

Outil automatique de décryptage

- Definition de Crypto par Ronald Rivest

- Definition de Crypto par Ronald Rivest

Les 3 critères

- Definition de Crypto par Ronald Rivest

Les 3 critères

- Confidentialité,

- Definition de Crypto par Ronald Rivest

Les 3 critères

- Confidentialité,
- Authenticité,

- Definition de Crypto par Ronald Rivest

Les 3 critères

- Confidentialité,
- Authenticité,
- intégrité

Phases de développement

Phases de développement

- 1 Identification,

Phases de développement

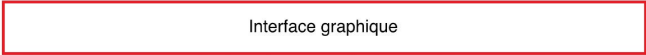
- 1 Identification,
- 2 Définition,

Phases de développement

- 1 Identification,
- 2 Définition,
- 3 Réalisation,

Phases de développement

- 1 Identification,
- 2 Définition,
- 3 Réalisation,
- 4 Finalisation



```
graph TD; A[Interface graphique];
```

Interface graphique

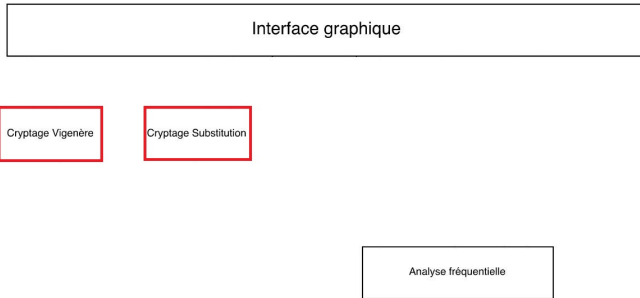
Module principal dont le rôle est de mettre une interface à disposition de l'utilisateur.

Interface graphique

Analyse fréquentielle

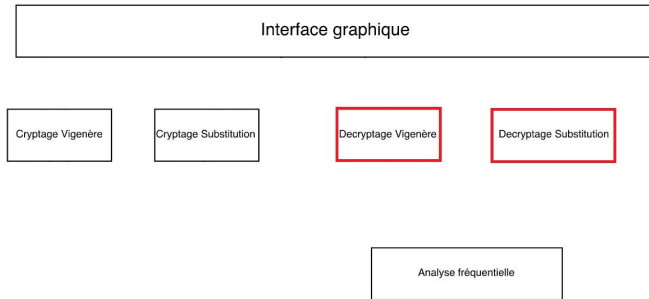
Module qui compte le nombre de caractères, de digrammes et de trigrammes du texte.

Organigramme



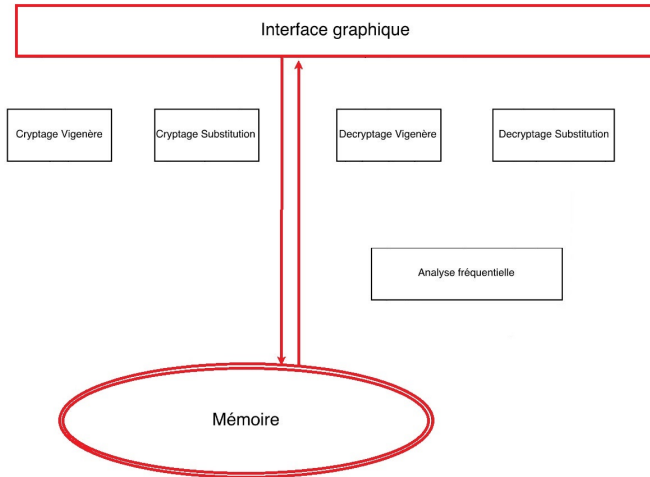
Module permettant le cryptage d'un texte en clair et la génération de clefs de cryptage.

