Cryptage version 1.3

Based on an Alexander Pukall's algorithm

PRINCIPLE

The cryptosystem used by this software is based on the **PC1 algorithm** (Pukall Cipher 1). This is a stream cipher (each byte is separately encrypted) in PFB mode (Plaintext Feddback : each plaintext byte modify the others crypted bytes). It was designed in 1991 by **Alexander Pukall**.

The algorithm is under copyright but the exploitation rights for this software have been delivered by the Author.

USE OF THE SOFTWARE

It's a very easy soft : you have only to enter a password, type or paste the plaintext and click on the *Crypt* button, to obtain the ciphertext.

A crypted text will be decrypted by clicking on the *Decrypt* button : the password must be the same !

PASSWORD

The **password** can be up to **10 characters**, but don't forget that if the password is longer, then the ciphertext is stronger.

In fact, a **10 characters** password is a **80 bit** key. To crack a 80 bit key with 1 million key per second, this will take 38 billion years !

To choose your **password**, you should use a hashed key. You choose an easy sentence (a 10 words sentence) and you use as the password the first letter of each word.

This is an example :

Sentence : **M**y **c**omputer **a**nd **I** **a**re **v**ery **v**ery **g**ood **f**riends !
Password : **Mcalavvgf!**

This is a 10 characters password (80 bits).

// Note that the lower and upper letters are not the same, and you can use special letters (!,;.?%-_)

PLAINTEXT

The **plaintext** is the text which will be encrypted. You can use the special characters : dot, slash, carriage return (even blank lines) : all this text will be encrypted.

- With the *Font* button, you can choose a proportional font or not.
- With the *Copy* button, you can copy the text.
- With the *Paste* button, you can paste the text.
- With the *Crypt* button, you crypt the plaintext into the ciphertext area.

With the option *Format the crypted text to x characters*, you can format the text as you want. It can be use for some remailer with SMTP protocol. The number can be from 1 up to 255 characters.

// The plaintext must not exceed 16 Kb !

CRYPTED TEXT

The **crypted text** is the text which will be decrypted. If the crypted text comes from a paper, you must carefuly type in. If the text comes from a disk, a remailer ... you can simply "Paste" it.

- With the *Font* button, you can choose a proportional font or not.
- With the *Copy* button, you can copy the text.
- With the *Paste* button, you can paste the text.
- With the *Decrypt* button, you decrypt the ciphertext into the plaintext area.

To decrypt the ciphertext, you must have the correct password.

// The ciphertext must not exceed 32 Kb !

INFORMATIONS

This soft is for Windows **3.x / 95 / 98**. (it's a 16 bit soft)

The author give no warranty to you.
He's not responsible for your use of this soft.

The author, **Pierre TORRIS**

---

[1] ***PC1 Algorithm*** *(Pukall Cipher 1)*

- Designed in Motorola 6809 Assembler in 1991 by ***Alexander Pukall***
- Translate into Turbo C in 1991 by ***Alexander Pukall***
- Translate into Turbo Pascal (Delphi) in 1998 by ***Pierre Torris***

For information :

Others crypto softs are available for download on the author's web site.

E-mail : **Pierre.Torris@wanadoo.fr** Web : **http://www.mygale.org/11/ptorris**
