

Vulgarisation en sécurité

Pascal Lafourcade



Bourges, 30 novembre 2023

Vulgarisation ?

Vulgarisation ?

Processus par lequel des informations et des concepts scientifiques sont rendus accessibles et compréhensibles pour un public non spécialisé ou le grand public.

ChatGPT

Autres termes :

- ▶ Médiation scientifique
- ▶ Diffusion scientifique

Vulgarisation sur Youtube



Vulgarisation à la télévision



Vulgarisation à la radio/en podcast



Vulgarisation dans les magazines



Vulgarisation dans les musées



cit

sciences
et industrie



Palais
DÉCOUVERTE



Vulgarisation dans les musées



Activités autour de l'informatique débranchée

Informatique débranchée ?

- ▶ Enseigner des notions d'informatique de façon ludique, **sans utiliser d'ordinateur**
- ▶ Se concentrer sur les **concepts scientifiques**
- ▶ Ne pas se laisser éblouir ni rebuter par la technologie

Historique :

- ▶ **1992** : Publication scientifique, Université Canterbury, Nouvelle-Zélande
- ▶ **2006** : Soutien de Google
- ▶ **2016** : Soutien de Microsoft
- ▶ **2016** : Introduction dans les programmes scolaires

Computer Science Unplugged: school students doing real computing without computers

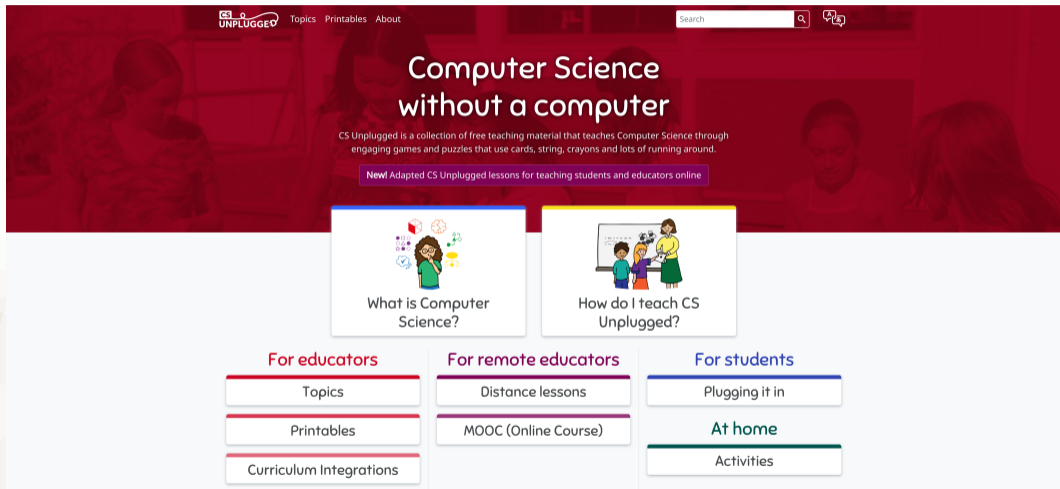
Tim Bell Computer Science and Software Engineering, University of Canterbury tim.bell@canterbury.ac.nz	Jason Alexander Computer Science and Software Engineering, University of Canterbury jason.alexander@pc.canterbury.ac.nz	Isaac Freeman Computer Science and Software Engineering, University of Canterbury isaac.freeman@itg.ac.nz	Mick Grimley School of Education Studies and Human Development, University of Canterbury michael.grimley@canterbury.ac.nz
--	---	---	---

Abstract
The Computer Science Unplugged project provides ways to expose students to ideas from Computer Science without having to use computers. This has a number of applications, including outreach, school curriculum support, and clubs.
The "Unplugged" project, based at Canterbury University, uses activities, games, magic tricks and competitions to show children the kind of thinking that is expected of a computer scientist. All of the activities are available free of charge at csunplugged.org.
The project has recently enjoyed widespread adoption internationally, and substantial industry support. It is recommended in the ACM K-12 curriculum, and has been translated into 12 languages. As well as simply providing teaching resources, there is a very active program developing and evaluating new formats and activities. This includes adaptations of the kinesthetic activities in

Mathematics. He has worked as a classroom teacher, and is now a fulltime web designer and developer.
Mick Grimley is a Senior Lecturer in the School of Educational Studies and Human Development at the University of Canterbury. Mick is interested in the enhancement of learning, and in particular as it relates to cognition, motivation, interest, interactivity, new technologies and e-learning. These interests have led him into the study of how technology can be leveraged to improve learning.

1 Introduction
The desire for a "knowledge-based economy" and a recognition that successful companies based on software and hardware development can make major contributions to a country's earnings has resulted in a push for students to become better skilled in "ICT". Unfortunately this term is very broad, and can include anything from knowing how to add on numbers on a spreadsheet, to developing a

Communauté internationale : csunplugged.org




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.

New! Adapted CS Unplugged lessons for teaching students and educators online



What is Computer Science?



How do I teach CS Unplugged?

