

UNIVERSITÉ DE LA RÉUNION

UFR SCIENCES ET TECHNOLOGIES

TRAVAIL D'ÉTUDE ET DE RECHERCHE, M1 - INFORMATIQUE

LABORATOIRE D'INFORMATIQUE ET DE MATHÉMATIQUES

Système de codage/décodage de résultats d'évaluations en ligne

Auteur :

Donovan ROULLAND

n° étudiant : 38000026

Encadrants :

Olivier SEBASTIEN

Porteur de projet :

Olivier SEBASTIEN

Structure du porteur de projet : Institut Indianocéanique du Numérique (IIN)

Période de travail sur le projet : Du 10 septembre au 22 novembre

Année Universitaire : 2021 - 2022 (Projet 1)

Table des matières

1	Introduction	2
1.1	Résumé	2
1.2	Présentation du sujet.	1
1.2.1	Contexte du sujet	1
1.2.2	Problématique du sujet	1
1.2.3	Vue globale de l'architecture du sujet	1
2	Gestion de projet	2
2.1	Organisation	2
2.2	Méthode de communication avec le porteur de projet	3
2.3	Outils utilisés pour gérer le projet	3
2.3.1	Logiciel Git et ses fonctions	3
2.3.2	Qu'est-ce que GitHub	3
3	Développement réalisé	4
3.1	Problèmes rencontrés et solutions apportées	4
3.1.1	Choix du protocole de chiffrement	4
3.1.1.1	Compléments d'informations sur le fonctionnement du protocole AES	4
3.1.2	Application de décodage	5
3.1.2.1	Pourquoi Java	5
3.1.2.2	Principaux problèmes rencontrés	6
3.1.3	Serveur Web	7
3.1.3.1	Pourquoi Node.Js	7
3.1.3.2	Le module Express	7
3.1.3.3	Le module Crypto	7
3.2	Résultats obtenus	8
3.2.1	Application Java	8
3.2.2	Serveur Node.Js	11
4	Conclusion	12

1 Introduction

1.1 Résumé

Ce sujet de TER (Travaux d'Enseignement et de Recherche) a pour vocation de permettre au corps enseignant de réaliser des nouvelles formes de devoirs en 100% distanciel, par exemple l'utilisation de serious games (devoir sous forme de jeu) qui est très compliquée à mettre en place sur les plateformes de l'Université telles que EDX ou Moodle, car elles demandent de délivrer des niveaux de privilège côté serveur trop élevés pour ce type d'applications non certifiées en terme de fiabilité/sécurité.

Pour pallier ce problème, on souhaite mettre en place un système anti-fraude qui à terme permettra de nous soustraire complètement des plateformes de cours en ligne.

Mots-clés

: Génie logiciel, cryptographie, hash code, robustesse, QR Code, contrôle de données, codage/décodage

Abstract

This TER (Teaching and Research Work) subject aims to allow teachers to carry out new forms of duty in 100% distance, for example the use of serious games (duty in the form of a game) is very complicated to set up on University platforms such as EDX or Moodle, because they require issuing too high level of privileges on the server side for this type of applications not certified in terms of reliability / security.

To overcome this problem, we want to set up an anti-fraud system which would ultimately allow us to completely escape from online course platforms.

Keywords

: Software engineering, cryptography, hash code, robustness, QR Code, data control, encoding / decoding

1.2 Présentation du sujet.

1.2.1 Contexte du sujet

L'Institut Indianocéanique du Numérique (IIN) est la composante de l'université dédiée à la transposition de ses activités dans le domaine numérique, afin de pouvoir toucher des publics qui ne peuvent pas physiquement venir sur les campus. A ce titre, elle développe des méthodes et outils pour faciliter l'enseignement en mode distanciel.

