

Manuel d'utilisation

Dcrypt



29 mai 2017

1 Introduction

L'application Dcrypt est un outil automatique d'aide au decryptage permettant à son utilisateur d'effectuer une cryptanalyse sur un fichier ou un texte à partir d'un ordinateur. Pour cela, le procédé de Vigenère ou de Substitution lui sera proposé.

Le client pourra aussi effectuer le cryptage à l'aide de ces 2 methodes ou encore lancer seulement une analyse frequentielle.

L'application se veut très simple d'utilisation. Ce guide a été conçu afin de répondre à toutes les questions d'utilisation que pourrait avoir le client.

2 Pré-conditions/Materiel necessaire

2.1 Installations requises

Certaines installations sont essentielles à l'utilisation de l'application.

Tout d'abord, celle de la bibliotheque GTK : `sudo apt-get install libgtk2.0-dev`

Enfin, pour Cunit : `sudo apt-get install libcunit1 libcunit1-doc libcunit1-dev`

2.2 Lancement de l'application

commande pour lancer appli : `make run`

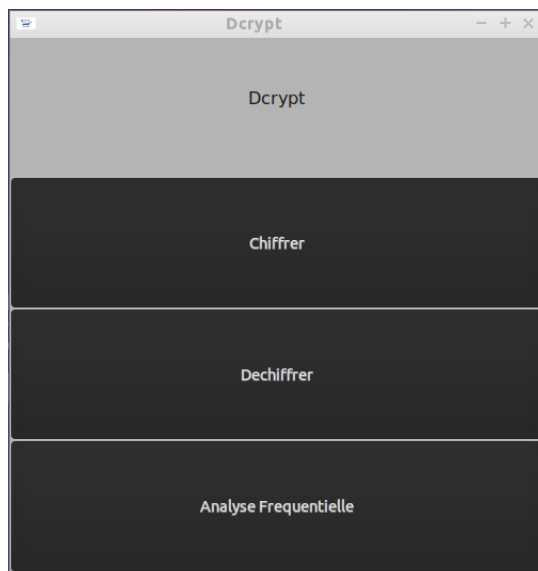
commande pour lancer tests : `make test`

3 Guide d'utilisation

Ce guide pratique a pour objectif de vous guider dans l'utilisation de l'application "Dcrypt" et de répondre aux éventuelles questions que vous pourriez vous poser au cours de son usage.

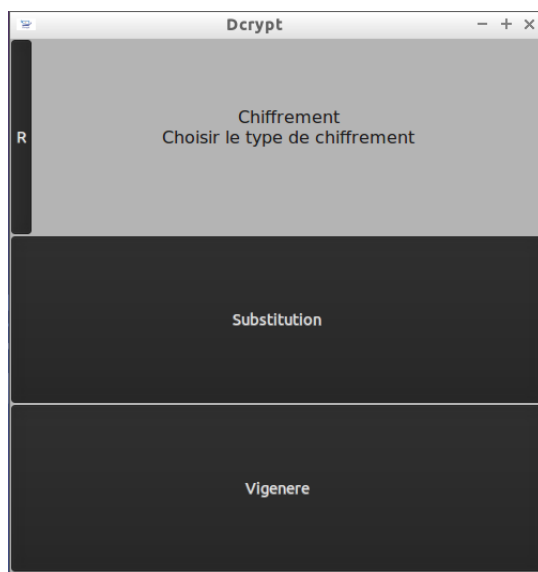
4 Menu/Accueil

Ici, vous vous trouvez sur le menu ou page d'accueil de l'application. Vous pouvez à l'aide de nos 3 boutons effectuer 3 actions différentes. Le premier bouton permet le cryptage (on se trouvera alors en (5)), le second de decrypter un texte (6) et enfin le dernier d'effectuer une analyse fréquentielle seule (7).



