

Rapport

# PROJET KEYSHARE - SOUTENANCE FINALE

Le 15 avril 2021

HERVAULT Jules, Intégrateur  
[jules.hervault@ecole.ensicaen.fr](mailto:jules.hervault@ecole.ensicaen.fr)  
LAMHAMDI Mehdi, Développeur  
[mehdi.lamhamdi@ecole.ensicaen.fr](mailto:mehdi.lamhamdi@ecole.ensicaen.fr)  
PEIGNE Steven, Développeur  
[steven.peigne@ecole.ensicaen.fr](mailto:steven.peigne@ecole.ensicaen.fr)

Client : Sébastien FOUREY  
[Sebastien.Fourey@unicaen.fr](mailto:Sebastien.Fourey@unicaen.fr)



# TABLE DES MATIERES

---

<b>LE PROJET</b>	<b>3</b>
1. Contexte	3
2. Présentation de notre solution	3
2.1. La bibliothèque	4
2.2. L'interface en ligne de commandes	5
2.3. L'interface graphique	6
3. Objectifs	7
3.1. Changements	7
<b>GESTION DE PROJET</b>	<b>8</b>
1. Méthodologie	8
2. Outils	8
<b>SITUATION ACTUELLE</b>	<b>9</b>
1. Objectifs et travail réalisé	9
2. Obstacles rencontrés	9
3. Objectifs non atteints	10
4. Suite du projet	10
<b>BILAN</b>	<b>11</b>
1. Ce qui a fonctionné	11
2. Ce qui n'a pas fonctionné	11
3. Les bénéfices du projet 2A	11

# TABLE DES FIGURES

---

Figure 1 Diagramme de séquence du logiciel KeyShare	4
Figure 2 Capture d'écran d'un terminal pour la réception du transfert avec le code 123	5
Figure 3 Capture d'écran d'un terminal pour l'envoi du fichier README.md avec le code 123	5
Figure 4 Capture d'écran fenêtre recevoir	6
Figure 5 Capture d'écran fenêtre envoyer	6
Figure 6 Capture fenêtre recevoir avec langue française	6
Figure 7 Diagramme de GANTT créé pour le kick-off	7

# LE PROJET

---

*Cette partie a pour vocation de rappeler le contexte du projet et de faire une présentation générale du produit.*

## 1. Contexte

L'échange de données est très répandu à travers le monde. On trouve ces données sous plusieurs formes : audios, vidéos, images, etc. Ainsi, de nombreux outils, comme les drives ou les serveurs distants, ont été mis en œuvre pour le partage de ces données entre plusieurs personnes. Cependant, n'existerait-il pas un outil spécialisé dans le partage local ?

On entend par partage local le partage à une personne qui est physiquement à proximité, par exemple dans le même bâtiment. Si on utilise un des outils précédemment cités, on envoie nos données à des dizaines, des centaines voire des milliers de kilomètres pour leur faire parcourir le chemin inverse. Cela est à la fois gourmand en énergie, en temps et en efficacité. Cet échange imparfait met en cause notre responsabilité sociétale et environnementale.

Cette dernière émerge depuis quelques années dans le monde de l'informatique. Pour cause, l'informatique s'étend dans de plus en plus de domaines pour permettre des avancées technologiques plus rapides. Cependant, il ne faut pas avancer au détriment de la société ou de l'environnement. Un exemple concret, mettant en avant la responsabilité sociétale, est la mise en place de l'open source qui d'ailleurs s'étend déjà au-delà de l'informatique.

## 2. Présentation de notre solution

Le projet a été nommé partage sur réseau local façon KISS par le client. L'équipe projet nomme la solution Keyshare. L'acronyme KISS signifie Keep It Simple, Stupid (*reste simple, idiot* en français).

Le produit réalisé est un logiciel qui permet le partage de fichiers entre deux ordinateurs sur un même réseau local tel que celui du bâtiment E de l'école d'ingénieur Ensicaen. L'acronyme KISS fait quant à lui référence à la simplicité d'utilisation du logiciel. Ce logiciel est destiné à n'importe quel utilisateur, peu importe ses connaissances en informatique.

Pour l'équipe projet, des compétences de programmation réseau sont donc mises en jeu mais aussi des compétences dans la conception d'interfaces graphiques.

