MANUAL

1. Introduction

1.1. Description

TheCry software allows you to have fun solving cryptograms. The method used is probably the simplest in Cryptography: simple substitution with word separation. However, the shorter the Cryptograms, the more difficult it is to find the solution.

1.2. Example

Consider the following puzzle:

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

It must be deciphered. Each letter of the cryptogram always has the same meaning. Thus the letter "W" of the cryptogram is equal to the letter "t" of the plaintext message.

After several attempts, we realize that

> E=b, H=e, Q=n, R=o, U=r, W=t, …

We finally decipher the message:

> to be, or not to be, that is the question:

2. Quick Start

2.1. – Random choice of cryptogram

The easiest way to get a cryptogram is to ask the software to display one. This operation is done using the menu command:

> File => New random puzzle

The software randomly chooses an existing problem in a database that can be increased. By default, several hundred messages are present.

WARNING! The plain-text of the chosen message belongs to the default language. This is reset at each start and by default it corresponds to English (EN). You can change the language (for the session), using a command in the "Computer" menu. A list of languages appears. Each language is represented by a two-letter code: EN=English, FR=French, …. This list depends on the problems installed. You can add problems and thus add languages (cf. 5.2). You can change the default language by modifying the software configuration (cf. A-2).

2.2. – Creation of the cryptogram by a human being

If you have a friend on hand, you can ask him to enter a plain text message that the software will encrypt and thus offer you a new puzzle. This operation is carried out using the menu command:

Human => New puzzle

A new window appears that allows the entry of the plain text message. When the entry is complete, the user presses the "OK" button. The window disappears and the encrypted message (by the software) appears.

Notes:
1) It is possible to obtain the text via a COPY/PASTE from the clipboard. The SELECT/COPY operation is carried out from another software (Browser, Word Processor, etc.) and in TheCry, the "From Clipboard" button is pressed.

2) Instead of entering a plain text and letting the software encrypt it, the user can directly provide the encrypted message by pressing the "Crypto/Plain" button.

3) If you have accidentally activated the window that offers to enter a new problem, you can press the cross at the top right which closes the window without doing any other action.

4) If the plain text includes proper names (character, place, etc.), they must be preceded by an asterisk. For example, if the plain text is "marco polo has been to china", we must write: *marco *polo has been to *china. The encryption will keep these asterisks (for example: *NBSDP *QPMP IBT CFFO UP *DJOB.), which will help the player.

Note: In addition to the two possibilities presented, we can obtain a Riddle via the concept of Challenge (see 5.)

2.3. – Solve a problem

How to propose a solution? In fact, we indicate our hypotheses letter by letter. Let's take the previous example (WR EH RU QRW ...). If we assume that the letter H of the cryptogram corresponds to the letter "e" of the plain-text, we press the "H" button of the "CRYPTO" row (the selected button appears in yellow). Then we press the "e" button of the "PLAIN" row (the selected button appears in red). Automatically all the "H" of the cryptogram are replaced by "e" in the lines following the lines containing the cryptogram.

If we made a mistake, we just have to select the wrong letter, for example the letter "H" of the "CRYPTO" row and associate it with the character "-" at the end of the "PLAIN" row. All the associated deductions disappear.

2.4. Resolution strategies

The most rewarding strategy (but the most difficult one) is to not use any help from the software.

If the problem becomes a puzzle and you no longer feel pleasure in solving it, you can use the help commands gathered in the "Information" menu.