1.2.2 Problématique du sujet

L'une des questions sur lesquelles elle travaille est celle de la qualité de l'évaluation quand on est à 100% en distanciel, sans possibilité de surveillance. A ce titre, des prototypes (web ou application locale) sont régulièrement développés souvent basés sur des serious games. Se pose alors le problème de la récupération des notes dans la plateforme de cours en ligne (Moodle ou EDX) : le mécanisme permettant de le faire nécessite des privilèges côté serveur qu'il est délicat d'octroyer à des applications peu éprouvées en terme de fiabilité et de sécurité. D'où la nécessité de trouver un mécanisme plus léger tout en étant robuste à la fraude.

1.2.3 Vue globale de l'architecture du sujet

Le projet présenté dans ce rapport, schématisé à la figure 1, comporte 2 modules distincts, une partie destinée aux utilisateurs (étudiants) et l'autre au client (université), le premier module sert principalement à ajouter un formulaire et ses fonctions sur une page html contenue par un serveur existant où les étudiants réaliseront leurs devoirs en distanciel afin de permettre le chiffrement de données sensibles, dont la note obtenue au devoir. Le deuxième module sert quant à lui aux professeurs et a pour vocation de déchiffrer les clés cryptées fournit par les étudiants sur Moodle par l'intermédiaire d'une application Java

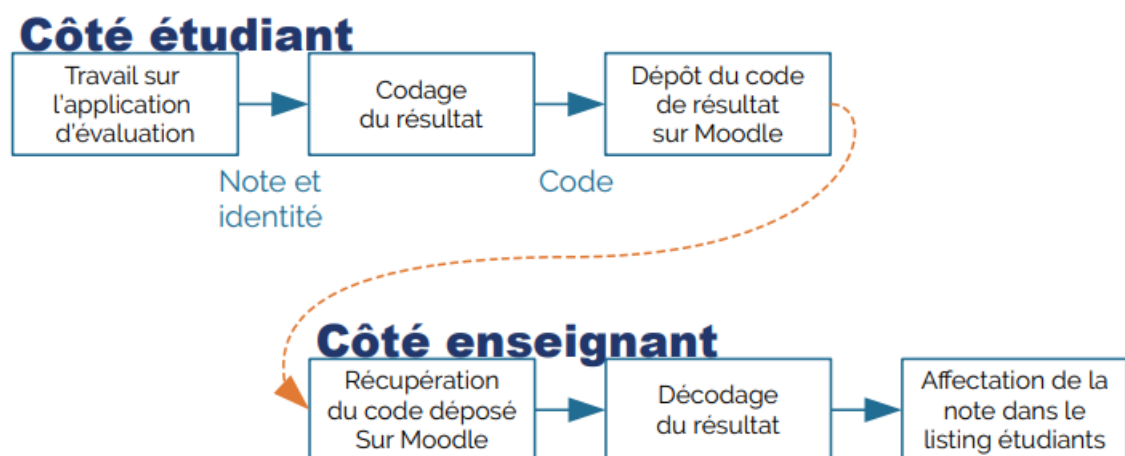


Figure 1

2 Gestion de projet

2.1 Organisation

Pour l'élaboration de ce projet, j'ai d'abord effectué des recherches dans le domaine de la cryptographie, les outils utilisés, la puissance/robustesse des protocoles actuels, mais également les méthodes permettant d'outrepasser ces diverses sécurités.

Par la suite, j'ai mis en place un cahier des charges contenant les tâches que je m'étais initialement fixées afin d'avoir une idée fixe du volume horaire nécessaire au bon déroulement du projet.

Puis, en accord avec le porteur de projet nous avons décidé d'adopter une gestion de projet en mode AGILE avec un sprint encre chaque rendez-vous.

Finalement, le diagramme de Gantt de la Figure 2 représente la répartition du travail effectué sur les semaines dédiées au projet :

<i>Tâches</i>	<i>Semaine 1</i>	<i>Semaine 2</i>	<i>Semaine 3</i>	<i>Semaine 4</i>	<i>Semaine 5</i>	<i>Semaine 6</i>
<i>Serveur Web</i>						
<i>Partie graphique de l'application java + page html du serveur web</i>						
<i>Chiffrement des données</i>						
<i>Application java</i>						
<i>Déchiffrement des données</i>						
<i>Documentation</i>						
<i>Rapport</i>						

Figure 2

2.2 Méthode de communication avec le porteur de projet

Afin d'échanger avec le porteur de projet, nous avons décidé d'utiliser le logiciel ZOOM qui est un logiciel de web conférence permettant de créer une salle virtuelle avec la vidéo des participants, il est très puissant et propose divers fonctionnalités intéressantes. Cela nous a permis de nous rencontrer en visioconférence et ainsi de me permettre d'expliquer et de montrer grâce au partage d'écran, l'évolution du projet semaine après semaine.