## 2.1. La bibliothèque

Le principe de notre solution est un échange codifié entre deux acteurs sur deux machines distinctes. Nous expliquons avec détail grâce au diagramme de séquence ci-dessous son fonctionnement actuel :

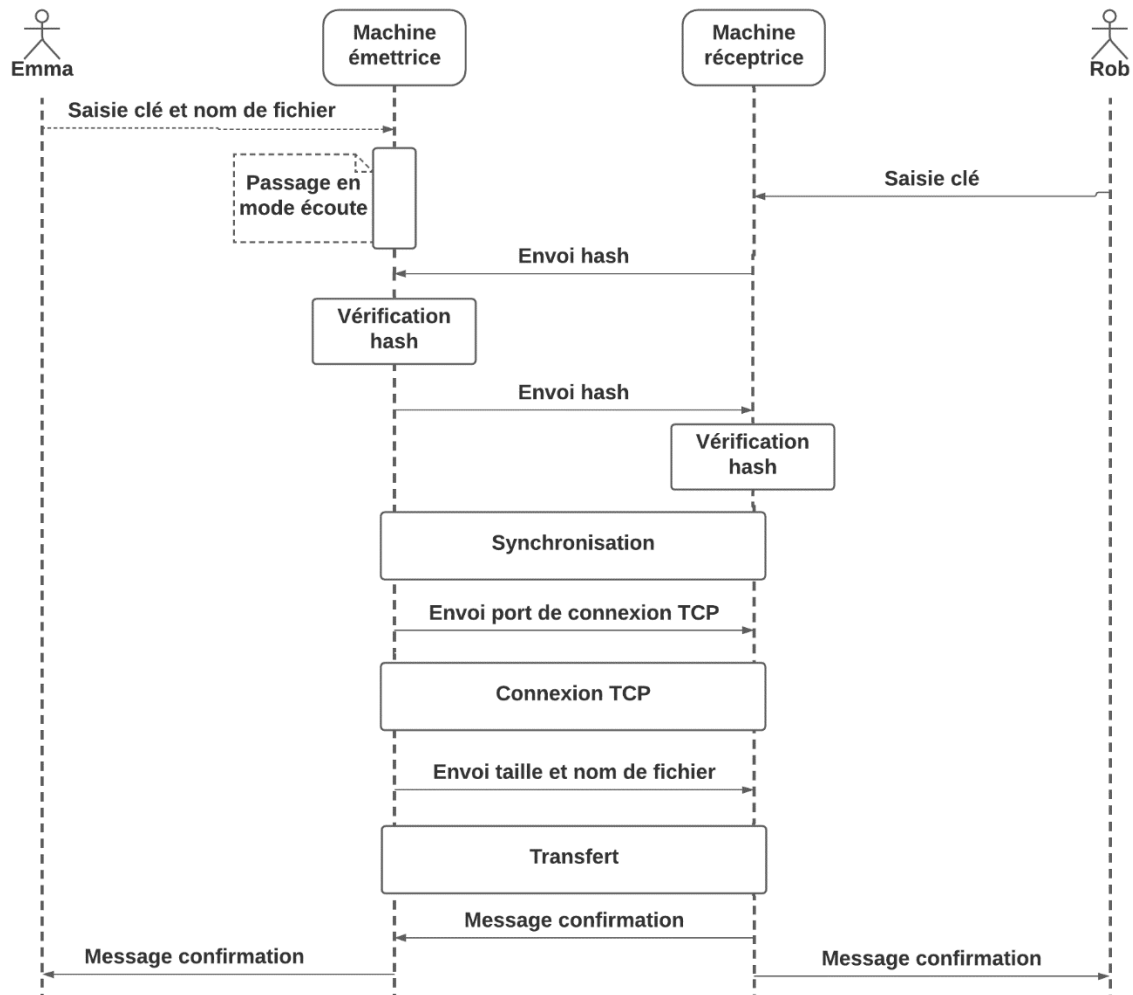


Figure 1 Diagramme de séquence du logiciel KeyShare

Imaginons que Emma, l'émettrice, initie le transfert de fichier donc que Rob, le récepteur, cherche à récupérer le fichier transféré. Emma doit d'abord entrer dans le logiciel une clé et le nom du fichier à échanger. Cette clé doit être transmise à Rob par Emma dans le monde physique par oral ou par écrit. Celle-ci n'est pas nécessairement un code indéchiffrable mais doit être tenue, dans la mesure du possible, secrète par Rob et Emma afin de sécuriser leur échange.

