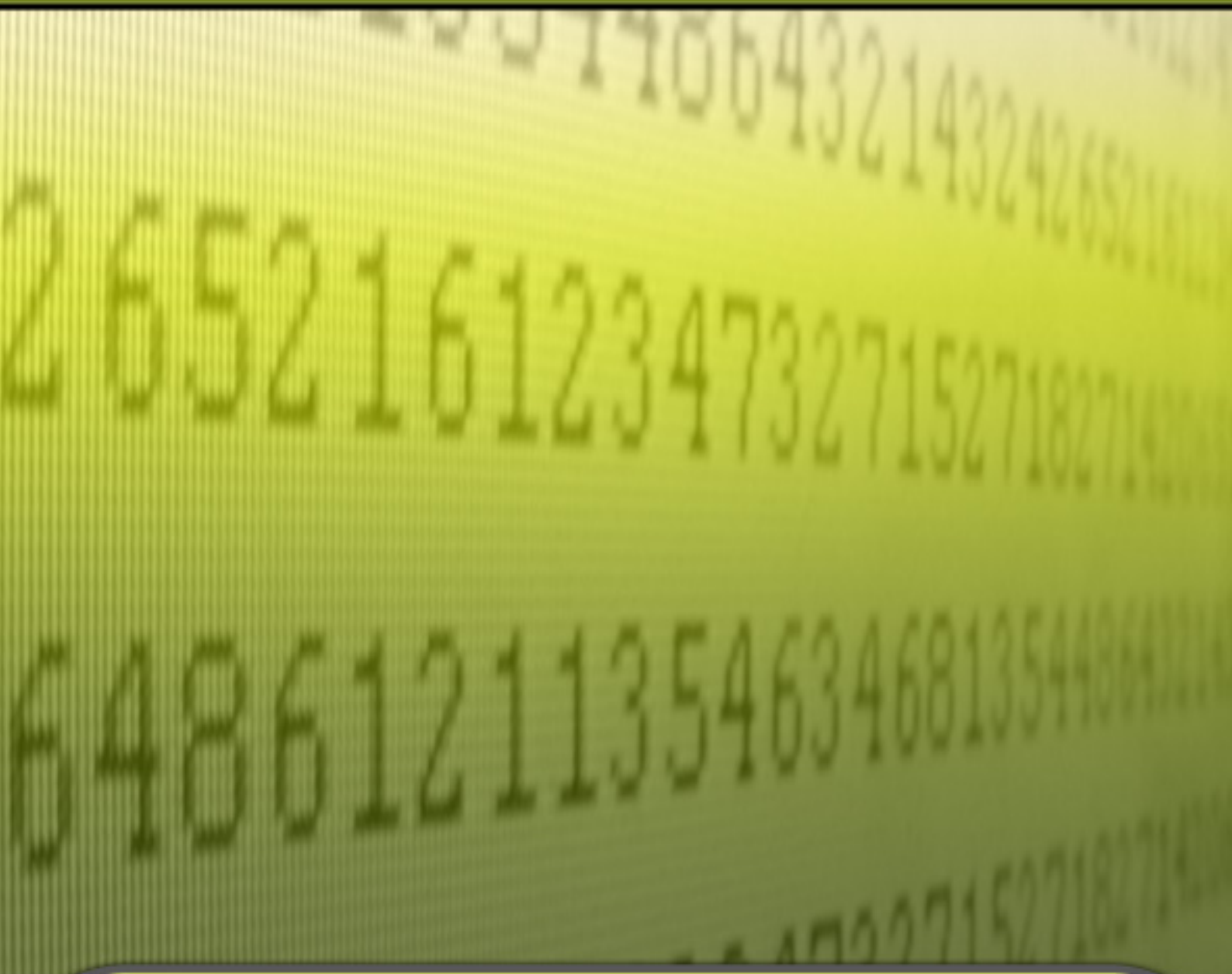
Guide de l'utilisateur

My Crypto

L'encryptage brut



DE BATZ Christophe
LEGUENNEC Alexis Groupe B
HUYHN Pascal

MyCrypto : l'encryptage brut !

Merci d'avoir choisi MyCrypto !

Introduction à MyCrypto

Qu'est-ce que MyCrypto ?

