



# Compétitions en informatique

---

Un tour d'horizon



# Comité départemental compétitions, événements et rayonnement

---

M. Jean Privat, Ph.D.

Professeur d'informatique

# Introduction

---

- Différents types de compétitions
  - Programmation
  - Sécurité
- Formats, déroulement et culture
- Exemples d'énoncés
- Pratique et préparation



# Compétitions de programmation

---

[Git Gud]



# Hackathons

---

Fin de semaine

24 - 48h de développement

Présentations

Juges

Prix

# Hackathon - Catégories

---

Souvent orientés vers un but

Hacking Health → Innovations en santé

WearHacks → Technologies portables

Web, mobile ou autre.

Livrer un concept (PoC)

# Hackathons - Exemple

---

GSoft - Slackathon

Slack

Bot

Productivité

Réalisation

# Hackathons - Liste (non-exhaustive)

---

McHacks - Hackathon de l'université McGill

EcoHack - Hackathon pour l'environnement

ConUHacks - Hackathon de l'université de Concordia

McGill Physics Hackathon - Hackathon concernant la physique

AngelHack - Hackathon pour une bonne cause

Hack The North - Le plus gros hackathon du Canada, sujet libre

AquaHacking - Hackathon pour le fleuve Saint-Laurent

BioHackathon - Hackathon lié aux sciences biologiques

Hacking Health - Hackathon sur la santé

# IEEE Xtreme

---

22 octobre 2016

24h de programmation

Compétition d'algorithmique

# IEEE Xtreme - Format

---

En ligne

HackerRank

Énoncés et tests

Liste de langages acceptés



All Domains



## Tutorials

[View all](#)

- [30 Days of Code](#)

## Algorithms

[View all](#)

- [Warmup](#)
  - [Strings](#)
  - [Implementation](#)
  - [Sorting](#)
- [view more](#) [Math Theory](#)

## Data Structures

[View all](#)

- [Arrays](#)
  - [Trees](#)
  - [Stacks](#)
  - [Linked Lists](#)
  - [Balanced Trees](#)
- [view more](#) [Trees](#)

## Mathematics

[View all](#)

- [Fundamentals](#)
  - [Combinatorics](#)
  - [Geometry](#)
  - [Number Theory](#)
  - [Algebra](#)
- [view more](#) [Probability](#)

## Artificial Intelligence

[View all](#)

- [Bot Building](#)
  - [Alpha Beta Pruning](#)
  - [Games](#)
  - [A\\* Search](#)
  - [Combinatorial Search](#)
- [view more](#) [Statistics and Machine Learning](#)

## C++

[View all](#)

- [Introduction](#)
  - [Classes](#)
  - [Inheritance](#)
  - [Strings](#)
  - [STL](#)
- [view more](#)

## Java

[View all](#)

- [Introduction](#)
  - [BigNumber](#)
  - [Object Oriented Programming](#)
  - [Strings](#)
  - [Data Structures](#)
- [view more](#) [Exception Handling](#)

## Python

[View all](#)

- [Introduction](#)
  - [Strings](#)
  - [Math](#)
  - [Basic Data Types](#)
  - [Sets](#)
- [view more](#) [Tools](#)

## Ruby

[View all](#)

- [Introduction](#)
  - [Arrays & Hashes](#)
  - [Methods](#)
  - [Control Structures](#)
  - [Enumerables](#)
- [view more](#) [Strings](#)

## SQL

[View all](#)

- [Basic Select](#)
  - [Aggregation](#)
  - [Advanced Join](#)
  - [Advanced Select](#)
  - [Basic Join](#)
- [view more](#) [Relative Queries](#)

## Databases

[View all](#)

## Distributed Systems

[View all](#)

# IEEE Xtreme - Exemples de questions

---

## Exemples de questions

Question D 2011

# IEEE Xtreme - Préparation

---

Algorithmes communs

HackerRank

Pratiques de compétitions de l'AGEEI

# IEEE Xtreme - Difficultés et approches

---

Adaptation d'algorithme

Solution ponctuelle (Ne pas essayer de généraliser les solutions)