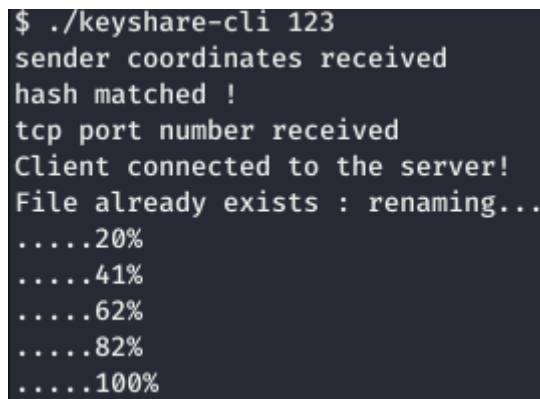
Ensuite, c'est à Rob de rentrer la clé comme paramètres dans le logiciel. Le transfert est lancé par les acteurs et s'effectue ensuite sans leur intervention sauf en cas d'erreur. En cas d'erreur pendant le transfert, un message est affiché et indique l'erreur qui a eu lieu. Dans la majorité des cas, retenter le transfert quelques instants plus tard permettra de finaliser l'échange. La fin de l'échange est annoncée par une confirmation pour chacun des acteurs.

Afin de sécuriser l'échange au mieux, l'information envoyée pour la connexion est un hash, une empreinte numérique spécifique de ses arguments initiaux. Chaque hash est généré avec l'adresse de l'acteur, un numéro de port choisi par les concepteurs et la clé d'échange. De ce fait, chaque hash est unique pour chaque échange et chaque acteur. Cela ajoute naturellement de la sécurité au programme.

## 2.2. L'interface en ligne de commandes

Afin de contrôler la bibliothèque, une interface dite en ligne de commande a été conçue. Cette interface permet d'exécuter le programme efficacement pour les connaisseurs du monde informatique. Le nombre de paramètres données au programme indique le mode d'utilisation du logiciel :

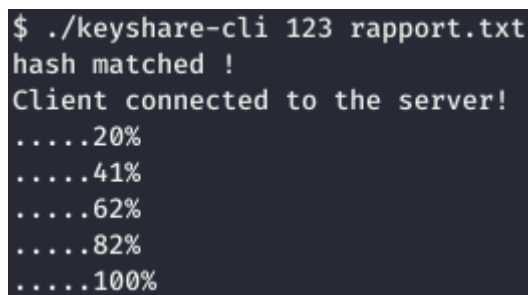
- 1 argument : la clé de l'échange invoque le receveur
- 2 arguments : la clé de l'échange et le nom du fichier invoque l'émetteur



```
$ ./keyshare-cli 123
sender coordinates received
hash matched !
tcp port number received
Client connected to the server!
File already exists : renaming...
.....20%
.....41%
.....62%
.....82%
.....100%
```

Figure 2 Capture d'écran d'un terminal pour la réception du transfert avec le code 123

On remarque que le mode réception vérifie si le fichier existe avant de l'enregistrer. Le cas échéant, le fichier est renommé avec l'heure du transfert accolé. De plus, un pourcentage est affiché pour permettre à l'utilisateur de suivre le transfert dans les deux modes.



```
$ ./keyshare-cli 123 rapport.txt
hash matched !
Client connected to the server!
.....20%
.....41%
.....62%
.....82%
.....100%
```

Figure 3 Capture d'écran d'un terminal pour l'envoi du fichier rapport.txt avec le code 123

## 2.3. L'interface graphique

Pour satisfaire au besoin de fournir une solution utilisable pour des utilisateurs néophytes, une interface graphique a été développée.

L'interface permet de faciliter certaines actions comme la recherche du fichier grâce à un bouton de recherche pour l'émetteur. En appuyant sur ce bouton, une fenêtre classique et connue de l'arborescence s'ouvre afin de ne pas perdre l'utilisateur. Des raccourcis sont implémentés pour faciliter certaines actions comme quitter le logiciel, consulter les logs ou lancer la recherche de fichier pour l'émetteur.

Pour information, le thème de l'interface est différent selon le système d'exploitation.