Organigramme



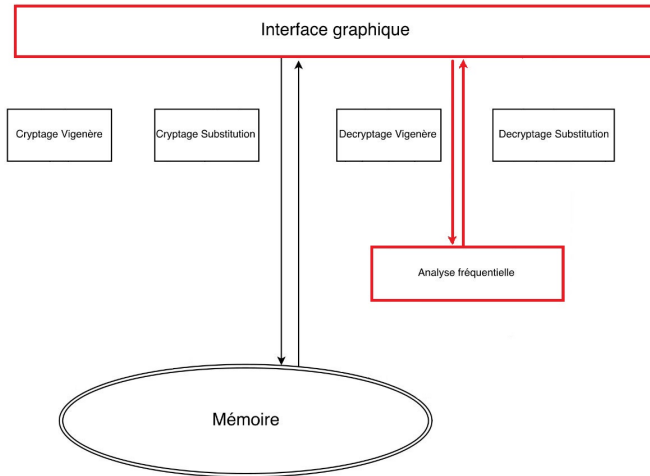
Module qui permet le décryptage d'un texte crypté et la récupération de clefs de cryptages.

Introduction



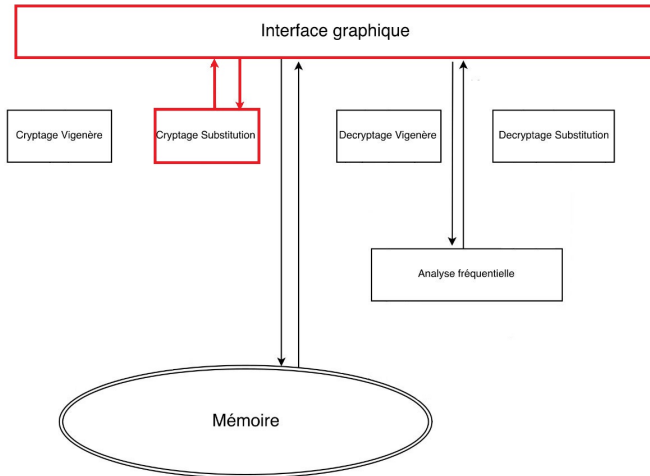
L'interface graphique envoie un nom de fichier et reçoit le texte correspondant.

Organigramme



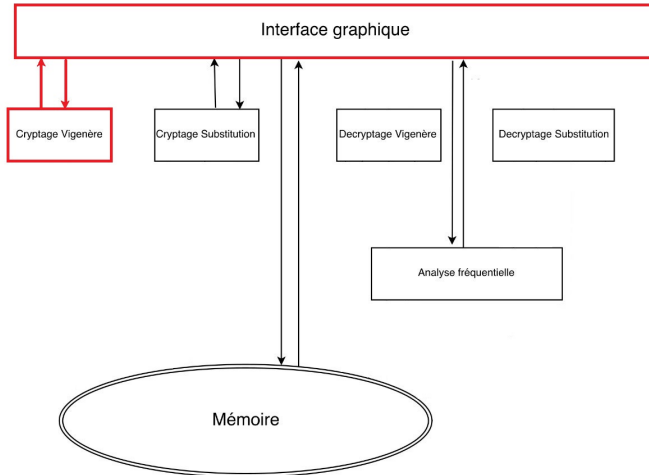
L'interface graphique envoie une chaîne de caractères et reçoit une structure contenant l'analyse fréquentielle.

Organigramme



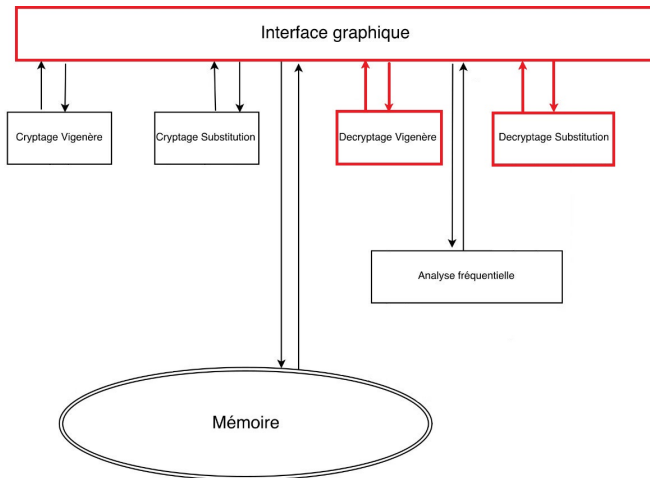
L'interface graphique envoie trois chaînes de caractères. Une contient le texte crypté et deux sont vides et seront remplies par le module de cryptage par substitution.