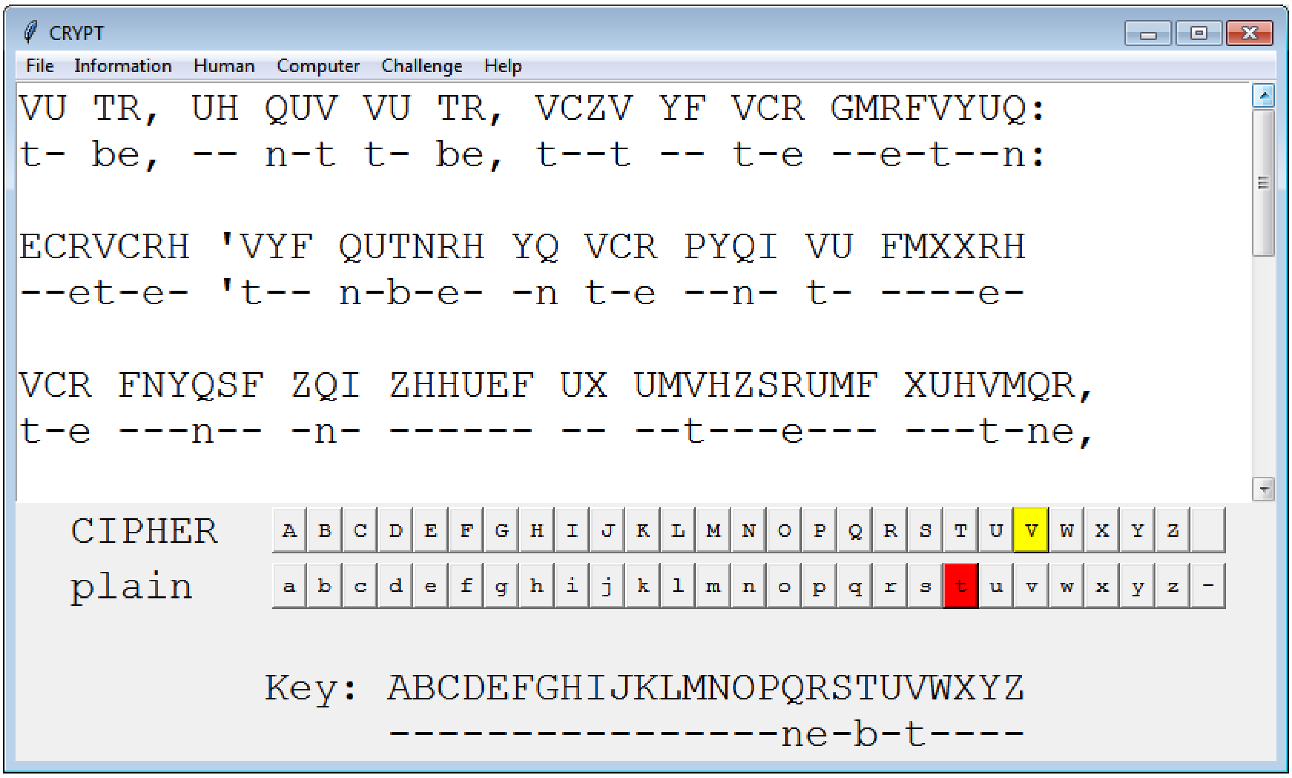
If you only use the statistics (of the language and the cryptogram), you are not cheating. On the contrary, using them is strongly recommended.

On the other hand, using the "Hint", "Beginning", "Is key correct" commands can be considered as cheating. It is acceptable to use them to practice decryption but you will not be able to measure your skills in cryptanalysis.

As a last resort, the "Solution" command in the "Information" menu gives you the solution ... if the software knows it!