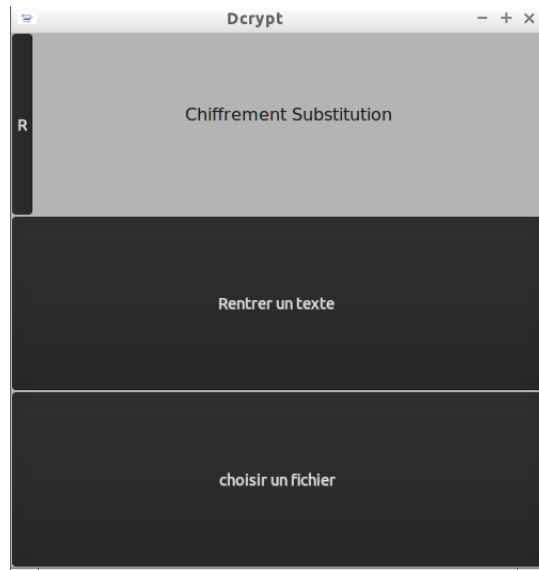
5 Menu Cryptage

Dans le menu cryptage, il est maintenant possible de choisir le type de cryptage voulu. Le choix de l'utilisateur peut alors se porter vers un cryptage par Substitution (5.1) ou bien vers un cryptage par Vigenère (5.2). Il lui est également possible de revenir en arrière (au menu précédent) à l'aide du bouton "R".



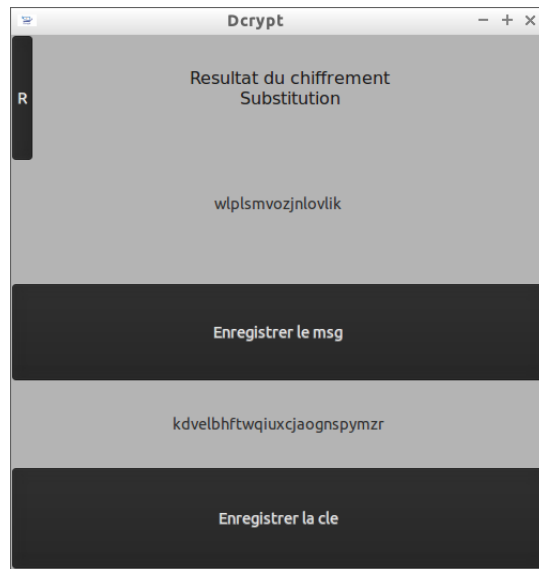
5.1 Cryptage Substitution

Vous pouvez maintenant rentrer/taper votre texte à l'aide de la zone d'entrée (8) ou bien le charger à l'aide de la fenetre de chargement (9).



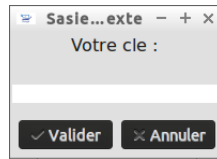
Le resultat sera maintenant affiché.

Vous pouvez maintenant enregistrer la clé et le texte chiffré à l'aide de la fenetre d'enregistrement (9).