For educators

- Topics
- Printables
- Curriculum Integrations

For remote educators

- Distance lessons
- MOOC (Online Course)

For students

- Plugging it in
- At home
- Activities

Groupe “Informatique sans Ordinateur”



Membres :

- ▶ Professeurs des écoles
- ▶ Enseignants de mathématiques et de NSI de collège et lycée
- ▶ Enseignants-chercheurs

Objectifs :

- ▶ Création d'activités débranchées
- ▶ Tests en classe avec les élèves
- ▶ Formation des enseignants, animation d'ateliers

Activité poster collaboratif

- ▶ Découverte du codage des images
- ▶ Découverte du binaire et de l'héxadécimal

0,1,1,1,1,1,3							
1,1,5,1							
1,7							
2,2,1,2,1							
1,7							
2,3,1,1,1							
4,2,2							
0,2,2,1,1,1,1							



0,1,1,1,1,1,3							
1,1,5,1							
1,7							
2,2,1,2,1							
1,7							
2,3,1,1,1							
4,2,2							
0,2,2,1,1,1,1							

Activité poster collaboratif



Exemples de posters collaboratifs



Alan Turing

Exemples de posters collaboratifs



Maryam Mirzakhani

Exemples de posters collaboratifs



Edward Snowden

Autres activités

- ▶ Cryptographie
- ▶ Images
- ▶ Architecture des ordinateurs
- ▶ Automates finis
- ▶ Bases de données
- ▶ ...

Activités en ligne autour de sécurité/ cryptographie



Informatique Sans Ordinateur

Initiation à la cryptographie

- ▶ Résoudre des challenges
- ▶ Activité ludique
- ▶ En groupe
- ▶ Disponible en ligne
- ▶ 1 concept = 1 challenge = 1 lettre

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

Mission Cryptographie

Cette activité permet de découvrir quelques chiffrements historiques et comment utiliser les mathématiques pour résoudre certaines énigmes. Si vous l'acceptez 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 : Décodez-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 Dixelhuh

D txl gh gurlw,

Mh yrlv txh yrxc dyhc frpsulv oh irqfwlrqqhphqw gx frgh gh FHVDU, txl frqvlvwh d ghfdohu fkdtxh ohwwuh gh wurlv srvlwlrqv 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 mxxa elhq soxv ylwh txh Vkhurfn hw Zdwvrq srxu ilqlu hw jdqhu !

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

Observation & déduction

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 & déduction

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 & déduction

Le 11 octobre 2018 à Aubière

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

Oh 11 rfwreuh 2018 d Dixelhuh

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

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 yrxc dyhc ...
-e -oi- que -ou- a-e- ...



Observation & déduction

Le 11 octobre 2018 à Aubière

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

Oh 11 rfwreuh 2018 d Dixelhuh

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 & déduction

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

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

$$H(\text{Pi}314) = H(\text{P}) + H(\text{i}) + H(3) + H(1) + H(4) = 80 + 105 + 51 + 49 + 52 = 337$$

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

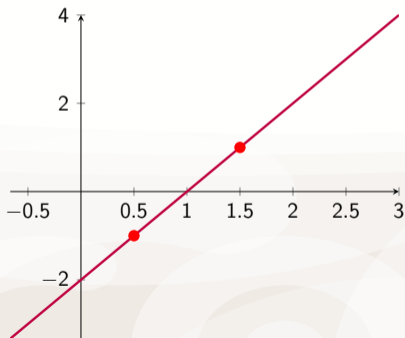
CHIFFRE : U L W R C Q G C E K Y E L S F P

	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.



Lettre 6/7

Principe Lettre 6

Comme la première lettre !
Clairs / Chiffrés à analyser.

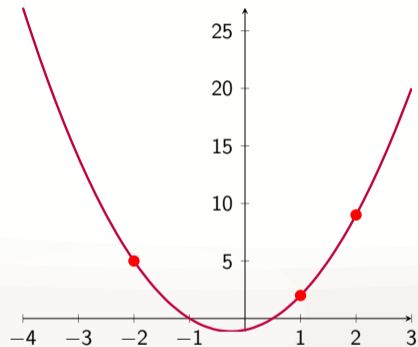
Principe Lettre 7

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

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 !

ISO

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



- ▶ Licence Pro Web (Lundi)
- ▶ Formation des professeurs du lycée

Mission 2, 3, 4 et 5 en ligne

- ▶ Dancing Men
- ▶ Hachage
- ▶ Transposition
- ▶ Aliens
- ▶ ...
- ▶ Morse
- ▶ Chiffrement visuel
- ▶ Alberti
- ▶ SSE
- ▶ Side Channel
- ▶ Scytale
- ▶ Stéganographie
- ▶ Chiffrement homomorphe
- ▶ ...
- ▶ Stéganographie
- ▶ Runes
- ▶ Pig Pen
- ▶ Atbash
- ▶ Polybe
- ▶ Cryptarythme
- ▶ Shadocks Base 4
- ▶ ...
- ▶ Téléphone
- ▶ Mary Stuart
- ▶ Bibinaire
- ▶ Bitcoin
- ▶ RSA
- ▶ MiM
- ▶ CRC
- ▶ Brute force
- ▶ Password