3. The screens

3.1. – The main screen

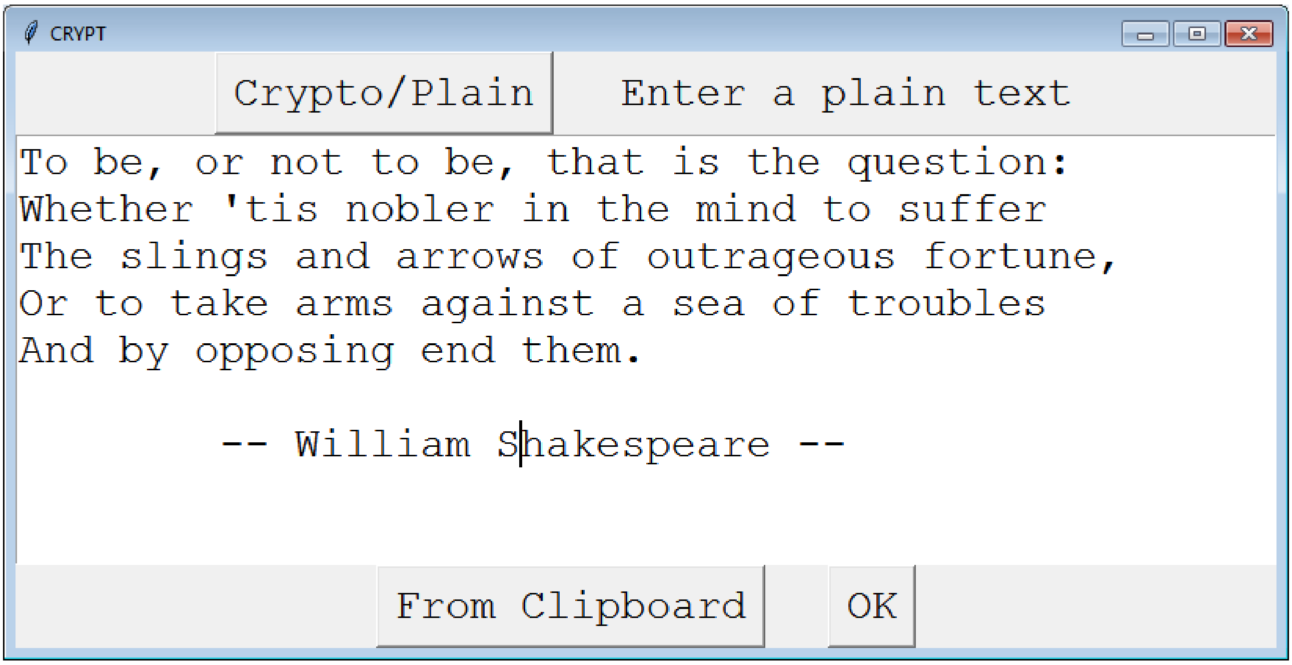


```
VU TR, UH QUV VU TR, VCZV YF VCR GMRFVYUQ:
t- be, -- n-t t- be, t--t -- t-e --e-t--n:

ECRVCRH 'VYF QUTNRH YQ VCR PYQI VU FMXXRH
--et-e- 't-- n-b-e- -n t-e --n- t- ----e-

VCR FNYQSF ZQI ZHHUEF UX UMVHZSRUMF XUHVMQR,
t-e ---n-- -n- ------ -- --t---e--- ---t-ne,

   CIPHER    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
   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 -

             Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ
                  ----------------ne-b-t----
```

The top window contains the cryptogram and your hypothesis. The text of the cryptogram is in uppercase. The text of your hypothesis is in lowercase. If you do not know the equivalent of a letter, it is replaced by the sign "-". Of course, at the beginning, above the letters of the cryptogram there are only "-".

In the grayed-out part, there are two alphabets. The one at the top corresponds to the encrypted letters ("Cipher"). The one below corresponds to the plain letters ("Plain"). To formulate a new hypothesis, click on a letter at the top ("Cipher") and click on a letter at the bottom ("Plain"). The key ("Key") memorizes all of your hypotheses. If you want to cancel a hypothesis, simply associate a letter of the alphabet "CIPHER" with the sign "-" present at the end of the alphabet "Plain". All the associated deductions disappear.