2.3 Outils utilisés pour gérer le projet

Pour permettre un suivi efficace du projet, j'ai opté pour l'utilisation de l'outil Git qui a permis le stockage du projet sur la plateforme GitHub. Cela apporte une garantie quant au bon développement du projet grâce au versioning, mais aussi un suivi en temps réel pour les acteurs au sein d'un projet.

2.3.1 Logiciel Git et ses fonctions

Git est un logiciel de versioning créé en 2005 par Linus Torvalds, le créateur de Linux. Un logiciel de versioning, ou logiciel de gestion de version est un logiciel qui permet de conserver un historique des modifications effectuées sur un projet afin de pouvoir rapidement identifier les changements effectuées et de revenir à une ancienne version en cas de problème.

2.3.2 Qu'est-ce que GitHub

GitHub est un service en ligne qui permet d'héberger des dépôts ou repo Git. C'est le plus grand hébergeur de dépôts Git du monde.

3 Développement réalisé

3.1 Problèmes rencontrés et solutions apportées

3.1.1 Choix du protocole de chiffrement

La première difficulté à laquelle j'ai dû faire face était le choix des technologies à utiliser pour le projet.

Pour le chiffrement, le domaine de la cryptographie étant extrêmement vaste, il existe énormément de méthodes différentes quant à la manière de crypter des données, après avoir effectué des recherches approfondies sur les principaux protocoles utilisés dans le monde de la sécurité informatique et les techniques pour les contourner dans le milieu de la cybercriminalité, j'ai opté pour l'utilisation du protocole AES pour sa résistance prouvée dans de multiples domaines, il a également été approuvé par la NSA (National Security Agency) dans sa suite B1 des algorithmes cryptographiques et fait partie des algorithmes de chiffrement le plus utilisé dans son domaine actuellement.

3.1.1.1 Compléments d'informations sur le fonctionnement du protocole AES

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

3.1.2 Application de décodage

3.1.2.1 Pourquoi Java

Pour développer l'application de déchiffrement, j'ai choisi d'utiliser le langage de programmation Java, car il fait partie des langages de programmation les plus utilisés au monde, en effet, selon Oracle, Java est le langage le plus utilisé dans le DevOps, l'intelligence artificielle, la réalité virtuelle, le big data, l'intégration continue, les chatbots et dans bien d'autres domaines.

Par ailleurs, on peut voir à la figure 3 les avantages qu'il propose par rapport à d'autres langages tels que Python et C++ :

