ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE – LAUSANNE
POLITECNICO FEDERALE – LOSANNA
SWISS FEDERAL INSTITUTE OF TECHNOLOGY – LAUSANNE

Faculté Informatique et Communications
Cours d'Information, Calcul et Communication, sections MA et PH
Chappelier J.-C.

NOM : Hanon Ymous
(000000)
Place : 0

#0000

Information, Calcul et Communication (SMA/SPH) : Examen final

21 décembre 2023

SUJET 1

INSTRUCTIONS (à lire attentivement)

IMPORTANT ! Veuillez suivre les instructions suivantes à la lettre sous peine de voir votre examen annulé dans le cas contraire.

1. Vous disposez de deux heures quarante-cinq minutes pour faire cet examen (8h15 – 11h00).
2. Vous devez **écrire à l'encre noire ou bleu foncée**, pas de crayon ni d'autre couleur.

   N'utilisez **pas non plus de stylo effaçable** (perte de l'information à la chaleur).
3. Vous avez droit à toute documentation papier.

   En revanche, vous ne pouvez pas utiliser d'ordinateur personnel, ni de téléphone portable, ni aucun autre matériel électronique.
4. Répondez aux questions directement sur la donnée, **MAIS** ne mélangez pas les réponses de différentes questions !

   Ne joignez aucune feuilles supplémentaires ; **seul ce document sera corrigé**.
5. Lisez attentivement et *complètement* les questions de façon à ne faire que ce qui vous est demandé. Si l'énoncé ne vous paraît pas clair, ou si vous avez un doute, demandez des précisions à l'un des assistants.
6. L'examen comporte 7 exercices indépendants sur 16 pages, qui peuvent être traités dans n'importe quel ordre, mais qui ne rapportent pas la même chose (les points sont indiqués, le total est de 120 points).

   Tous les exercices comptent pour la note finale.

$x \cdot d = 1$

$y \cdot d = 1$

$(x-y) \cdot d = 0$

RSA p q

$\rightarrow n = p \cdot q$

$d \rightarrow e \cdot d = 1 \mod \underbrace{(p-1)(q-1)}_{m}$

m

$\varphi(n)$

$\downarrow$

public (e, n)

Ça marche pq :

$M^{ed} = M \mod n$

$M^x \mod n$ le n du x

$x = e$ de l'autre (confid.)

$x = d$ de nous (respon. ; intégrité)

A

public : e_A n_A

B

e_B n_B

envoie →

$M' = M^{e_B} \bmod n_B$: que B décode : $M'^{d_B} \bmod n_B$

A veut signer :

$M'' = M^{d_A} \bmod n_A$

B vérifie

$M''^{e_A} \bmod n_A$

Question 1 – Diverses questions [14.5 points]

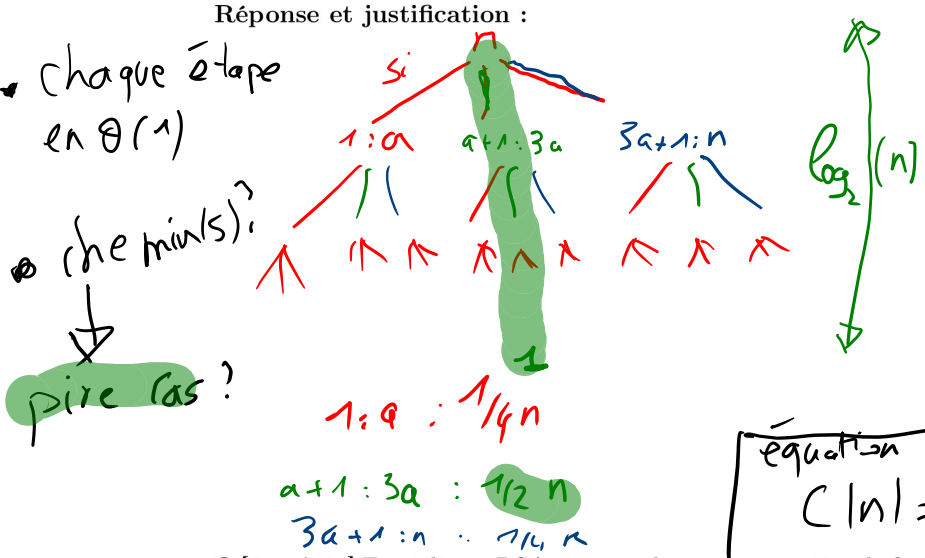
① **[4 points]** En supposant que **taille()** est en $\Theta(1)$, quelle est la complexité de l'algorithme ci-contre, où $\lfloor x \rfloor$ représente la partie entière inférieure de x et $L[i:j]$ représente la sous-liste $(L(i), ..., L(j))$ si $i \leq j$ ou la liste vide si $i > j$?

