TheCry - MANUEL

1. Introduction

1.1. Description

Le logiciel TheCry vous permet de vous amuser en résolvant des cryptogrammes. La méthode utilisée est sans doute la plus simple qui existe en Cryptographie : la substitution simple avec séparation des mots. Par contre, plus les Cryptogrammes sont courts, plus il est difficile de trouver la solution. Si vous ne maîtrisez pas la langue utilisée, c'est même presque impossible.

1.2. Exemple

Soit l'énigme suivante :

WR EH, RU QRW WR EH, WKDW LV WKH TXHVWLRQ :

Il faut la déchiffrer. Chaque lettre du cryptogramme à toujours la même signification. Ainsi la lettre « W » du cryptogramme est égale à la lettre « t » du message en clair.

Après plusieurs essais, on s'aperçoit que
E=b, H=e, Q=n, R=o, U=r, W=t, …

On déchiffre enfin le message :
to be, or not to be, that is the question :

2. Démarrage rapide (Quick Start)

2.1. – Choix aléatoire du cryptogramme

La manière la plus simple d'obtenir un cryptogramme et de demander au logiciel d'en afficher un. Cette opération est réalisée grâce à la commande du menu :

File => New random puzzle

Le logiciel choisit au hasard un problème existant dans une base de données qu'il est possible d'augmenter. Par défaut, plusieurs centaines de messages sont présents.

ATTENTION ! Le clair du message choisi appartient à la langue par défaut. Celle-ci est réinitialisée à chaque démarrage et par défaut elle correspond à l'Anglais (EN). Vous pouvez changer la langue (pour la session), grâce à une commande du menu « Computer ». Une liste de langues apparaît. Chaque langue est représentée via un code sur deux lettres : EN=Anglais, FR=Français, …. Cette liste dépend des problèmes installés. On peut ajouter des problèmes (cf. 5.2) et ainsi ajouter des langues. On peut changer la langue par défaut en modifiant la configuration du logiciel (cf. A-2)

2.2. – Choix humain du cryptogramme

Si vous avez sous la main un ami, vous pouvez lui demander de saisir un message en clair que le logiciel va chiffrer et vous proposer ainsi une nouvelle énigme. Cette opération est réalisée grâce à la commande du menu:

Human => New puzzle

Une nouvelle fenêtre s'affiche qui permet la saisie du message en clair. Quand la saisie est terminée l'utilisateur appuie sur le bouton OK. La fenêtre s'efface et le message chiffré (par le logiciel) apparaît.

Remarques:
1) Il est possible d'obtenir le texte via un COPIER/COLLER à partir du presse-papier. On fait l'opération SÉLECTIONNER / COPIER à partir d'un autre logiciel (Navigateur, Traitement de texte, …) et dans TheCry on appuie sur le bouton « From Clipboard ».

2) Au lieu de saisir un texte clair et laisser le logiciel le chiffrer, l'utilisateur peut lui-même fournir directement le message chiffré en appuyant sur le bouton « Crypto/Plain ».

3) Si on a activé par erreur la fenêtre qui propose de saisir un nouveau problème, il est possible d'appuyer sur la croix en haut et à droite qui ferme la fenêtre sans faire aucune autre action.

4) Si le texte clair comprend des noms propres (personnage, lieu, …) il faut les précéder d'une étoile. Par exemple, soit le texte clair « marco polo has been to china », on doit écrire : *marco *polo has been to *china. Le chiffrement conservera ces étoiles (par exemple : *NBSDP *QPMP IBT CFFO UP *DJOB.), ce qui aidera le joueur.

Note: En plus des deux possibilités présentées, on peut obtenir une Énigme via la notion de Challenge (cf. 5.)

2.3. – Résoudre un problème

Comment proposer une solution ? En fait, on indique lettre par lettre ses hypothèses. Reprenons l'exemple précédent (WR EH RU QRW …). Si on suppose que la lettre H du cryptogramme correspond à la lettre « e » du clair, on appuie sur le bouton « H » de la rangée CRYPTO (le bouton sélectionné apparaît en jaune). Ensuite on appuie sur le bouton « e » de la rangée « PLAIN » (le bouton sélectionné apparaît en rouge). Automatiquement tous les « H » du cryptogramme sont remplacés par des « e » dans les lignes qui suivent les lignes contenant le cryptogramme.

Si on a commis une erreur, il suffit de sélectionner la lettre fausse, par exemple la lettre « H » de la rangée « CRYPTO » et de l'associer au caractère « - » en fin de la rangée « PLAIN ». Toutes les déductions associées disparaissent.

2.4. - Stratégies de résolution

La stratégie la plus valorisante (mais la difficile) est de n'utiliser aucune aide provenant du logiciel.

Si le problème devient un casse-tête et que l'on éprouve plus de plaisir à le résoudre, on peut utiliser les aides suivantes réunies dans le menu « Information ».

