[Titre du document]

[Attirez votre lecteur avec un résumé attrayant. Il s’agit généralement d’une brève synthèse du document. Lorsque vous êtes prêt à ajouter votre contenu, cliquez ici et commencez à taper.]

[Sous-titre du document]

Tables des matières

[I. Introduction 2](#_Toc128067391)

[1. Objectif du projet 2](#_Toc128067392)

[2. Présentation du chiffrement solitaire 2](#_Toc128067393)

[II. Analyse et conception 2](#_Toc128067394)

[1. Analyse des besoins 2](#_Toc128067395)

[a. Fonctionnalités attendues 2](#_Toc128067396)

[b. Utilisateurs de l’application 2](#_Toc128067397)

[c. Sécurité 2](#_Toc128067398)

[d. Performance 2](#_Toc128067399)

[2. Conception de l’application 2](#_Toc128067400)

[a. Diagramme de classe 2](#_Toc128067401)

[b. Diagramme de dépendances 2](#_Toc128067402)

[c. Conception de l’algorithme 2](#_Toc128067403)

[d. Conception de l’interface utilisateur 2](#_Toc128067404)

[e. Tests unitaires 2](#_Toc128067405)

[III. Tests et résultats 2](#_Toc128067406)

[1. Scénario des tests 2](#_Toc128067407)

[2. Résultats des tests 2](#_Toc128067408)

[IV. Conclusion 2](#_Toc128067409)

[1. Bilan du projet 2](#_Toc128067410)

[2. Perspectives d'amélioration 2](#_Toc128067411)

# Introduction

## Objectif du projet

Le projet consiste à utiliser la méthode de cryptographie Solitaire, conçue par le spécialiste de cryptographie Bruce Schneier, qui permet de coder des messages à l'aide d'un jeu de 54 cartes. L'objectif de ce projet est de proposer une méthode de cryptage fiable, équivalente aux meilleurs algorithmes utilisés aujourd'hui, et de concevoir un procédé de création de suites pseudo-aléatoires afin de produire une clé pseudo-aléatoire en continu. Cette méthode de cryptage par addition d'un message avec une clé est considérée comme la seule méthode de cryptographie mathématique prouvée sûre d'une manière absolue. Le projet à tout de même une contrainte, la clé générée doit être de la même longueur que le message à envoyer. Ainsi, la méthode de Schneier peut être utilisée pour crypter des messages avec une sécurité optimale.

## Description de la méthode de cryptage Solitaire

La méthode de cryptage Solitaire est basée sur l'utilisation d'un jeu de cartes pour générer une suite pseudo-aléatoire, qui sera utilisée comme clé de chiffrement. Cette suite est générée en utilisant des mouvements de cartes spécifiques, que nous détaillerons plus tard, qui sont déterminés par un algorithme précis. Cette suite est utilisée pour chiffrer le message en additionnant chaque caractère du message avec la valeur numérique des cartes présente dans la clé de chiffrement.

Pour déchiffrer le message, il suffit d'utiliser la même suite de clés, c’est-à-dire la clé de cryptage pour soustraire chaque caractère chiffré. La sécurité de cette méthode repose sur la complexité de la génération de la suite de clés pseudo-aléatoires, qui rend difficile la détermination de la clé par une personne qui ne possède pas l’ordre du paquet initial. En d’autres termes, l’état du paquet juste avant de commencer à réaliser les manipulations. De plus, cette méthode est particulièrement robuste face aux attaques de type brute force, qui consiste à essayer toutes les combinaisons possibles de clés pour déchiffrer le message.

# Analyse et conception

## Analyse des besoins

### Fonctionnalités attendues

Pour les fonctionnalités attendues de l'application, il est nécessaire de pouvoir générer une clé pseudo-aléatoire de la même longueur que le message à crypter, ainsi que de pouvoir crypter et décrypter des messages à l'aide de cette clé. Nous disposerons également d'une interface utilisateur conviviale pour faciliter l'utilisation de l'application.

### Utilisateurs de l’application

Pour simuler l'utilisation de notre application, nous avons supposé qu'elle serait utile à toute personne souhaitant chiffrer ou déchiffrer un message. La seule condition est que les deux personnes doivent disposer de l'application sur leur ordinateur.

### Sécurité

La sécurité est un élément clé de ce projet. Il est crucial de garantir la confidentialité des messages échangés en utilisant une méthode de cryptage fiable et éprouvée, ainsi qu'en veillant à la sécurité des clés de cryptage générées par l'application.

Étant donné que nous avons choisi de ne pas utiliser de communication réseau, les problèmes de sécurité devraient être limités. Cependant, il est important de s'assurer que la clé de base de la communication entre les deux personnes reste confidentielle. Si quelqu'un découvre l'ordre initial des cartes, la sécurité des messages cryptés pourrait être compromise.

### Performance

En ce qui concerne les performances, l'application devra être en mesure de générer rapidement des clés pseudo-aléatoires de grande longueur, tout en assurant un temps de cryptage et de décryptage raisonnable pour les messages à échanger.

## Conception de l’application

### Diagramme de classe

### Diagramme de dépendances

### Conception de l’algorithme

### Conception de l’interface utilisateur

### Tests unitaires

# Tests et résultats

## Scénario des tests

## Résultats des tests

# Conclusion

## Bilan du projet

## Perspectives d'amélioration