Organigramme



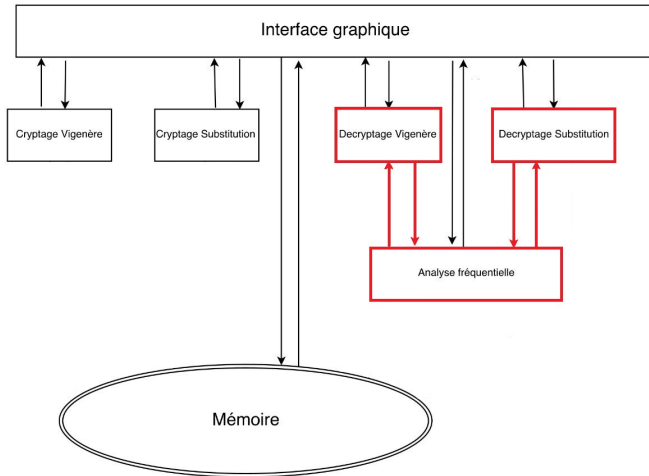
Pour le cryptage par la méthode de vigenère l'interface graphique envoie trois chaînes de caractères dont une contenant le texte en clair, une contenant la clef de cryptage et une vide qui sera remplie par le module.

Organigramme



Pour les deux decryptages, l'interface graphique envoie trois chaînes de caractères. Une correspondant au texte crypté et deux vides qui seront remplies par les deux modules.

Organigramme



L'analyse fréquentielle reçoit une chaîne de caractères contenant le texte à analyser et renvoie une structure contenant l'analyse fréquentielle.

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.
- Réponse : Le langage C
 - Programmation fonctionnelle(idéale pour traitement de données).
 - Langage performant et complet (source : IEEE)
 - Recompilation permet execution sur différents environnements.

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.
- Réponse : Le langage C
 - Programmation fonctionnelle(idéale pour traitement de données).
 - Langage performant et complet (source : IEEE)
 - Recompilation permet execution sur différents environnements.
 - *De plus, langage C maîtrisé par toute l'équipe.

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.
- Réponse : Le langage C
 - Programmation fonctionnelle(idéale pour traitement de données).
 - Langage performant et complet (source : IEEE)
 - Recompilation permet execution sur différents environnements.
 - *De plus, langage C maîtrisé par toute l'équipe.

Les critères de sélection de la bibliothèque graphique

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.
- Réponse : Le langage C
 - Programmation fonctionnelle(idéale pour traitement de données).
 - Langage performant et complet (source : IEEE)
 - Recompilation permet execution sur différents environnements.
 - *De plus, langage C maîtrisé par toute l'équipe.

Les critères de sélection de la bibliothèque graphique

- Besoin de l'application :
 - Création de boutons, Zones de texte, Traitement de fichiers.

Langage et bibliothèque graphique choisie

Les critères de la sélection du langage

- Besoin programmeur :
 - Traitement de données, langage performant et complet, installer l'application sur différents environnements.
- Réponse : Le langage C
 - Programmation fonctionnelle(idéale pour traitement de données).
 - Langage performant et complet (source : IEEE)
 - Recompilation permet execution sur différents environnements.
 - *De plus, langage C maîtrisé par toute l'équipe.

Les critères de sélection de la bibliothèque graphique

- Besoin de l'application :
 - Création de boutons, Zones de texte, Traitement de fichiers.
- Réponse => GTK+ (The GIMP Toolkit) : ensemble de bibliothèques logicielles qui permettent la création d'une interface graphique.
- De plus, bibliothèque complète et non spécifique a un OS.

Utilisation de la librairie de Tests CUnit

Utilisation de la librairie de Tests CUnit

Utilisation de la librairie de Tests CUnit

- CUnit possède les fonctions nécessaires pour gérer une suite de tests.

Utilisation de la librairie de Tests CUnit

- CUnit possède les fonctions nécessaires pour gérer une suite de tests.
- Permet une maintenance et facilite l'amélioration de l'application

Utilisation de la librairie de Tests CUnit

- CUnit possède les fonctions nécessaires pour gérer une suite de tests.
- Permet une maintenance et facilite l'amélioration de l'application
- Les tests lancent les fonctions de façon séparée avec un ASSERT qui vérifie par exemple si une variable contient le résultat attendu.