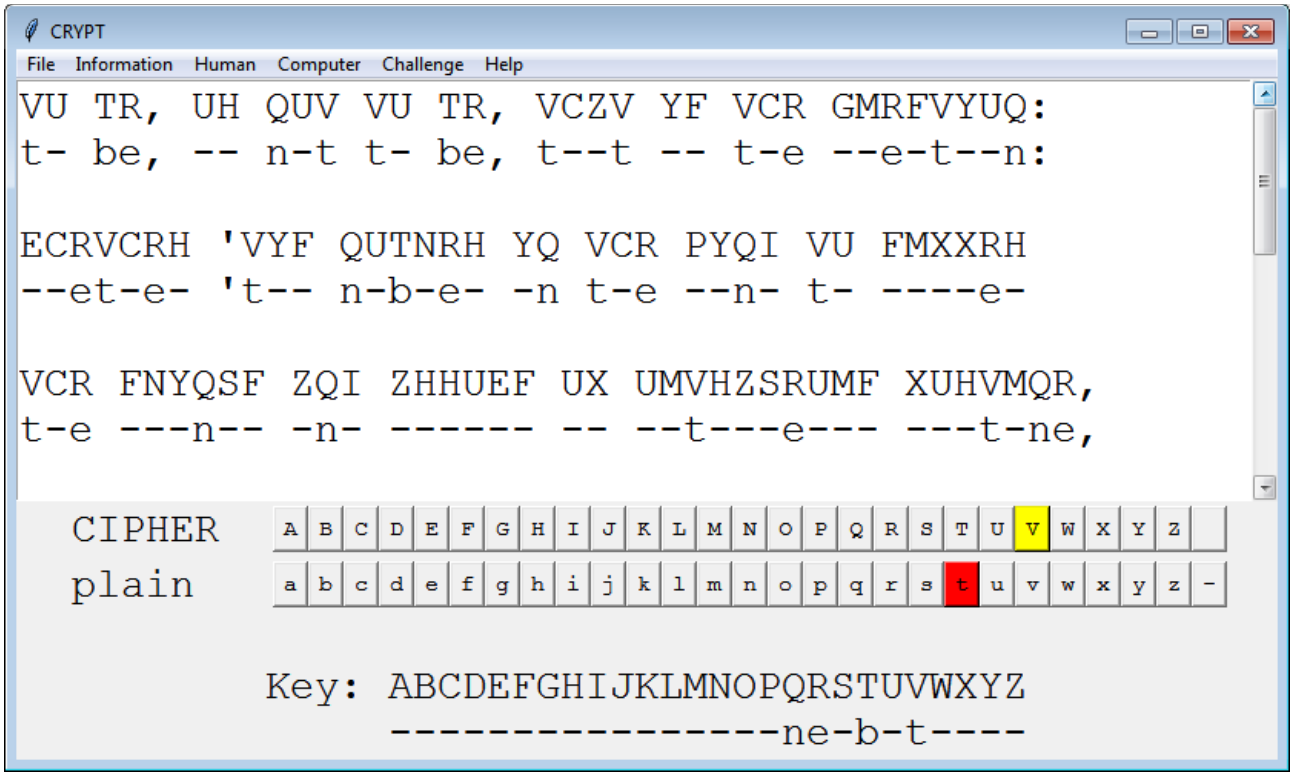
Si on n'utilise que les statistiques (de la langue et du cryptogramme), on ne triche pas. Les utiliser est au contraire vivement conseillé.

Par contre, utiliser les commandes « Hint », « Beginning », « Is key correct » peut-être considéré comme tricher. Il est acceptable de les utiliser pour s'entraîner au déchiffrement mais vous ne pourrez pas mesurer vos compétences en cryptanalyse.

En désespoir de cause, la commande « Solution » du menu « Information » vous livre la solution … si le logiciel la connaît !