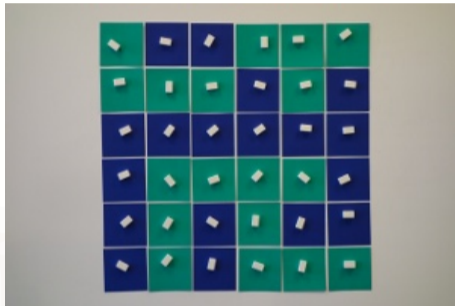
Conclusion



- ▶ Travail en équipe
- ▶ Étudiants actifs
- ▶ Découverte ... imagination

Tour de Magie

Tour de magie

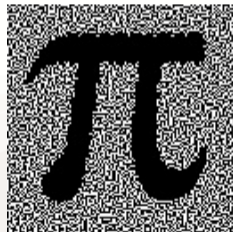
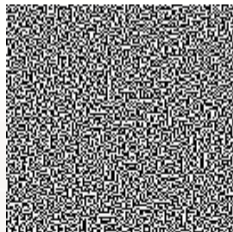
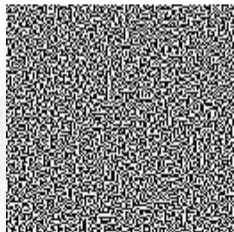


Code correcteur

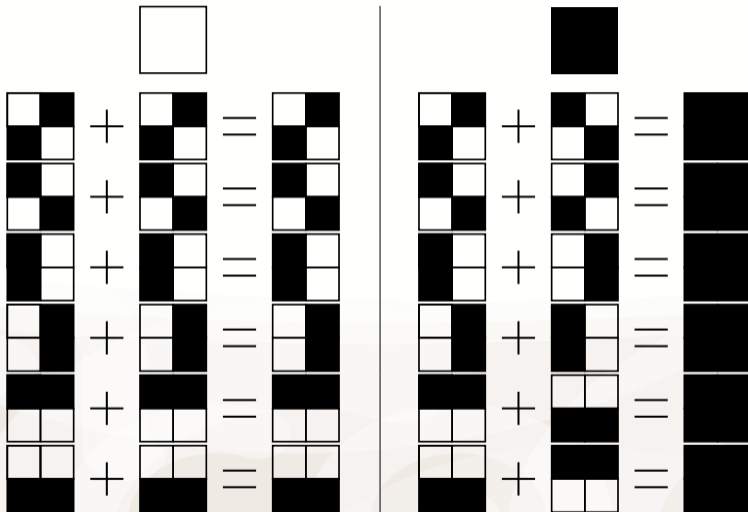
Cryptographie Visuelle

π

π



Cryptographie visuelle



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

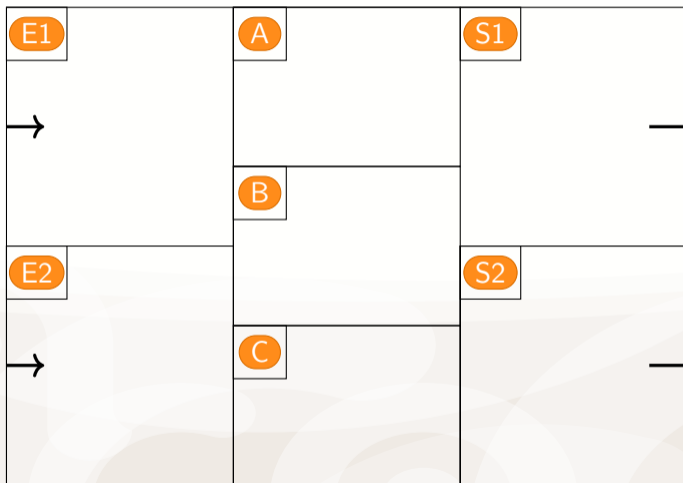
Antivirus (Halting)

Antivirus parfait existe-t-il ?

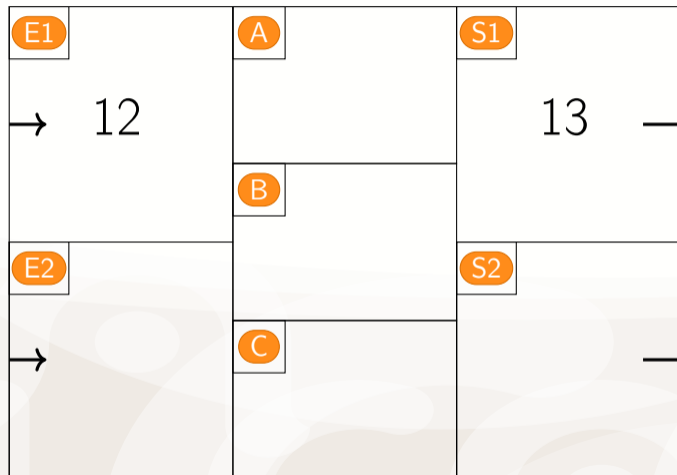


Journault Matthieu, Lafourcade Pascal, More Malika, Poulain Rémy, Léo Robert,
How to teach the undecidability of malware detection problem and halting problem.
In WG 11.8 - 13th World Conference on Information Security Education, WISE 2020.

