Safe for all version 1.0
Logiciel de chiffrement-déchiffrement-attaque en JAVA

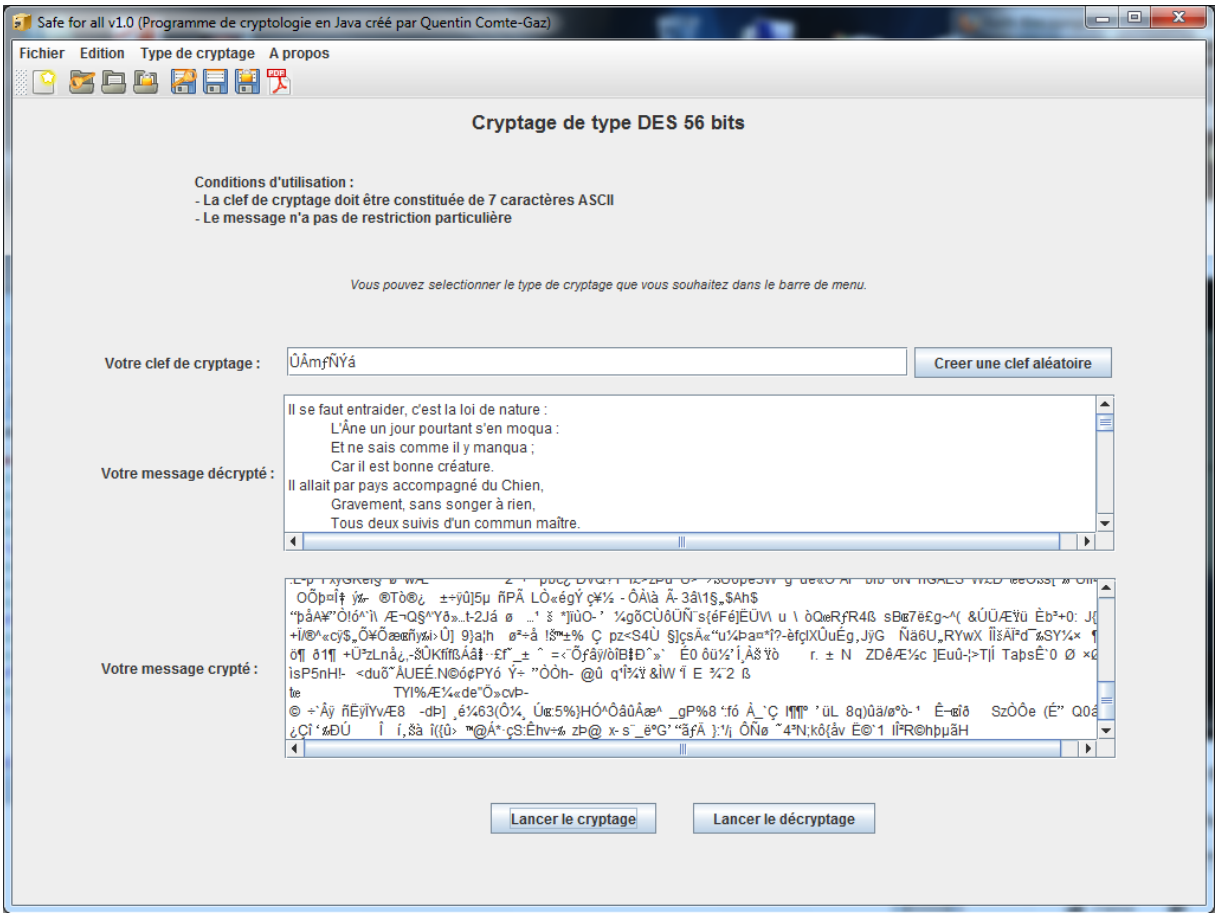
Par Quentin Comte-Gaz

Sommaire

1 Introduction

Safe for all v1.0 est une application de cryptographie en JAVA.
Elle permet entre autre de chiffrer-déchiffrer ses données avec les chiffrements DES, Vigenère, César et César amélioré.
Il est également possible d'ouvrir/enregistrer une clef de chiffrement, un texte clair et un texte crypté.
Enfin, il est possible d'exporter le projet (clef+texte clair+texte chiffré) au format PDF.
Cette application est téléchargeable à l'adresse : http ://quentincg.free.fr/safeforall/

Voici l'apparence de l'application :



2 Les différents chiffrements possibles

2.1 DES 56 bits

Le Chiffrement DES permet de chiffrer n'importe quel type de message (en ASCII).
Ce chiffrement est attaquable, mais demande une certaine puissance de calcul.
Ainsi, l'AES est correct pour des échanges de faibles importances même si l'AES est bien plus fiable.