3. Les écrans

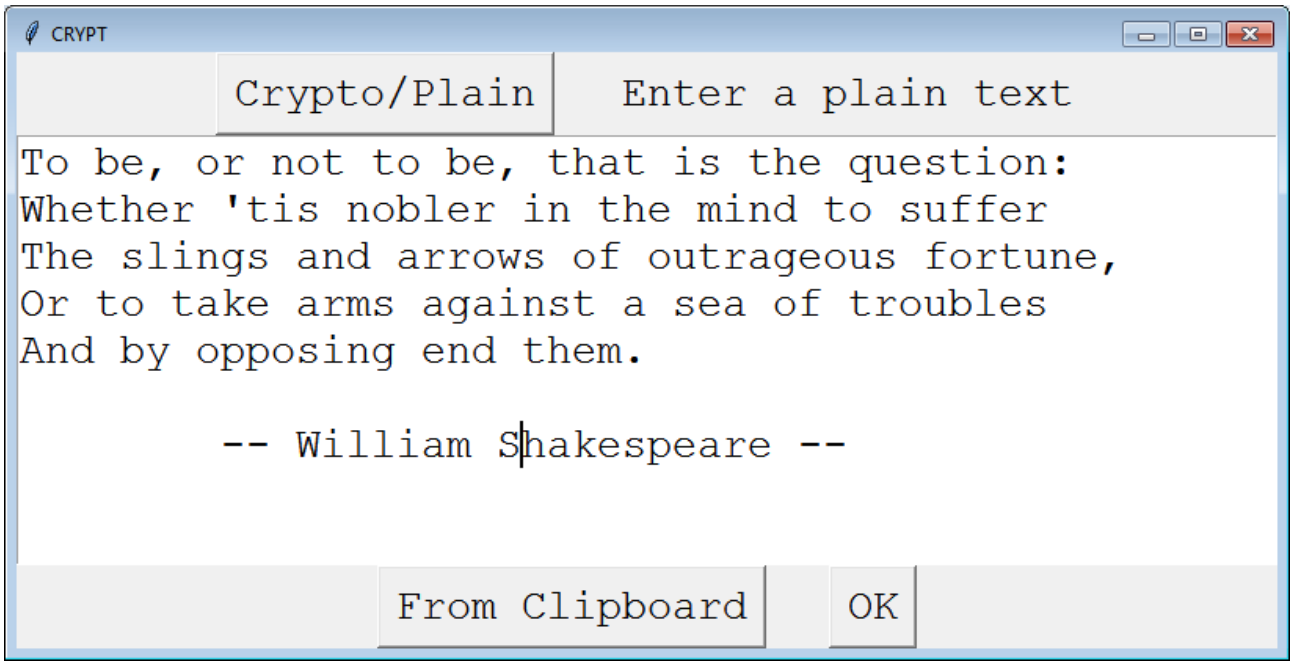
3.1. – L'écran principal



La fenêtre du haut contient le cryptogramme et votre hypothèse. Le texte du cryptogramme est en majuscules. Le texte de votre hypothèse est en minuscule. Si vous ne savez pas l'équivalent d'une lettre, elle est remplacé par le signe « - ». Bien sur, au début, en dessus des lettres du cryptogramme il n'y a que des « - ».

Dans la partie grisé, il y a deux alphabets. Celui du haut correspond aux lettres chiffrées (« CIPHER »). Celui en dessous correspond aux lettres en clair (« plain »). Pour formuler une nouvelle hypothèse, on clique sur une lettre du haut (chiffrée) et on clique sur une lettre du bas (en clair). La clé (« Key ») mémorise l'ensemble de vos hypothèses. Si on veut annuler une hypothèse, il suffit d'associer une lettre de l'alphabet « CIPHER » au signe « - » présent en bout de l'alphabet « plain ». Toutes les déductions associées disparaissent.

3.2. – L’écran de saisie d’un nouveau problème



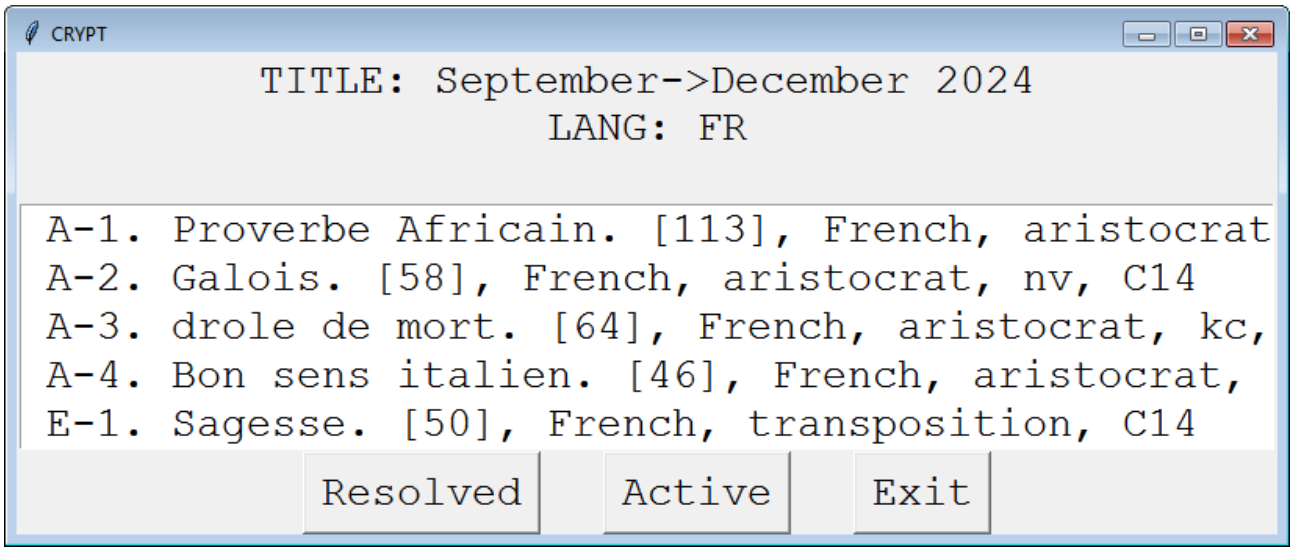
Cet écran de saisie d’un nouveau problème est affiché à la suite de la commande « New Puzzle » du menu « Human ». Un de vos amis peut saisir un texte en clair. A la suite de l’appui sur le bouton « OK », le texte est chiffré et devient le nouveau problème à résoudre.