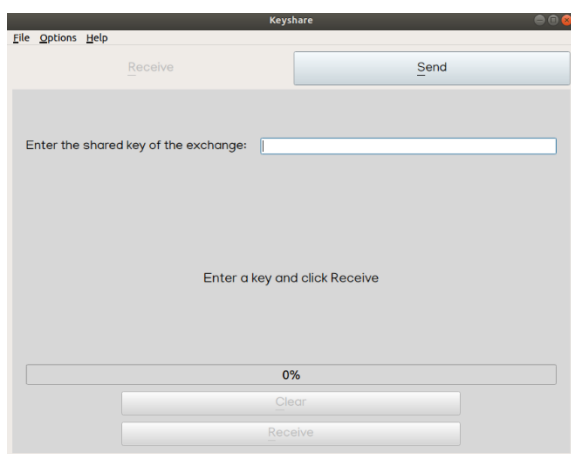


Figure 4 Capture d'écran fenêtre recevoir

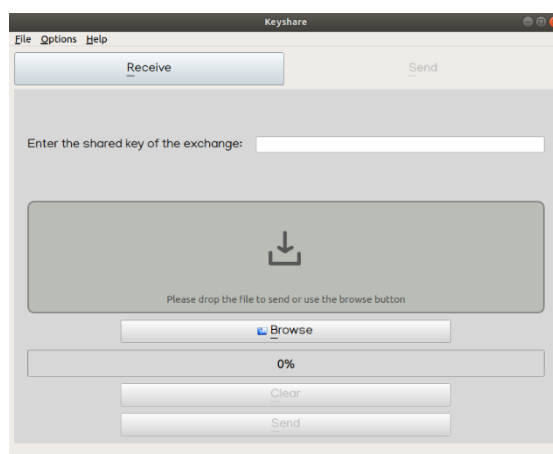


Figure 5 Capture d'écran fenêtre envoyer

Enfin, elle est traduite en français sur un ordinateur en langue française pour faciliter l'utilisation du logiciel pour des personnes ne maîtrisant pas la langue anglaise.

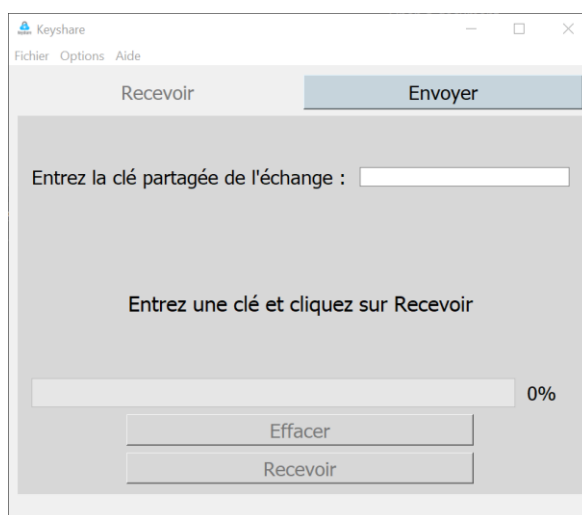


Figure 6 Capture fenêtre recevoir avec langue française

### 3. Objectifs

Les objectifs originaux ci-dessous reprennent le diagramme de GANTT suivant :

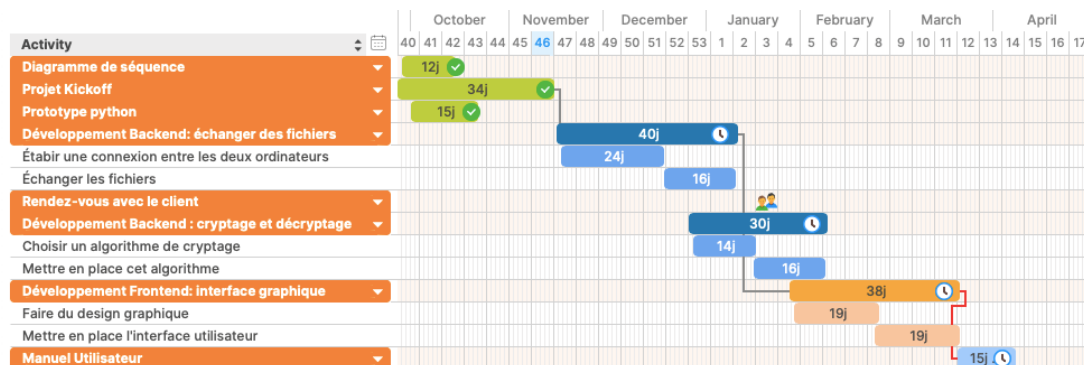


Figure 7 Diagramme de GANTT créé pour le kick-off

#### 3.1. Changements

Les objectifs suivants ont été enlevés pour le deuxième semestre :

- Implémenter une couche forte de sécurité après avoir conclu son inefficacité dans ce projet car l'échange est suffisamment sécurisé, par nature
- Préparer un manuel utilisateur pour l'interface graphique car l'objectif initial est de créer une interface intuitive

Ces changements ont permis de faciliter l'avancée du projet car certains détails ont été tardivement repérés et ont donc pu être corrigés sans dépasser le temps de travail initialement alloué.