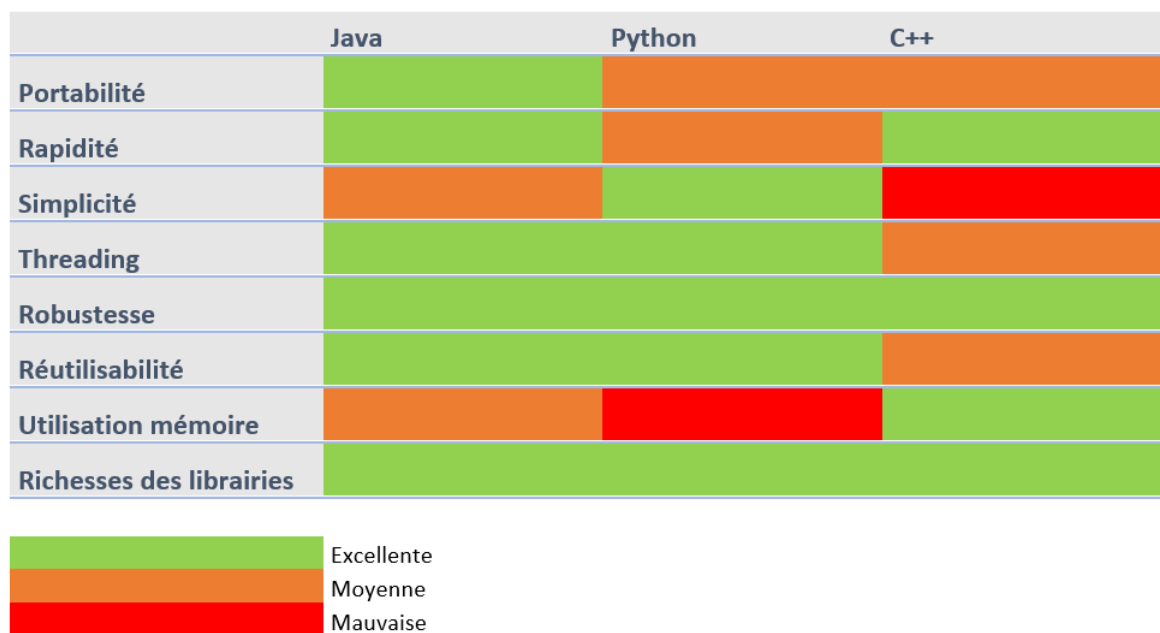


Figure 3

L'intérêt d'utiliser Java pour cette application réside principalement dans les atouts suivants :

- La facilité à compiler et déboguer grâce au bytecode Java, qui fonctionne sur différents systèmes d'exploitation.
- Des bibliothèques riches, avec une large gamme de classes.
- Programmation orientée objet, permet la création de programmes modulaires et de code réutilisable.
- Multi-thread, capable d'effectuer différentes tâches simultanément au sein d'un programme

3.1.2.2 Principaux problèmes rencontrés

Les principales difficultés que j’ai pu rencontrer quant à la réalisation de l’application Java permettant de déchiffrer des données sont :

- La création des algorithmes intermédiaires nécessitant des méthodes pour lesquelles il n’existe aucune librairie permettant de simplifier le développement en Java tel que la compression/décompression de fichier ZIP ou encore la génération de fichier CSV,TXT.
- La conversion des clés chiffrées de la base 64 en hexadécimal, pour y parvenir j’ai utilisé les fonctionnalités de conversion libres de droit fournit par la société Apache.
- La réalisation d’une version locale d’un formulaire permettant le chiffrement des données de manière sécurisée (l’utilisateur ne devant pas avoir accès aux informations sensibles du code).

Cependant, il reste très compliqué de rendre le code d’une application java en locale illisible, les fichiers Java pré-compilés (.class) pouvant être dé-compilés par des logiciels tiers.

Pour essayer de rendre la fraude plus difficile, nous avons décidé de rajouter des informations supplémentaires telles que la date et l’heure de l’exécution du chiffrement à la chaîne produite, qui sera par la suite chiffrée.

3.1.3 Serveur Web

Afin de pouvoir traiter les données de manière sécurisée, il était nécessaire que toutes les fonctions de chiffrement soient inaccessibles par les utilisateurs, j'ai donc fait le choix de faire passer toutes les informations sensibles du côté serveur en utilisant la technologie Express de Node.js, cela m'a permis de simuler l'exécution code contenant les méthodes de chiffrement fournit par le module Crypto côté serveur et ainsi d'empêcher toute tentative de fraude par les utilisateurs.

3.1.3.1 Pourquoi Node.js

J'ai choisi pour cette partie du projet, d'opter pour la réalisation du serveur avec la technologie de Node.js car c'est une technologie appréciée par de plus en plus d'entreprises, dont plusieurs géants du web tel que Microsoft, Google, Yahoo, Mozilla et Github.