Au lieu de saisir le texte, on peut le sélectionner et le copier dans le presse-papier à partir d’une autre application (comme le navigateur). L’appui sur le bouton « From Clipboard » le fait apparaître dans la fenêtre. Vous pouvez le modifier avant d’appuyer sur « OK ».

Enfin il est possible de saisir directement un cryptogramme en ayant appuyé au paravent sur le bouton « Crypto/Plain » (il fonctionne comme une bascule : si on appuie de nouveau dessus, on revient au mode normal : « Enter a Plain text »).

Remarque: Si l’on désire revenir à la fenêtre principale sans valider le nouveau problème, il suffit d’appuyer sur la petite croix en haut à droite, ce qui provoque la fermeture de la fenêtre sans aucune autre conséquence.

3.3. L’écran qui liste les problèmes d’un challenge



Si vous voulez résoudre un problème appartenant au Challenge courant, il faut activer la commande :

Challenges => List Challenges

Si un Challenge est présent (via la commande « Challenge » => « Load file »), l’écran ci-dessus s’affiche. Est indiqué à minima son titre qui normalement spécifie sa date de parution ainsi que la langue principale. D’autres informations (auteur, éditeur, …) peuvent apparaître.

Pour chaque problème du Challenge est spécifié ses caractéristiques (cf. 5.1 et 5.3). En bref, son numéro, son titre, sa taille, sa langue, la méthode de cryptage, son type de clé et son auteur. On peut aussi avoir un indice entre parenthèse chiffré en Jules César.

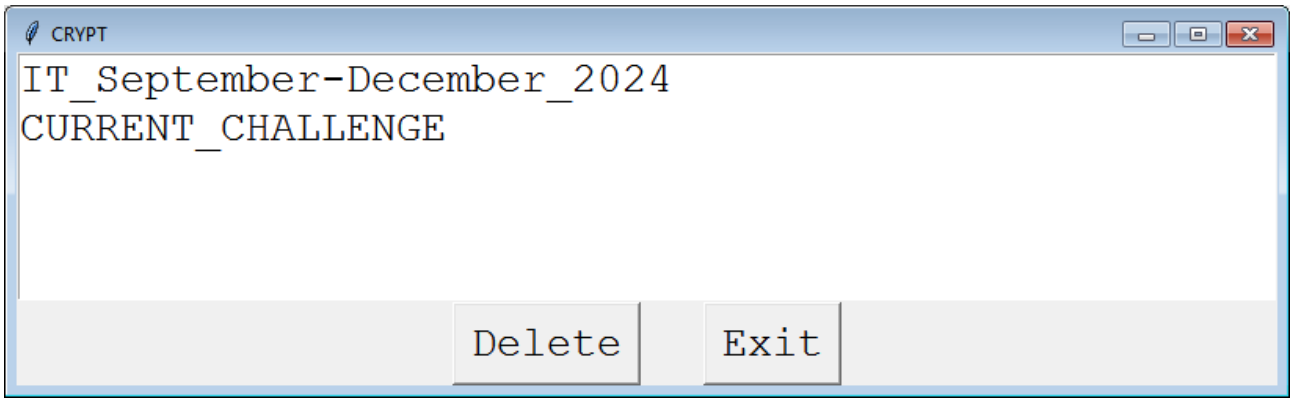
Le bouton « Resolved » permet d’ajouter une étoile précédant un problème pour spécifier que vous avez résolu le problème. En cas d’erreur, vous pouvez de nouveau appuyer sur ce bouton pour enlever l’étoile.

Le bouton « Exit » permet de revenir au problème courant.

Le bouton « Active » active le problème sélectionné qui devient le problème courant.

ATTENTION ! Contrairement à la fenêtre principale il n’y a pas d’ascenseur. Si l’on veut parcourir la liste ou voir tous les champs, il faut utiliser les flèches (dans les 4 directions).