Materiel



Programme Simple: Incrément

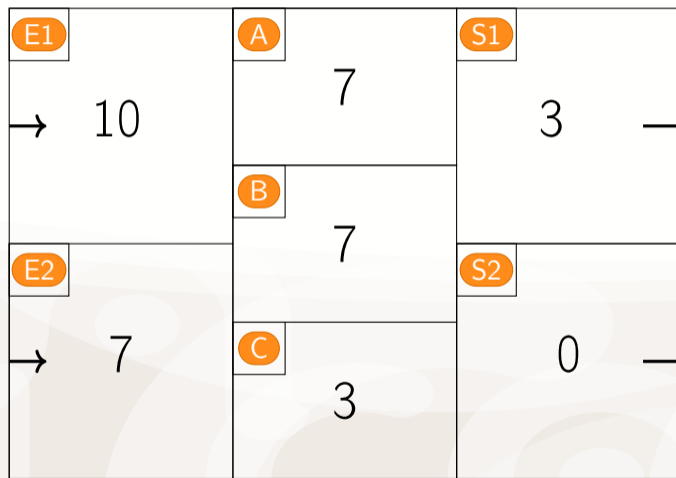


quand **E1** est présent

mettre **S1** à **E1 + 1**

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**

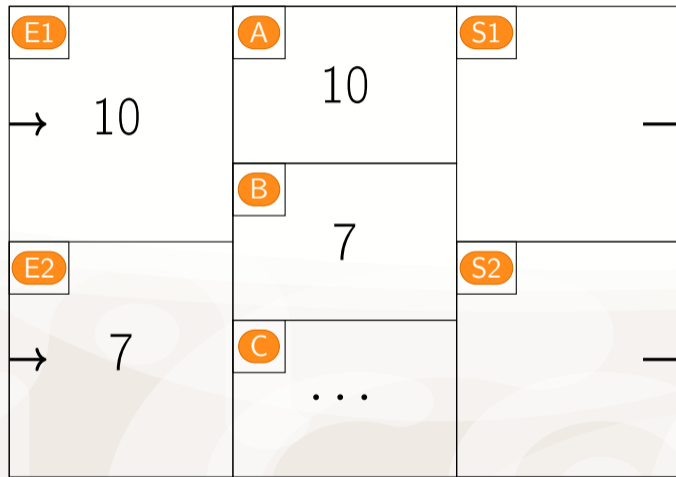
mettre **A** à **A - 1**

mettre **S1** à **C**

mettre **S2** à 0

stop

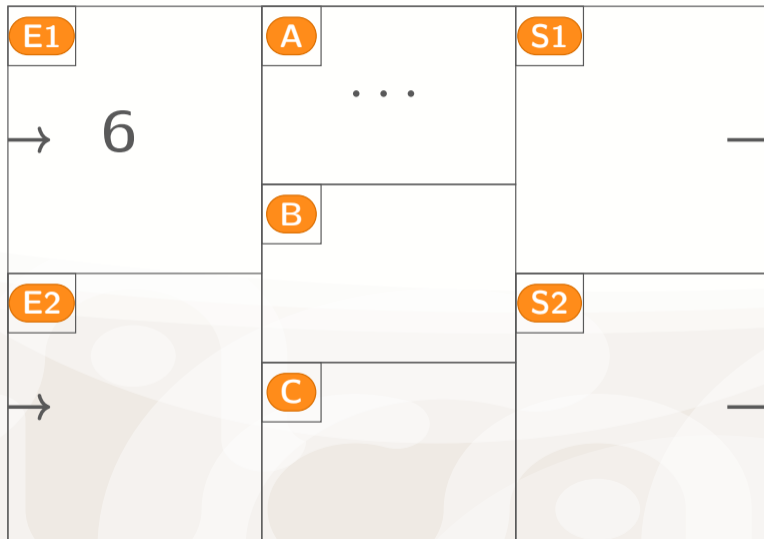
Programme Simple: Moins*



```
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
```

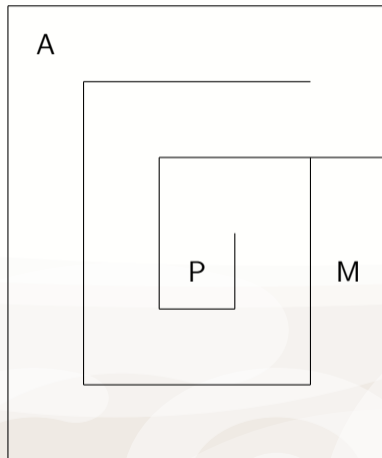
Programme Simple : Super

(termine ou pas)

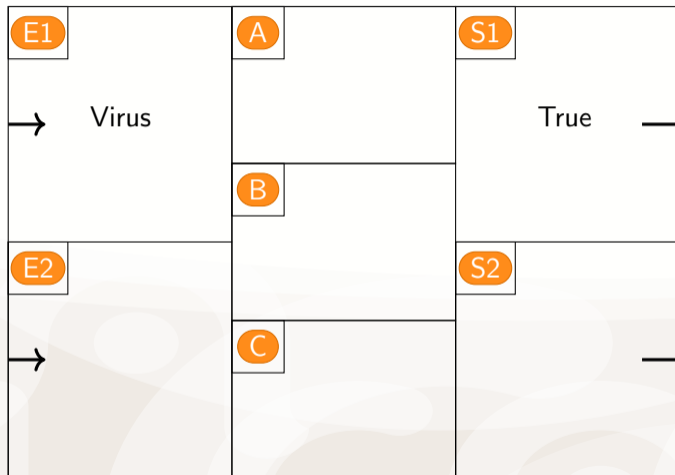


```
quand E1 est présent
mettre A à E1
répéter jusqu'à A = 0
  mettre A à A + 1
mettre S1 à A
stop
```

