

Задание на лабораторную №2

Разработать на выбранном языке программирования программу шифрования и дешифрирования произвольного файла по алгоритму шифрования TEA и алгоритму создания цепочек OFB (<http://www.intuit.ru/studies/courses/14248/1285/lecture/24208?page=6>). Блок-схема алгоритмов шифрования и дешифрирования приведены на рис. 1 и рис. 2.

Результат в виде исполняемого файла и исходного текста должен быть сохранен в папку студента по пути «ИБ\Лр2*.».

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. Для шифрования берется произвольный файл с размером не менее 4 Мб и не кратным длине блока 8 байт.
4. Для шифрования определить количество блоков кратных 8 байтам и их зашифровать отдельным потоком (циклом шифрования).
5. Проверить последний блок на кратность 8 байтам. Если не кратен 8 байтам зашифровать его отдельной функцией и дописать в конец зашифрованного файла.
6. Запрещается читать полностью файл для шифрования или дешифрирования в ОЗУ. Разрешается читать файлы блоками кратными 8 байтам. Размер блока должен быть согласован с размером свободной оперативной памяти.
7. 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/>).
8. Запуск шифрования и дешифрирования выполняется с помощью одного 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 дешифрирования файла.
9. В результате шифрования к имени файла дописывается расширение «enc», информирующее, что файл зашифрован. Размер зашифрованного файла (криптограммы) должен быть равен размеру исходного файла.
10. При дешифрировании 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. Размер дешифрованного файла должен быть равен размеру исходного файла.