3.2. – The screen for entering a new problem



```
To be, or not to be, that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles
And by opposing end them.

        -- William Shakespeare --
```

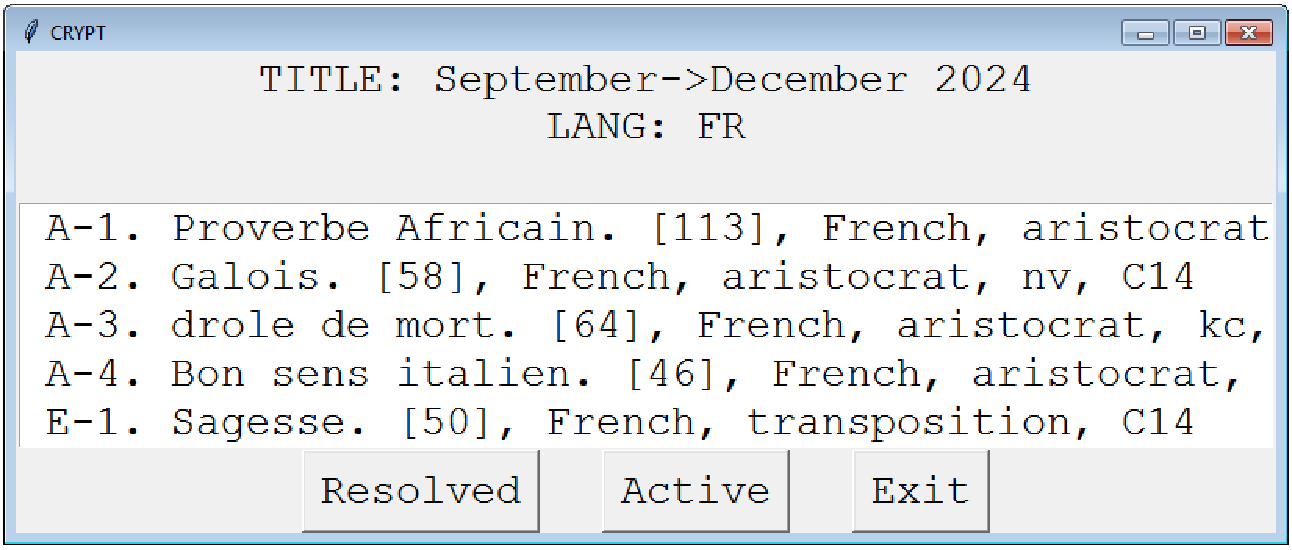
This screen for entering a new problem is displayed following the "New Puzzle" command in the "Human" menu. One of your friends can enter a plain text. After pressing the "OK" button, the text is encrypted and becomes the new problem to solve.

Instead of entering the text, you can select it and copy it to the clipboard from another application (such as a browser). Pressing the "From Clipboard" button makes it appear in the window. You can modify it before pressing "OK".

Finally, it is possible to enter a cryptogram directly by having previously pressed the "Crypto/Plain" button (it works like a toggle: if you press it again, you return to normal mode: "Enter a Plain text").

Note: If you want to return to the main window without validating the new problem, simply press the small cross at the top right, which closes the window without any other consequences.

3.3. The screen that lists the problems of a challenge



```
TITLE: September->December 2024
LANG: FR

A-1. Proverbe Africain. [113], French, aristocrat
A-2. Galois. [58], French, aristocrat, nv, C14
A-3. drole de mort. [64], French, aristocrat, kc,
A-4. Bon sens italien. [46], French, aristocrat,
E-1. Sagesse. [50], French, transposition, C14
```

If you want to solve a problem belonging to the current Challenge, you must activate the command:

Challenges => List Challenges

If a Challenge is present (via the command "Challenge" => "Load file"), the screen above is displayed. At a minimum, its title is indicated, which normally specifies its publication date as well as the main language. Other information (author, publisher, etc.) may appear.

For each problem in the Challenge, its characteristics are specified (see 5.1 and 5.3). In short, its number, title, size, language, encryption method, key type and author. You can also have an index in parentheses encrypted in Julius Caesar.