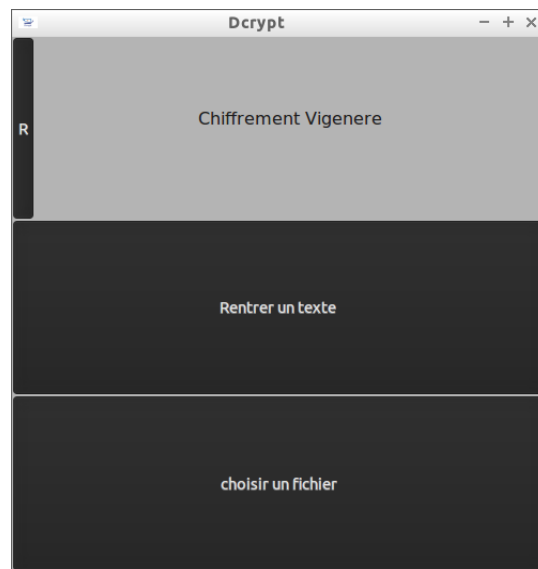


5.2 Cryptage Vigenere

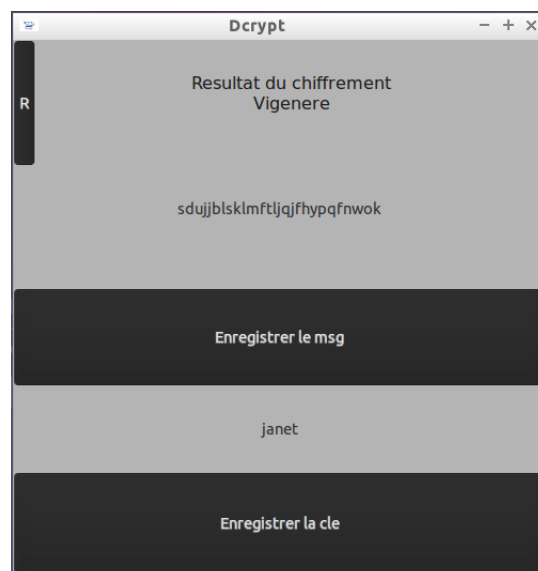
Dans ce menu on vous demande tout d'abord d'entrer la clé de cryptage. Cette dernière ne doit contenir que des lettres et sa taille doit être inférieure ou égale à 12.



À présent, vous devez indiquer le texte que vous voulez crypter. Vous pouvez soit le rentrer directement (8) ou bien le charger (9).

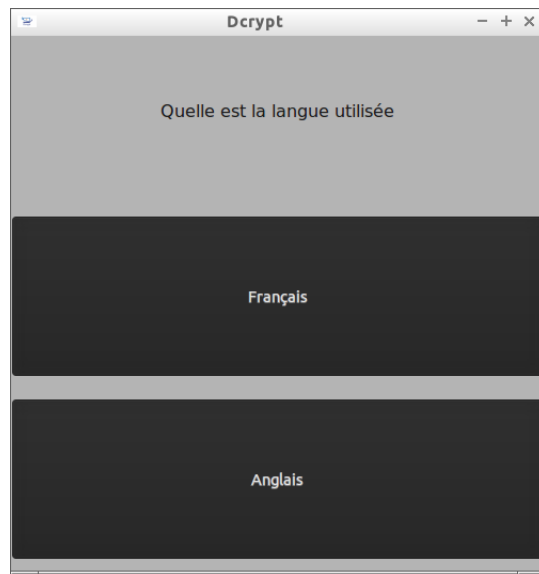


Le résultat sera alors affiché et il est possible pour l'utilisateur d'enregistrer la clé utilisée et le texte maintenant crypté (9).

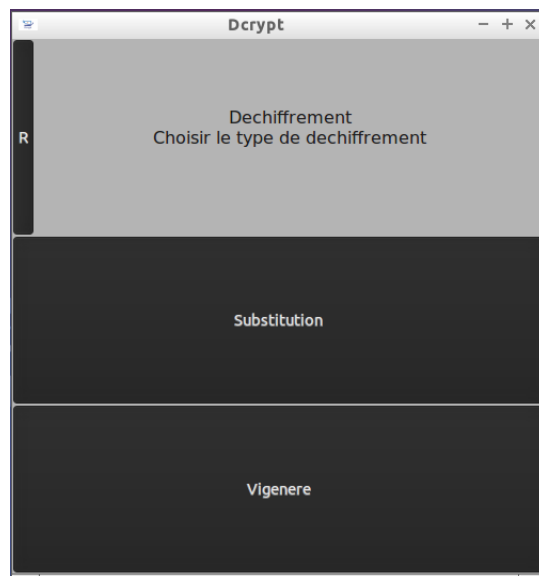


6 Menu Decryptage

Avant tout, vous devez indiquer la langue du texte que vous voulez decrypter.
Les ressources utilisées pour le decryptage ne sont pas les memes en francais et en anglais.

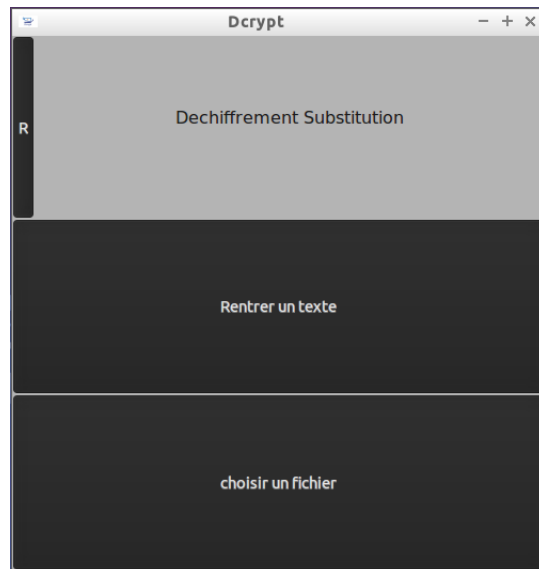


Dans le menu decryptage, vous pouvez soit choisir le type de decryptage (methode de Vigenere ou Substitution) ou bien revenir au menu principal à l'aide du bouton "R".