Preuve par disjonction et par l'absurde

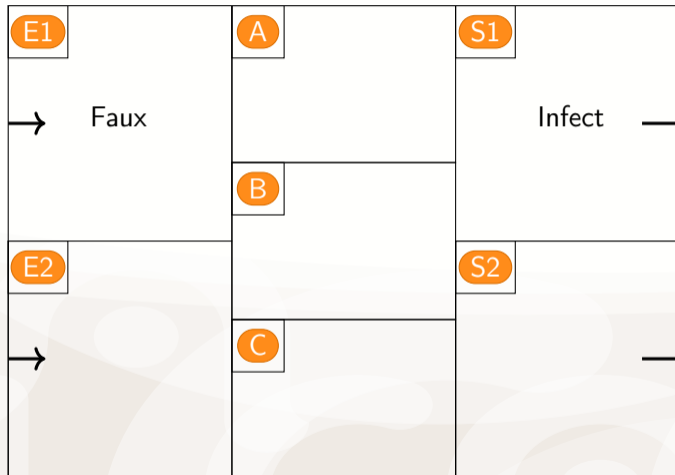


Programme EstVirus



```
quand E1 est present
si E1 est un VIRUS alors
  mettre S1 =VRAI
sinon
  mettre S1 =FAUX
stop
```

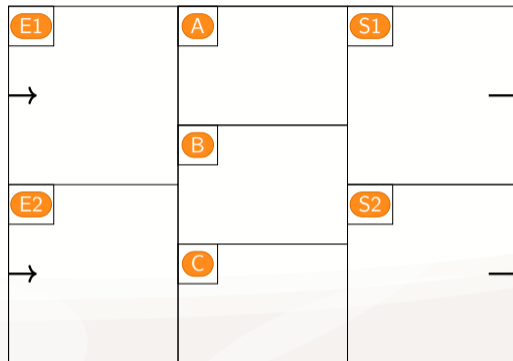
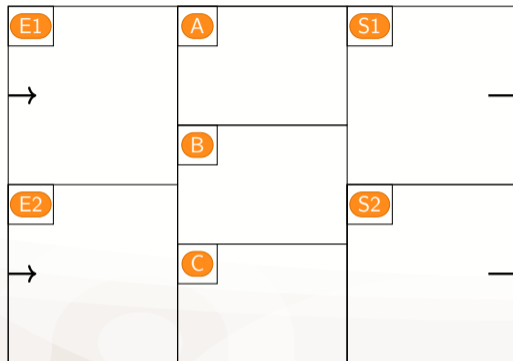
Program Test



Indecidabilité de EstVirus

EstVirus

Test



quand E1 est present

si E1 est un VIRUS alors

mettre S1 = VRAI

sinon

mettre S1 = FAUX

quand E1 est present

si E1 = VRAI alors

mettre S1 à 0

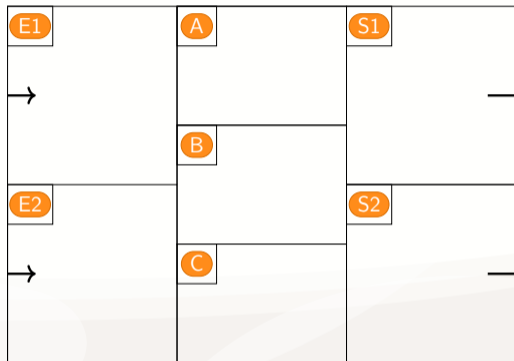
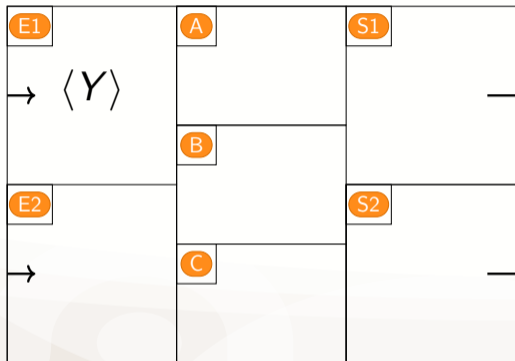
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1** à **0**