# Game Jams

---

Création de jeux vidéo

Exemples:

- Global Game Jam
- Ludum Dare
- Project One Game a Month
- Montreal Game Jam

# CSGames

---

Interuniversitaire (Nord-est)

1er cycle

~30 équipes sur place

Commanditaires sur place



# CSGames - Format

---

Compétitions en blocs de 3h

2-3 personnes par équipe par compétition

Compétitions 48h

Compétitions sociales





Malware detected!!!  
**STUXNETS**

Malware detected!!!  
**STUXNETS**

Malware detected!!!  
**STUXNETS**

   
Le génie pour l'industrie

   
Le génie pour l'industrie  
**GSOFT**





# CSGames - Catégories

---

Programmation Extrême

Intelligence Artificielle

Algorithmes

Programmation à relais

Systemes d'exploitation

Compilation

Informatique théorique

Développement Web

Sports

Gaming

Sécurité

Débug

Mobile

Parallélisme

# CSGames - Social

---

Flashouts

Costumes

Festivités

Mauvais coups

“La Machine”

Banquet





# CSGames - Préparation

---

Pratiques de compétition de l'AGEEI

Connaître les domaines

Connaître les technos

Pression

Solutions ad-hoc

# CSGames - Difficultés et approche

---

Problèmes non-réalisables (non-réalistes)

Environnement (IRL et technologique)

Attaquer ce qui est résolvable

Code jetable



# Compétitions de insécurité



[Shell or GTFO]



# CTF - WTF

---

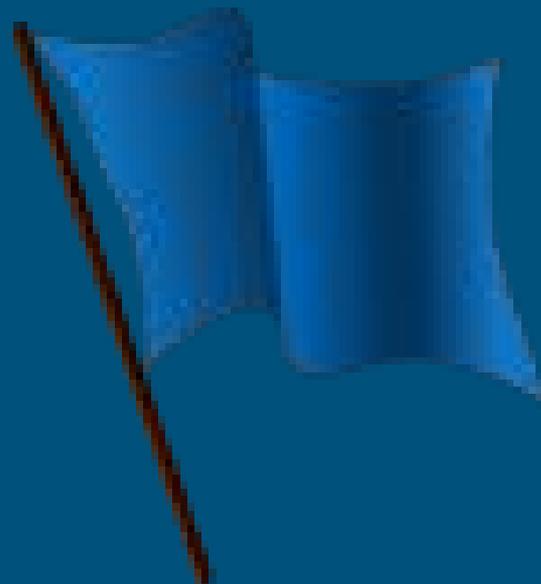
Compétition de sécurité informatique

Offensif

Flag == Secret

Exemple de flag:

```
flag{17s_0k_8i7s_n3v4r_fL!p_1RL}
```



# CTF - Objectif (Haut niveau)

---

Voler de l'information secrète

Aux organisateurs

Aux autres participants

“Vendre” l'information pour de points

# CTF - Objectifs (Moins haut niveau)

---

Briser des programmes

Utiliser les programmes des autres pour faire nos trucs

Utiliser une multitude de ruses pour abuser du comportement des systèmes à notre avantage

# CTF - Sur place - Formats

---

Blue Team / Red Team

Attaque / Défense

Hacking Quest

Cyber Warfare

Jeopardy

DEFCON (ou "Batshit Insane")

# CTF - En ligne - Formats

---

Jeopardy

[Attaque / Défense]

6/16/2013 5:54:05 PM <global> PPP solved everything with two hours to spare! Call Heinz 'cause y'all need to ketchup!

6/16/2013 5:51:03 PM >private< Your teammate PPP solved bob [OMGACM] for 4 points.

6/16/2013 5:50:58 PM >private< Your teammate PPP solved bob [OMGACM] for 4 points.

6/16/2013 2:11:12 PM <global> You should totally check out OMGACM5.