Le premier objectif supprimé aurait eu un impact fort sur le budget et la structuration du projet si nous avions adaptés une approche peu flexible de la gestion de projet. Grâce à une approche plus flexible, on a pu donc rediriger les ressources facilement.

# GESTION DE PROJET

---

*Cette partie se concentre sur la gestion de projet et les outils utilisés par l'équipe lors du développement.*

## 1. Méthodologie

Les tâches proposées correspondent au diagramme de GANTT précédemment cité (voir Figure 7 Diagramme de GANTT créé pour le kick-off). Dans un premier temps, il n'y avait pas de hiérarchie au sein de l'équipe. Mais par suite du retour de la soutenance de mi-parcours, un chef de projet a été sélectionné. L'équipe a profité de rôles mieux définis et d'un respect plus strict des tâches imposées.

En parallèle de ce choix, une augmentation de la fréquence des rendez-vous avec le client a été organisée. Le tuteur a profité d'un suivi plus régulier et le client d'une meilleure visualisation de l'avancement du projet.

## 2. Outils

Afin de partager le code entre les différents acteurs, un dépôt GitLab dont le serveur est hébergé par l'école d'ingénieur Ensicaen est utilisé. Pour le développement, afin de faciliter l'accès à certaines données comme les adresses IP des utilisateurs, nous utilisons la bibliothèque réseau SFML. Elle est légère et efficace quant à la récupération de données réseau. Cette bibliothèque permet aussi de résoudre efficacement des problèmes réseaux comme la correspondance BIG ENDIAN et LITTLE ENDIAN. Elle est de plus portable sur les systèmes d'exploitation autre que Linux.

Pour la communication, nous utilisons Facebook Messenger pour les messages d'information dans l'équipe, Microsoft Outlook pour la communication avec le client, Discord pour les réunions de l'équipe et Big Blue Button pour les réunions avec le client. Facebook Messenger est beaucoup utilisé dans la vie étudiante donc nous avons profité d'être tous présents sur l'application pour l'utiliser.

Pour le développement de la bibliothèque, les environnements de développements (IDE) utilisés sont différents. Pour la conception de l'interface graphique, nous favorisons l'IDE utilisé pour les travaux pratiques de conception d'interface graphique, QtCreator. Nous utilisons donc la bibliothèque Qt pour l'interface graphique et pour son avantage d'être multiplateforme. Cette bibliothèque est aussi utilisée pour sa gestion efficace des signaux et des slots, permettant un échange de données faciles entre des threads.



# SITUATION ACTUELLE

---

*Cette partie fait un bilan de la situation actuelle du projet. Elle liste les objectifs non réalisés et des pistes d'améliorations.*

## 1. Objectifs et travail réalisé

Nous avons réalisé les tâches suivantes :

1. Echanger les fichiers avec un programme exécutable en ligne de commande
  - a. Créer un protocole d'échange
  - b. Prouver que ce protocole est cohérent grâce à un prototype
  - c. Etablir une connexion entre deux ordinateurs qui souhaitent communiquer
  - d. Echanger un fichier entre ces deux ordinateurs
2. Ajouter de la sécurité à l'échange par du cryptage et décryptage de données
  - a. S'assurer qu'un cryptage des données est utile pour notre échange
  - b. Etudier les algorithmes de cryptage et décryptage existants
3. Façonner une interface graphique cohérente et naturelle d'utilisation
  - a. Faire un croquis des fenêtres utiles pour notre logiciel
  - b. S'assurer de la simplicité et du naturel de l'interface
  - c. Implémenter cette interface

Cela implique que nous avons un programme fonctionnel en ligne de commande et avec une interface graphique.

## 2. Obstacles rencontrés

En cours de développement du projet, la nécessité d'avoir une architecture projet claire s'est fait sentir. De ce fait, quelques semaines avant la fin du projet, une réforme de son architecture a été menée afin de faciliter toute demande d'aide auprès du tuteur. On évite ainsi la duplication de code mais aussi les duplicatas de librairies.

