
Remi	Mendeleiev Strontium Peintre	829
Robert	Amadeus Annee de naissance	742
Stephane	Grenoble Pablo	829
Valery	Compositeur Clermont	742
Xavier	Marche Turque Maison	742

$$H(W) = \sum_{w_i \in W} ASCII(w_i)$$

$$H(Pi314) = H(P) + H(i) + H(3) + H(1) + H(4) = 80 + 105 + 51 + 49 + 52 = 337$$

Lettre 4 : VIGENERE

CLAIR : S H E R L O C K E T W A T S O N

CLEF : C E S A R C E S A R C E S A R C

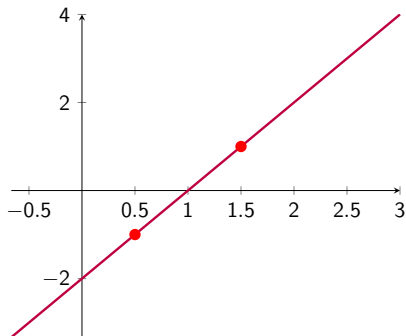
CHIFFRE : U L W R C Q G C E K Y E L S F P

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Lettre 5 : Partage de secret (Shamir)

Méthode

Avec les 2 points des lettres précédentes.
Résoudre un système de deux équations.



Principe Lettre 6

Clairs / Chiffrés à analyser.

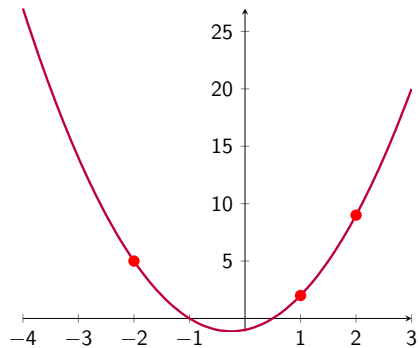
Principe Lettre 7

Chaque symbole correspond à un chiffre compris entre 0 et 9. Retrouvez les correspondances entre les symboles et les chiffres.

Lettre 8 : Bandelettes



Lettre 9 : Shamir again



$$y = ax^2 + bx + s$$

Lettre 10 : Victoire

Découverte de l'Agent0111.

PS : vous auriez pu le deviner !



- ▶ Math C2+ 2nd
- ▶ Fête de la science (2nd, 1ère, BTS)
- ▶ Gagnants auvergnats concours Alkindi



- ▶ Licence Pro Web
- ▶ Formation des professeurs du lycée
- ▶ Atelier APMEP
- ▶ Salon Culture % Jeux Mathématiques en 2020
- ▶ RJMI à Clermont en 2020

Mission 2 en ligne

- ▶ Dancing Men
- ▶ Hachage
- ▶ Transposition
- ▶ Aliens
- ▶ ...

Mission 3 en ligne

- ▶ Morse
- ▶ Chiffrement visuel
- ▶ Alberti
- ▶ SSE
- ▶ Side Channel
- ▶ Scytale
- ▶ Stéganographie
- ▶ Chiffrement homomorphique
- ▶ ...

Mission 4 en ligne

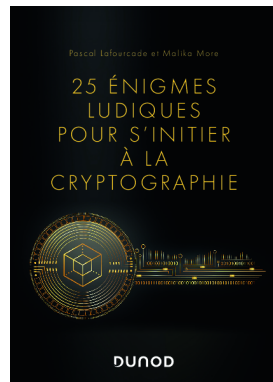
- ▶ Stéganographie
- ▶ Runes
- ▶ Pig Pen
- ▶ Atbash
- ▶ Polybe
- ▶ Cryptarythme
- ▶ Shadocks Base 4
- ▶ ...

Mission 5 en ligne !

- ▶ Téléphone
- ▶ Mary Stuart
- ▶ Bibinaire
- ▶ Bitcoin
- ▶ RSA
- ▶ MiM
- ▶ CRC
- ▶ Brute force
- ▶ Password



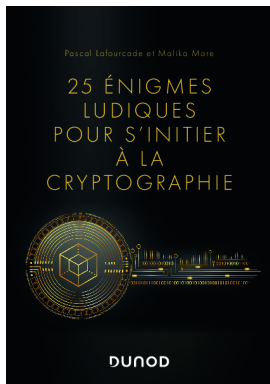
Merci à Cédric Lauradoux



Conclusion



- ▶ Apprendre en s'amusant
- ▶ Travail en équipe
- ▶ Étudiants actifs
- ▶ Découverte ... imagination
- ▶ Initiation à la cryptographie moderne



Questions ?

pascal.lafourcade@uca.fr