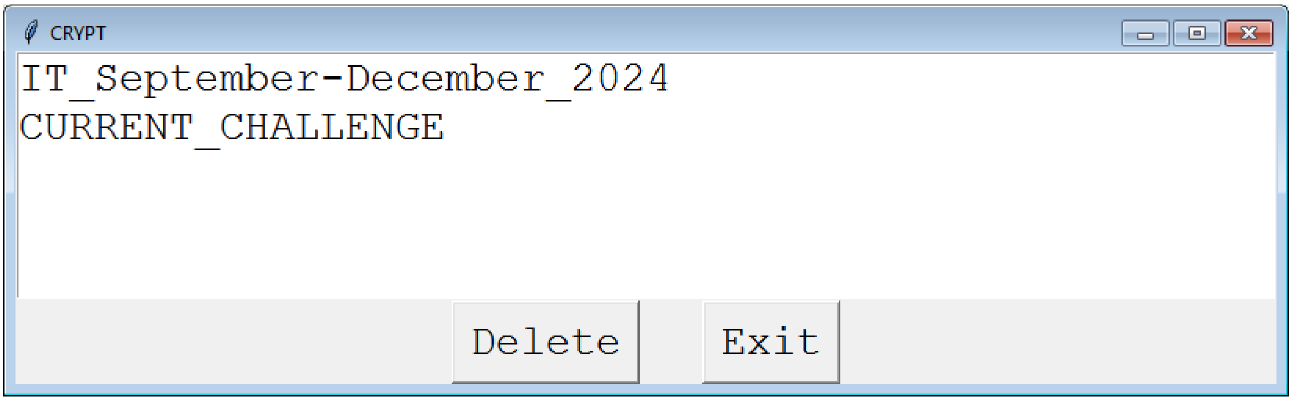
The "Resolved" button allows you to add a star preceding a problem to specify that you have solved the problem. In case of error, you can press this button again to remove the star.

The "Exit" button allows you to return to the current problem.

The "Active" button activates the selected problem which becomes the current problem.

WARNING! Unlike the main window there is no scroll bar. If you want to browse the list or see all the fields, you must use the arrows (in the 4 directions).

3.4. The File Deletion Screen



IT_September-December_2024
CURRENT_CHALLENGE

The "Challenge" => "Delete file" menu allows you to delete problems. Either the problems of the Current Challenge, or the problems associated with the same language from a particular archive.

Concretely, we select the file associated with a language and click on the "Delete" button. The name of the archive begins with the name of the language (in the example above: IT = Italian).

The "Exit" button allows you to abandon the form without destroying files.

4. The menus

4.1. – The "File" Menu

1) New random Puzzle: proposes a new problem. A confirmation request is asked. Then, the solution of the previous problem is displayed. The choice of the problem is random but depends on the current language (see 4.4 [Menu Computer]).

2) Open Puzzle via MD5: Each problem is identified by an MD5 sum. You can recall a problem by giving the beginning of this sum. For example, if another person has solved a problem and memorized the MD5 sum that identifies the problem, you can confront them by trying to solve (faster for example) the same problem. Note: the MD5 sum appears in the meta-data that are displayed by the "Information => Meta-data" menu and also in the clipboard following the "To Clipboard" command.

3) Reset: Clears all your deductions. This resets the problem.

4) Save: Saves the current problem and your deductions.

5) Restore: Restores the current problem as it was at the last save.

6) Close: Deletes the current problem and its backup. You can restore it only if you have kept its MD5 sum.

7) To Clipboard: Copies the problem to the clipboard, along with the deductions you have made, as well as the MD5 sum, its length, statistics concerning the cryptogram and the meta-data (and in particular its language). If you copy the contents of the clipboard into a word processor and print it,

you can solve the problem on paper. Warning! It is strongly recommended to use the "Courier" font and a sufficient font size.

8) Exit: The program is terminated but the current problem is saved.