Exemple concret :
Clef : "§?ð½®£)"
Message : "Bonjour, j'ai 5 ans!? :)"
Message chiffré : "¶? ûuK ó‘ 9/h??wCm??MÃ 4.,T?Uû"

Brève explication de ce chiffrement :
Le DES (Data Encryption Standard) est un standard de chiffrement avancé non linéaire faisant notamment intervenir des XOR et des permutations.

2.2 Vigenère classique

Le Chiffrement de Vigenère ne permet de chiffrer que les lettres en majuscules.
Le logiciel ne va donc ni chiffrer, ni conserver, les autres caractères (notons quand même qu'il transforme les lettres minuscules en lettres majuscules).
Ce chiffrement est facile à attaquer si la longueur de la clef est très inférieure à celle du message.
Au contraire, si la longueur de la clef est égale à celle du message, il est alors impossible d'attaquer ce chiffrement.

Exemple concret :
Clef : "AZERTYUIOP"
Message : "BONJOURMOICESTQUENTIN"
Message chiffré : "BNRAHSLUCXCDWKJSYVHXN"

Brève explication de ce chiffrement :
Il permet de remplacer une lettre par une autre qui n'est pas toujours la même. Pour ce faire on utilise un tableau à double entrée.

2.3 Vigenère amélioré

Ce chiffrement est l'amélioration logique du chiffrement de Vigenère.
Il permet de chiffrer tous les lettres minuscules et majuscules et ne supprime pas les éléments de la table ASCII.
Ce chiffrement est facile à attaquer si la longueur de la clef est très inférieure à celle du message.
Au contraire, si la longueur de la clef est égale à celle du message, il est alors impossible d'attaquer ce chiffrement.

Exemple concret :
Clef : "AZERTYUIOPQSDSGFBC"
Message : "Bonjour, j'ai 5 ans ! ? :)"
Message chiffré : "Bnrahsl, y'sl 5 bps ! ? :)"

Brève explication de ce chiffrement :
Il permet de remplacer un caractère par un autre qui n'est pas toujours le même. Pour ce faire on utilise un tableau à double entrée.

2.4 César classique

Le Chiffrement de César ne permet de chiffrer que les lettres en minuscules et en majuscules.
Le logiciel ne va donc pas chiffrer les autres caractères, mais va cependant les conserver.
Ce chiffrement est l'un des plus faciles à attaquer (26 clefs possibles).

Exemple concret :
Clef : "12"
Message : "Bonjour, j'ai 5 ans ! ? :)"
Message chiffré : "Nazvagd, v'mu 5 mze ! ? :)"

Brève explication de ce chiffrement :
Il consiste en une substitution de lettres par une autre plus loin dans l'alphabet. Par exemple, si l'on utilise un décalage de 3, A serait remplacé par D, B deviendrait E, et ainsi de suite.

2.5 César amélioré

Le chiffrement de César ne permet pas de chiffrer tous les caractères de la table ASCII.
Il faut donc utiliser le chiffrement de César amélioré pour les chiffrer.
Ce chiffrement est facilement attaquable (224 clefs possibles).

Exemple concret :
Clef : "122"
Message : "Bonjour, j'ai 5 ans ! ? :)"
Message chiffré : "$\frac{1}{4}$éèäéïì ?ä Ûã ?Ûèí ? ? ? £"

Brève explication de ce chiffrement :
Il consiste en une substitution d'un caractère par une autre plus loin dans la table ASCII. Par exemple, si l'on utilise un décalage de 110, "-" serait remplacé par ">" et ainsi de suite.

3 Création (aléatoire) de clefs

3.1 DES 56 bits

La clef de chiffrement du DES 56 bits est constituée de sept caractères quelconques.
Il est possible de générer aléatoirement une clef de cette nature en cliquant sur "Creer une clef aléatoirement".

3.2 Vigenère classique-amélioré

La clef de chiffrement de Vigenère est constituée uniquement de lettres.
Sachez que plus votre clef est longue, plus votre message sera sécurisé.
En effet, une clef de longueur égale à celle du message rend le message chiffré inviolable.
Il est possible de générer aléatoirement une clef de 26 lettres en cliquant sur "Creer une clef aléatoirement".

3.3 César classique-amélioré

La clef de chiffrement de César classique est un nombre compris entre 0 et 26.
Pour le César amélioré, la clef est comprise entre 0 et 224.
Il est possible de générer aléatoirement une clef de cette nature en cliquant sur "Creer une clef aléatoirement".