Justifiez votre réponse.

algo1
entrée : *une liste L non vide*
sortie : *? ?*

```
n ⟵ taille(L)
Si n = 1
    Sortir : (L(1))²
a ⟵ ⌊n/4⌋
Si a = 0
    a ⟵ 1
Si L(1) ≥ L(a)
    b ⟵ algo1(L[1 : a])
Sinon, si L(1) ≥ L(3a)
    b ⟵ algo1(L[a + 1 : 3a])
Sinon
    b ⟵ algo1(L[3a + 1 : n])
Sortir : b²
```

Réponse et justification :



② **[3 points]** En utilisant RSA, vous souhaitez transmettre de façon confidentielle une information que vous envoyez à un ami dont la clé publique est $(53, 183)$ et dont la clé privée est 77. Votre clé publique est $(97, 201)$ et votre clé privée est 49.

Votre ami reçoit `10001110` (en binaire). Quelle est la valeur déchiffrée par votre ami ?
Exprimez votre réponse sous la forme « $x^y \mod z$ » (x, y et z en décimal) et **justifiez** pleinement votre réponse.

Réponse et justification :

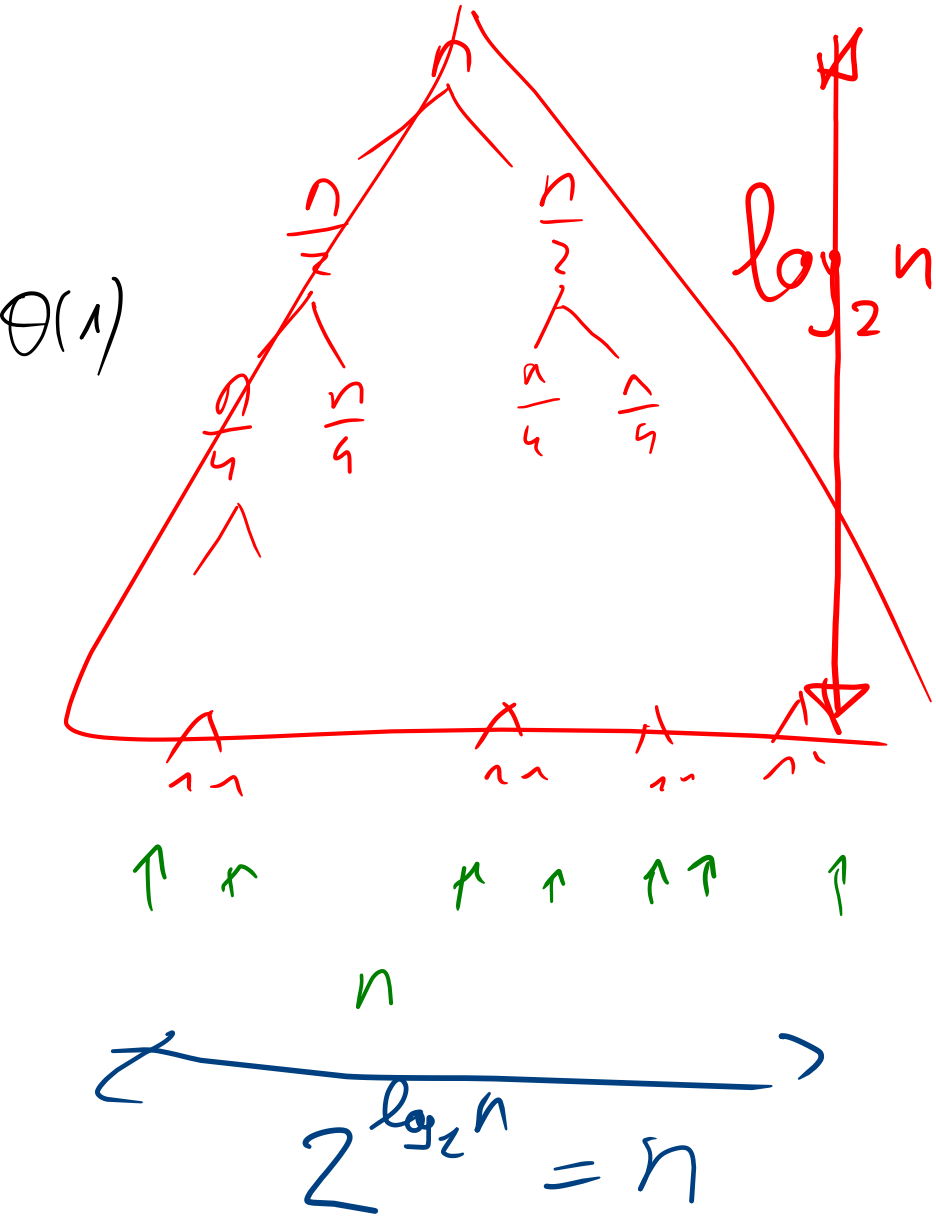
Ne pas écrire dans cette zone.