Note: If you want to exit the program without saving, simply press the cross at the top right of the application window.

4.2. – The "Information" Menu

1) Print Statistics: Displays the frequency of the letters of the cryptogram (those that appear at least twice). It display the bigrams and trigrams frequencies too.

2) Hint: Displays an equivalence between a letter of the cryptogram and the corresponding plaintext letter.
Note: using this help is called cheating.

3) Beginning: Displays the meaning of the first three letters of the cryptogram. In ordinary times, this is called cheating. However, for more complex problems, it can be tolerated.

4) Meta-Data: Displays meta-data such as the language, MD5 sum, etc.

5) Plain letters not found: Displays the letters of the plaintext for which you have no hypothesis.

6) Is solved: Checks that you have made a hypothesis for each of the letters of the Cryptogram.

7) Is key correct: Check the validity of the assumptions you made. Using this command may be considered cheating unless you have solved the problem ("Is solved" is true).

8) Solution: Displays the solution. Note: This may be ignored by the software.

4.3. – The "Human" Menu

1) New Puzzle : This command asks a human (e.g. a friend of the player) to propose a new problem. Screen 3.2 is displayed (The screen for entering a new problem).

4.4. – The "Computer" Menu

1) New Puzzle: This command is identical to the "New Random Puzzle" command in the "File" menu.

The following commands correspond to the different languages for which there are problems, for example EN for English, DE for German, FR for French, etc...
If you press one of the languages, it becomes the current language (only for the session).

The current language appears preceded by a check mark.

4.5. - The "Challenge" menu

1) List Challenge: this command lists the problems of the current Challenge and allows you to choose to solve one of these problems (see screen 3.3).

2) Load file: this command allows you to load problems, either from a new Challenge or from an archive associated with a specific language. These files are typically retrieved from the official

website of the software (see menu "Help" => "About").

3) Delete files: this command allows you to delete the problems loaded via the previous menu ("Challenge" => "Load file) (see screen 3.4).

4.6. – The “Help” menu

1) Manual: Displays this manual.

2) Statistics: Displays statistics for the current language, by default for English.

Note: The manual and statistics are stored in PDF format. The software must be configured correctly to display a PDF file. If this is not the case, the user can either configure the software (see Appendix A-2), or display the PDF files included in the software himself, or finally retrieve or display these files from the official website of the software (indicated in the following menu “Help” => “About”.

3) About: Displays the software version, its author, its official website, …

5. Challenges

5.1. The concept

As we have seen, this program mainly allows you to solve puzzles chosen randomly from a database provided with the software (but which can be increased). A puzzle is a cryptogram encrypted via a simple substitution.

I have added another source of puzzles: Challenges. A challenge corresponds to a set of cryptograms but for which *the solution is not provided*. In addition, the majority of problems come from plain texts in the same language (English, French, ...). The software allows you to install a challenge that replaces the old one. My website can contain a few Challenges. The format of a Cryptogram and a Challenge are given in the Appendix, which allows anyone to create challenges (if they are computer scientists). In short, a Challenge is an archive file (TAR) composed of JSON files.

Typically a Challenge is composed of several types of problems:
- Simple substitutions with word separation (Aristocrat), numbered from A-1 to A-x.
- Simple substitutions without word separation (Patristocrat), numbered from P-1 to P-x.
- Aristocrats but in a language that differs from the main language. For example, if the main language is English, we will use languages such as French, German, Latin, etc. These problems are numbered X-1 to X-x (X for Xenocrypt). If the language is unknown, it will be indicated by "??".
- Encrypted messages not using simple substitution, for example the full-table transposition, numbered from E-1 to E-x.

Note: In a cryptogram, a proper name (a character, a place, etc.) is normally preceded by an asterisk. For example, the plain text "marco polo has been to china". The cryptogram will be (via JC substitution): *NBSDP *QPMP IBT CFFO UP *DJOB.

