

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

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 p. 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 permettrai 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 per. 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 p. 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.

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 1 représente la répartition du travail effectué sur les semaines dédiées au projet :

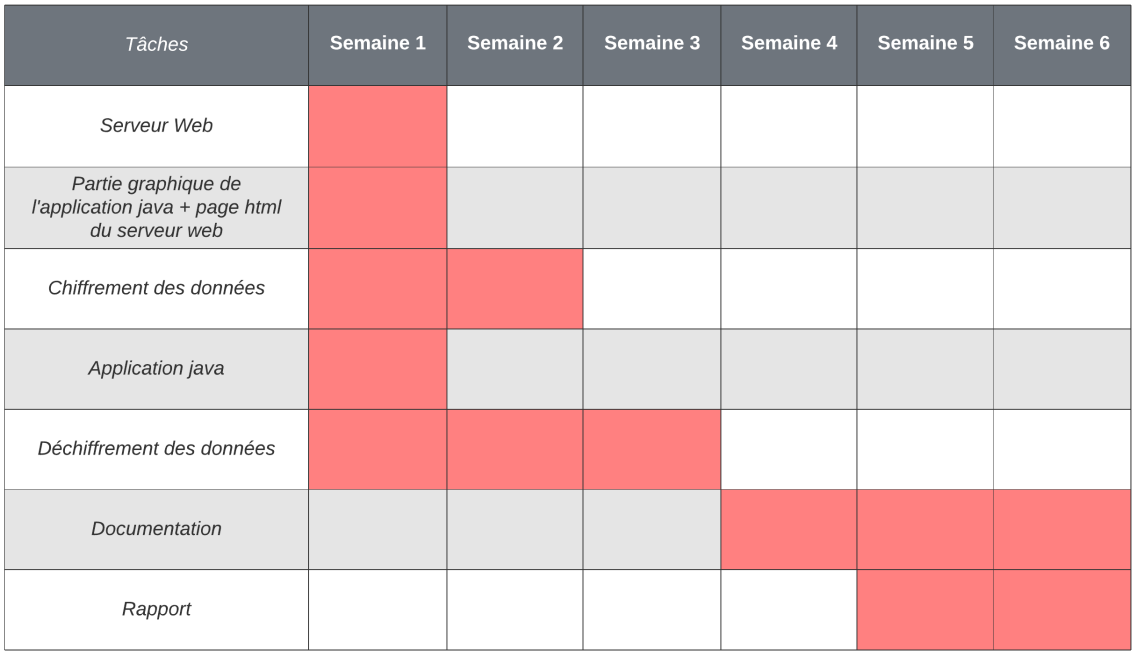

Figure 1

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 outil très puissant et propose des fonctionnalités intéressantes telles que le partage d'écran.
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.

Compléments d'informations sur l'outil Zoom

Zoom recouvre les principaux cas d'usage de la web conférence, du chat et la réunion en ligne au séminaire digital. Zoom permet de créer une salle virtuelle avec la vidéo des participants en mosaïque. Les utilisateurs peuvent y interagir aussi bien depuis leur ordinateur que depuis leur tablette ou leur smartphone. La plateforme prend en charge la transcription et la traduction en temps réel dans 30 langues. Elle gère aussi les réservations de salles de réunion équipées d'écran Zoom. En parallèle, Zoom propose divers fonctionnalités collaboratives.

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.

Compléments d'informations sur l'outil Git

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.

Compléments d'informations sur la plateforme 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.

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 Java

Les principaux problèmes que j'ai pu rencontré 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 Node.Js

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.

Compléments d'informations sur le module Express

ExpressJS 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.

Compléments d'informations sur le module Crypto

Le module Node.js Crypto prend en charge la cryptographie. Il fournit des fonctionnalités cryptographiques 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 2 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 :

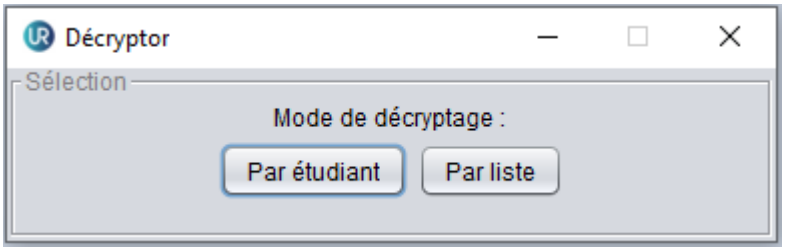

Figure 2

La fenêtre de la Figure 3 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 3

La fenêtre de la Figure 4 ouverte à la sélection du mode déchiffrement par liste, contient les éléments suivants :