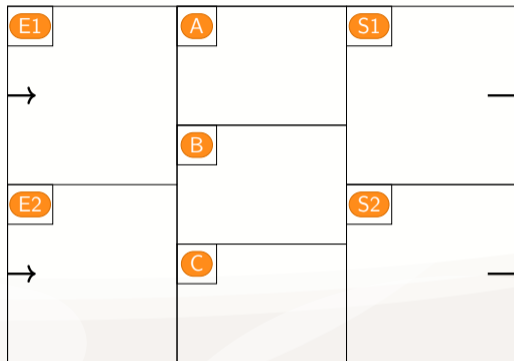
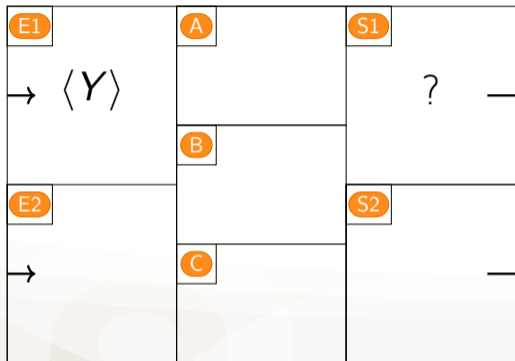
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1** à **0**

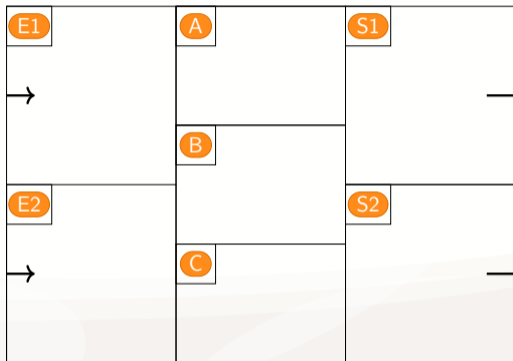
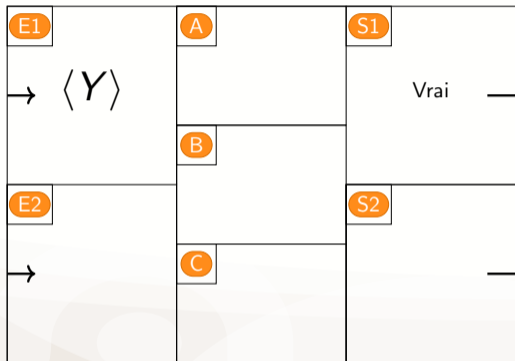
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1** à **0**

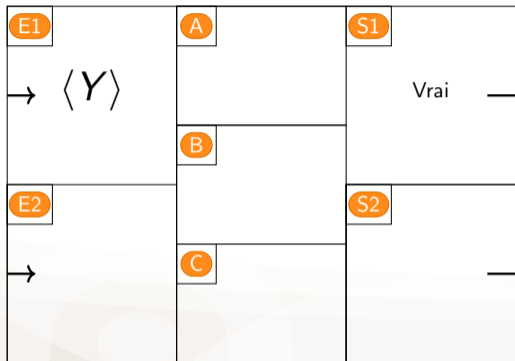
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1 à 0**

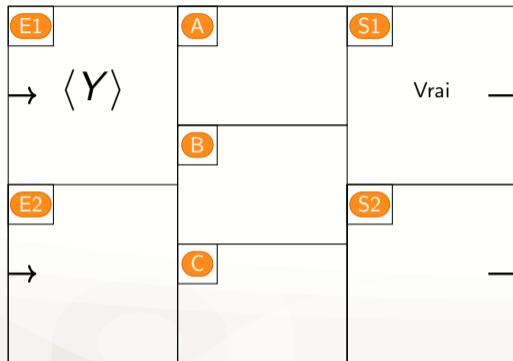
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1 à 0**

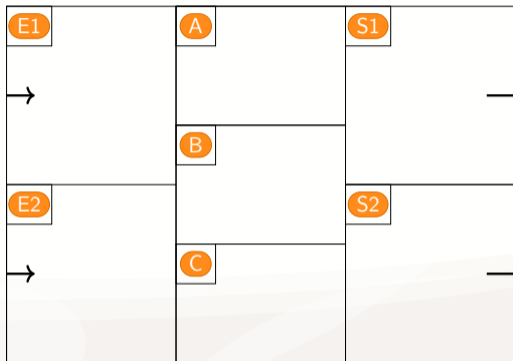
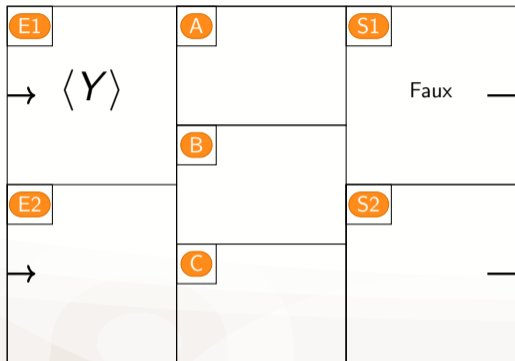
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1** à **0**