MyCrypto est un programme de chiffrage / déchiffrage écrit en langage C++ et conçu lors d'un projet de programmation des étudiants de deuxième année à l'EFREI. Ce petit programme qui ne nécessite aucune installation, permet à l'utilisateur de chiffrer et de déchiffrer des mots et des textes en choisissant l'algorithme de cryptage voulu. MyCrypto est distribué en License Creative Commons c'est-à-dire que vous pouvez l'utiliser et le modifier à votre guise mais sa distribution ne doit être en aucune façon commerciale.

Ce guide d'utilisateur vous permettra de facilement prendre en main l'interface de traduction. Ce guide vous a été livré avec la version MyCrypto 1.0 build 5.

Compatibilité

Ce programme a été testé sous Windows XP, Windows Vista et Windows 7. Il fonctionne sous Linux également (testé et approuvé en quelques minutes !). Ce programme ne nécessite aucune configuration particulière.

A propos de MyCrypto

Les auteurs du freeware MyCrypto sont trois étudiants de l'Ecole Française pour L'Electronique et l'Informatique (EFREI) :

- **Christophe DE BATZ** : un ex' d'EPITA qui s'est occupé de la conception de l'interface graphique utilisateur (GUI) ainsi que de toute la charte graphique tournant autour du logiciel.

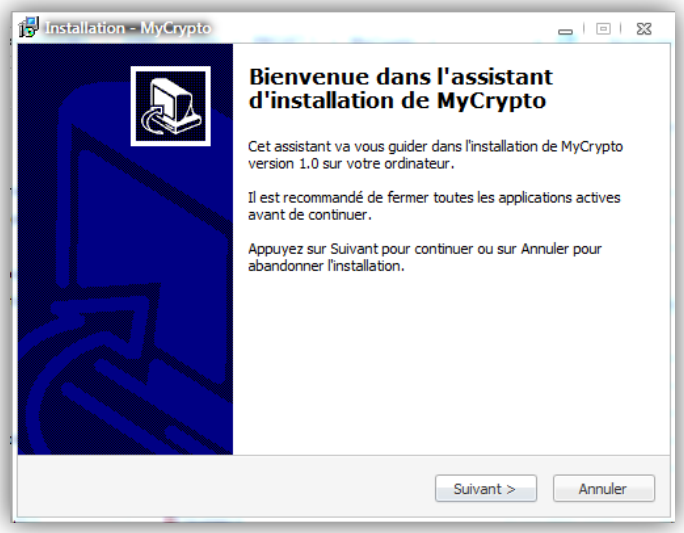
- **Pascal HUYNH** : un ex' de SupInfo. Il s'est occupé de plusieurs fonctions au cœur du projet et notamment de Vigenère.

- **Alexis LEGUENNEC** : encore un ex' SupInfo. Lui s'est occupé d'autres algorithmes dont Scytale.