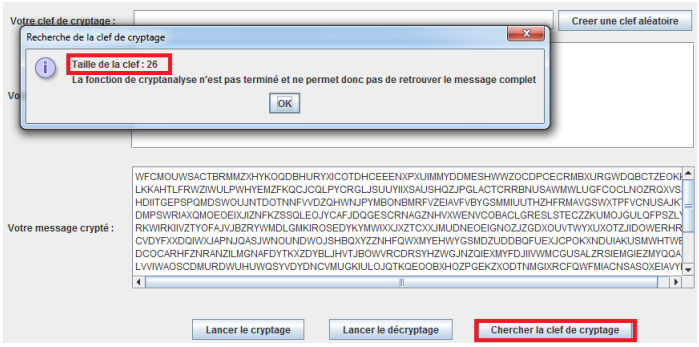
4 Les attaques

4.1 DES 56 bits

L'attaque du chiffrement DES est possible mais prendrait bien trop de temps pour un ordinateur classique.
Je n'ai donc pas implémenté cette fonction.

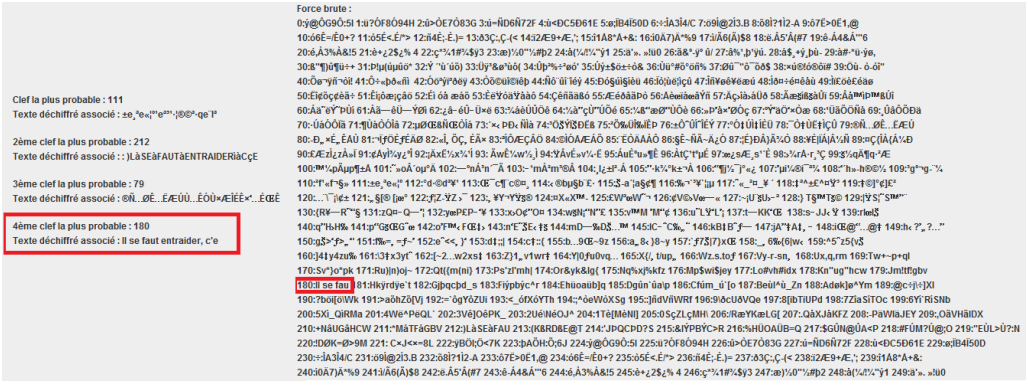
4.2 Vigenère classique-amélioré

L'attaque du chiffrement Vigenère est en cours de conception.
Vous pouvez pour le moment connaitre la longueur de la clef en cliquant sur "Chercher la clef de chiffrement".



4.3 César classique-amélioré

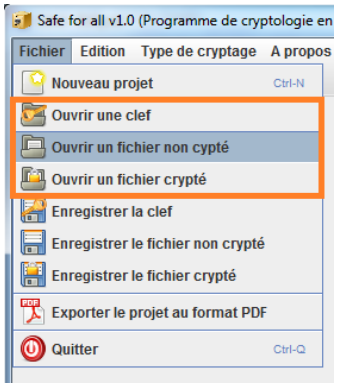
L'attaque du chiffrement César est opérationnel.
En cliquant sur "Chercher la clef de chiffrement", le logiciel vous donnera les clefs les plus probables en supposant que le texte soit en français/anglais et fera ensuite une attaque de type "Force Brute" permettant d'afficher toutes les clefs possibles avec un affichage partiel de chaque message déchiffré.



5 Importation et exportation

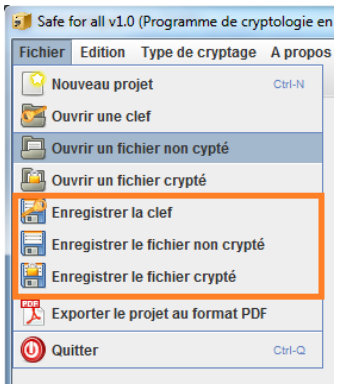
5.1 Importation d'une clef ou/et d'un message

L'importation d'une clef de chiffrement-message chiffré-message clair se lance à partir du menu et se fait à partir d'un fichier quelconque.
L'importation se fait à partir d'un fichier quelconque.
Cependant, le fichier importé doit suivre la norme ASCII.
Le message (ou la clef) importée se placera directement dans le bloc de texte approprié.
Il faut cependant noter que le logiciel ne sait pas quel type de chiffrement est utilisé lorsque vous importez la clef.
Il faudra donc faire attention à lancer le bon chiffrement-déchiffrement.