6.1 Decryptage Substitution

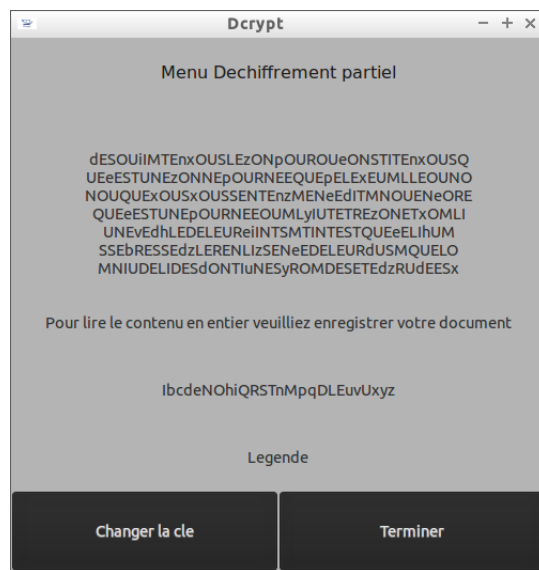
Vous devez desormais rentrer votre texte (8) ou bien le charger (9).



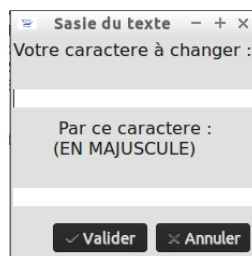
Maintenant vous avez une partie de la clé qui est decryptée et vous allez essayer de trouver quelques autres caracteres.

Exemple :

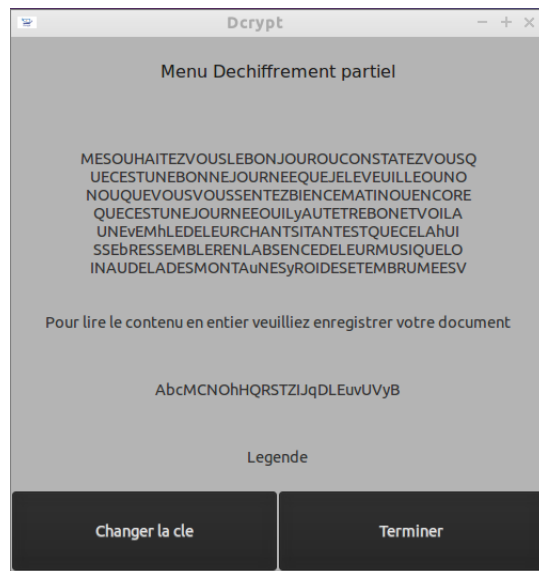
Si le resultat est "kONvOUR...", vous pouvez etre sur que k correspond a B et v a J.



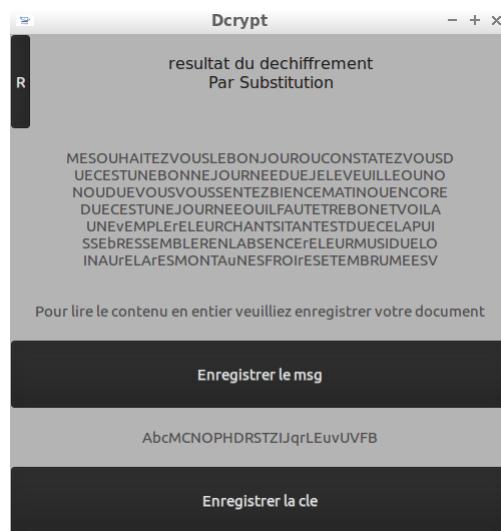
Vous pouvez faire les modifications avec le menu "changer clé".