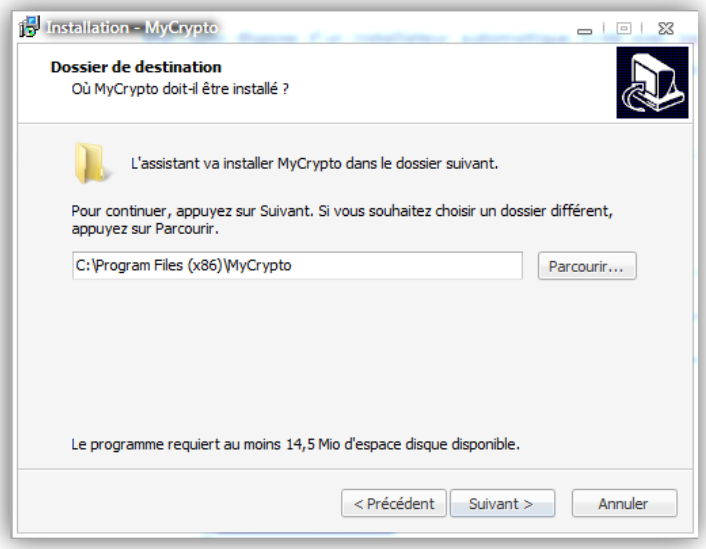
Prise en main et installation

Avec installateur

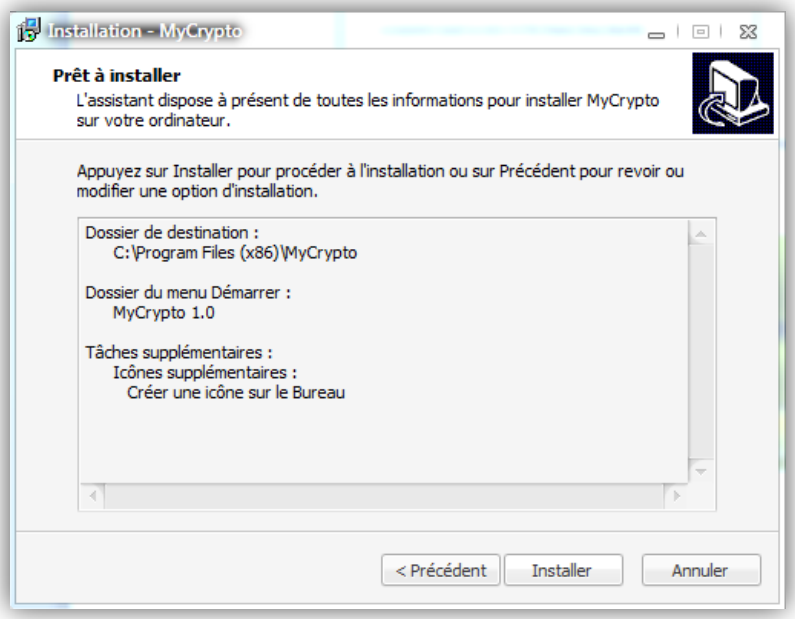
MyCrypto dispose d'un installateur automatique (créé avec innoSetup). Pour installer le programme, vous n'avez donc qu'à lancer le programme « MyCrypto Setup.exe ». La fenêtre suivant devrait s'ouvrir :



Cliquez sur « Suivant »…



Rentrez l'emplacement où devront se copier les fichiers nécessaires au fonctionnement du programme. Remplissez les informations demandés jusqu'à arriver à cet écran :



Vérifiez bien tous les paramètres de l'installation et cliquez sur le bouton « Installer ». L'installateur va créer automatiquement les raccourcis d'utilisation à votre place et vous proposera de dans MyCrypto dès la fin de l'installation !

Sans installateur

Ce programme ne nécessite pas forcément d'installation automatique. Pour utiliser MyCrypto sans installation, il vous suffit de :

- Extraire l'archive « MyCrypto 1.0.rar » dans un dossier de votre choix.
- Cliquer sur le fichier « MyCrypto 1.0.exe » situé dans « MyCrypto 1.0/exec/ ».

Vous pouvez facilement créer un raccourci de ce fichier exécutable via le menu contextuel.

Utilisation

Chiffrage

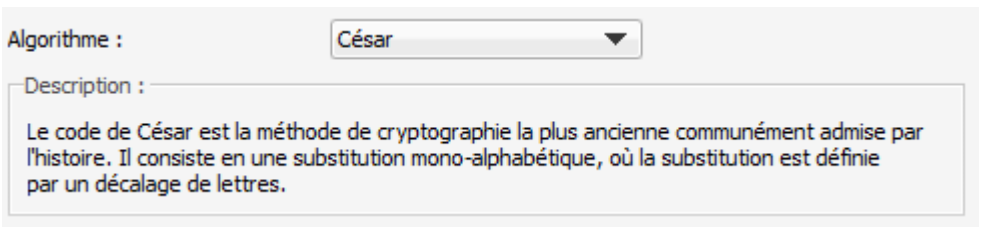
Une fois ouvert, MyCrypto vous permettra de chiffrer une chaîne de caractère en se servant de l'un des quatre algorithmes de d'encryptage mis à disposition. Il s'agit de :

- **César**
- **Scytale**
- **Vigenère**
- **Enigma**

Sélection de l'algorithme de traitement

Vous pouvez sélectionner n'importe lequel à n'importe quel moment en le sélectionnant via la boîte de sélection située tout en haut de la fenêtre, sous le logo MyCrypto (voir la capture ci-dessous).

