Донецький Національний Технічний Університет

Лабораторна робота № 6

«Дослідження програмних реалізацій з застосуванням методу експерименту»

Виконав:

ст. групи ІПЗІм -17

Лисенко А. С.

Перевірила:

доцент каф. ПМІ

Маслова Н. О.

Покровськ 2017

Вариант 9

Выполнив архивацию выбранных файлов file1.txt и file2.txt с использованием разных методов шифрования (store, best) получаем файлы file1.rar и file2.rar затем ещё раз архивируем архивируемый файл на место прежнего для выполнения поиска марканта в криптосистемы, сравниваем файлы по битам и получаем такой же файл, скриншоты представлены ниже

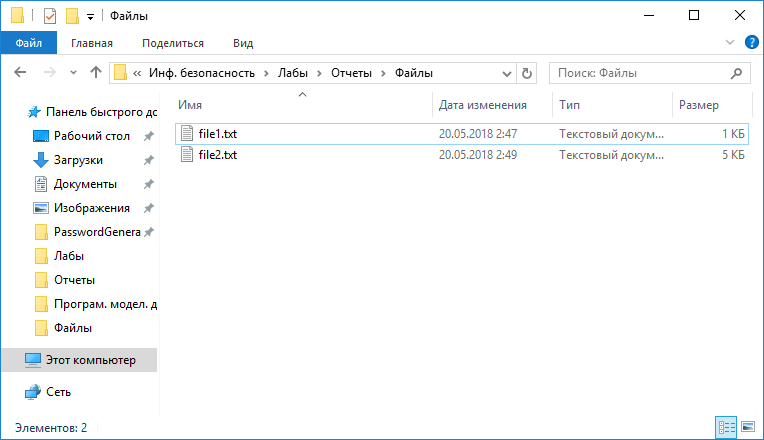


Рис. 1 – Каталог файлов

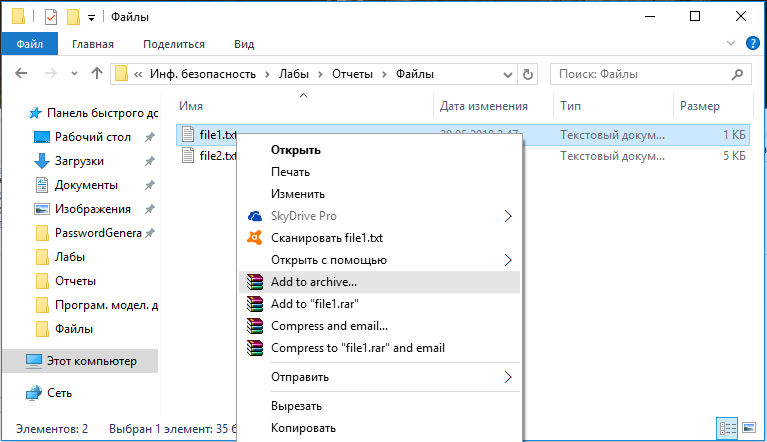


Рис. 2 – Добавление в архив

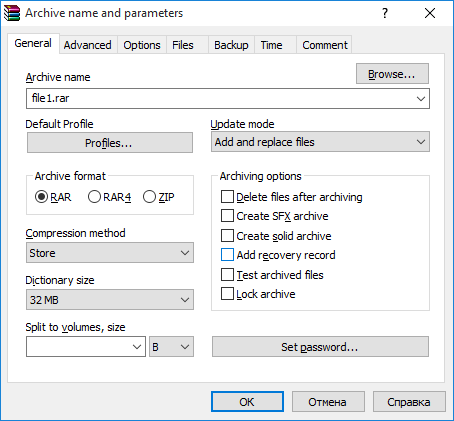


Рис. 3 – Создание архива методом store

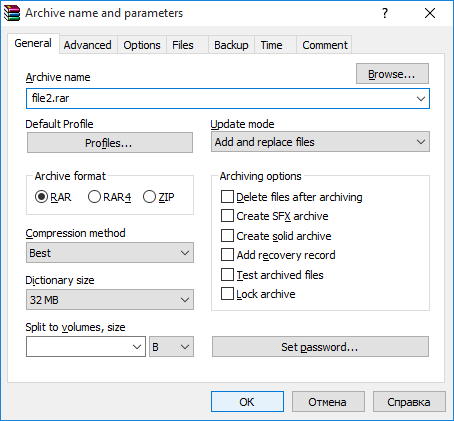


Рис. 4 – Создание архива методом best

