LIRMM

Cahier des charges

Analyse statistique du cryptosystème de Paillier appliqué à des images

Rédigé par :
Katia Auxilien

Supervisé par William Puech

12.05.2024 (V1.0)

Table des matières

1 Présentation de l'entreprise 1
1.1 Introduction . . . 1
1.2 Historique de l'entreprise . . . 1
1.3 Mission et Vision . . . 1
1.4 Valeurs . . . 1
1.5 Structure de l'entreprise . . . 1
1.6 Produits/Services . . . 2
1.7 Clientèle cible . . . 2
1.8 Concurrents . . . 2
1.9 Stratégie commerciale . . . 2
1.10 Réalisations et Succès . . . 2
1.11 Perspectives d'avenir . . . 2

2 Projet 3
2.1 Présentation du projet . . . 3
2.2 Contexte et problématique . . . 3
2.3 Objectifs du projet . . . 3
2.4 Équipe de recherche et domaine d'expertise . . . 3
2.5 Méthodologie et approche . . . 3
2.6 Livrables attendus . . . 4

3 Objectifs 5
3.1 Objectifs qualitatifs . . . 5
3.2 Objectifs quantitatifs . . . 5
3.3 Cible . . . 5

4 Caractéristiques 7

5 Fonctionnalités 8

6 Contraintes 10
6.1 Contraintes techniques . . . 10
6.2 Contraintes ergonomiques . . . 10
6.3 Contraintes juridiques . . . 11

7 Structure 12

8 Déroulement du projet **13**

Table des figures **15**

1 Présentation de l'entreprise

1.1 Introduction

Le Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM) est une unité mixte de recherche (UMR 5506). Il regroupe des informaticiens, des microélectroniciens et des roboticiens et mène des recherches dans les domaines de l'informatique, de la robotique et de la microélectronique.

1.2 Historique de l'entreprise

Fondé en 1992, par le CNRS et l'Université de Montpellier, le LIRMM a été créé sur la base de la fusion de deux laboratoires, le CRIM et le LAMM. Depuis sa création, le LIRMM s'est développé et a étendu ses domaines de recherche, s'inscrivant désormais dans le contexte de l'i-Site MUSE.

1.3 Mission et Vision

Le LIRMM a pour mission de mener des recherches d'excellence dans les domaines de l'informatique, de la robotique et de la microélectronique, et de contribuer au transfert de technologies vers le monde économique. Ainsi, le LIRMM souhaite être un acteur majeur de l'innovation et du développement économique régional, en associant étroitement recherche d'excellence, transfert de technologies et compétences dans le domaine des TIC.

1.4 Valeurs

Tout d'abord, le LIRMM est engagé dans une démarche de développement durable et de réduction de son impact environnemental. De plus, Le LIRMM promeut la science ouverte et l'accès libre aux publications et aux données de recherche. Enfin, le LIRMM est engagé en faveur de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations.

1.5 Structure de l'entreprise

Le LIRMM est organisé en trois départements scientifiques : Informatique (INFO), Microélectronique (MIC) et Robotique (ROB). Chaque département est subdivisé en équipes de recherche.

1.6 Produits/Services

Le LIRMM offre des services de recherche et développement, de transfert de technologies et d'expertise dans les domaines de l'informatique, de la robotique et de la microélectronique.

1.7 Clientèle cible

Le LIRMM s'adresse aux entreprises, aux organismes de recherche et aux institutions académiques qui souhaitent bénéficier de son expertise et de ses compétences en matière de recherche et d'innovation.

1.8 Concurrents

Le LIRMM évolue dans un environnement concurrentiel composé d'autres laboratoires de recherche, centres de recherche et développement, et entreprises spécialisées dans les domaines de l'informatique, de la robotique et de la microélectronique.

1.9 Stratégie commerciale

Le LIRMM met en œuvre une stratégie commerciale basée sur le transfert de technologies, la création de start-up et de spin-off, l'accompagnement scientifique de projets de création d'entreprise, les collaborations directes contractualisées et les collaborations à travers des projets de recherche labellisés et financés par des acteurs régionaux, nationaux ou européens.