Node.js démontre sa puissance sur plusieurs points :

- Sa rapidité : les entreprises admirent la rapidité de Node.js. Pourquoi ? Parce qu'il utilise la version 8 du moteur développé par Google qui compile le JavaScript en code machine natif et fonctionne à la vitesse de l'éclair.
- Son évolutivité : Node vous permet d'étendre les demandes simultanées, ce que les autres langages ne peuvent faire. Certains ont atteint des niveaux d'extensibilité de plus d'un million de requêtes simultanées. Bien sûr, tout dépend du travail que vous faites derrière chaque requête et du nombre de ressources dont vous disposez, même si Node est toujours aussi performant pour faire évoluer les choses.
- Son extensibilité : Parmi les autres avantages de Node.js, il y a la possibilité de l'intégrer avec une variété d'outils utiles. Node.js peut être facilement personnalisé. Il peut être étendu par exemple avec des API intégrées pour le développement de serveurs HTTP ou DNS. Pour faciliter le développement frontend avec d'anciennes versions de Node ou de navigateurs. Node.js peut être intégré à un compilateur JS Babel.

3.1.3.2 Le module Express

Pour pouvoir simulé un serveur web, j'ai choisi d'utiliser ExpressJS pour sa simplicité d'utilisation et sa légèreté, en effet c'est un framework qui se veut minimaliste. Très léger, il apporte peu de surcouches pour garder des performances optimales et une exécution rapide. Express ne fournit que des fonctionnalités d'application web (et mobile) fondamentales, mais celles-ci sont extrêmement robustes et ne prennent pas le dessus sur les fonctionnalités natives de NodeJS.

3.1.3.3 Le module Crypto

Pour le chiffrement des données, j'ai utilisé le module Crypto, car il fournit des fonctionnalités cryptographiques très complète, qui incluent un ensemble de wrappers pour les fonctions de hachage SSL's hash HMAC, de chiffrement, de déchiffrement, de signature et de vérification.

3.2 Résultats obtenus

3.2.1 Application Java

La fenêtre principale de la Figure 4 ouverte à l'exécution du programme Jar est une simple fenêtre de sélection qui permet de choisir le mode de déchiffrement souhaité et ouvre les fenêtres correspondantes :

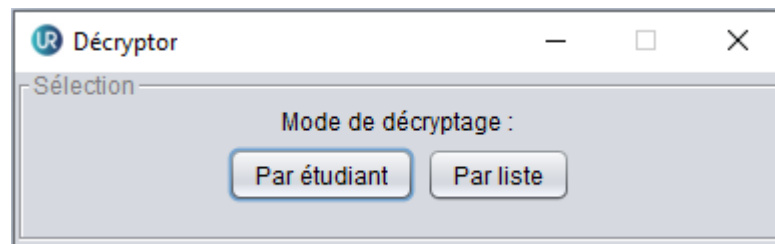


Figure 4

La fenêtre de la Figure 5 ouverte à la sélection du mode déchiffrement par étudiant, contient un champ à remplir avec une clé chiffrée, le bouton "décrypter" permet l'exécution des fonctions nécessaires à l'affichage du résultat déchiffré dans le champ "Résultat" qui est non éditable :