— Un bouton "Sélection" permettant d'ouvrir une boite 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 :

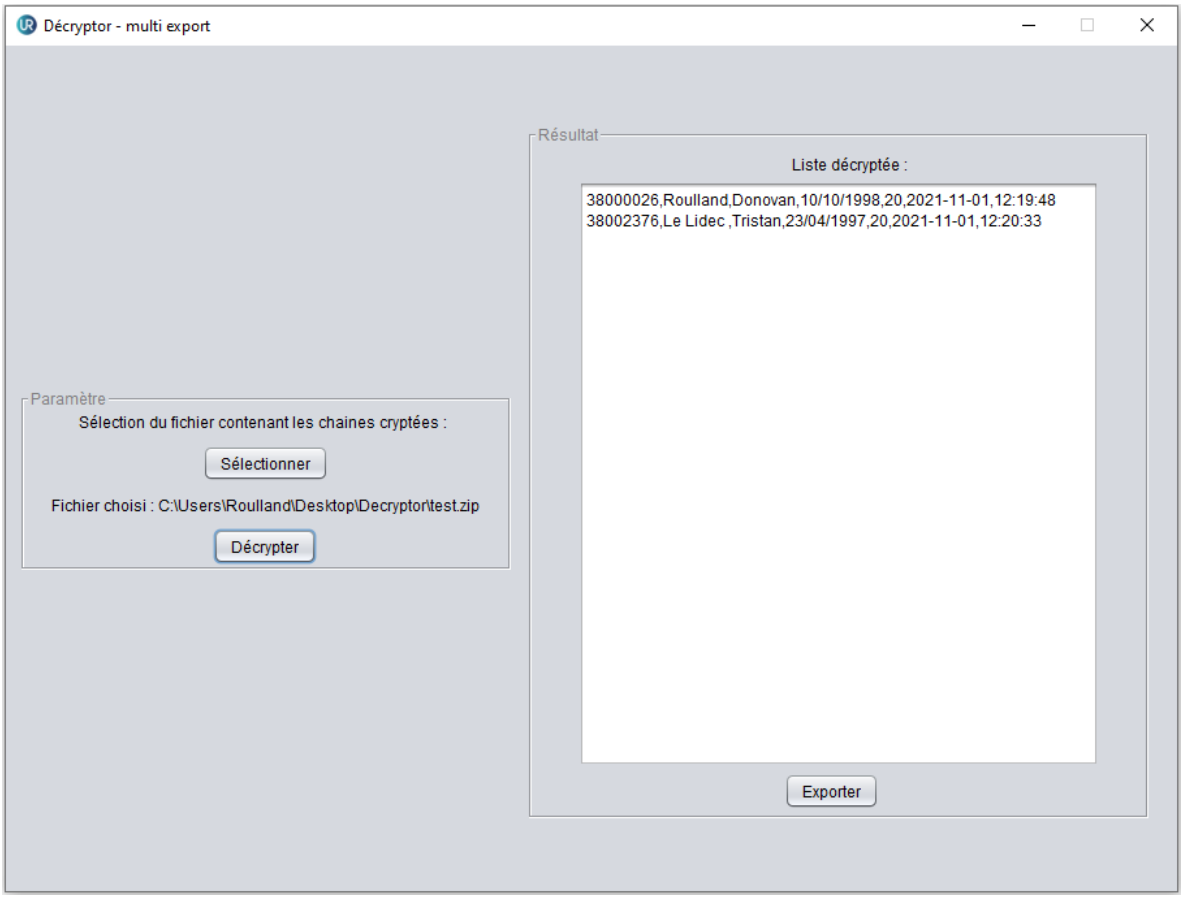

Figure 4

La figure 5 ci-dessous nous montre la fenêtre de la version locale du formulaire de chiffrement :