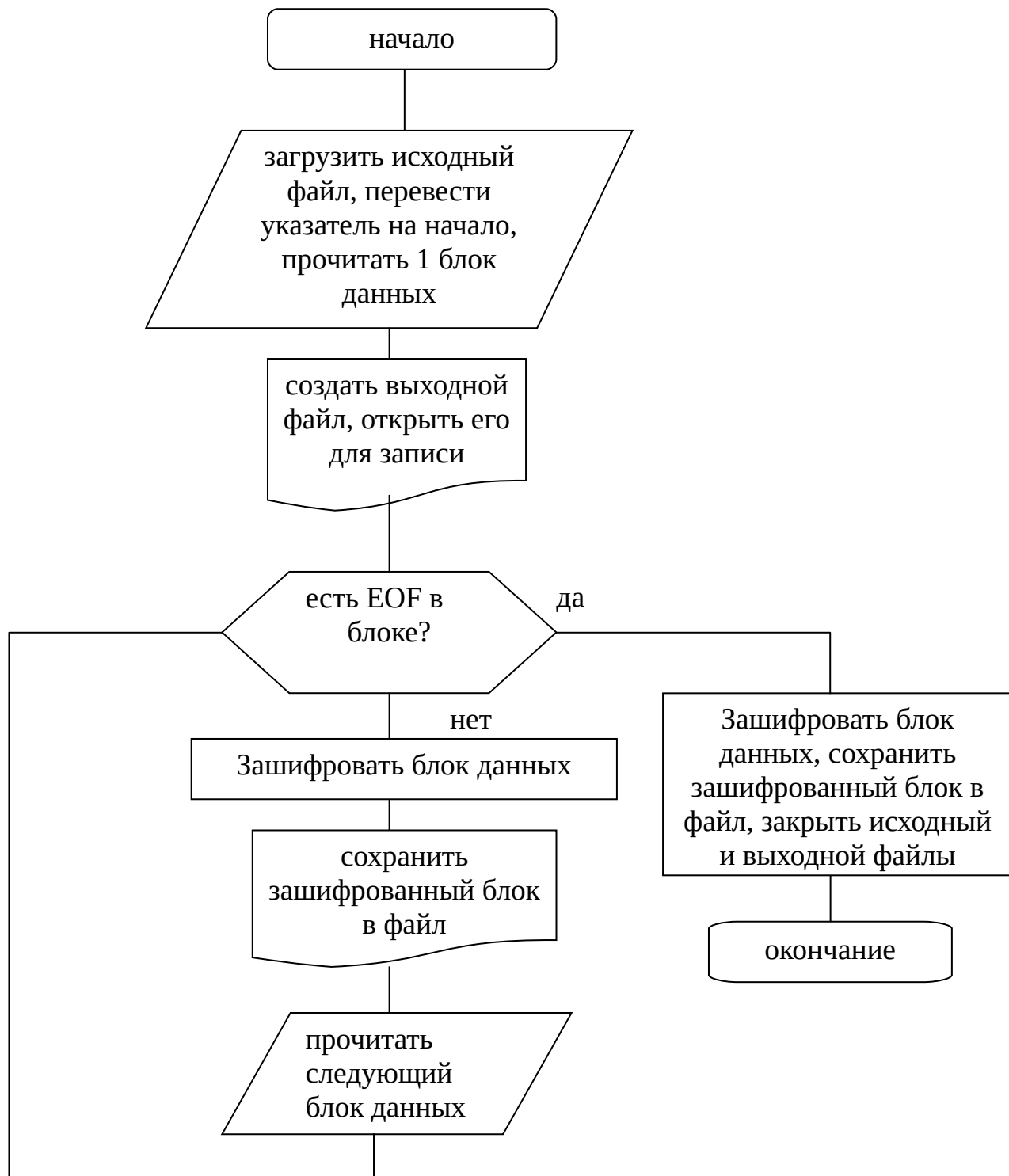


Рисунок 1. Блок схема алгоритма шифрования

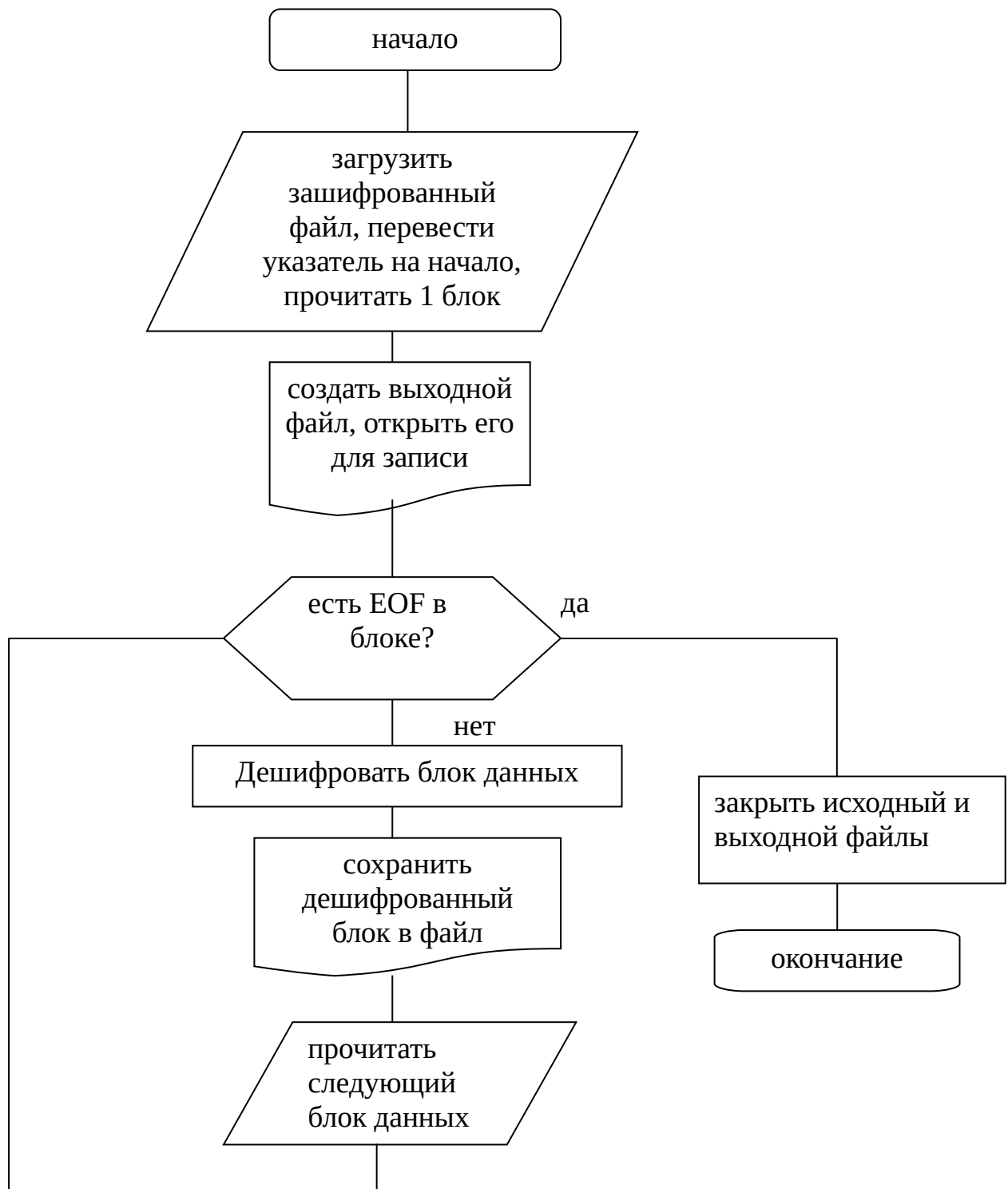


Рисунок 2. Блок схема алгоритма дешифрования