3.4. L’écran de suppression de fichiers



Le menu « Challenge » => « Delete file » permet de supprimer des problèmes. Soit les problèmes du Challenge Courant, soit les problèmes associés à une même langue provenant d’une archive particulière.

Concrètement, on sélectionne le fichier associé à une langue et on clique sur le bouton « Delete ». Le nom de l’archive commence par le nom de la langue (dans l’exemple ci-dessus : IT = Italien).

Le bouton « Exit » permet d’abandonner le formulaire sans détruire des fichiers.

4. Les menus

4.1. – Le Menu « File »

1) New random Puzzle : propose un nouveau problème. Une demande de confirmation est demandé. Ensuite, la solution du problème précédent est affiché. Le choix du problème est aléatoire mais dépend de la langue courante (cf. 4.4 [le Menu « Computer »]).

2) Open Puzzle via MD5 : Chaque problème est identifié par une somme MD5. Vous pouvez rappeler un problème en donnant le début de cette somme. Par exemple si une autre personne a résolu un problème et a mémorisé la somme MD5 qui identifie le problème, vous pouvez vous confronter à elle en essayant de résoudre (plus vite par exemple) le même problème. Remarque : la somme MD5 apparaît dans les meta-data qui sont affichés par le menu « Information => MetaData » et aussi dans le presse-papier à la suite de la commande « To Clipboard ».

3) Reset : Efface l’ensemble de vos déductions. Cela permet de réinitialiser le problème.

4) Save : Sauvegarde le problème et vos déductions.

5) Restore : Restaure le problème en cours tel qu’il était lors de la dernière sauvegarde.

6) Close : Supprime le problème en cours et sa sauvegarde. Vous pourrez le restaurer que si vous avez conservé sa somme MD5.

7) To Clipboard : Copie dans le presse-papier le problème ainsi que les déductions que vous avez effectuées ainsi que la somme MD5, sa longueur, les statistiques concertants le cryptogramme et les meta-data (et notamment sa langue). Si on copie le contenu du presse-papier dans un traitement de texte et qu’on l’imprime, on pourra résoudre le problème sur papier. Attention ! Il est vivement conseillé d’utiliser la police « Courrier » et une taille de police suffisante.

8) Exit : On met fin au programme mais la sauvegarde du problème courant est effectué.

Remarque : Si l'on désire sortir du programme sans sauvegarder, il suffit d'appuyer sur la croix qui se trouve en haut et à droite de la fenêtre applicative.

4.2. – Le menu « Information »

1) Print Statistics : affiche la fréquence des lettres du cryptogramme (celles qui apparaissent au moins deux fois). On affiche également la fréquence des bigrammes et trigrammes.

2) Hint : Affiche une équivalence entre une lettre du cryptogramme et la lettre clair correspondante. Remarque : utiliser cette aide, s'appelle tricher.

3) Beginning : Affiche la signification des trois premières lettres du cryptogramme. En temps ordinaire, cela s'appelle tricher. Par contre, pour les problèmes les plus complexes, on peut le tolérer.

4) Meta-Data : Affiche les meta-data comme la langue, la somme MD5, etc...

5) Plain letters not found : Affiche les lettres du clair pour lesquelles vous n'avez pas d'hypothèse.

6) Is solved : Vérifie que vous avez émis une hypothèse pour chacune des lettres du Cryptogramme.

7) Is key correct : Vérifier le bien fondé des hypothèses que vous avez faite. Utiliser cette commande peut-être considérer comme tricher sauf si vous avez résolu le problème (« Is solved » est vrai).

8) Solution : Affiche la solution. Remarque : celle-ci peut-être ignoré du logiciel.

4.3. – Le menu « Human »

1) New Puzzle : cette commande propose à un humain (par exemple un ami du joueur) de proposer un nouveau problème. La fenêtre 3.2 s'affiche (L'écran de saisie d'un nouveau problème) .

4.4. – Le menu « Computer »

1) New Puzzle : cette commande est identique à la commande « New Random Puzzle » du menu « File ».

Les commandes suivantes correspondent aux différentes langues pour lesquelles il y a des problèmes, par exemple EN pour l'Anglais, DE pour l'allemand, FR pour le français, etc...
Si on appuie sur une des langues, elle devient la langue courante (uniquement pour la session).

La langue courante apparaît précédée d'une coche.

4.5. - Le menu « Challenge »

1) List Challenge : cette commande liste les problèmes du Challenge courant et vous permet de choisir de résoudre un de ces problèmes (cf. l'écran 3.3).

2) Load file : cette commande permet de charger des problèmes, soit provenant d'un nouveau Challenge, soit provenant d'une archive associée à une langue spécifique. Ces fichiers sont typiquement récupérés à partir du site officiel du logiciel (cf. menu « Help » => « About »).

3) Delete files : cette commande permet de supprimer les problèmes chargés via le menu précédent (« Challenge » => « Load file) (cf. l'écran 3.4).