1.10 Réalisations et Succès

Les recherches menées au LIRMM trouvent généralement une finalisation dans des domaines applicatifs aussi divers que la biologie, la chimie, les télécommunications, la santé, l'environnement, et ont donné lieu à de nombreuses publications scientifiques, brevets et récompenses.

1.11 Perspectives d'avenir

Le LIRMM s'inscrit dans le contexte de l'i-Site MUSE et poursuit son développement en renforçant ses partenariats avec les acteurs académiques et industriels, en étendant ses domaines de recherche et en contribuant au transfert de technologies et à la création d'entreprises innovantes.

2 Projet

2.1 Présentation du projet

Ce projet porte sur la réduction de la taille des chiffrés sur cryptosystème de Paillier pour des images basée sur des calculs statistiques

2.2 Contexte et problématique

Le projet s'inscrit dans le cadre de la sécurité multimédia et vise à résoudre le problème de la taille des chiffrés obtenus avec le cryptosystème de Paillier, qui est deux fois plus volumineuse que le message initial. Cette situation peut entraîner des difficultés lors du stockage et de la transmission des données chiffrées, en particulier pour les images.

2.3 Objectifs du projet

L'objectif principal du projet est de développer et implémenter une méthode innovante pour réduire la taille des chiffrés sur le cryptosystème de Paillier, en se concentrant sur les images et en utilisant des calculs statistiques. Cette approche permettra d'améliorer l'efficacité du chiffrement et de faciliter le stockage et la transmission des données chiffrées.

2.4 Équipe de recherche et domaine d'expertise

Le projet de recherche est mené au sein de l'équipe ICAR (Image et Interaction), qui fait partie du LIRMM et réunit des chercheurs des départements Robotique et Informatique. Cette équipe se spécialise dans la thématique de l'image et des données visuelles, et ce projet est principalement concerné par l'axe de Sécurité Multimédia.

2.5 Méthodologie et approche

L'approche consistera à explorer et à implémenter des techniques de réduction taille de chiffrés basées sur des calculs statistiques, pour vérifier l'uniformité des chiffrés en fonction d'un paramètre, tout en préservant la confidentialité et l'intégrité des données chiffrées. Les méthodes développées pourront être évaluées et comparées à d'autres implémentations de chiffrement en termes d'intégrité, de confidentialité et performance.

2.6 Livrables attendus

— Un rapport détaillant la méthode développée et les résultats obtenus (compte-rendu hebdomadaire)
— Le code source implémentant la méthode de réduction de la taille des chiffrés et bien plus.
— Une documentation sur le code source.
— Une notice d'installation du programme sur le dépôt GitHub.
— Une notice d'utilisation du programme sur aussi le dépôt GitHub.

3 Objectifs

3.1 Objectifs qualitatifs

— Améliorer la sécurité des données chiffrées : en réduisant la taille des chiffrés sur le cryptosystème de Paillier, le projet vise à faciliter le stockage et la transmission des données sensibles, en particulier pour les images, sans compromettre la sécurité et l'intégrité des informations.

— Développer des compétences techniques en sécurité multimédia : en menant des recherches sur la réduction de la taille des chiffrés et en utilisant des calculs statistiques, le projet permettra de renforcer l'expertise de l'équipe ICAR dans le domaine de la sécurité multimédia.

— Contribuer à l'avancement de la recherche scientifique : les résultats du projet seront partagés avec la communauté scientifique à travers des publications, des conférences et des collaborations, contribuant ainsi à l'avancement des connaissances dans le domaine de la sécurité des données et du traitement des images.

— Renforcer les partenariats académiques et industriels : en collaborant avec des partenaires intéressés par les applications de la sécurité multimédia et la protection des données, le projet permettra de créer et de renforcer des liens avec des acteurs clés du secteur.

3.2 Objectifs quantitatifs

— Réduction de la taille des chiffrés : le projet vise à réduire la taille des chiffrés d'au moins 30% par rapport à la taille initiale, sans perte de sécurité ni d'intégrité des données.