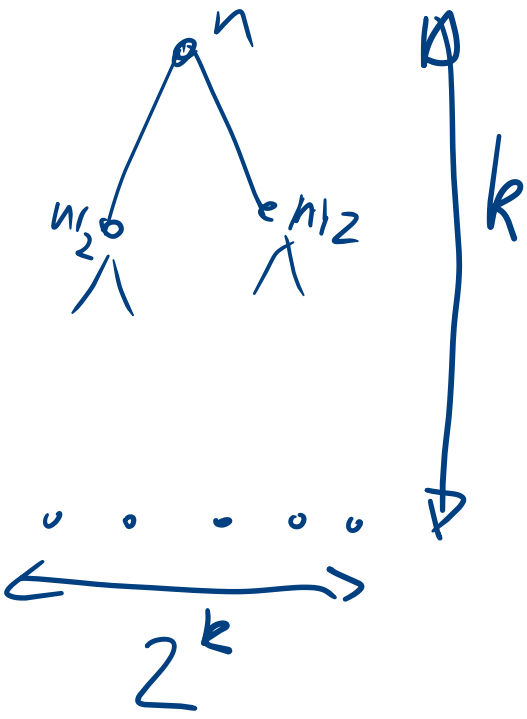
2022 Q 1.6

$a \leftarrow \lfloor \frac{n}{3} \rfloor$

algo(L[1:a])

algo(L[a+1:n])





noeuds ?

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$$

③ **[5 points]** Qu'affiche l'extrait de code ci-dessous ? Si nécessaire, mettez « `???` » pour toute valeur inconnue ou « `Segmentation fault` » si vous pensez que le programme plante (à cet endroit).

Justifiez vos réponses (vous pouvez aussi annoter le code).