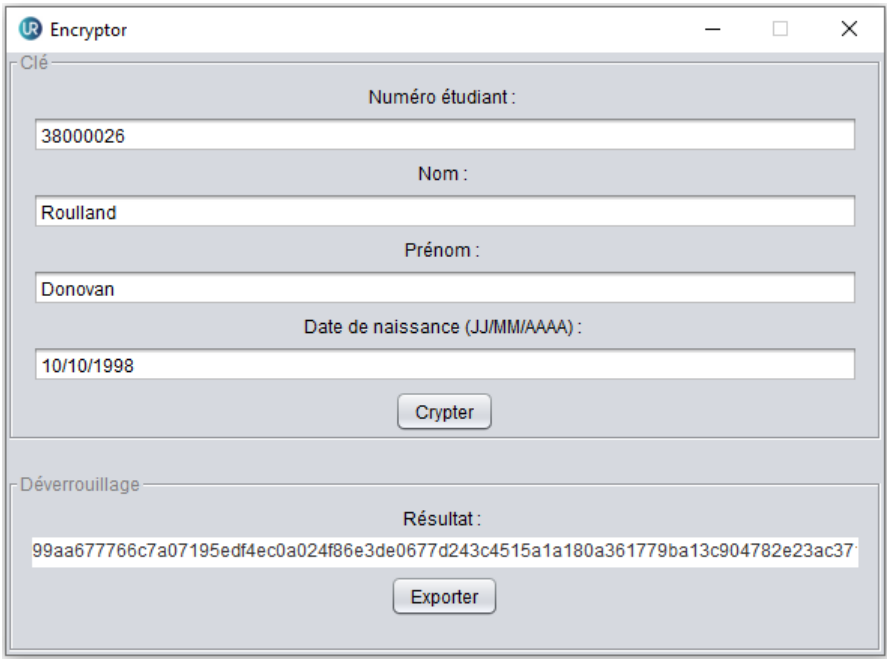

Figure 5

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 6 ci-dessous nous montre la page du sérious 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 :

Figure 6

La figure 7 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 :

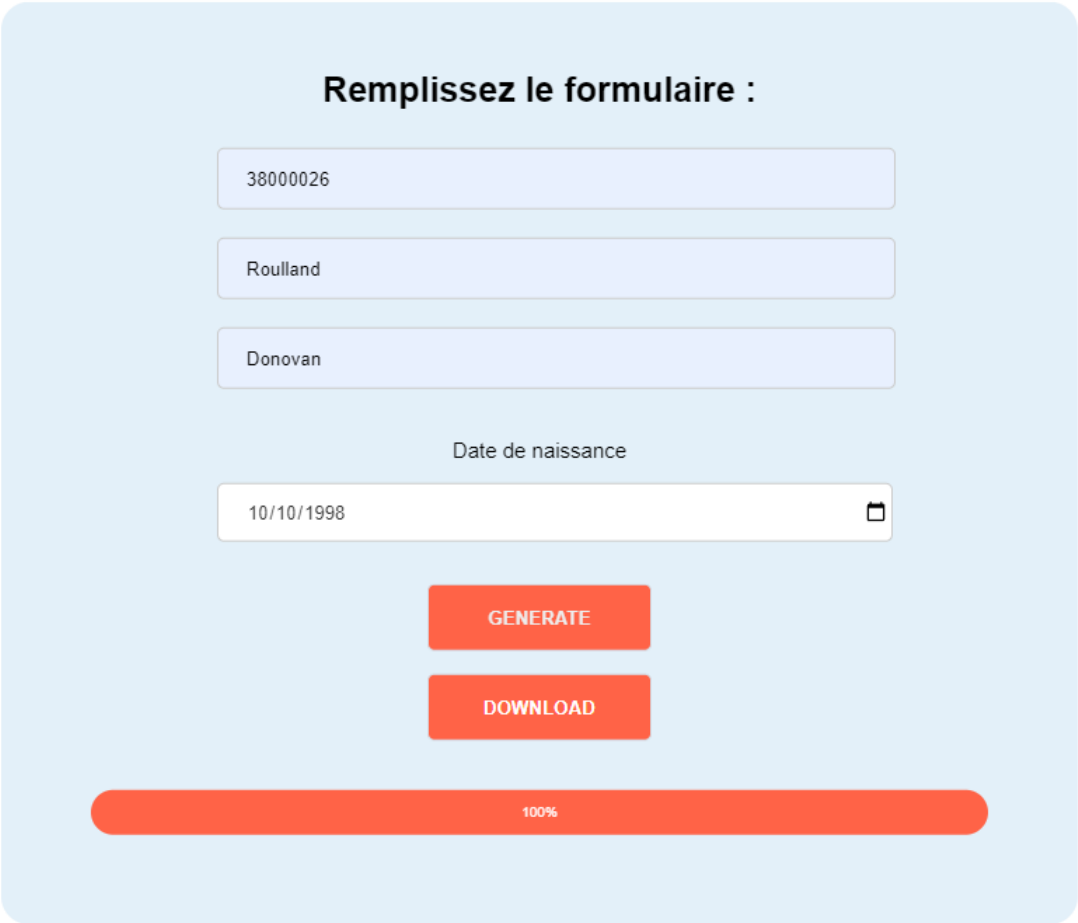

Figure 7

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 dévellopement 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.