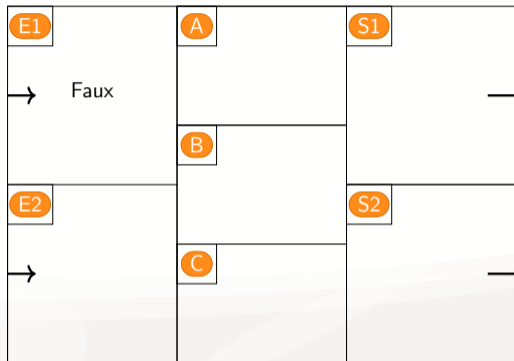
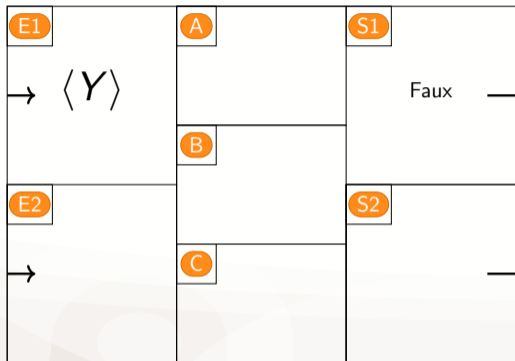
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1 est un VIRUS** alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

si **E1 = VRAI** alors

mettre **S1** à **0**

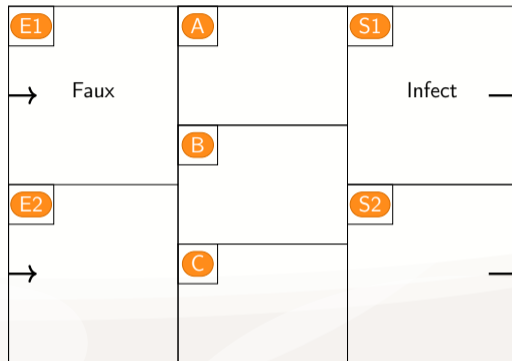
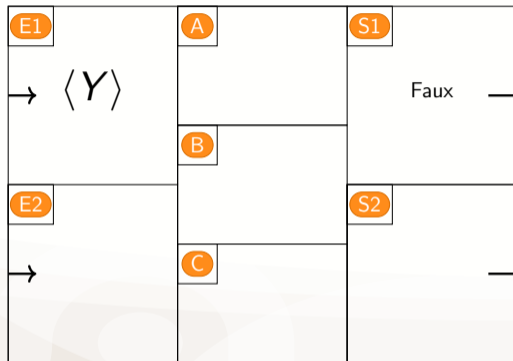
sinon

Infect

Indecidabilité de EstVirus

EstVirus

Test



quand **E1** est present

si **E1** est un VIRUS alors

mettre **S1 = VRAI**

sinon

mettre **S1 = FAUX**

quand **E1** est present

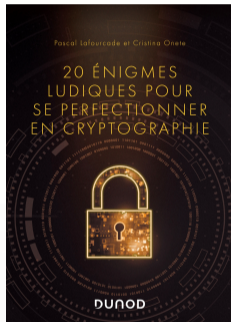
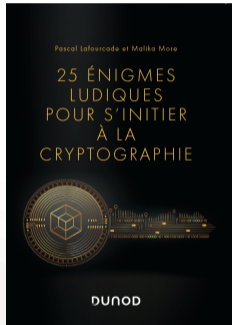
si **E1 = VRAI** alors

mettre **S1** à 0

sinon

Infect

Livres



Livre 1 : 25 + 1 énigmes

- 1 Un message dans le texte
- 2 Les secrets de Jules
- 3 Une image mystérieuse
- 4 Un chiffrement presque allemand
- 5 Un méli-mélo de caractères
- 6 Vous avez dits ûr,... sûr
- 7 Une modification invisible
- 8 Chiffrer deux fois n'est pas deux fois plus sûr
- 9 Le protocole de Diffie-Hellman pour établir une clé
- 10 Le partage de Shamir
- 11 Un regroupement de nombres
- 12 Des chiffrés mélangés
- 13 Prouver sans dévoiler
- 14 Le mythe de l'antivirus
- 15 Désassembler une fonction de hachage
- 16 Des images qui en cachent d'autres
- 17 L'homme du milieu
- 18 La consommation électrique en dit trop
- 19 Le digicode lumineux
- 20 Des couples clairs chiffrés
- 21 Un chiffrement malléable
- 22 Payer en bitcoins
- 23 La solidité d'un mot de passe
- 24 Un vote naïf
- 25 Des indices qui deviennent compromettants

Livre 2 : 20 + 1 énigmes

- 1 Bandelettes
- 2 Une démarche anonyme
- 3 Route666
- 4 Une pique de rappel 5
- 5 Tel un orgue de Barbarie
- 6 Chercher des collisions
- 7 Test du canard
- 8 Un couple en trop
- 9 Les tribulations d'un ménage français
- 10 L'usurpateur de signatures
- 11 Découplage
- 12 Jouer à Tetris post-quantique
- 13 Tracer une BMW
- 14 Jeu de mots ... de passe
- 15 Où ira l'Amiral Yamamoto?
- 16 Edwards vs Weierstrass
- 17 Attaque de type
- 18 Miroir, mon beau miroir
- 19 Consensus divergeant
- 20 Malléabilité

Comment construire une mission ?

