Cyber FizzBuzz: réflexion sur la sélection de candidats dans le domaine de la SSI

Éric Jaeger Olivier Levillain Christian Lixi

Mercredi 23 mai 2018

Qui suis-je ?

Olivier Levillain

Qui suis-je ?

Olivier Levillain

- @pictyeye sur Twitter
- `https://paperstreet.picty.org/yeye`

Qui suis-je ?

Olivier Levillain

- @pictyeye sur Twitter
- `https://paperstreet.picty.org/yeye`

Parcours

- stage de DEA en cryptographie sur une fonction de hachage
- membre du laboratoire « système » de l'ANSSI (2007-2012)
- responsable du laboratoire « réseau » de l'ANSSI (2012-2015)
- responsable du CFSSI, centre de formation de l'ANSSI (2015-)

Présentation rapide de l'ANSSI

- L'agence nationale de la sécurité des systèmes d'information, créée en 2009 pour remplacer la DCSSI
- Son objectif est la prévention et la réaction dans le domaine de la sécurité du numérique
- L'ANSSI est rattachée au SGDSN, qui dépend du Premier Ministre
- Effectifs : environ 500 personnes aujourd'hui

Le CFSSI (1/2)

Un centre de formation pour l'administration

- activité principale : dispenser à Paris des cours aux fonctionnaires et aux militaires français
- aucun formateur en propre
- les cours sont intégralement dispensés par des vacataires (appartenant à 80 % à l'ANSSI)

Le CFSSI (1/2)

Un centre de formation pour l'administration

- activité principale : dispenser à Paris des cours aux fonctionnaires et aux militaires français
- aucun formateur en propre
- les cours sont intégralement dispensés par des vacataires (appartenant à 80 % à l'ANSSI)

Catalogue de formations

- une vingtaine de stages « courts » (1800 pers./an)
  - 1 : panorama de la SSI (1 jour)
  - 8a : organisation des audits (2 jours)
  - 10 : cryptologie (20 jours)
  - 14 : traitement d'incidents (4 jours)
- une formation longue menant au titre ESSI (10 pers./an)
  - une vision technique et large de la sécurité
  - la curiosité et la rigueur comme principes
  - la capacité à conseiller et convaincre comme objectif

Le CFSSI (2/2)

Depuis 2013, lancement de nouvelles activités

2013 : CyberEdu
Intégration de la sécurité dans les formations en informatique

2015 : SecNum*edu*
Labellisation des formations de spécialistes

2015 : SecNum*académie*
Modules de sensibilisation en ligne à la sécurité du numérique
60 000 inscrits, 2 000 attestations

Le CFSSI (2/2)

Depuis 2013, lancement de nouvelles activités

2013 : CyberEdu — Présenté à RESSI 2015

Intégration de la sécurité dans les formations en informatique

2015 : SecNum*edu* — Présenté à RESSI 2017

Labellisation des formations de spécialistes

2015 : SecNum*académie* — Présenté à RESSI 2017

Modules de sensibilisation en ligne à la sécurité du numérique

60 000 inscrits, 2 000 attestations

Motivation

Pourquoi *FizzBuzz* ?

Un jeu d'enfant... et un test de recrutement pour les développeurs utilisé par *Jeff Atwood*

> *Write a program that prints the numbers from 1 to 100. But for multiples of three print "Fizz" instead of the number and for the multiples of five print "Buzz". For numbers which are multiples of both three and five print "FizzBuzz".*

Pourquoi *FizzBuzz* ?

Un jeu d'enfant... et un test de recrutement pour les développeurs utilisé par *Jeff Atwood*

> *Write a program that prints the numbers from 1 to 100. But for multiples of three print "Fizz" instead of the number and for the multiples of five print "Buzz". For numbers which are multiples of both three and five print "FizzBuzz".*

En plus il paraît que c'est aussi un jeu à boire !

Et pourquoi un *Cyber* Fizzbuzz ?

Plusieurs années d'expérience de recrutements

- Laboratoires de l'ANSSI
- Formation ≪ Expert en SSI ≫ du CFSSI

Mise au point progressive de questions non sur les connaissances mais révélatrices d'un état d'esprit, d'une aptitude

Et pourquoi un *Cyber* Fizzbuzz ?