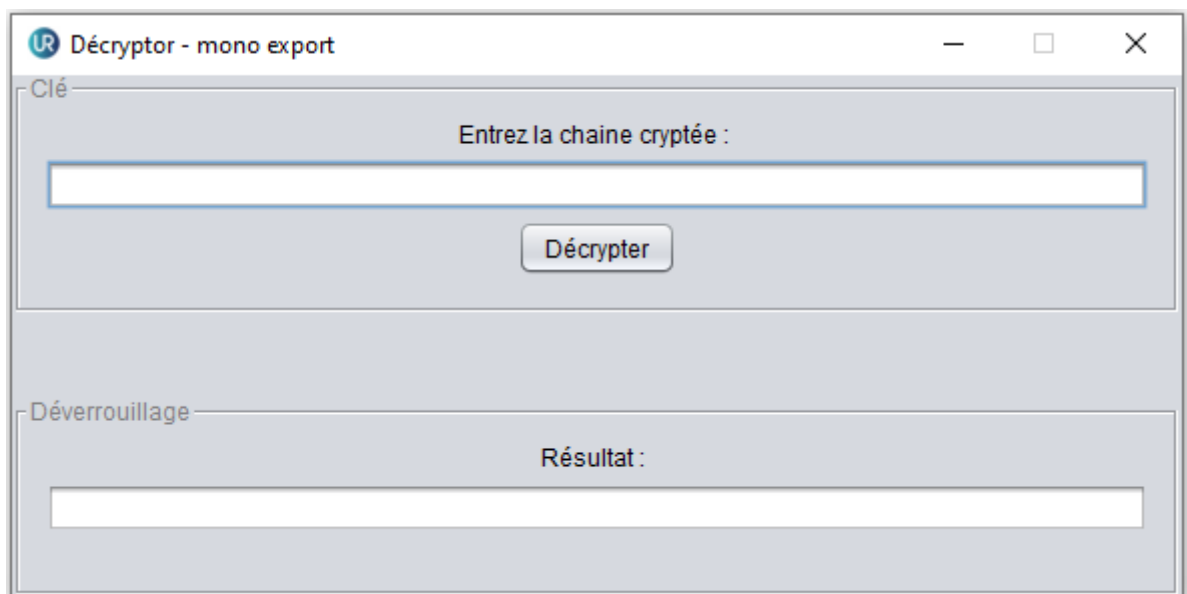


Figure 5

La fenêtre de la Figure 6 ouverte à la sélection du mode déchiffrement par liste, contient les éléments suivants :

- Un bouton "Sélection" permettant d'ouvrir une boîte de dialogue où l'on peut choisir l'emplacement du fichier ZIP contenant les clés chiffrées.
- Un bouton "Décrypter" qui s'affiche suite à la sélection du fichier et permet d'activer les fonctions nécessaires au déchiffrement par liste, puis d'afficher le résultat dans la zone de texte "Liste décryptée".
- Un bouton "Exporter" s'affiche et permet de générer un fichier CSV contenant la liste résultant du déchiffrement :

