Mission Cryptographie

Pascal Lafourcade

LIMOS

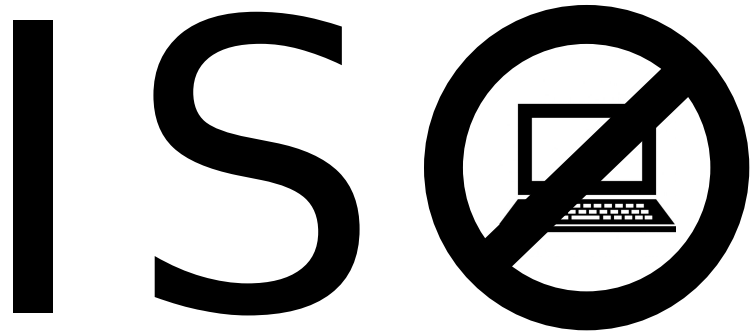
UNIVERSITÉ Clermont Auvergne

APMEP 2020

Les Maths en Scène

LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Objectif



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-clermont.uca.fr/ lafourcade/

LIMOS

- Accueil / Home
- Recherche
- Enseignement
- Pédagogie
- Miscellaneous

Pascal LAFOURCADE

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.

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 Cryprographie.

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

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 révèlera 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 yrxv 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 rugrqqhh prlqv ylqjw 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 & 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 yrxv ...

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 yrxv ...

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 yrxv 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 Dxelhuh

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

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 yrxv 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 Dxelhuh

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

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 yrxv 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 yrxv ...

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

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

LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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 enchantee 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
```

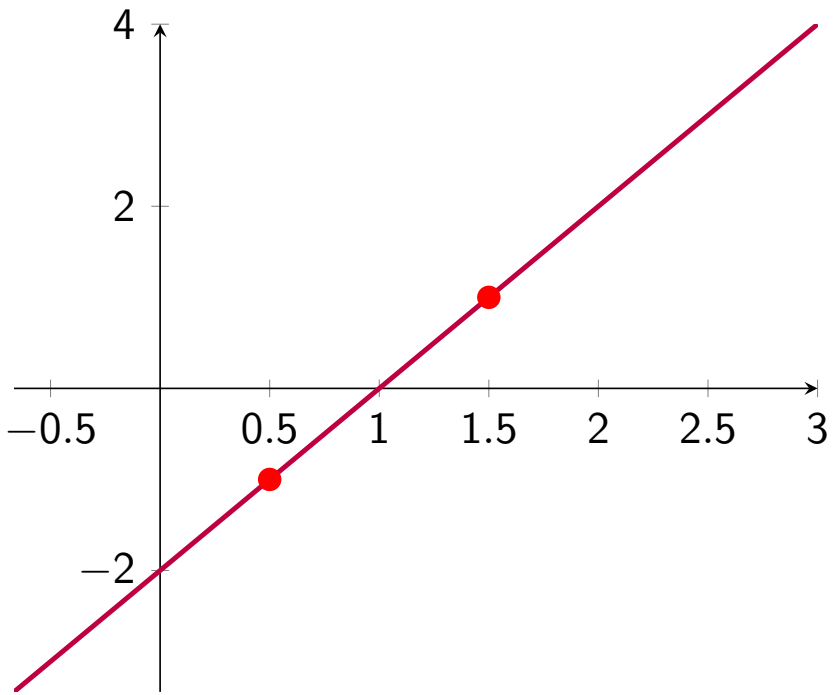
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

LIMOS

Lettre 5 : Partage de secret (Shamir)

Méthode

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



Lettre 6/7

Principe Lettre 6

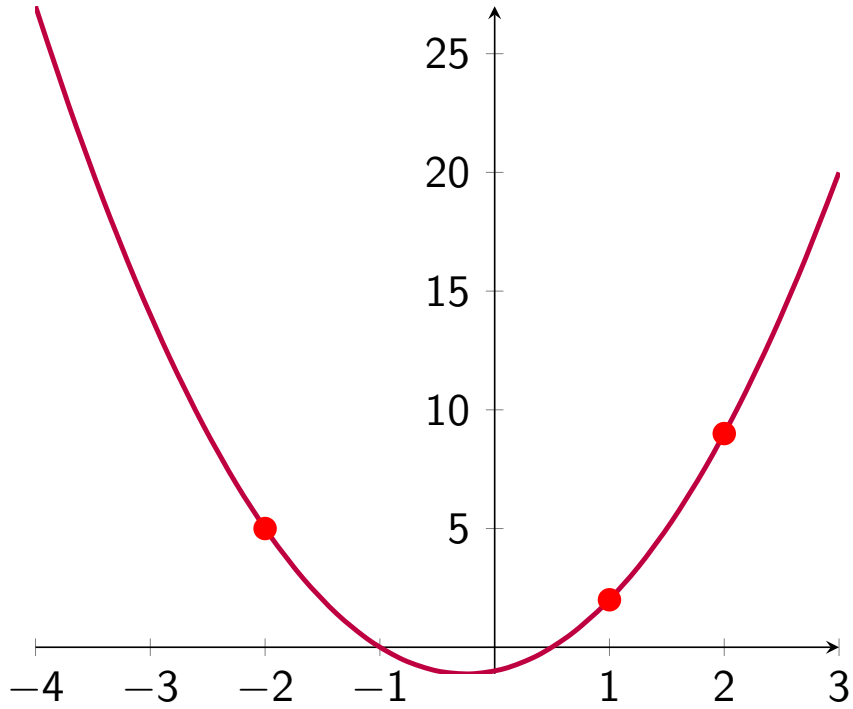
Comme la première lettre !
Clairs / Chiffrés à analyser.

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



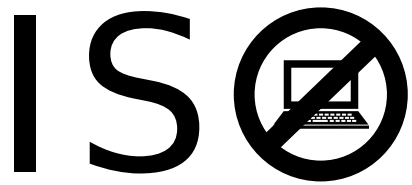
$$y = ax^2 + bx + s$$

Lettre 10 : Victoire

Découverte de l'Agent0111.

PS : vous auriez pu le deviner !

Retour d'expériences



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

- Licence Pro Web
- Formation des professeurs du lycée

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

Conclusion

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

20 énigmes stimulantes pour s'initier à la cryptographie

Pascal Lafourcade et Malika More, Dunod 2021

pascal.lafourcade@uca.fr

Questions ?

Les Maths en Scène

https://lesmathsenscene.fr

https://sancy.iut-clermont.uca.fr/ lafourcade/

LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Merci à Cédric Lauradoux