3.3 Cible

Le projet de recherche sur la réduction de taille des chiffrés sur cryptosystème de Paillier pour des images s'adresse principalement aux professionnels et aux chercheurs du domaine de la sécurité multimédia et du traitement des images. Les utilisateurs potentiels des méthodes et des outils développés dans le cadre du projet sont :

— Les entreprises et les organisations qui traitent et stockent des données sensibles, en particulier des images, et qui ont besoin de solutions de chiffrement efficaces et sécurisées.

— Les chercheurs et les étudiants travaillant dans le domaine de la sécurité multimédia, du traitement des images et de la cryptographie, qui pourront bénéficier des avancées et des connaissances générées par le projet.

— Les partenaires académiques et industriels impliqués dans la recherche et le développement de solutions pour la sécurité des données et la protection de la vie privée.

4 Caractéristiques

Le programme devra être supporté sur Windows, mais aussi Linux et éventuellement macOS. La diffusion sera principalement Open-Source, ainsi Le code source du programme sera gratuit et disponible sur GitHub tout au long de son développement, conformément au principe de science ouverte du LIRMM. Il s'agira d'un programme de sécurité.
En ce qui concerne les programmes existants, on retrouve des applications de chiffrement de partition, comme Folder Lock et CryptBox, ou encore qui permettent de chiffrer des clés USB, Rohos Mini Drive, ou de protéger des keylogger comme ProxyCrypt. Certaines applications proposent de nombreuses méthodes de chiffrement tel que VeraCrypt.

