

Задание на лабораторную №1 (время 4 акад. часа)

Разработать на выбранном языке программирования программу шифрования и дешифрования 1 блока данных длиной 64 бита, находящемся в произвольном файле по алгоритму шифрования TEA (<http://143.53.36.235:8080/tea.htm>). Блок-схема алгоритмов шифрования и дешифрования приведены на рис. 1 и рис. 2.

Результат в виде исполняемого файла и исходного текста должен быть сохранен в папку студента по пути «ИБ\Лр1*.».

При реализации программы выполнить следующие требования:

1. Исходный текст должен содержать комментарии ко всем переменным и функциям.
2. Все переменные и функции должны содержать в начале имени инициалы студента и символ подчеркивания. Пример: «КАВ_key».
3. Имя файла шифрования является произвольным, длина файла для проверки работоспособности программы 8 байт.
4. Имя файла для хранения ключа шифрования key.txt, длина файла 16 байт. Ключ генерируется псевдослучайной функцией с полным набором используемых символов (<https://ravesli.com/urok-71-generatsiya-sluchajnyh-chisel-funktsii-srand-i-rand/>).
5. Запуск шифрования и дешифрования выполняется с помощью одно файла-программы с использованием ключей (<http://cppstudio.com/post/421/>). Пример:
encrypt -e test.txt — пример запуска программы для шифрования файла.
encrypt -d test.txt.enc key.txt - пример запуска программы для дешифрования файла.
6. В результате шифрования к имени файла дописывается расширение «enc», информирующее, что файл зашифрован.
7. При дешифровании расширение «enc» отбрасывается, то есть имя исходного файла восстанавливается. Если файл с таким именем имеется в каталоге назначения к имени файла перед расширением добавляется в скобках целое число, например test(1).txt.



Рисунок 1. Блок схема алгоритма шифрования

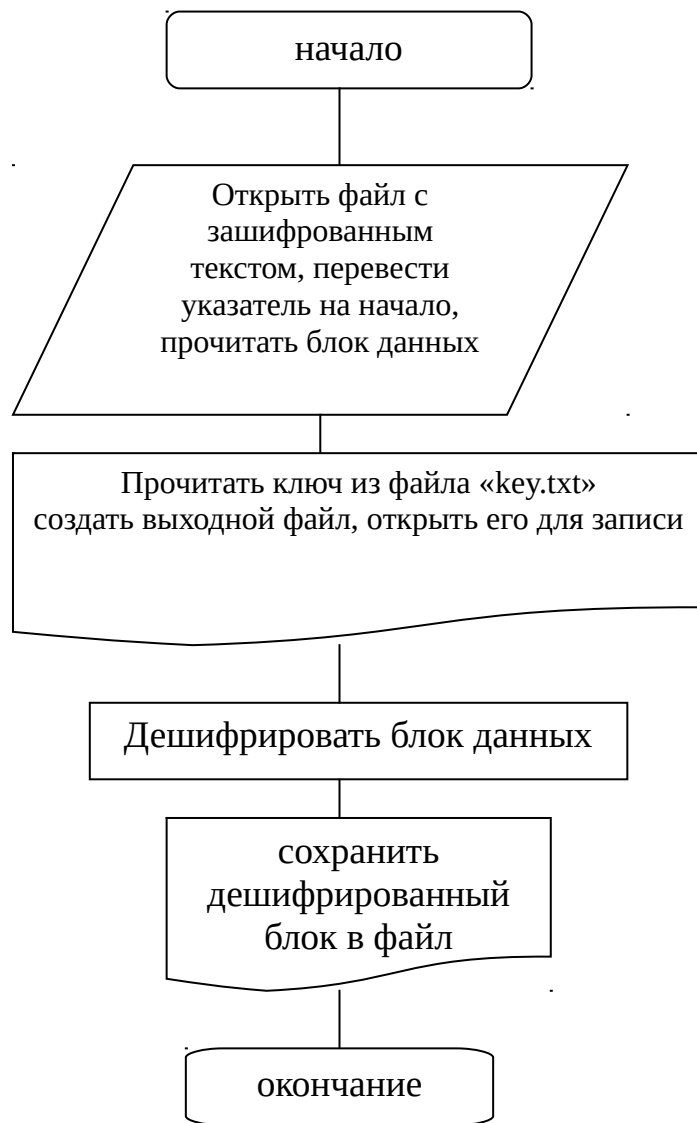


Рисунок 2. Блок схема алгоритма дешифрования