A noter qu'en sélectionnant un algorithme d'encryptage, le programme vous donnera une brève description sur l'utilisation et l'histoire de celui-ci.



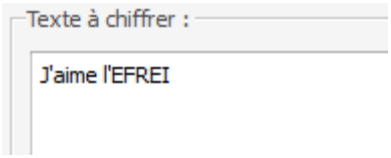
Choix de la clé

La clé de chiffrage ou de déchiffrage va permettre à l'algorithme de crypter ou décrypter votre texte selon certaines règles Ces règles sont en fait cette clé. Selon les algorithmes, il peut y avoir une ou plusieurs clés à renseigner. Le type de donnée peut lui aussi dépendre…

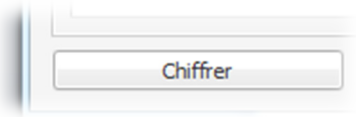
- Pour César, il faudra renseigner un décalage donc un nombre entier.
- Pour Scytale, pareil que pour César.
- Pour Vigenère, la clé doit être une chaîne de caractères.
- Pour Enigma, il y a trois clés numériques à renseigner pour chacun des rotors.

Donnée à chiffrer

Une fois la clé de chiffrage choisie, il est de rigueur d'entrer un texte (qui peut aller de une lettre à un long texte !) à chiffrer dans la zone indiquée.

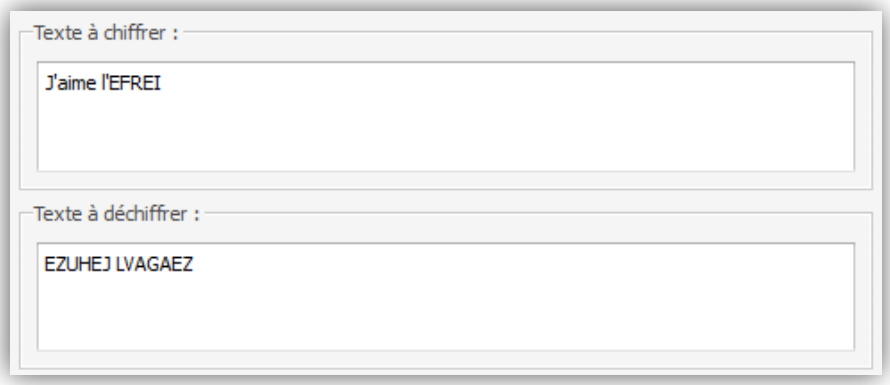


Puis, une fois le texte entré, il faudra valider en cliquant sur le bouton « Chiffrer » situé en bas à gauche.



Lecture du chiffrage

Le résultat du chiffrage sera disponible dans la zone de texte intitulée « Texte à déchiffrer ».



Déchiffrage

Sélection d'un algorithme de déchiffrage

Pour cette première étape, veuillez vous référer à la section « Sélection de l'algorithme de traitement » située plus haut dans ce guide.

Choix de la clé

Pour cette deuxième étape, veuillez vous référer à la section de même nom située plus haut dans ce guide.

Donnée à déchiffrer

Choisissez une donnée (texte, mot, lettre…) à déchiffrer et entrez ce contenu directement dans la zone de texte intitulée « Texte à déchiffrer ».

Lecture du déchiffrage

La lecture du déchiffrage se fait rapidement dans la zone de texte du dessus : « Texte à chiffrer ». Voici un exemple de déchiffrage sous Enigma :

La cryptanalyse

La cryptanalyse permet de restituer un texte chiffré mais sans posséder la clé du chiffrement d'origine. Cette technique n'est pas une science exacte et ne fonctionne donc pas dans tous les cas.

Pour cryptanalyser un texte, il suffit d'entrer ce texte dans la zone de texte « Texte à déchiffrer ». Vous pouvez à présent enlever la clé (mettre à 0 ou à vide) et cliquer sur le bouton « Cryptanalyse ». Le résultat apparaîtra ainsi dans la zone de texte « Texte à chiffrer ».

Les meilleurs résultats sont obtenus pour l'algorithme de César à condition d'avoir une phrase avec quelques « e » (l'algorithme se base en effet sur cette lettre très utilisée en Français pour cryptanalyser).