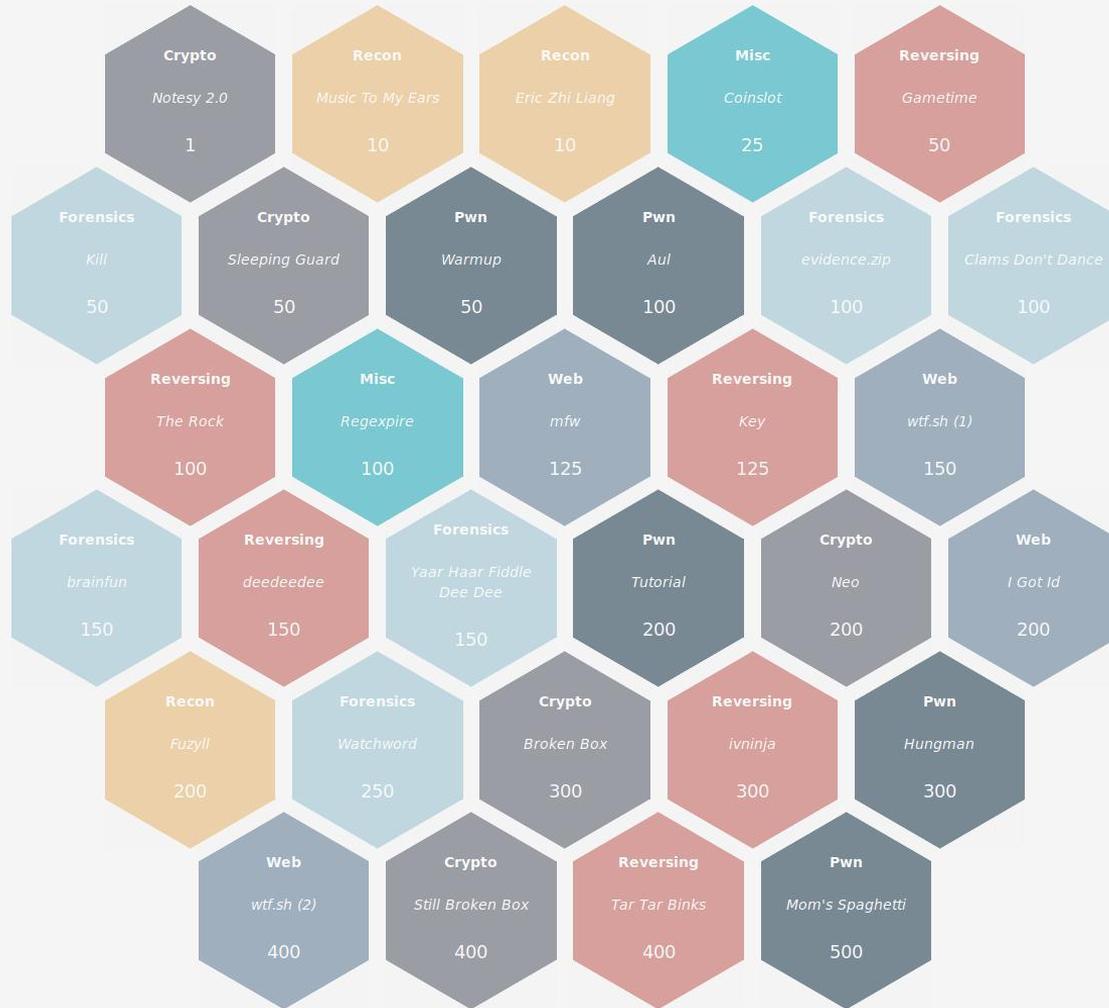
6/16/2013 3:28:18 PM >private< Your teammate PPP solved tastycloud [gnireenigne] for 5

3dub	0x41414141	\xff\xe4\xcc	OMGACM	gnireenigne
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4
5	5	5	5	5

1:49:00 left

PPP	75
European NOPSled Team	70
More Smoked Leet Chicken	68
blue-lotus	64
Shellphish	60
WHAT_Mafia	59
Men in Black Hats	58
clgt	58
9447	58
Routards	56
WOWHACKER-B105	56
Shell Corp	56
Samurai	54
sutegoma2	54
APT8	54
Alternatives	53
pwningyeti	53
[TechnoPandas]	51
RDot.Org	51
United States of Russia	51
Marauders	50
CodeRed	50
KAIST GoN	50
int3pids	47
Robot Mafia	47