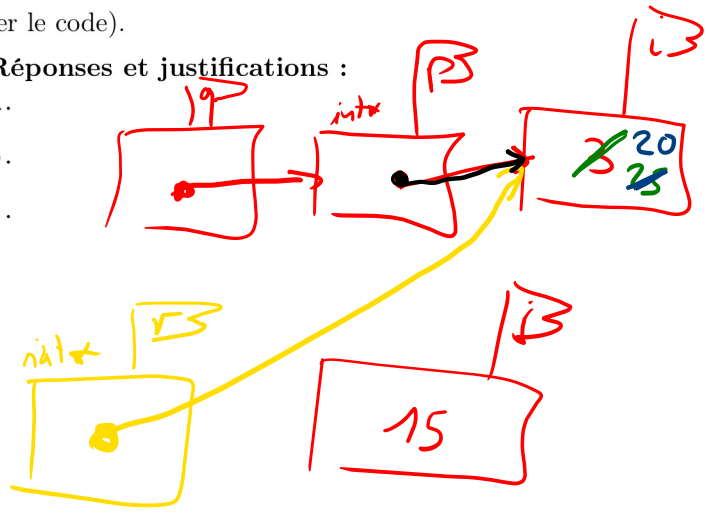
```
int i(3);
int* p(&i);
int** q(&p);

**q = 25;
p = &i;

int j(i - 10);

cout << "a. " << *p << endl;
cout << "b. " << j << endl;

i = *p;

int* r(*q);

i = i - *r + 20;
*q = &i;
cout << "c. " << *r - **q << endl;
```

Réponses et justifications :

a.

b.

c.



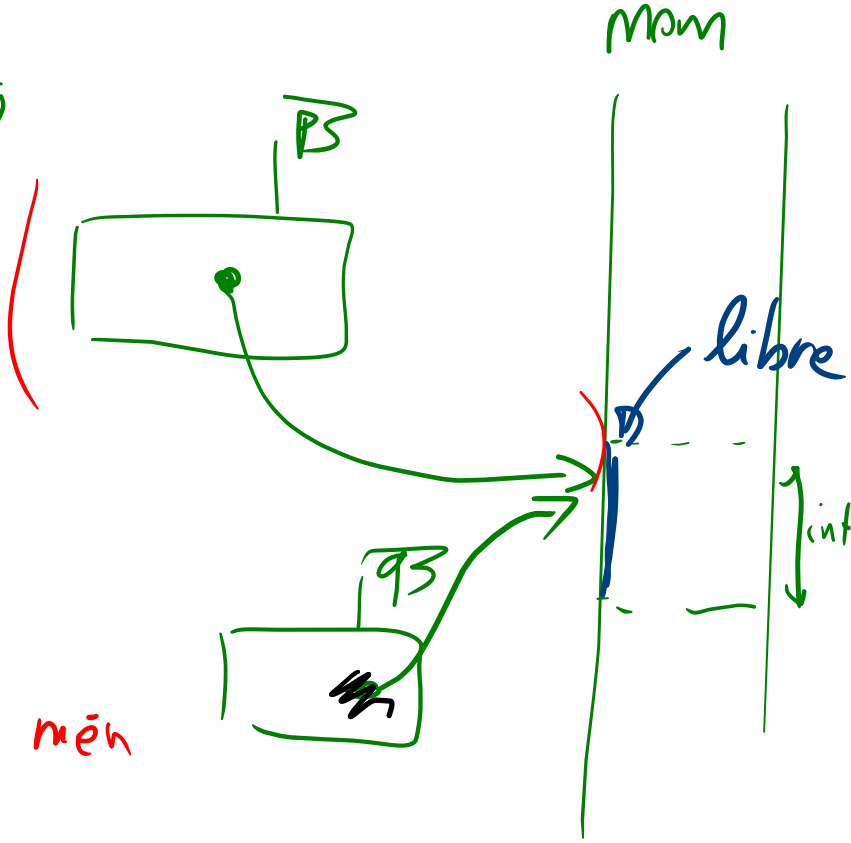
Ne pas écrire dans cette zone.

④ **[2.5 points]** Si un nombre décimal q s'écrit `0.0001` en binaire à virgule fixe, comment s'écrit $\log_2(q)$ en binaire entier signé sur 6 bits ? **Justifiez** votre réponse.