Ensuite, une fois l'interface graphique suffisamment avancée, nous avons observé des comportements trop brusques qui ne respectent pas les pratiques d'ergonomie. L'interface se fermait si une erreur avait lieu. La cause était une mauvaise gestion des erreurs dans la bibliothèque. Ainsi, son remodelage a permis de corriger cette erreur.

Finalement, un obstacle n'a pas été surmonté : l'application est devenue inutilisable sur le réseau local de certains membres de l'équipe projet. La cause n'a pas été identifiée clairement : d'autres appareils sur le réseau connectés aux ports utilisés, gestion des erreurs pas assez fine et autres causes sont envisagées.

### 3. Objectifs non atteints

Les tests unitaires et fonctionnels de notre programme n'ont pas été réalisés.

Par suite d'une étude sur l'utilité d'implémenter une sécurité forte par cryptage, la tâche a été supprimé du calendrier. L'étude menée montre que le cryptage est utile pour des réseaux locaux publics par Wifi dans le cas d'un échange de documents précieux ou confidentiels.

Enfin, aucun manuel utilisateur n'a été écrit. En effet, le défi est de rendre l'interface graphique tellement intuitive que l'utilisateur n'a pas besoin de se renseigner sur les contrôles disponibles. Cependant, à notre niveau d'expertise actuelle, ce n'est pas entièrement envisageable. En effet, nous n'avons pas la théorie d'User Expérience (UX) pour nous guider dans nos choix de conception d'interface.

### 4. Suite du projet

Les différentes versions du programme sont utilisables sous Linux et, sous réserve d'une configuration adéquate, sous Windows. Il s'agit donc dans un premier temps d'améliorer certains services de la bibliothèque : ajouter une option permettant de choisir le chemin de destination, proposer l'affichage ou non des erreurs, rendre la partie réseau plus flexible dans le choix des ports par exemple. Ensuite, il faudrait consolider l'interface avec des connaissances plus profondes sur l'ergonomie et l'UX.

Finalement, un travail de déploiement est à organiser. Pour cela, il faudrait créer des scripts d'installation pour satisfaire les différentes dépendances du programme. De ce fait, un travail sur les bibliothèques utilisées se retrouve nécessaire afin de réduire voire de supprimer certaines dépendances et ainsi faciliter le déploiement sur toutes les plateformes. Dans tous les cas, l'utilisation de QtCreator pour la conception de l'interface graphique et de SFML pour le réseau sont les premiers pas vers un programme simple et multi plateforme.

# BILAN

---

## 1. Ce qui a fonctionné

Le diagramme de Gantt et les autres diagrammes permettent d'analyser de manière concise le projet dans ses contraintes et ses objectifs. Cela permet de bien démarrer le projet et de mieux visualiser les objectifs pour l'équipe. Ainsi, nous avons pu découper le travail en tâches bien distinctes et organiser ce travail de manière efficace.

La première soutenance a mise en évidence la nécessité de choisir un chef de projet. Ce chef de projet est responsable de la communication avec le client, de l'écriture des compte rendus de réunion et de la répartition des tâches sur les différentes semaines. Cela a permis de faciliter le dialogue avec le client, le suivi du projet et son avancée quasi constante pendant le second semestre.

## 2. Ce qui n'a pas fonctionné

Le diagramme de Gantt n'a pas été suivi à la lettre car nous n'avions pas d'organisation interne afin de s'assurer d'une avancée constante du projet. Cependant, une hiérarchie a été instauré au second semestre du projet pour pallier ce défaut.

Il a été suggéré par le client de travailler avec le moins de dépendances possibles donc de ne pas utiliser la bibliothèque SFML. Pour un compromis d'efficacité car cette librairie résout facilement les problématiques réseaux, nous avons préféré la garder. De plus, la bibliothèque SFML existe aussi sous Windows et permet de faciliter le développement du logiciel sur plusieurs systèmes d'exploitation.

## 3. Les bénéfices du projet 2A

Grâce à ce projet, nous avons expérimenté pour la première fois une gestion de projet sur une année complète. De plus, nous avons réalisé un projet entier pour un client : c'est une première mise en situation parfaite et bienvenue dans notre formation. Le projet nous a permis de mieux appréhender le besoin du client mais aussi la coopération avec un tuteur.

Finir le projet quelques semaines avant de commencer le stage de 2<sup>ème</sup> année permettra de faciliter notre insertion dans notre établissement d'accueil grâce à cette première expérience en travail d'équipe sur le long terme.



## Ecole Publique d'Ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053  
14050 CAEN cedex 04