# CHALLENGES







e.g. "wonderland" or "alewife" or "bu central"

Search

## Boston Key Party 2015 » Pwning Reversing Crypto "School Bus"

**Airport**

The timing in this challenge is clearly not very realistic—but the methods you'll use here can be extended to real-world implementations of modular exponentiation. Server at 52.1.245.61, port 1025. My solution takes a little while. Good luck. : 500

Dane do Mapy ©2015 Google    Warunki korzystania z programu    Zgłoś błąd w mapach

# CTF - Catégories de défis

---

Cryptographie

Stéganographie

Rétro-ingénierie

Exploitation binaire

Sécurité Mobile

Sécurité Web

Informatique légale (Forensics)

Programmation

Reconnaissance

Administration système et réseau

Trivia

# Exemples

43wdxz 4edcvt5 65rdcvb 6tfcgh8uhb 9ijn

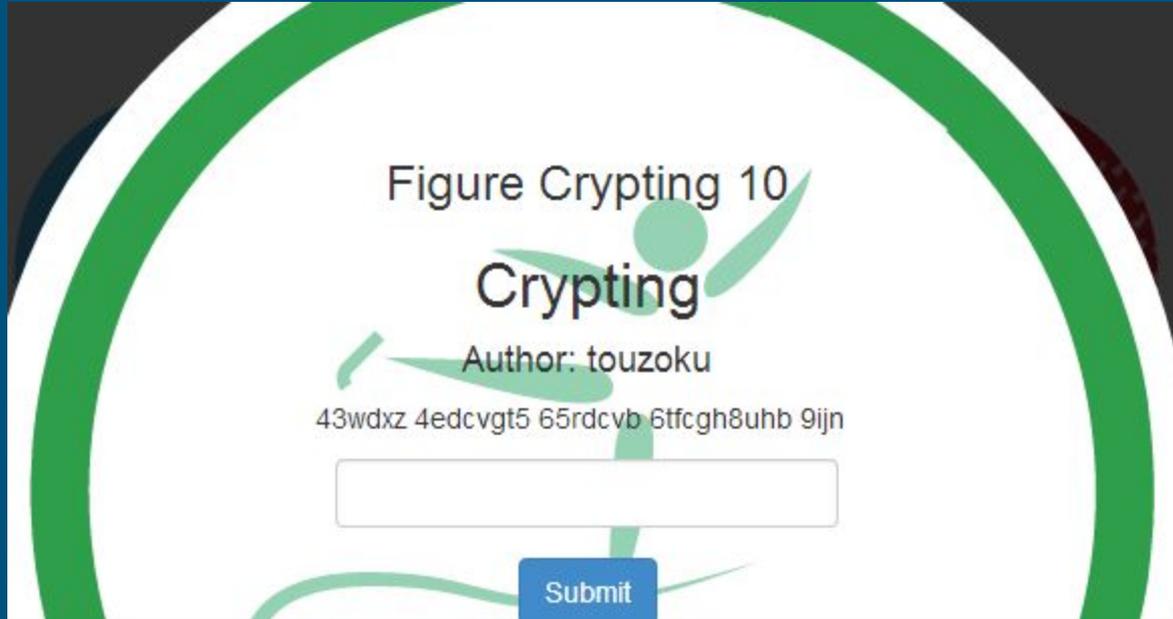


Figure Crypting 10

Crypting

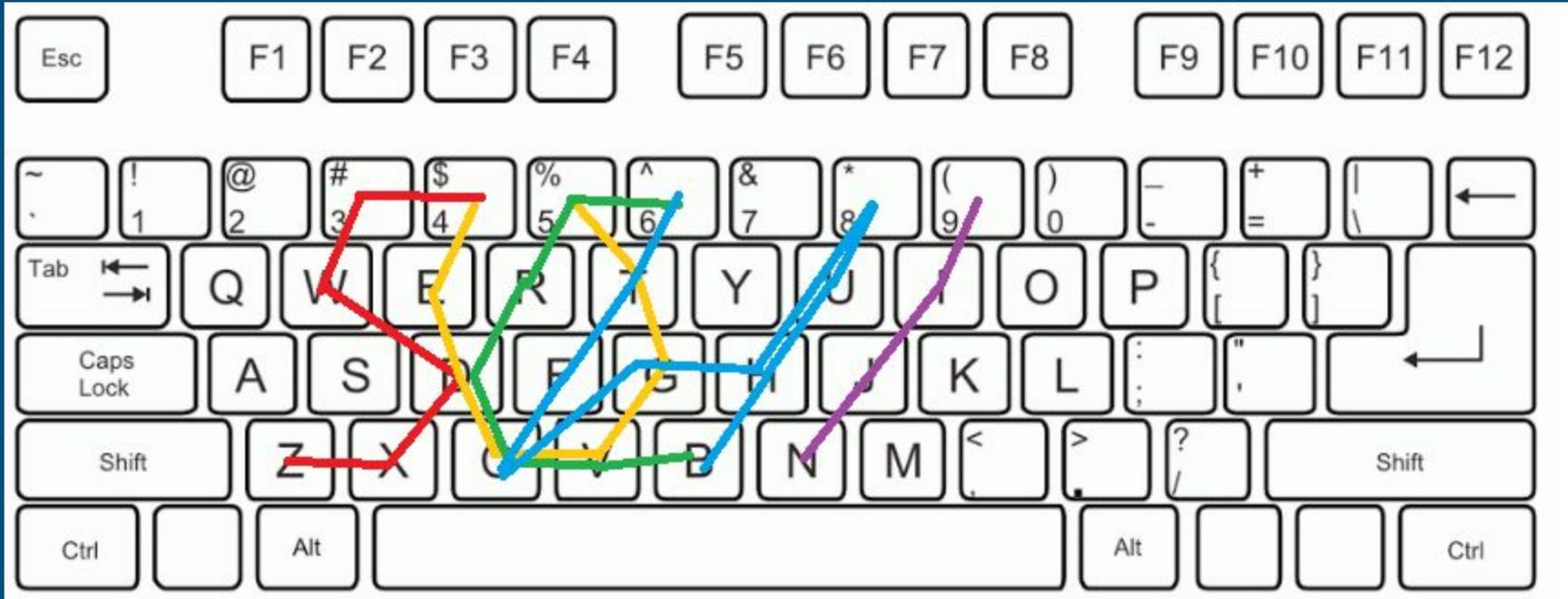
Author: touzoku

43wdxz 4edcvt5 65rdcvb 6tfcgh8uhb 9ijn

Submit

The image shows a web application interface with a white background and green decorative elements. At the top, the text 'Figure Crypting 10' is displayed. Below it, the word 'Crypting' is written in a large, bold font. Underneath, the author's name 'Author: touzoku' is shown. The example text '43wdxz 4edcvt5 65rdcvb 6tfcgh8uhb 9ijn' is displayed. A text input field is located below the text, and a blue 'Submit' button is positioned at the bottom center.