4.6. – Le menu « Help »

1) Manual : Affiche le présent manuel.

2) Statistics : Affiche des statistiques pour la langue courante, par défaut pour l'anglais.

Remarque : Le manuel et les statistiques sont mémorisés au format PDF. Le logiciel doit être configuré correctement pour qu'il puisse afficher un fichier PDF. Si ce n'est pas le cas, l'utilisateur peut, soit configurer le logiciel (cf. Annexe A-2), soit afficher lui-même les fichiers PDF inclus dans le logiciel, soit enfin récupérer ou afficher ces fichiers sur le site officiel du logiciel (indiqué dans le menu suivant « Help » => « About ».

3) About : Affiche la version du logiciel, son auteur, son site officiel, ...

5. Les challenges

5.1. Le concept

On l'a constaté, ce programme permet principalement de résoudre des énigmes choisis de manière aléatoire à partir d'une base de données fournie avec le logiciel (mais que l'on peut augmenter). Une énigme est un cryptogramme chiffré via une substitution simple.

J'ai ajouté une autre source d'énigme : les Challenges. Un challenge correspond à un ensemble de cryptogrammes mais pour lesquelles la *solution n'est pas fournie*. De plus la majorité des problèmes proviennent de textes clair d'une même langue (l'anglais, le français, ...). Le logiciel permet d'installer un challenge qui remplace l'ancien. Mon site Web peut contenir quelques Challenges. Le format d'un Cryptogramme et d'un Challenge sont donnés en Annexe, ce qui permet à tout un chacun de créer des challenges (si il est informaticien). En bref, un Challenge est un fichier archive (TAR) composé de fichiers JSON.

Typiquement un Challenge est composé de plusieurs types de problèmes :

- Des substitutions simples avec séparation des mots (Aristocrat), numérotées de A-1 à A-x.

- Des substitutions simples sans séparation des mots (Patristocrat), numérotés de P-1 à P-x.

- Des Aristocrats mais dans une langue qui diffère de la langue principale. Par exemple si la langue principale est l'Anglais, on utilisera des langues comme le français, l'allemand, le latin, … Ces problèmes sont numérotés X-1 à X-x (X = Xenocrypt). Si la langue est inconnue, elle sera indiquée par « ?? ».

- Des messages chiffrés n'utilisant pas la substitution simple, par exemple la transposition à tableau complet, numérotés de E-1 à E-x.

Remarque: Dans un cryptogramme, un nom propre (un personnage, un lieu, …) est normalement précédé d'une étoile. Par exemple, soit le texte clair « marco polo has been to china ». Le cryptogramme sera (via la substitution JC) : *NBSDP *QPMP IBT CFFO UP *DJOB.

5.2. Installer un Challenge

Le menu « Challenge » => « Load File » permet de charger de nouveau cryptogrammes. La commande vous affiche la boite de dialogue de recherche de fichiers. On reconnaît un fichier de type TheCry car son nom commence par TC en majuscules et que son extension est « .tar » (format TAR). Il y a deux type de fichiers TC :

- Les fichiers qui contiennent des cryptogrammes provenant de textes dans une langue particulière et qui sont destinés à être choisi de manière aléatoire. La langue apparaît juste après TC.

- Les Challenges. La langue principale apparaît à la fin du nom (avant l'extension tar).

Dans le cas où vous installez un Challenge, le programme vous demande confirmation. En effet l'installation d'un nouveau Challenge supprime le Challenge courant.

Remarque : Si le problème sélectionné est de type « Exchange » (c'est-à-dire n'est pas une substitution simple), le logiciel TheCry ne vous permet pas de vous aider à résoudre le problème. L'écran principal devient plus simple : il n'affiche que le Cryptogramme. Vous avez intérêt à utiliser la commande « File => To Clipboard » pour pouvoir résoudre le problème sur papier ou via un autre logiciel.

5.3. Choisir un problème qui fait partie du Challenge courant

Le menu « Challenge => List Challenge » liste les problèmes qui composent le challenge courant ainsi que des meta-data sur le Challenge lui-même : son auteur, son éditeur, sa date de parution, le nombre de problème et surtout la langue principale.

Pour chaque challenge est indiqué (si les informations sont présentes dans le problème) :
- Son numéro (A-x, P-x, X-x, E-x, …) qui notamment précise son type (A = Aristocrat, P = Patristocrat, X = Xenocrypt, E = Exchange [méthode differente de la substitution simple])
- Son titre (cela peut aider dans certains cas).
- Sa taille (le nombre de lettres qui composent le cryptogramme).
- Sa langue (c'est surtout pertinent pour les problèmes de type Xenocrypt)
- La méthode de chiffrement (Aristocrat, Patristocrat, Beaufort, Transposition à tableau complet, …)
- La formation de la clé de chiffrement (k0, ka, kb, kc, …) (cf. Annexe A-4).
- L'auteur du cryptogramme (différent généralement de l'auteur du texte clair).