Au bout de 4 ou 5 caractères retrouvés le texte sera decrypté (car plus de la moitié des caracteres est decryptée par l'application) et vous aurez :

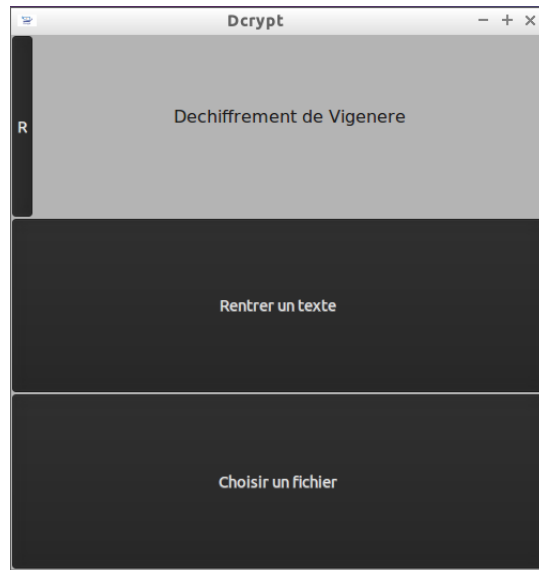


Vous pouvez cliquer sur "terminer" qui vous emmenera sur ce menu qui vous permet comme pour les cryptages d'enregistrer le resultat et la clé.

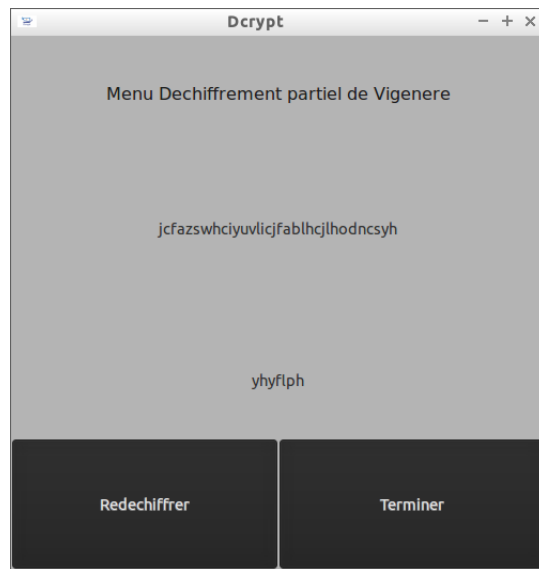


6.2 Decryptage Vigenere

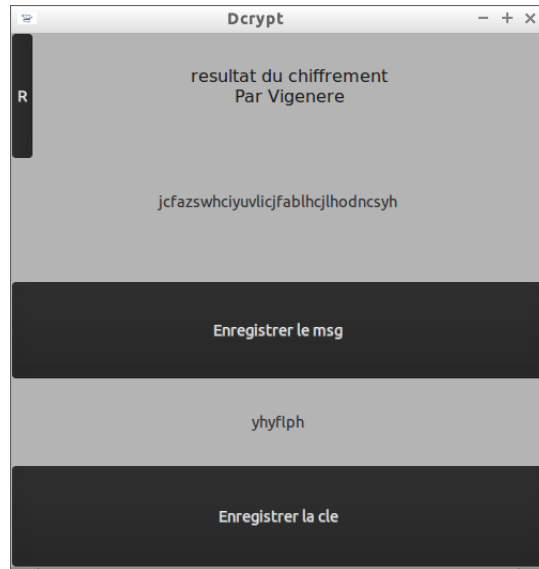
La vous pouvez soit rentrer votre texte a l'aide de la zone d'entrée(8) soit le charger a l'aide de la fenetre de chargement (9).



La vous avez une cle et un texte decrypté, normalement la clé obtenu est la bonne. Si le texte est assez long. Si le texte est illisible alors la clé est incorrecte et dans ce cas il suffit de choisir le bouton "redéchiffrer" qui va ressayer avec une autre taille de clé. Une fois le resultat trouvé vous pouvez a l'aide du bouton terminer aller au menu de resultat final.