# Exemple - Solution



# Exemple - Reversing

```
File Edit View Search Terminal Help
ppp@debian:~/Downloads$ ./crackme1
Loading...
Where is the flag?
ppp@debian:~/Downloads$
```

```
gdb-peda$ pdisass main
```

```
Dump of assembler code for function main:
```

```
0x0804846c <+0>:    push   ebp
0x0804846d <+1>:    mov    ebp,esp
0x0804846f <+3>:    push   edi
0x08048470 <+4>:    and    esp,0xffffffff
0x08048473 <+7>:    sub    esp,0x30
0x08048476 <+10>:   mov    DWORD PTR [esp+0x2c],0x0
0x0804847e <+18>:   mov    DWORD PTR [esp],0x18
0x08048485 <+25>:   call   0x8048330 <malloc@plt>
0x0804848a <+30>:   mov    DWORD PTR [esp+0x2c],eax
0x0804848e <+34>:   mov    DWORD PTR [esp+0x8],0x18
0x08048496 <+42>:   mov    DWORD PTR [esp+0x4],0x0
0x0804849e <+50>:   mov    eax,DWORD PTR [esp+0x2c]
0x080484a2 <+54>:   mov    DWORD PTR [esp],eax
0x080484a5 <+57>:   call   0x8048370 <memset@plt>
0x080484aa <+62>:   mov    eax,DWORD PTR [esp+0x2c]
0x080484ae <+66>:   mov    DWORD PTR [eax],0x47414c46
0x080484b4 <+72>:   mov    DWORD PTR [eax+0x4],0x3930342d
0x080484bb <+79>:   mov    WORD PTR [eax+0x8],0x32
0x080484c1 <+85>:   mov    eax,DWORD PTR [esp+0x2c]
0x080484c5 <+89>:   mov    DWORD PTR [esp+0x1c],0xffffffff
0x080484cd <+97>:   mov    edx,eax
```

```
[-----registers-----]
EAX: 0x804b008 ("FLAG-4092")
EBX: 0xf7fab000 --> 0x1a8da8
ECX: 0x18
EDX: 0x804b020 --> 0x0
ESI: 0x0
EDI: 0x0
EBP: 0xffffd238 --> 0x0
ESP: 0xffffd200 --> 0x804b008 ("FLAG-4092")
EIP: 0x80484c1 (<main+85>:      mov     eax,DWORD PTR [esp+0x2c])
EFLAGS: 0x212 (carry parity ADJUST zero sign trap INTERRUPT direction overflow)
```

```
[-----code-----]
0x80484ae <main+66>: mov     DWORD PTR [eax],0x47414c46
0x80484b4 <main+72>: mov     DWORD PTR [eax+0x4],0x3930342d
0x80484bb <main+79>: mov     WORD PTR [eax+0x8],0x32
=> 0x80484c1 <main+85>: mov     eax,DWORD PTR [esp+0x2c]
0x80484c5 <main+89>: mov     DWORD PTR [esp+0x1c],0xffffffff
0x80484cd <main+97>: mov     edx,eax
0x80484cf <main+99>: mov     eax,0x0
0x80484d4 <main+104>: mov     ecx,DWORD PTR [esp+0x1c]
```

```
[-----stack-----]
0000 | 0xffffd200 --> 0x804b008 ("FLAG-4092")
0004 | 0xffffd204 --> 0x0
0008 | 0xffffd208 --> 0x18
0012 | 0xffffd20c --> 0x80485b2 (<__libc_csu_init+82>:  add     esi,0x1)
0016 | 0xffffd210 --> 0x1
0020 | 0xffffd214 --> 0xffffd2d4 --> 0xffffd448 ("/home/ppp/Downloads/crackme1")
0024 | 0xffffd218 --> 0xffffd2dc --> 0xffffd465 ("XDG_VTNR=7")
0028 | 0xffffd21c --> 0xf7e333fd (<__cxa_atexit+29>:  test   eax,eax)
```

```
[-----]
Legend: code, data, rodata, value
0x080484c1 in main ()
gdb-peda$
```

# Difficultés, attitude et approche

---

Difficile :

- Multidisciplinaire
- Au delà des programmes universitaires
- Volontairement difficile et étrange

Échouer pour mieux apprendre (“On apprend pas sans saigner un peu”)

La culture CTF...

# CTF - Préparation

---

[Trail of Bits CTF Field Guide](#)

[github.com/ctfs](https://github.com/ctfs)

L'algorithme du hacker :

```
while not understand do learn
```

Montréhack

Wargames ([Enigma Group](#), [RingZero](#), [Exploit-Exercises](#), [Over The Wire](#))

[CTFs](#) → [Write-ups](#) ([CTF Time](#), [ctfs/write-ups](#))



# Ressources Générales

---

`[$ man git-gud]`



# #Slack

---

Slack.com → Domaine [ageei-uqam@slack.com](mailto:ageei-uqam@slack.com)

#securite

#ringzer0

#compe-pratiques

#programmation

#annonces