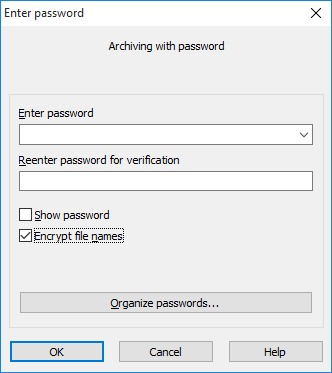


Рис. 5 – Шифрование имени заголовка

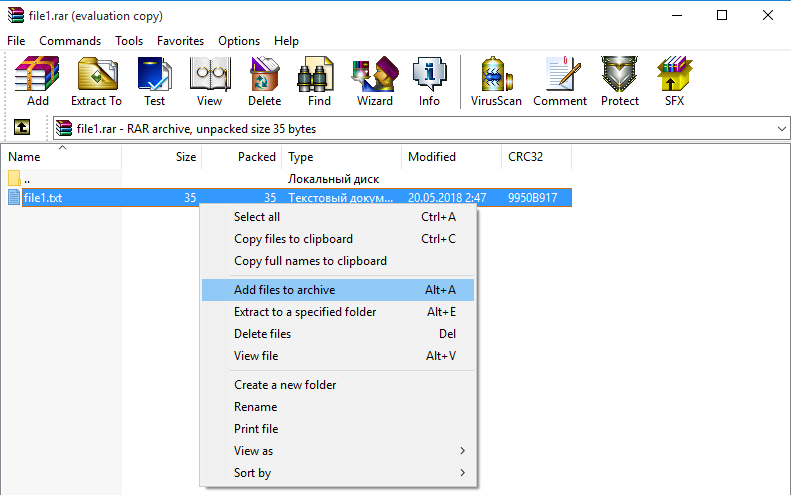


Рис. 6 – Добавление в архив архивированного файла для проверки манката

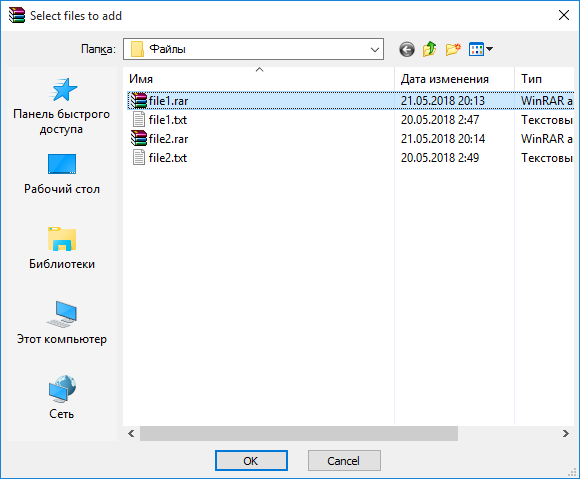


Рис. 7 – Добавление в архив

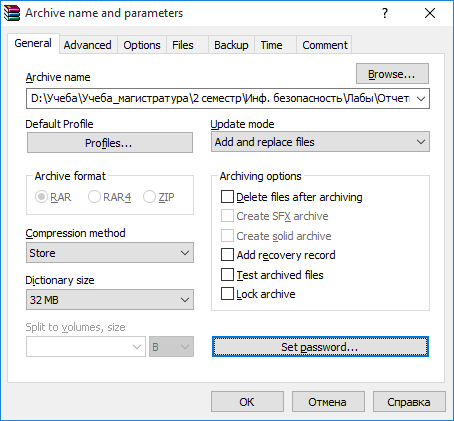


Рис. 8 – Архивирование

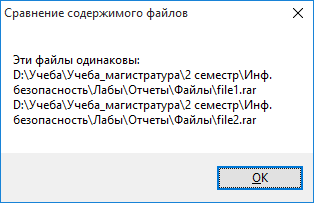


Рис. 9 – Сравнение файлов с помощью Total Commander

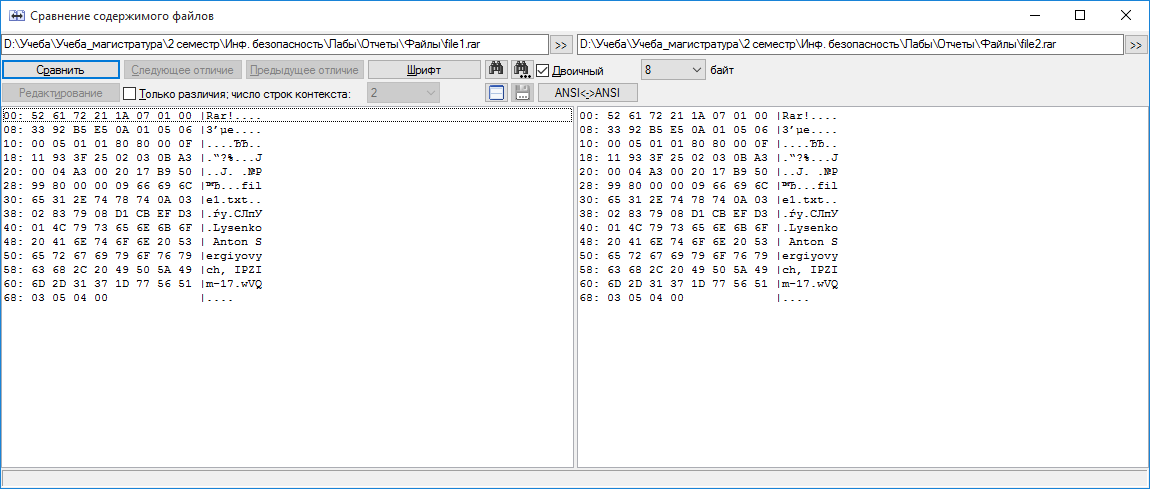


Рис. 10 – Сравнение содержимого файлов по битам в двоичном виде

Наличие или отсутствие марканта в криптосистеме.

Проводим двукратное шифрование одного и того же открытого текста на одном и том же ключе.

Если в результате двух шифрований получены разные шифртексты, значит, в криптографическом преобразовании используется маркант — случайно генерируемое число или строка, предназначенное для затруднения выявления в потоке зашифрованных данных одинаковых фрагментов.