5 Fonctionnalités

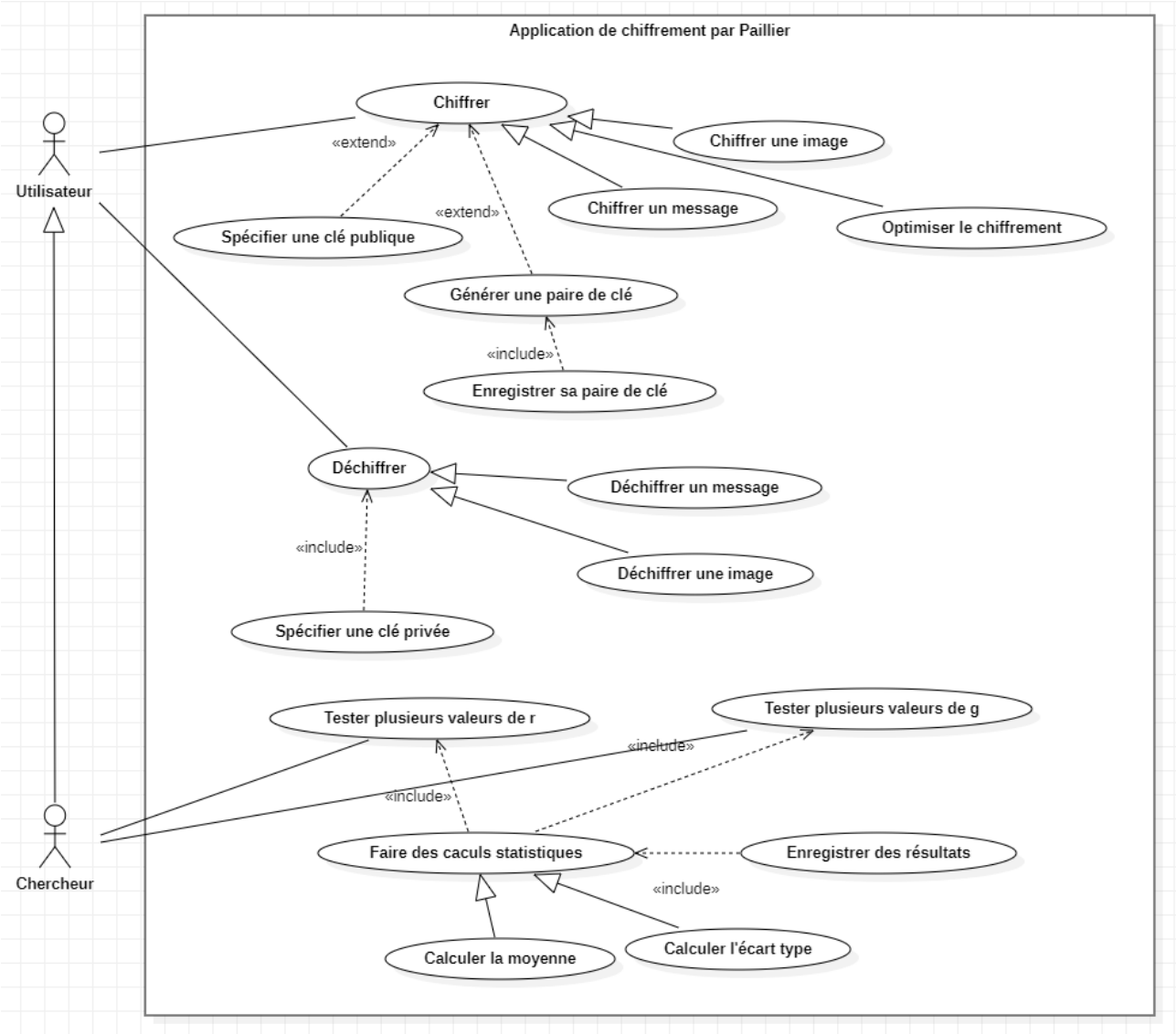

FIGURE 5.1 – Diagramme des cas d'utilisation du programme

En s'appuyant sur la figure 5.1, le programme devra implémenter les fonctionnalités suivantes :

- Chiffrement et déchiffrement d'image : Le programme sera capable de chiffrer et de déchiffrer des images en nuances de gris au format .pgm en utilisant le cryptosystème de Paillier.
- Optimisation de la taille du chiffré : Le programme offrira différentes méthodes d'optimisation de la taille du chiffré, telles que la distribution du pixel chiffré sur deux pixels et l'expansion d'histogramme.

- Gestion des clés : Le programme permettra de générer, d'enregistrer les clés privées et publiques nécessaires au chiffrement et au déchiffrement des images.
- Gestion des arguments : Le programme offrira la possibilité de préciser de nombreux arguments pour son lancement tel que :
  - Le mode chiffrement ou déchiffrement.
  - Le chemin de fichier de l'image en claire ou chiffrée.
  - Si l'on souhaite générer une clé, on pourra préciser les paramètres de sa génération.
  - Si on souhaite utiliser une clé publique ou privée existante, on devra pouvoir préciser le chemin de ce fichier binaire.
  - Si l'on souhaite ou non effectuer une expansion d'histogramme.
  - Si l'on souhaite distribuer le pixel chiffré sur deux pixels.
- Vérification des arguments : Le programme vérifiera la validité des arguments entrés par l'utilisateur pour éviter les erreurs et faciliter son utilisation.
- Ergonomie et facilité d'utilisation : Le programme sera conçu pour être facile à utiliser par les utilisateurs non techniques, avec des messages d'erreur utiles, des instructions claires et des temps de chargement et de traitement raisonnables.
- Calculs statistiques : La structure du code source devra avoir une partie dédiée aux calculs statistiques sur les différentes implémentations du cryptosystème de Paillier, permettant ainsi d'effectuer des comparaisons.
- Modularité et extensibilité : Le programme sera développé en respectant les principes SOLID, afin de garantir sa modularité et son extensibilité pour permettre l'ajout de fonctionnalités supplémentaires de manière simple et l'optimisation de la taille du chiffré en jouant avec tous les paramètres.

6 Contraintes

OpenSSL est une bibliothèque logicielle open source largement utilisée et appréciée pour sa mise en œuvre fiable et sécurisée de divers algorithmes cryptographiques, dont le cryptosystème RSA. Dans le cadre de notre projet, nous pourrions nous inspirer de la rigueur et de la qualité de l'implémentation d'OpenSSL pour garantir la sécurité et la fiabilité de notre propre implémentation du cryptosystème de Paillier. En nous inspirant d'OpenSSL, un logiciel apprécié pour sa mise en œuvre fiable et sécurisée de divers algorithmes cryptographiques, nous pouvons définir les contraintes techniques suivantes pour notre projet.