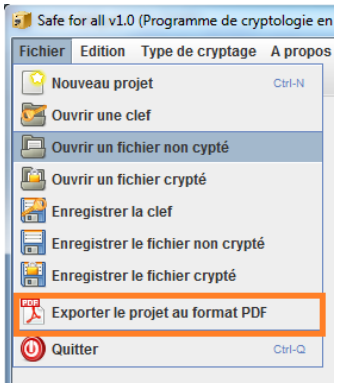
5.2 Exportation d'une clef ou/et d'un message

L'exportation permet d'enregistrer une clef ou un message clair/chiffré au format ".txt".
Il ne vous est pas necessaire de noter l'extension ".txt" lors de l'enregistrement.



5.3 Exportation du projet au format PDF

L'exportation du projet permet d'enregistrer au format ".pdf" le projet au complet (clef+message clair+message chiffré).
Il ne vous est pas nécessaire de noter l'extension ".pdf" lors de l'enregistrement.



Voici un exemple de fichier PDF exporté :

6 Les améliorations en cours de conception

6.1 chiffrement AES 128-192-256 bits

L'AES est un chiffrement symétrique incassable à l'heure actuelle.
Il sera mis en place dès la prochaine mise à jour de l'application.
Comme pour les autres chiffrements, il y aura la possibilité de chiffrer-déchiffrer un message avec une clef que l'on pourra generer aléatoirement.

6.2 chiffrement RSA 1024-4096 bits

Le RSA est un chiffrement asymétrique incassable à l'heure actuelle.
Il sera mis en place dès la prochaine mise à jour de l'application. Comme pour les autres chiffrements, il y aura la possibilité de chiffrer-déchiffrer un message avec une clef que l'on pourra generer aléatoirement.

6.3 Faciliter le multichiffrement d'un message

L'application ne permet à l'heure actuelle que de chiffrer-déchiffrer avec UN TYPE de chiffrement.
Dans une future mise à jour de l'application, il sera possible de combiner différents chiffrements.
Il sera par exemple possible chiffrer un message avec de l'AES puis avec du vigenère puis avec du DES.
Pour déchiffrer le message, il suffira de déchiffrer le DES puis le Vigenère puis l'AES.

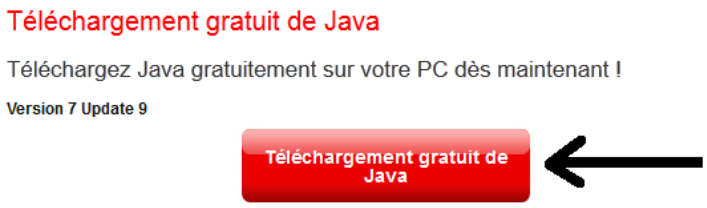
6.4 Améliorer le chiffrement-attaque de Vigenère

Il est possible d'améliorer le chiffrement-déchiffrement de Vigenère en chiffrant sur l'ensemble de la table ASCII.
Il est également possible de finir l'attaque de Vigenère (en cours de conception).

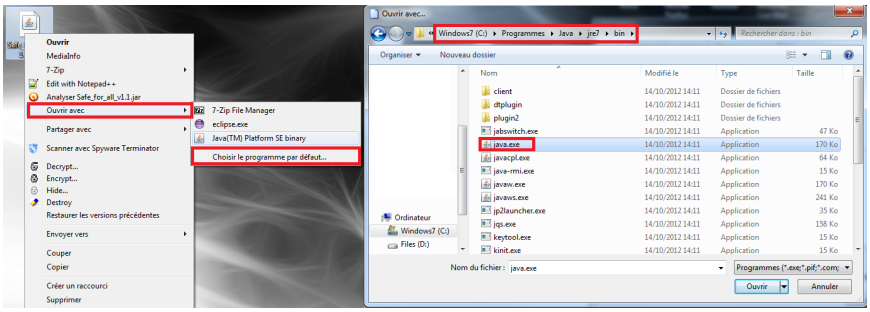
7 Aide

7.1 Le programme ne se lance pas

Pour lancer un fichier en .jar (ce qui est le cas pour cette application), il faut installer une JVM (Java Virtual Machine).
Voici le lien de téléchargement : http ://www.java.com/fr/download/ (il faut cliquer sur "Téléchargement gratuit de JAVA").



Si vous n'arrivez toujours pas à lancer le programme, faites un clic doit sur celui-ci puis cliquez sur "Ouvrir avec" puis sur "Choisir le programme par défaut" et enfin selectionnez "C :/Program Files/Java/-jre7/bin/java.exe"



7.2 Le chiffrement-déchiffrement ne fonctionne pas

Si le chiffrement ou le déchiffrement ne fonctionne pas correctement, je vous conseille de lire les "consignes d'utilisations" qui se trouvent au-dessus des zones de texte clef/chiffrement/déchiffrement.
Si le problème persiste, veuillez m'envoyer un message électronique à l'adresse quentincg@free.fr