- ▶ Un concept cryptographique
- ▶ Une idée d'énigme
- ▶ Un prototype
- ▶ Des essais / erreurs

Un exemple : La stéganographie

- ▶ Un concept cryptographique : La stéganographie
- ▶ Une idée d'énigme : Cacher des bits dans une image ASCII
- ▶ Un prototype jp2a et 1 0
- ▶ Des essais / erreurs

```
.....          ...          .          ...          ...          .....  
.kkkkkkkkk.      :kkko.      .,c.      .cccc,'';1ll:;:0xkkk. ,kkkkkkkkkkkkkl  
      ;kk.          ;kkokkl      .' ;.      .cccccc:cc:llxkxxkk. ,kk  
      ,kk.          :xk: :kkc      .,:.      .cc;.:;:;:c;:;:,' lkk. ,kk:  
      ,kk.          :kkc ;xk:      .' ;.      .cc; ',;:;,,.. lkk. ,kkdccccccc;  
      ,kk.          :kkx,'..'1kk: .;c.      .cc;      lkk. ,kk0,,,,,.  
      .      ckk.      ;kkdddddddxkc      .' ;.      .cc;      lkk. ,kk:  
.lxo:;:dkk:      ,kk:          ;kk1      .,:.      .cc;      lkk. ,kko;:;:;:;:;  
      .,clooc;.      .cc;          ;cc' ..'      ,,,      ;cc. 'ooooooooo0l.
```

Un exemple : La stéganographie

- ▶ Un concept cryptographique : La stéganographie
- ▶ Une idée d'énigme : Cacher des bits dans une image ASCII
- ▶ Un prototype jp2a et 1 0
- ▶ Des essais / erreurs

```
.....          ...          .          ...          ...          .....  
.kkkkkkkkk.      :kkko.      .,c.      .cccc,'';1ll:;:0xkkk. ,kkkkkkkkkkkkkl  
      ;kk.          ;kkokkl      .' ;.      .cccccc:cc:llxkxxkk. ,kk  
      ,kk.          :xk: :kkc      .,:.      .cc;.:;:;:c;:;:,' lkk. ,kk:  
      ,kk.          :kkc ;xk:      .' ;.      .cc; ',;:;,.. lkk. ,kkdccccccc;  
      ,kk.          :kkx,'..'1kk: .;c.      .cc;      lkk. ,kk0,,,,,.  
      .      ckk.      ;kkdddddddxkc      .' ;.      .cc;      lkk. ,kk:  
.lxo:;:dkk:      ,kk:          ;kk1      .,:.      .cc;      lkk. ,kko;:;:;:;:;  
      .,clooc;.      .cc;          ;cc' ..'      ,,,      ;cc. 'ooooooooo0l.
```

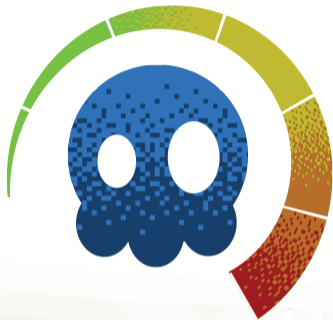
101010 = 42

CTF

CTF Time

- ▶ InsomnHack : 22-24 avril 2024 (Lausanne, CH)
- ▶ Hack.lu : 2023 is the 13th edition (Luxembourg)
- ▶ Ph0wn : November 24-25, 2023 (Sophia)
- ▶ BlackAlps : NOV 2-3, 2023 (Yverdon-les-Bains, CH)
- ▶ THCON 2024 : 4-5 avril 2024 (Toulouse)
- ▶ Breizhctf : 17 au 18 mars 2023 (Rennes)
- ▶ Hack'Lantique 11 mars 2023 (Rennes)
- ▶ INS'HACK 29 - 30 avril 2023 (Kryptosphère INSA Lyon)
- ▶ ComCyber sur l'OSINT
- ▶ HACKFEST (Canada)

<https://ctftime.org/ctfs>



New is not always better.

GREHACK

11

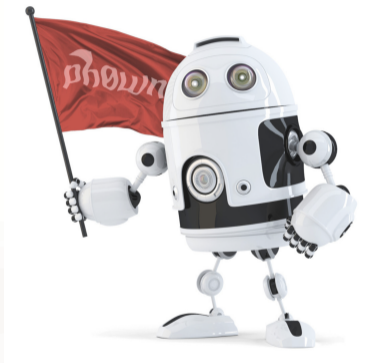
- ▶ 1 jour de conférences + Workshops
- ▶ 1 jour de CTF
- ▶ 500 personnes

CSAW'23

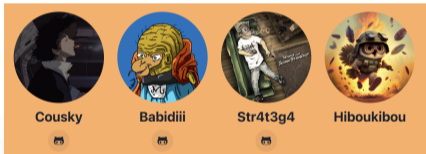
- ▶ Valence
- ▶ 1 Rejeu papiers + conférence
- ▶ 1 jour CTF (Embedded, RED, ...)

Ph0wn depuis 2012

A Capture The Flag for Smart Devices



- ▶ 1/2 journées Workshop
- ▶ 1 jour CTF



- ▶ 1 jour de CTF
- ▶ 13 décembre 2021
- ▶ 11 mars 2023

<https://zitf.fr/>

Conclusion

Conclusion

- ▶ Partir d'un concept
- ▶ Prendre en compte le niveau
- ▶ Tester
- ▶ Le côté ludique

Questions ?

pascal.lafourcade@uca.fr

Merci