6.1 Contraintes techniques

— Compatibilité multiplateforme : Le programme doit être développé en C++ et être compatible avec différents systèmes d'exploitation (Windows, Linux), ce qui implique de prendre en compte les spécificités de chaque plateforme et d'écrire un code portable.
— Adaptation des chemins de fichiers : Le programme doit être capable de gérer les différences de conventions de chemins de fichiers entre les systèmes d'exploitation, ce qui implique de prévoir des mécanismes d'adaptation pour assurer la compatibilité.
— Compatibilité avec le format d'image .pgm : Le programme doit être capable de chiffrer et de déchiffrer des images en nuances de gris au format .pgm, ce qui implique de prendre en compte les spécificités de ce format et de développer les fonctions de lecture et d'écriture adaptées.
— Utilisation du cryptosystème de Paillier : Le programme doit être basé sur le cryptosystème de Paillier, ce qui implique de maîtriser les principes de fonctionnement de cet algorithme et de l'implémenter correctement pour garantir la sécurité des données chiffrées.
— Gestion des ressources : Le programme doit être conçu pour optimiser l'utilisation des ressources système (mémoire, processeur, etc.) et offrir des performances satisfaisantes, même lors du traitement d'images de grande taille.
— Modularité et extensibilité : Le programme doit être conçu selon les principes SOLID pour garantir sa modularité et son extensibilité, facilitant ainsi l'ajout de nouvelles fonctionnalités et l'adaptation aux évolutions futures.

6.2 Contraintes ergonomiques

— Ergonomie et facilité d'utilisation : Le programme doit être conçu pour être facile à utiliser par les utilisateurs non techniques, avec des messages d'erreur utiles, des instructions

claires et des temps de chargement et de traitement raisonnables.
— Documentation et support : Nous devons fournir une documentation complète et précise sur notre programme, y compris des instructions d'installation, des exemples d'utilisation et des explications sur les fonctionnalités et les algorithmes utilisés.

6.3 Contraintes juridiques

— Science ouverte : Le code source du programme doit être gratuit et disponible sur GitHub, conformément au principe de science ouverte du LIRMM, ce qui implique de documenter correctement le code et de gérer les éventuelles contributions externes.
— Respect des principes de Kerckhoffs : Le programme doit respecter certains principes de Kerckhoffs, tels que la simplicité d'utilisation et l'absence de connaissance d'une longue série de règles à observer pour les utilisateurs.
— Respect des licences et droits d'auteur : Le programme doit respecter les licences des logiciels et des bibliothèques utilisées dans son développement et ne pas enfreindre les droits d'auteur.

7 Structure

Le C++ étant un langage orienté objet, nous appliquerons le principe SOLID et les design patterns pour faciliter le développement.
En termes de packages, nous partirons sur cette base :