Plusieurs années d'expérience de recrutements

- Laboratoires de l'ANSSI
- Formation ≪ Expert en SSI ≫ du CFSSI

Mise au point progressive de questions non sur les connaissances mais révélatrices d'un état d'esprit, d'une aptitude

Un outil pour des entretiens efficaces

- sans documentation
- sans ordinateur ni calculatrice
- sans appel à un ami

et des réponses parfois surprenantes

Admission à la formation ESSI

ESSI : un cursus de 13 mois qui mène à un titre RNCP I

- vision technique et large de la sécurité
- développement de la curiosité
- école de la rigueur
- capacité à convaincre

Admission à la formation ESSI

ESSI : un cursus de 13 mois qui mène à un titre RNCP I

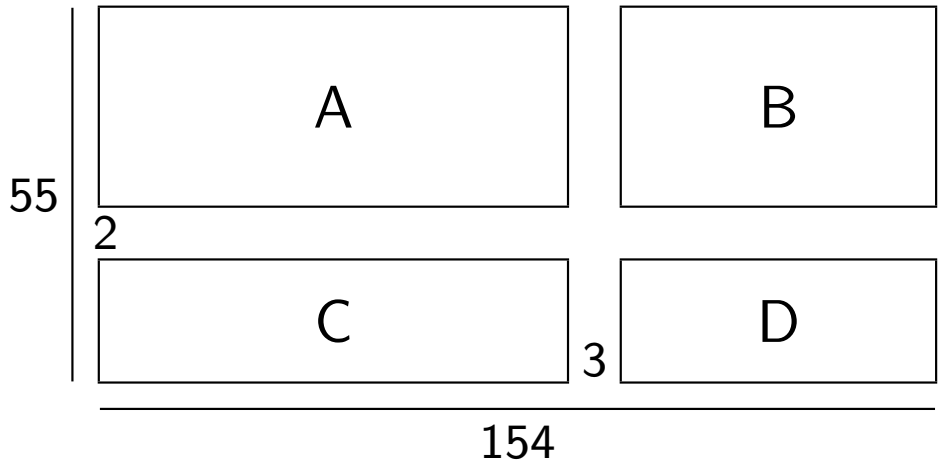
- vision technique et large de la sécurité
- développement de la curiosité
- école de la rigueur
- capacité à convaincre

Entretien (2-3 heures)

- analyse du parcours
- discussion autour du questionnaire
- évaluation de la motivation

Exemples de questions

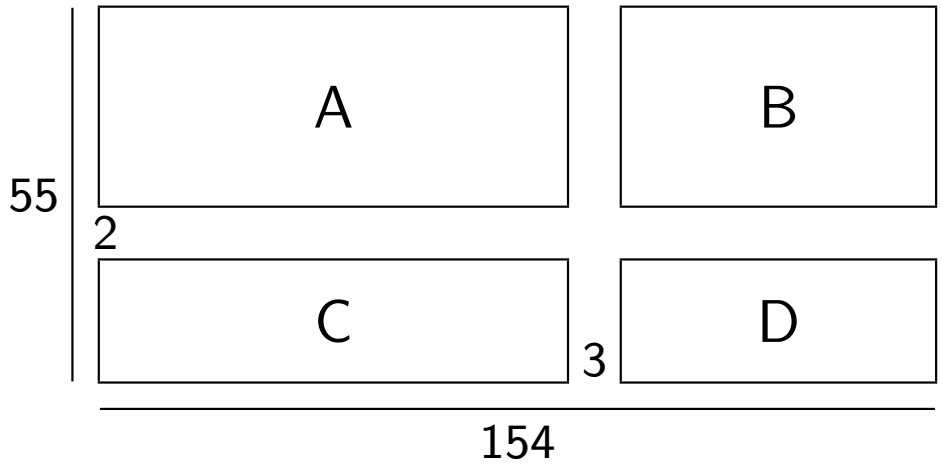
Ce ne sont pas des questions de calcul (1/2)



Pour fleurir les parcelles A (de 21 m par 85 m), B, C et D de ce jardin, à raison de 17 bulbes par m^2, il faut :

- ☐ 134147 bulbes
- ☐ 136051 bulbes
- ☐ 138323 bulbes

Ce ne sont pas des questions de calcul (1/2)



Pour fleurir les parcelles A (de 21 m par 85 m), B, C et D de ce jardin, à raison de 17 bulbes par m^2, il faut :

- ☐ 134147 bulbes
- ☐ 136051 bulbes
- ☐ 138323 bulbes

Un indice, chez vous : il suffit de regarder les unités

Ce ne sont pas des questions de calcul (2/2)

Que pouvez-vous dire du nombre en hexadécimal `0x13260` ?

- ☐ C'est un nombre pair
- ☐ C'est un multiple de 3
- ☐ C'est un multiple de 10
- ☐ C'est un multiple de 16

Ce ne sont pas des questions de calcul (2/2)

Que pouvez-vous dire du nombre en hexadécimal `0x13260` ?

- ☐ C'est un nombre pair
- ☐ C'est un multiple de 3
- ☐ C'est un multiple de 10
- ☐ C'est un multiple de 16

Indices

- pour 2 et 16, le résultat est relativement immédiat
- pour 3, ça rappelle une règle connue, mais s'applique-t-elle ?