Réponse et justification :

suite au dos ☞

```
int * p = new int;
   :
   :
   q = p
   :
   :
delete q;
q = nullptr;
```



libère mém

Question 6 – Bon voyage ! [29 points]

Note : (comme toujours, mais particulièrement ici) nous vous conseillons, afin de faire les bons choix, de lire *entièrement* cette question avant de commencer.

On s'intéresse ici à écrire des *parties* d'un programme C++ permettant de représenter un réseau de transport. Le réseau que nous souhaitons représenter est un ensemble de gares, dont certaines sont reliées par des liaisons ayant une durée (en minutes) et un prix (en francs).
Chaque gare aura un nom et l'ensemble de ses destinations (c.-à-d. des liaisons : durée, prix, et indication de la gare d'arrivée).

① **[4 points]** Définissez les types de données que vous jugez nécessaires pour représenter le problème spécifié ci-dessus.

Réponse :

```
struct Gare;
struct liaison
{ unsigned int durée;
  double prix;
  [String gare;]
};
ou
{ const Gare * gare;
  Gare& gare;
```

```
struct Gare
{ string nom;
  Vector<liaison> dest;
};
```

```
typedef Vector<Gare> reseau;
```

② **[4 points]** Écrivez le code C++ permettant de représenter le réseau simple constitué de deux gares, Lausanne et Renens, tel que la liaison Lausanne–Renens prend 6 minutes et coûte 2.45 francs, et la liaison Renens–Lausanne prend 7 minutes et coûte 2.20 francs.

Réponse :