Si on sélectionne un problème et que l'on appuie sur le bouton « Active », ce problème devient le problème courant (cf. écran 3.3).

Annexes (aspects avancés et compléments)

A-1. La genèse du programme

Ce programme dérive de toute une lignée de logiciels que j'ai conçu depuis plusieurs dizaines d'années.

La première version était écrite en Perl et fonctionnait en mode texte. Elle me permettait de chiffrer un texte choisi aléatoirement à partir d'une base de données constituée d'un seul fichier composé de plusieurs textes séparés par une ligne composées de « - » . J'utilisai la substitution simple avec séparation des mots. Comme mes connaissances linguistiques étaient très faible j'utilisai uniquement des textes en français. J'étais le seul utilisateur de ce programme.

Rapidement j'ai constaté que l'ajout de textes clair me prenait beaucoup trop de temps. J'ai découvert alors le logiciel Fortune qui affiche un texte (un proverbe, une citation, une blague, …) de manière aléatoire à partir de bases de données externes que l'on pouvait ajouter. Il m'a suffit de créer un « parser » pour avoir à ma disposition plusieurs milliers de textes utilisable par mon programme.

Ensuite, j'ai découvert le langage Python et j'ai amélioré mes connaissances en Cryptographie et en Informatique. J'ai naturellement réécrit mon programme en Python. J'ai décris ma passion (la cryptographie) à des voisins. J'ai commencé à leur envoyer des problèmes par email presque toutes les semaines que je générais avec mon programme. Ceci a booster mon intérêt d'améliorer mon programme. Je voulais en final leur donner pour qu'ils puissent eux-mêmes générer les problèmes. Évidemment cette version devait être graphique pour être utilisable par n'importe qui.

Entre temps, j'ai découvert « The Cryptogram », le journal anglais de l'ACA (American Cryptogram Association). Je me suis abonné, mais malheureusement, l'éditeur a suspendu mon abonnement sans raison. Je repris des éléments de ce journal. Notamment, j'ai adopté son vocabulaire (Aristocrat, …) et le format d'un problème (numéro, titre, …).

J'ai aussi fait le choix de mémoriser un problème au format JSON et de l'identifier par une somme MD5. Ainsi même si je créais des milliers de cryptogrammes, ils seront toujours identifiables. Ainsi, des personnes différentes pourront s'attaquer au même problème même si au départ il a été choisi de manière aléatoire.

Récemment, j'ai découvert la version « en ligne » du programme de l'ACA qui permet de générer des problèmes basés sur la substitution simple. Cela ma permit de corriger l'interface graphique de mon logiciel et de la simplifier.

J'ai plusieurs idées d'améliorations de mon programme, mais je vais attendre un peu le retour des utilisateurs maintenaient que je l'ai publié sur Internet (mes voisins ont pu ainsi le récupérer :-).

A-2. La Configuration

1) Le fichier DATA/lang.txt contient la langue par défaut. Il contient (à priori) EN qui correspond à l'anglais. Vous pouvez changer sa valeur.

2) Le fichier DATA/cmd_pdf.txt contient la commande qui permet l'affichage d'un PDF. Elle dépend du système d'exploitation et de l'application que vous utiliser pour afficher un PDF (Acrobat Reader, Firefox, …, evince, …).

Par exemple, sous Windows, j'utilise Acrobat Reader. J'utilise ainsi la commande :

```
acrobat
        ou
start acrobat
```

J'utilise aussi les commandes suivantes (sous Windows) :

firefox	(Le navigateur Firefox [il faut l'installer])
start acrord32.exe	(Toujours Acrobat, mais sur certaines versions de Windows)
start firefox	(Le navigateur Firefox [il faut l'installer])

ATTENTION! Il faut que l'utilisateur modifie le chemin d'accès aux commandes en modifiant la variable PATH en y ajoutant le répertoire qui contient la commande. Pour cela, sous Windows 10, il doit activer le formulaire suivant:

Settings => System => About => System Info => Advanced System Settings => Environment Variables => Path

Sous Linux, on indique directement le nom du logiciel graphique qui affiche un PDF (là encore, la commande doit être dans un des répertoires du PATH [modifié via le fichier ~/.profile]):

```
firefox
```

Remarque : j'aurai pu utiliser une bibliothèque Python au lieu d'utiliser une commande du système d'exploitation, mais je voulais que mon programme n'utilise QUE la bibliothèque standard.