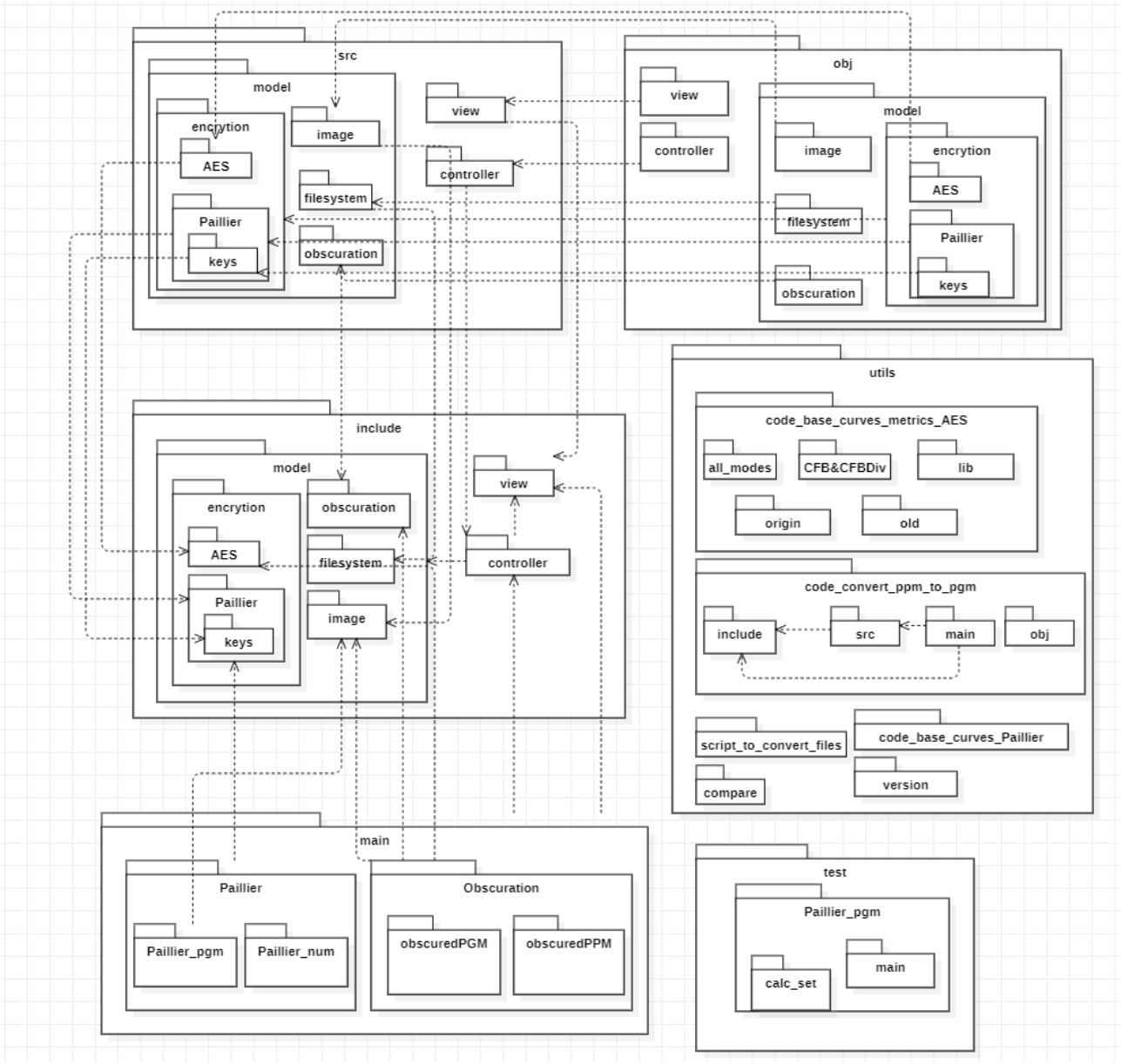

FIGURE 7.1 – Diagramme de package de la structure du code

8 Déroulement du projet

Le suivi du développement sera effectué avec des compte-rendus d'activité et des réunions hebdomadaires.

Bibliographie

[1] ANSSI. (2023). L'ANSSI publie le panorama de la cybermenace 2023. https://cyber.gouv.fr/actualites/lanssi-publie-le-panorama-de-la-cybermenace-2023

[2] LIRMM. (s.d.). Chiffres clés. https://www.lirmm.fr/chiffres-cles/

[3] IONOS. (s.d.). Logiciels de chiffrement : les meilleures solutions pour crypter vos données. https://www.ionos.fr/digitalguide/serveur/securite/logiciels-de-chiffrement/

[4] Avast. (s.d.). Les meilleurs logiciels de chiffrement de 2023. https://www.avast.com/fr-fr/c-best-encryption-software

[5] Putaux, P., Vialle, M., & Puech, W. (2020). Homomorphic Encryption-Based LSB Substitution for High Capacity Data Hiding in the Encrypted Domain. IEEE Access, 8, 111547-111562. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9115625

[6] Simkin, M. (s.d.). Michael Simkin's Home Page. https://msimkin.github.io/

[7] Cahier des Charges. (s.d.). Cahier des charges - Développement logiciel informatique. https://cahiersdescharges.com/telechargement/cahier-charges-developpement-logiciel-informatique/

Table des figures

5.1 Diagramme des cas d'utilisation du programme 8

7.1 Diagramme de package de la structure du code 12