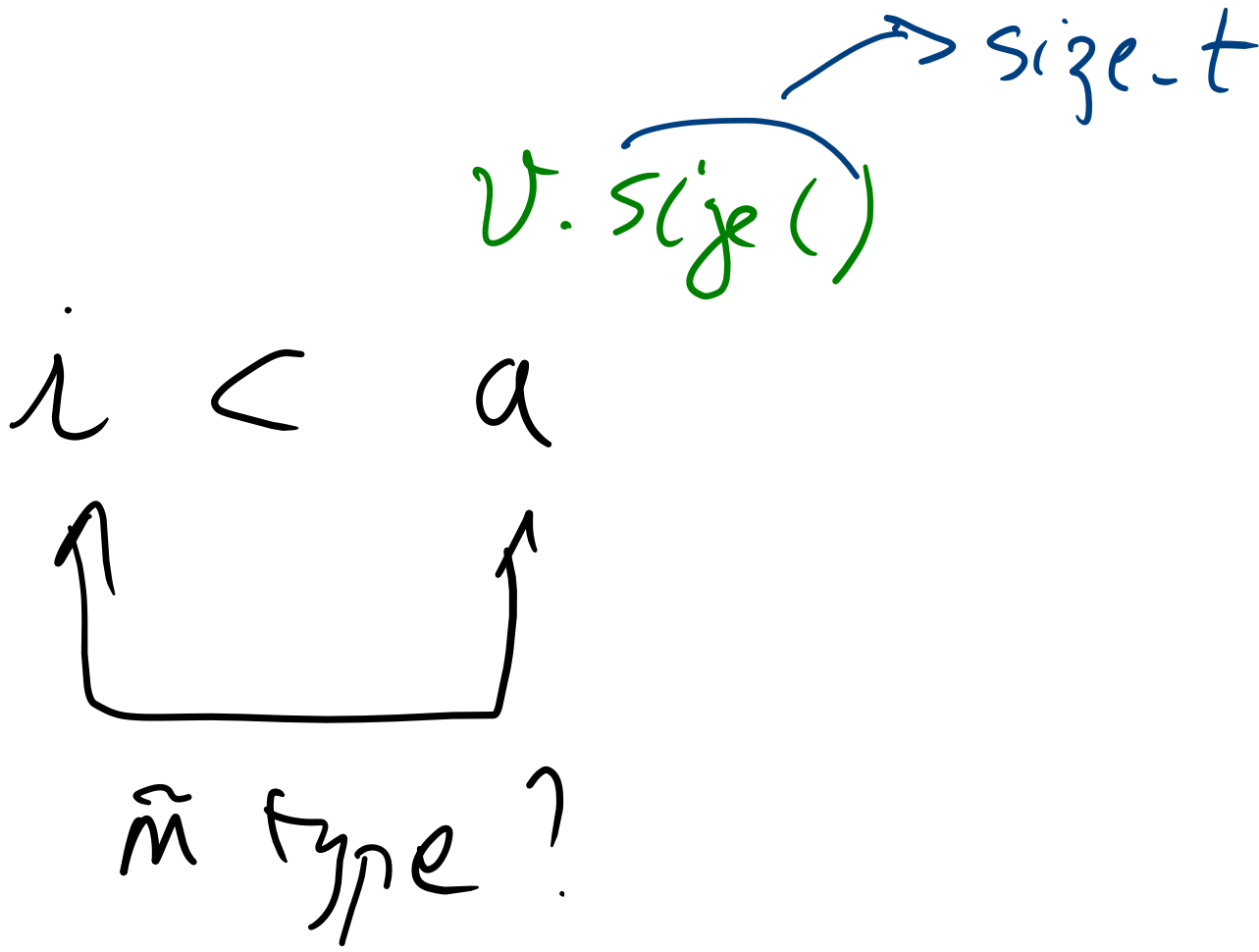
```
size_t index_gare;
```

liaison
- durée
- prix
- gare arrivée

gare :
- nom
- {destinations}

destination :
liaison

Ne pas écrire dans cette zone.


size_t
v.size()
i < a
mismatch type?

③ **[5 points]** Écrivez une fonction `prix()` qui permet de tester si un ensemble de liaisons contient une gare donnée. Cette fonction retournera un booléen indiquant si l'ensemble de liaisons contient la gare fournie et, si oui, le prix de cette liaison (sinon un prix quelconque).
Vous êtes libre de choisir les arguments qui vous conviennent le mieux pour cette fonction.

Réponse :

④ **[1 point]** Définissez un type `Trajet` qui permet de représenter un trajet dans le réseau, c.-à-d. un ensemble de gares à parcourir. Vous êtes libre de choisir la représentation qui vous convient le mieux.

Réponse :

⑤ **[10 points]** Écrivez une fonction `prix()` qui permet de calculer le prix total d'un trajet donné. Cette fonction retournera un booléen indiquant si le trajet est valide ou non et son prix total (si c'est le cas, sinon une valeur quelconque).

Pour être considéré comme valide, un trajet doit contenir un ensemble de gares tel que chaque gare est contenue dans l'ensemble des destinations de la gare qui la précède dans le trajet.

Vous êtes libre de choisir les arguments qui vous conviennent le mieux pour cette fonction.

Réponse :

suite au dos ☞

⑥ **[5 points]** Pour pouvoir appliquer des algorithmes de plus court chemin (sur les durées), il est nécessaire de produire une matrice représentant les durées entre chacune des gares du réseau :

- à la position (i,j) de la matrice sera stockée la durée de la liaison de la i-ème gare à la j-ème gare ;
- si les deux gares ne sont pas connectées, on mettra `numeric_limits<X>::max()`, où `X` est le type que vous avez choisi pour les durées ;
- et on mettra 0 sur la diagonale.

Par exemple, si Lausanne est la première gare et Renens la seconde dans l'exemple donné en sous-question ②, la matrice à produire serait

$$\begin{pmatrix} 0 & 6 \\ 7 & 0 \end{pmatrix}$$

Écrivez une fonction `connexions()` qui prend en paramètre un réseau et qui retourne la matrice correspondante, telle que définie ci-dessus.

Réponse :

Ne pas écrire dans cette zone.