5.2. Installing a Challenge

The "Challenge" => "Load File" menu allows you to load new cryptograms. The command displays the file search dialog box. A TheCry file type is recognized because its name begins with TC in capital letters and its extension is ".tar" (TAR format).

There are two types of TC files:
- Files that contain cryptograms from texts in a particular language and that are intended to be chosen randomly. The language appears just after TC.
- Challenges. The main language appears at the end of the name (before the tar extension).

If you install a Challenge, the program asks you for confirmation. Indeed, installing a new Challenge deletes the current Challenge.

Note: If the selected problem is of the "Exchange" type (i.e. is not a simple substitution), TheCry software does not allow you to help you to solve the problem. The main screen becomes simpler: it only displays the Cryptogram. You should use the "File => To Clipboard" command to be able to solve the problem on paper or via another software.

5.3. Choose a problem that is part of the current Challenge

The "Challenge => List Challenge" menu lists the problems that make up the current challenge as well as meta-data on the Challenge itself: its author, its publisher, its publication date, the number of problems and especially the main language.

For each challenge is indicated (if the information is present in the problem):
- Its number (A-x, P-x, X-x, E-x, …) which notably specifies its type (A = Aristocrat, P = Patristocrat, X = Xenocrypt, E = Exchange [method different of the simple substitution])
- Its title (this can help in some cases).
- Its size (the number of letters that make up the cryptogram).
- Its language (this is especially relevant for Xenocrypt type problems)
- The encryption method (Aristocrat, Patristocrat, Beaufort, Full Table Transposition, …)
- The formation of the encryption key (k0, ka, kb, kc, …) (see Appendix A-4).
- The author of the cryptogram (usually different from the author of the plaintext).

If you select a problem and press the “Active” button, this problem becomes the current problem (see screen 3.3).

Appendices (advanced aspects and supplements)

A-1. The genesis of the program

This program derives from a whole line of software that I have designed for several decades.

The first version was written in Perl and worked in text mode. It allowed me to encrypt a text chosen randomly from a database consisting of a single file composed of several texts separated by a line composed of "-". I used simple substitution with word separation. As my linguistic knowledge was very weak, I only used texts in French. I was the only user of this program.

I quickly realized that adding plain texts took me far too much time. I then discovered the Fortune software which displays a text (a proverb, a quote, a joke, ...) randomly from external databases that could be added. I only had to create a "parser" to have at my disposal several thousand texts usable by my program.

Then, I discovered the Python language and improved my knowledge in Cryptography and Computer Science. I naturally rewrote my program in Python. I described my passion (cryptography) to neighbors. I started to send them problems by email almost every couple week that I generated with my program. This boosted my interest in improving my program. I wanted to finally give it to them so that they could generate the problems themselves. Obviously this version had to be graphical to be usable by anyone.

In the meantime, I discovered "The Cryptogram", the journal of the ACA (American Cryptogram Association). I subscribed, but unfortunately, the publisher suspended my subscription for no reason. I took elements from this journal. In particular, I adopted its vocabulary (Aristocrat, ...) and the format of a problem (number, title, ...).

I also chose to memorize a problem in JSON format and to identify it by an MD5 sum. So even if I created thousands of cryptograms, they will still be identifiable. Thus, different people will be able to tackle the same problem even if it was initially chosen randomly.

Recently, I discovered the "online" version of the ACA program which allows to generate problems based on simple substitution. This allowed me to correct the graphical interface of my software and simplify it.

I have several ideas for improvements to my program, but I will wait a little for feedback from users now that I have published it on the Internet (my neighbors were able to get it :-).

A-2. Configuration

1) The DATA/lang.txt file contains the default language. It contains (a priori) EN which corresponds to the English language. You can change its value.

2) The DATA/cmd_pdf.txt file contains the command that allows you to display a PDF. It depends on the operating system and the application you use to display a PDF (Acrobat Reader, Firefox, …, evince, …).