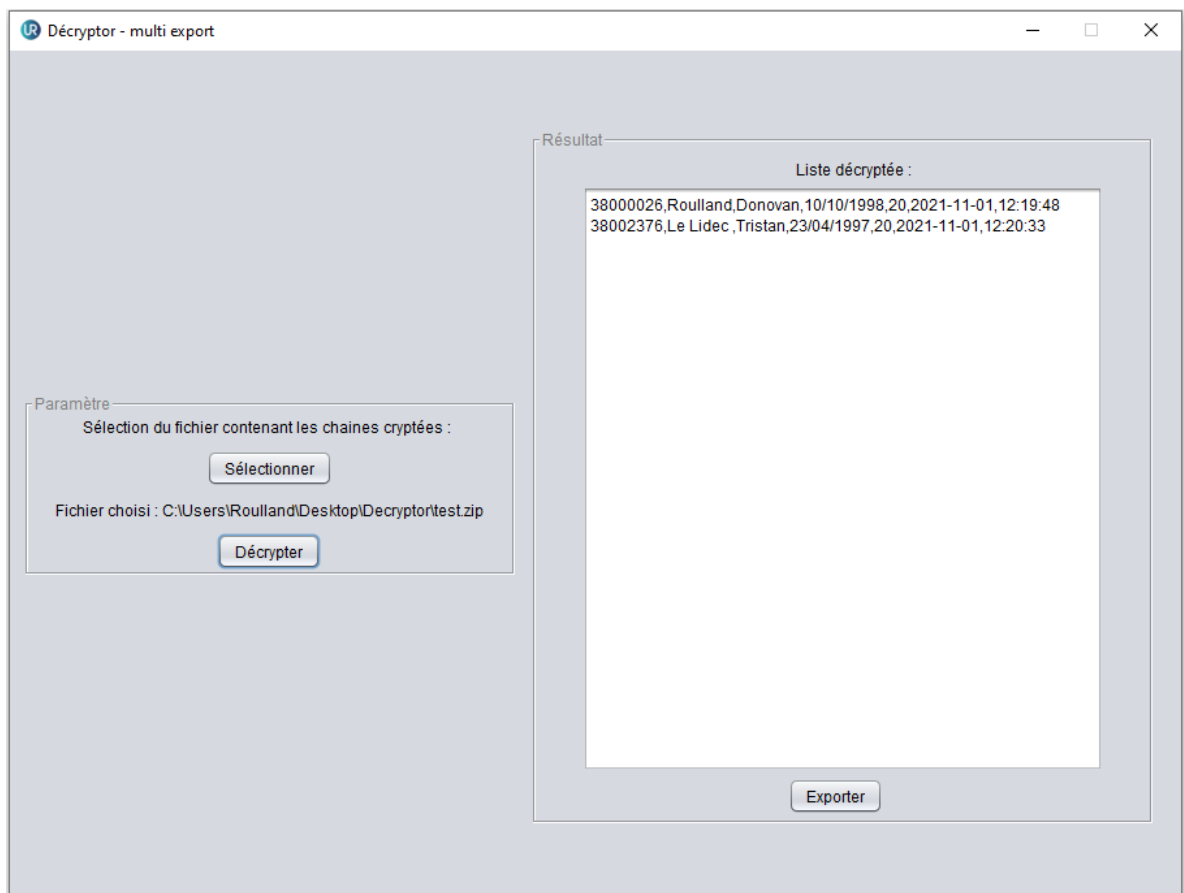


Figure 6

La figure 7 ci-dessous nous montre la fenêtre de la version locale du formulaire de chiffrement :

Encryptor

Clé

Numéro étudiant :

38000026

Nom :

Roulland

Prénom :

Donovan

Date de naissance (JJ/MM/AAAA) :

10/10/1998

Crypter

Déverrouillage

Résultat :

99aa677766c7a07195edf4ec0a024f86e3de0677d243c4515a1a180a361779ba13c904782e23ac37

Exporter

Figure 7

Elle contient les éléments suivants :

- 4 champs "JTextField" à remplir par l'utilisateur.
- Un JButton Crypter qui déclenche les fonctions de chiffrement.
- Un champ "JTextArea" qui affiche le résultat et qui est non éditable.
- Un bouton "Exporter" qui permet de générer un fichier texte contenant la clé chiffrée.

3.2.2 Serveur Node.Js

La figure 8 ci-dessous nous montre la page du sérieux game simulée avec l'extension développée durant ce projet.

Cette extension contient un bouton permettant d'afficher un formulaire destiné aux étudiants ayant terminé leurs devoirs :

Page du sérieux game :

AFFICHE POPUP

Figure 8

La figure 9 ci-dessous nous montre le formulaire qui s'affiche au-dessus de la page html et qui est à la position fixed, elle suit donc les mouvements réalisés par l'utilisateur comme le scrolling :

Remplissez le formulaire :

38000026

Roulland

Donovan

Date de naissance

10/10/1998

GENERATE

DOWNLOAD

100%

Figure 9

Le bouton "Generate" crée la clé chiffrée obtenue à partir des informations saisies et fait apparaître un bouton "Download" permettant de télécharger un fichier texte contenant le résultat chiffré.

4 Conclusion

Au début, cela me paraissait compliqué de réaliser un système anti-fraude comme celui-ci en travaillant en local sur des données fictives, cependant n'ayant aucune connaissance dans le domaine de la cryptographie, je souhaitais impérativement réaliser ce projet pour acquérir les connaissances nécessaires à mon propre projet professionnel.

Ce projet m'a donné l'opportunité de me plonger dans cet univers inconnu qu'est la sécurité informatique. J'ai donc pu obtenir de nouvelles compétences notamment en matière de cryptographie, mais aussi dans le développement logiciel en Java, la mise en place de serveur web, le traitement d'informations côté serveur avec Node.js et plus encore.

Par ailleurs, le plus gros progrès a été de d'avoir un aperçu de la vie professionnelle dans le milieu du développement grâce à la méthode de travail adoptée dans le cadre de cette UE, la réalisation du projet voulu par le client, mais aussi tout ce qui accompagne cette démarche : le contact client - prestataire, les échanges entre professionnels, les méthodes de travail, etc.