Агент 007

ПРОГРАМА ЗА КРИПТОГРАФСКО ПРЕОБРАЗУВАНЕ

НА

ИНФОРМАЦИЯ

УПЪТВАНЕ

(13.07.2005)

С т а н и с л а в З Л А Т И Н О В

ВЕЛИКО ТЪРНОВО

П Р Е Д И С Л О В И Е

1. Програмата е разработена от Станислав Златинов, гр. Велико Търново, България.

2. Права на ползване и разпространение: програмата Агент 007 (в.0.04), може да се използва и разпространявана свободно от всеки.

3. За осигуряването на по-голяма сигурност на информацията е препоръчително, информацията да бъде компресирана (архивирана) преди процеса на шифриране.

4. Агент 007 (в.0.04) е абсолютно безплатна програма за шифриране на всякакъв тип файлове, с помощта на криптографския алгоритъм Blowfish, с дължина на ключа – 512 бита (64 символа).

5. ЗАПОМНЕТЕ!!!

За осигуряването на реална сигурност на файловете, които шифрирате, използвайте парола с дължина не по малка от 8 символа (и не по-голяма от 64). Не е препоръчително използването на думи и изречения (от който и да е естествен език). По добре е да използвате случайна комбинация от букви и цифри.

6. ВНИМАНИЕ!!!

Изключително важно е правилното използване на потребителската парола. Ако загубите паролата с която сте шифрирали даден файл, Вие няма да бъдете в състояние да прочетете или използвате този файл. Авторът на програмата също няма да може да Ви помогне по никакъв начин.

7. Авторът на програмата не носи никаква отговорност за възможни последствия от използването и!

ВЪВЕДЕНИЕ

В програмата Агент 007 е реализиран *64* битовия блоков алгоритъм *Bowfish* (в тази версия временно е премахнат алгоритъма *GOST*), с фиксирана дължина на ключа равна на 512 бита, с помощта, на който се осигурява много добра защита на обработваните файлове. Алгоритъмът работи в режим на гамиране с обратна връзка (*CFB mode*).

Защо точно *Bowfish*? Този алгоритъм е избран неслучайно. *Bowfish* е един впечатляващ, със своите качества, алгоритъм. Той е бърз и сигурен. Реализиран е в много програмни продукти и е достатъчно щателно изследван. Досега неговата сигурност не предизвиква никакви съмнения. Подходящ е за многократно шифриране с един и същ ключ. Освен това *Bowfish* не е патентован и е подходящ за общо ползване.

Какво е новото в тази версия?

- Опростена среда за ползване.
- Въведено е ограничение за минималната дължина на паролата (мин. 6 символа).
- Функцията за криптографско преобразуване (*Blowfish*) използва, като ключ хешираната стойност на паролата (с това се цели премахването на статистически зависимости между естествените езици и текущия ключ).
- Модифициран е криптографският алгоритъм. Вместо досега използвания алгоритъм Blowfish, със максимална дължина на ключа 448 бита, в тази версия на Агент007 се използва модифициран Blowfish алгоритъм с разширена дължина на ключа – 512 бита.

За контакти:

Станислав Златинов, Велико Търново, България

моб: 0899/ 34 67 53

e-mail: *agent007.bg@gmail.com*

---

1. ОБЛАСТ НА ИЗПОЛЗВАНЕ

Настоящата програма е пригодена за шифриране на най-разнообразна информация. Това означава, че потребителят може да шифрира всякакъв тип файлове на своя настолен или преносим компютър.

2. НАЧИН НА ИЗПОЛЗВАНЕ

ШИФРИРАНЕ

Стъпка 1. Потребителят избира входен файл, който ще желае да бъде шифриран.

Стъпка 2. Потребителят избира изходна директория, в която ще се разполага шифрираният файл.

Стъпка 3. Потребителят въвежда ключова информация (за по кратко парола), като е желателно тя да бъде с максимално допустимата дължина от 64 символа. Това изискване носи препоръчителен характер, при по малка парола се намаля-ва устойчивостта на шифрирания файл, към различни атаки.

Стъпка 4. Потребителят потвърждава, въведената в Стъпка3 парола, като я въвежда отново.

Стъпка 5. Потребителят се уверява че е избрана операцията “Шифрирай”.

Стъпка 6. Потребителят избира операцията “ЗАПОЧНИ”.

ДЕШИФРИРАНЕ

Стъпка 1. Потребителят избира операцията “Decrypt”

Стъпка 2. Потребителят избира входен файл, който ще желае да бъде дешифриран (с разширение “.ag”).

Стъпка 3. Потребителят избира изходна директория, в която ще се разполага дешифрираният файл.

Стъпка 4. Потребителят избира операцията “Start”.

Стъпка 5. Потребителят въвежда съответната парола.

За контакти:

Станислав Златинов, Велико Търново, България

моб: 0899/ 34 67 53

e-mail: *agent007.bg@gmail.com*