For example, on Windows, I use Acrobat Reader. I use the command:

```
acrobat
```

```
        or
    start acrobat
```

I also use the following commands (on Windows):

```
    firefox
    start acrord32.exe          (Still Acrobat, but on some versions of Windows)
    start firefox               (The Firefox browser [you have to install it])
```

WARNING! I need to modify the user's PATH variable to add the path of the software I use (firefox.exe, acrobat.exe, …). To do that, I activate the following form :

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

On Linux, we directly indicate the name of the graphics software that displays a PDF (if the software path is part of the PATH variable):

```
    firefox
```

Note: I could have used a Python library instead of using an operating system command, but I wanted my program to use ONLY the Python standard library.

A-3 - Data files (cryptograms), add cryptograms

Cryptograms are stored in JSON format files whose name corresponds to the MD5 sum of the cryptogram (CRYPTO field) and which have the extension ".cry". Here is an example of a file:

```
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"
}
```

The only mandatory field is the "CRYPTO" field, all other fields are optional and many other attributes can be added (AUTHOR, TITLE, NUMBER, HINT, ...). If they exist, they will appear via the "Meta-Data" command in the "Information" menu. The PLAIN attribute is used by the commands of the "Information" menu.

For a cryptogram to be taken into account by the software, it must be in a tree structure starting from a two-letter directory present itself in the "CRYPTOS" directory. The philosophy of the software is that this two-letter directory corresponds to a language (DE, EN, FR, ...). But this directory can be for example ZZ and thus isolate a set of problems.

It is possible to add a problem or a set of problems by putting them in a TAR file whose content are "*.cry" files in the format described above and inside the correct directory (for example : CRYPTOS/EN/). On my website, I provide some files containing thousands of new problems for different languages.

Notes:

1) The Cryptograms that were generated from plaintext via the "Human => New Puzzle" menu command are stored in the CRYPTOS/WORK directory.

2) The cryptograms that make up a challenge are stored in the CRYPTOS/CHALL/ directory.

A-4. Key generation

TheCry software handles (essentially) simple substitutions. The problems that I generated automatically each use a key also created automatically that corresponds to a mixture of letters of the alphabet.

When I decided to add the possibility of solving Challenges, I was inspired by The Cryptogram journal which offers several methods of key generation (8 in total). I describe below the methods K1, K2 and Caesar which are the most used.

I also created the methods Ka, Kb and Kc. I named K0 my initial method (random mixture of letters of the alphabet) JC the Caesar method, Ka (corresponding to the ACA K2 method) and Kc (corresponding to the ACA K1 method).

1) The ACA methods:

K1: the encrypted alphabet is in the normal order (but perhaps shifted). The plain alphabet contains a 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: the plain alphabet is in normal order, the cipher alphabet contains a keyword.

```
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: we use the Julius Caesar substitution method. We shift the plain and cipher alphabets by a certain number of letters. I call this method JC.

2) My methods

K0: does not use a keyword. The key is random.

Ka: Corresponds to the K2 method of the ACA, but without shifting the cipher alphabet.

Kb: Corresponds to the K2 method of the ACA.

Kc: Corresponds to the K1 method of the ACA.

JC: Corresponds to the Caesar method of the ACA.

NV: Corresponds to the US Army cipher circle method and used in the M-209: we have two alphabets in the normal order but one is reversed and shifted relative to the other.

A-5. Add documentation in PDF format

By default, only the English version of the manual (the documentation you are currently reading) is available from TheCry software. Similarly, the statistics present only concern the three installed languages: English, French and German.

Other files are available on the official website of this software. You can download and install them in the THE_CRY/DATA directory.

Here are the naming conventions for the documentation:
- The manual: ZZ_manual.pdf
- The statistics: ZZ_tests.pdf

ZZ being the code specifying the language: EN, FR, DE, IT, ES, …