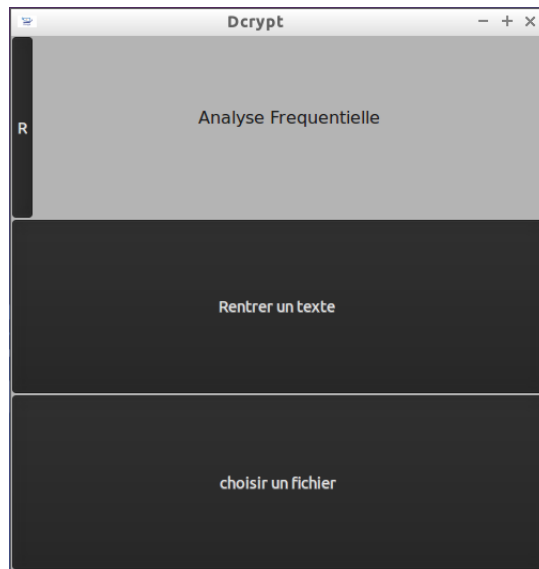


Ce menu vous permet comme pour les cryptages d'enregistrer le resultat et la clé.



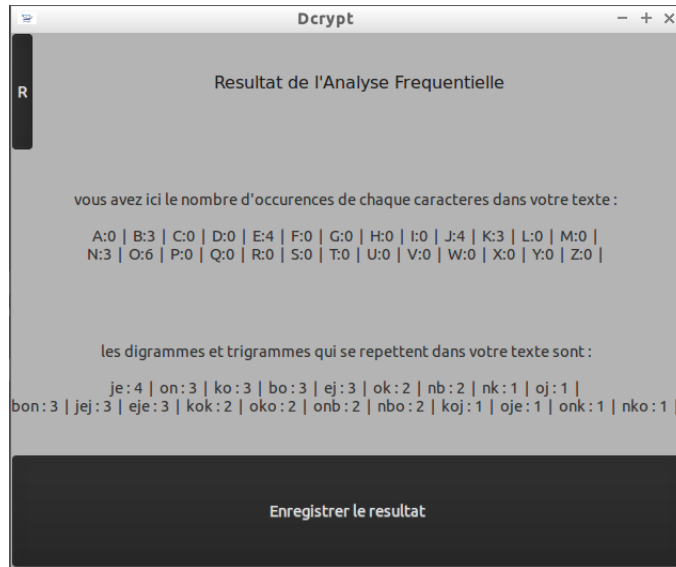
7 Menu Analyse Frequentielle

Afin d'effectuer l'analyse frequentielle sur un texte il faut evidemment le renseigner. Pour se faire, l'utilisateur peut le rentrer directement (8) ou bien charger le texte (9).



Présentement, vous aurez les frequences dans le texte de chaque lettre de l'alphabet ainsi que celle de chaque digramme et trigramme de lettres.

Remarque : Si le texte est trop long, elle n'affichera que ceux qui se repetent le plus.



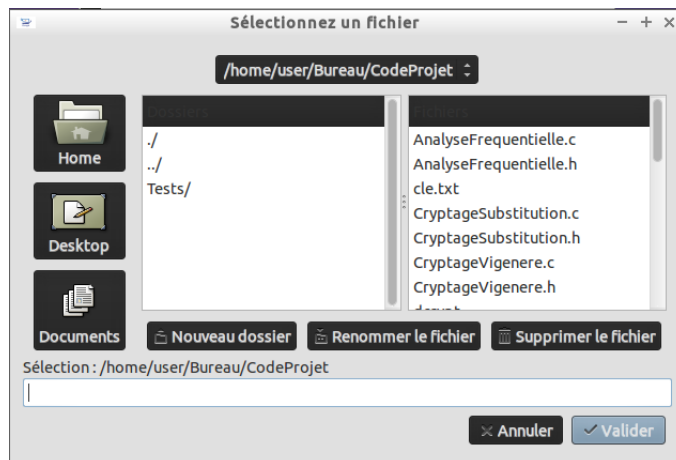
8 Entrer un texte

A chaque fois que vous allez essayer de rentrer un texte cette fenetre s'affichera devant vous.



9 les Chargements/Enregistrement de fichiers

A chaque fois que vous allez essayer de charger un texte cette fenetre aparaitra.



A chaque fois que vous allez essayer d'enregistrer un texte cette fenetre s'affichera devant vous.