Зависимость марканта, используемого криптосистемой, от текущего времени

Повторяем предыдущий эксперимент в условиях, когда с точки зрения анализируемой программы системные часы остановлены.

В Windows это можно сделать, например, модифицировав машинный код функции GetTickCount в образе библиотеки kernel32.dll, загруженном в адресное пространство анализируемой программы. Если в результате двух шифрований, проведенных в ходе настоящего эксперимента получены одинаковые шифртексты, значит, маркант, генерируемый анализируемой программой, зависит только от текущего времени.

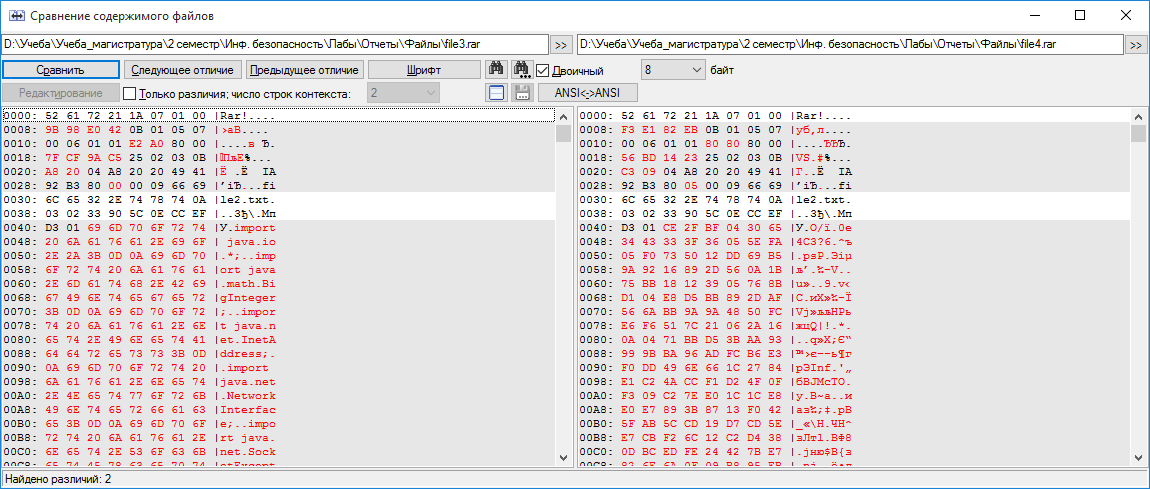


Рис. 11 – Сравнение файлов большей длины

Как видим из предыдущего рис. 11 количество содержимого влияет на архивирование файлов, мы проделали те же операции, что в предыдущем файле и Total Commander обнаружил 2 различия.