A-3. Les fichiers de données (les cryptogrammes), ajouter des cryptogrammes

Les cryptogrammes sont mémorisés dans des fichiers au format JSON dont le nom correspond à la somme MD5 du cryptogramme et qui ont l'extension « .cry ». Voici un exemple de fichier :

```
C:\> more fec5a1fc2daf3988722d7e4b3169546e.cry
{
        "CRYPTO": "AK COJDUDFK, SIEJGUK, EL CONC COJ ZHEQJILJ VNL BEMCNCJB SZC HDC LEFHJB.\n\t\t-- MOIELCDPOJI ADIUJK\n",
        "PLAIN": "My theology, briefly, is that the universe was dictated but not signed.\n\t\t-- Christopher Morley\n",
        "KEY": "NSMBJGFOEXTUAHDPWILCZQVRKY",
        "METHOD": "aristocrat",
        "LANG": "EN"
}
```

Le seul champ obligatoire est le champ « CRYPTO », tous les autres champs sont optionnels et on peut ajouter pleins d'autres champs (AUTHOR, TITLE, NUMBER, HINT, …). Si ils existent, ils apparaîtront via la commande « Meta-Data » du menu « Information ».

Pour qu'un cryptogramme soit pris en compte par le logiciel, il doit être dans une arborescence dont le nom du répertoire racine est composé de deux lettres. Ce répertoire doit lui-même être présent dans le répertoire « CRYPTOS ». La philosophie du logiciel est que ce répertoire de deux lettres correspond à une langue (DE, EN, FR, …).

Il est possible d'ajouter un problème ou un ensemble de problèmes en les mettant dans un fichier TAR dont le contenu sont des fichiers « *.cry » au format décrit précédemment. Sur mon site Web, je fournis quelques archives contenant des milliers de nouveaux problèmes.

Remarques :
1) Les cryptogrammes qui ont été générés à partir d'un texte en clair via le menu « Human => New Puzzle » sont mémorisés dans le répertoire CRYPTOS/WORK (ainsi qu'une copie des cryptogrammes qui deviennent le problème courant).
2 Les cryptogrammes qui appartiennent à un Challenge sont stockés dans le répertoire CRYPTOS/CHALL.

A-4. La génération des clés

Le logiciel TheCry manipule (essentiellement) des substitutions simples. Les problèmes que j'ai générés automatiquement utilisent chacun une clé créé également de manière automatiquement qui correspond à un mélange des lettres de l'alphabet.

Quand je décidais d'ajouter la possibilité de résoudre des Challenges, je me suis inspiré du journal The Cryptogram qui propose plusieurs méthodes de génération de clés (en tout 8). Je décris ci-après les méthodes K1, K2 et Caesar qui sont les plus utilisés.

Je créais en plus les méthodes Ka, Kb et Kc. Je nommais K0 ma méthode initiale (mélange aléatoire des lettres de l'alphabet) JC la méthode César, Ka (la méhode K2 de l'ACA) et Kb (la méthode K1 de l'ACA).

1) Les méthodes de l'ACA :

K1 : l'alphabet chiffré est dans l'ordre normal (mais peut-être décalé). L'alphabet clair contient un mot clé (Keyword).

```
plain:    p o u l t r y a b c d e f g h i j k m n q s v w x z
CHIPHER:  R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
```

K2 : l'alphabet clair est dans l'ordre normal, l'alphabet chiffré contient un mot clé.

```
plain:    a b c d e f g h i j k l m n o p q r s t u v w x y z
CHIPHER:  V W X Z K E Y B O A R D C F G H I J L M N P Q S T U
```

Caesar : on utilise la méthode de substitution de Jules César. On décale les alphabets clair et chiffré d'un certain nombre de lettres. J'appelle cette méthode JC.

2) Mes méthodes

K0 : n’utilise pas de mot clé. La clé est aléatoire.

Ka : Correspond à la méthode K2 de l’ACA, mais sans décalage de l’alphabet chiffré.

Kb : Correspond à la méthode K2 de l’ACA.

Kc : Correspond à la méthode K1 de l’ACA.

JC : Correspond à la méthode Caesar de l’ACA.

NV : Correspond à la méthode du cercle de chiffrement de l’armée américaine et utilisé dans la M-209 : on a deux alphabet dans l’ordre normal mais l’un est inversé et décalé par rapport à l’autre.

A-5. Ajouter une documentation au format PDF

Par défaut, seul la version anglaise du manuel (la documentation que vous lisez actuellement) est disponible à partir du logiciel TheCry. De même les statistiques présentes ne concerne que les trois langues installées : l’anglais, le français et l’allemand.

D’autres fichiers sont disponibles sur le site officiel du logiciel. Vous pouvez les télécharger et les installer dans le répertoire THE_CRY/DATA.

Voici les conventions de nommage de la documentation :
- Le manuel : ZZ_manual.pdf
- Les statistiques : ZZ_tests.pdf

ZZ étant le code spécifiant la langue : EN, FR, DE, IT, ES, …