- et pour 10, pourquoi ne pas définir une règle similaire ?

Ce ne sont pas des questions de calcul (2/2)

Que pouvez-vous dire du nombre en hexadécimal `0x13260` ?

- ☐ C'est un nombre pair
- ☐ C'est un multiple de 3
- ☐ C'est un multiple de 10
- ☐ C'est un multiple de 16

Indices

- pour 2 et 16, le résultat est relativement immédiat
- pour 3, ça rappelle une règle connue, mais s'applique-t-elle ?
  - 16, comme 10 est congru à 1 modulo 3
- et pour 10, pourquoi ne pas définir une règle similaire ?
  - 16^n est congru à 6 modulo 10 (pour $n \geq 1$)

Enseignements

- L'objectif n'est pas le résultat...
- ... mais la manière d'y arriver
- ... et la manière de l'expliquer

- Intérêt des questions à plusieurs niveaux

Ce ne sont pas des questions sur l'encodage binaire

La représentation des nombres en virgule flottante. . .

- permet de représenter n'importe quel réel
- est de taille fixe
- contient une indication de la position de la virgule

Ce ne sont pas des questions sur l'encodage binaire

La représentation des nombres en virgule flottante. . .

- permet de représenter n'importe quel réel
- est de taille fixe
- contient une indication de la position de la virgule

Il est toujours intéressant d'avoir un candidat répondant vrai aux deux premières lignes

Enseignements

- L'objectif n'est pas le résultat...
- ... mais de s'assurer que le candidat sait raisonner
- ... d'une manière cohérente

Ce ne sont pas des questions de cryptographie (1/2)

Un certificat électronique. . .

- ☐ doit rester secret pour jouer son rôle
- ☐ permet l'authentification
- ☐ contient la clé utilisée pour déchiffrer les communications
- ☐ peut contenir une clé publique ECDSA

Ce ne sont pas des questions de cryptographie (1/2)

Un certificat électronique. . .

- ☐ doit rester secret pour jouer son rôle
- ☐ permet l'authentification
- ☐ contient la clé utilisée pour déchiffrer les communications
- ☐ peut contenir une clé publique ECDSA

Ma question préférée...

- ... pour tester la rigueur dans le discours du candidat
- ... pour vérifier la compréhension des concepts (sans magie)
- ... pour demander une définition des certificats

Ce ne sont pas des questions de cryptographie (1/2)

Un certificat électronique. . .

- ☐ doit rester secret pour jouer son rôle
- ☐ permet l'authentification
- ☐ contient la clé utilisée pour déchiffrer les communications
- ☐ peut contenir une clé publique ECDSA

Ma question préférée...

- ... pour tester la rigueur dans le discours du candidat
- ... pour vérifier la compréhension des concepts (sans magie)
- ... pour demander une définition des certificats
- intérêt de la deuxième affirmation pour la discussion
- c'est une question à tiroirs (auto-signés, IGC...)

Ce ne sont pas des questions de cryptographie (2/2)

Une fonction de chiffrement E prend en entrée une clé et un message clair, et retourne un chiffré ; E doit être :

- ☐ injective
- ☐ surjective
- ☐ déterministe

Ce ne sont pas des questions de cryptographie (2/2)

Une fonction de chiffrement E prend en entrée une clé et un message clair, et retourne un chiffré ; E doit être :

- ☐ injective
- ☐ surjective
- ☐ déterministe

Ici, on teste la compréhension *réelle* de notions vu comme abstraites

Ce ne sont pas des questions sur le *shell* (1/2)

Quelles commandes peuvent mener (sans redirection) à une perte de données ?

- ☐ `ls`
- ☐ `rm`
- ☐ `mv`
- ☐ `cat`
- ☐ `cp`

Ce ne sont pas des questions sur le *shell* (1/2)

Quelles commandes peuvent mener (sans redirection) à une perte de données ?

☐ `ls` ☐ `rm` ☐ `mv` ☐ `cat` ☐ `cp`

Souvent, cette question est mal interprétée :

- au lien de répondre à « quelles commandes peuvent... »
- les candidats répondent à « quelles commandes ont pour but de... »

Cette erreur d'interprétation est un véritable problème de sécurité !

Ce ne sont pas des questions sur le *shell* (2/2)

Un utilisateur tape la ligne « `cat * ` » dans un *shell*. Le répertoire courant peut contenir...

- ... un fichier "`*`" dont le contenu sera affiché
- ... un fichier "`-v`" dont le contenu sera affiché
- ... un fichier "`; rm *`" et les fichiers du répertoire seront effacés

Ce ne sont pas des questions sur le *shell* (2/2)

Un utilisateur tape la ligne « `cat * ` » dans un *shell*. Le répertoire courant peut contenir...