Utilisation de la librairie de Tests CUnit

- CUnit possède les fonctions nécessaires pour gérer une suite de tests.
- Permet une maintenance et facilite l'amélioration de l'application
- Les tests lancent les fonctions de façon séparée avec un ASSERT qui vérifie par exemple si une variable contient le résultat attendu.

Exemple du lancement d'une suite test

```
Run Summary:  Type  Total  Ran  Passed  Failed  Inactive
               suites    1     1     n/a      0        0
               tests   11    11     11      0        0
               asserts  22    22     22      0       n/a
```

Interface graphique

Interface graphique

- passage d'arguments

Interface graphique

- passage d'arguments
- switch

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

- strcpy

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

- strcpy

Decryptage Vigenere

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

- strcpy

Decryptage Vigenere

- kasiski

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

- strcpy

Decryptage Vigenere

- kasiski

Decryptage Substitution

Interface graphique

- passage d'arguments
- switch
- erreur de mémoire suite à l'enregistrement

Analyse fréquentielle(Tri)

- strcpy

Decryptage Vigenere

- kasiski

Decryptage Substitution

- estimations

Organisation interne et repartition des tâches

Tableau de repartition des tâches

Module	Personne(s)
Décryptage Vigenere	Chouipe et Alabi
Décryptage Substitution	Lienhardt et Alabi
Cryptage Vigenere	El harti et Chouipe
Cryptage Substitution	El harti et Lienhardt
Analyse Fréquentielle	El harti
Interface Graphique	Capdenat et Benyamna

- Organisation
- Répartition des tâches respectée
- Avancement du projet

Points importants

- L'interface graphique
- Codage et tests de chaque module séparément
- Assemblage de l'application
- Priorité

Nombre de lignes de code des modules

Tableau comparatif

Module	Nombre de lignes de code (estimation)	Nombre de lignes de code (avéré)
Décryptage Vigenere	200	160
Décryptage Substitution	150	380
Cryptage Vigenere	50	25
Cryptage Substitution	50	65
Analyse Fréquentielle	50	110
Interface Graphique	1000	1300
Total	1500	

Nombre de lignes de code des modules

Cryptage substitution

Module	Nombre de lignes de code (estimation)	Nombre de lignes de code (avéré)
Décryptage Vigenere	200	160
Décryptage Substitution	150	380
Cryptage Vigenere	50	25
Cryptage Substitution	50	65
Analyse Fréquentielle	50	110
Interface Graphique	1000	1300
Total	1500	

Nombre de lignes de code des modules

Analyse frequentielle

Module	Nombre de lignes de code (estimation)	Nombre de lignes de code (avéré)
Décryptage Vigenere	200	160
Décryptage Substitution	150	380
Cryptage Vigenere	50	25
Cryptage Substitution	50	65
Analyse Fréquentielle	50	110
Interface Graphique	1000	1300
Total	1500	

Nombre de lignes de code des modules

Décryptage substitution

Module	Nombre de lignes de code (estimation)	Nombre de lignes de code (avéré)
Décryptage Vigenere	200	160
Décryptage Substitution	150	380
Cryptage Vigenere	50	25
Cryptage Substitution	50	65
Analyse Fréquentielle	50	110
Interface Graphique	1000	1300
Total	1500	

Nombre de lignes de code des modules

Interface graphique

Module	Nombre de lignes de code (estimation)	Nombre de lignes de code (avéré)
Décryptage Vigenere	200	160
Décryptage Substitution	150	380
Cryptage Vigenere	50	25
Cryptage Substitution	50	65
Analyse Fréquentielle	50	110
Interface Graphique	1000	1300
Total	1500	

Modifications et Améliorations

Modifications et Ameliorations

- Ajouter un dictionnaire
- Modifier Cahier des Specifications

Modifications et Ameliorations

- Ajouter un dictionnaire
- Modifier Cahier des Specifications
- Plus de langues
- Plus de choix de chiffrement