- ... un fichier "`*`" dont le contenu sera affiché
- ... un fichier "`-v`" dont le contenu sera affiché
- ... un fichier "`; rm *`" et les fichiers du répertoire seront effacés

Où tout est question d'interprétation

- par le *shell* ?
- par la commande `cat` ?

Ce ne sont pas des questions sur le *shell* (2/2)

Un utilisateur tape la ligne « `cat * ` » dans un *shell*. Le répertoire courant peut contenir...

- ... un fichier "`*`" dont le contenu sera affiché
- ... un fichier "`-v`" dont le contenu sera affiché
- ... un fichier "`; rm *`" et les fichiers du répertoire seront effacés

Où tout est question d'interprétation

- par le *shell* ?
- par la commande `cat` ?

Variantes classiques à proposer en TP

- comment créer un fichier `*` avec `touch` ?
- comment supprimer un fichier appelé `-rf` ?

Ce ne sont pas des questions sur la programmation (1/2)

```
void main(void) {
   int x=3; int y=4;
   float z=x/y;
   printf("%f\n",z);
}
```

Quelle est la valeur affichée ?

- ☐ le programme ne compile pas
- ☐ il provoque une erreur
- ☐ 0
- ☐ 0.000000
- ☐ 0.750000

Ce ne sont pas des questions sur la programmation (1/2)

```
void main(void) {
   int x=3; int y=4;
   float z=x/y;
   printf("%f\n",z);
}
```

Quelle est la valeur affichée ?

- ☐ le programme ne compile pas
- ☐ il provoque une erreur
- ☐ 0
- ☐ 0.000000
- ☐ 0.750000

Ici encore, c'est le cheminement de pensée qui est intéressant

- que signifient les objets manipulés ?
- que veut dire / ?
- qu'est-ce qui relève de la compilation et de l'exécution ?

Ce ne sont pas des questions sur la programmation (1/2)

```
void main(void) {
   int x=3; int y=4;
   float z=x/y;
   printf("%f\n",z);
}
```

Quelle est la valeur affichée ?

- ☐ le programme ne compile pas
- ☐ il provoque une erreur
- ☐ 0
- ☐ 0.000000
- ☐ 0.750000

Ici encore, c'est le cheminement de pensée qui est intéressant

- que signifient les objets manipulés ?
- que veut dire / ?
- qu'est-ce qui relève de la compilation et de l'exécution ?

Interlude : transposez cet exemple en OCaml ou en Python (2 ou 3)

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Plusieurs niveaux de compréhension de l'exercice

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Plusieurs niveaux de compréhension de l'exercice

- exécution étape-par-étape

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Plusieurs niveaux de compréhension de l'exercice

- exécution étape-par-étape
- identification de la factorielle

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Plusieurs niveaux de compréhension de l'exercice

- exécution étape-par-étape
- identification de la factorielle
- prise en compte du principe de réalité : 40! est un gros nombre

Ce ne sont pas des questions sur la programmation (2/2)

```
int f(int x) {
    if (x==0 || x==1) return 1;
    return x * f(x-1);
}
```

- Que vaut `f(5)` ?
- Que calcule `f` ?
- Que retourne `f(40)` ?

Plusieurs niveaux de compréhension de l'exercice

- exécution étape-par-étape
- identification de la factorielle
- prise en compte du principe de réalité : 40! est un gros nombre
- compréhension de l'arithmétique modulo

Ce sont des questions de sécurité. . .

Avez-vous déjà constaté/eu à traiter un incident de sécurité ?

Ce sont des questions de sécurité. . .

Avez-vous déjà constaté/eu à traiter un incident de sécurité ?

Que retenez-vous des révélations d'*Edward Snowden* ?

Ce sont des questions de sécurité. . .

Avez-vous déjà constaté/eu à traiter un incident de sécurité ?

Que retenez-vous des révélations d'*Edward Snowden* ?

Quelle actualité SSI a récemment retenu votre attention ?

Éléments complémentaires sur la formation

Impact sur le taux d'échec

- élevé lors du passage de la formation de 2 ans à 13 mois
- maîtrisé grâce à l'entretien

Le questionnaire est représentatif de l'esprit de la formation

- inciter à la rigueur
- favoriser la curiosité
- développer l'autonomie
- certains exemples sont d'ailleurs discutés pendant la scolarité

Merci pour votre attention

Questions ?

Qx *Parmi les trois propositions suivantes, lesquelles sont vraies ?*

Tout multiple de 4 est un multiple de 2	Ⓥ ×
Tout multiple de 3 est un multiple de 6	∨ ⊗
Une seule des 3 propositions de cette question est vraie	∨ ×

olivier.levillain@ssi.gouv.fr

Planches disponibles sur `https://paperstreet.picty.org/yeye`