Задача № 2
Реализация и исследование блочного шифра Кузнечик

Описание шифра Кузнечик, который вошёл в состав стандарта РФ ГОСТ Р 34.12-2015, приведено в документе GOST_R_3412-2015.pdf (папка Кузнечик). Программная реализация на языке Си, предоставленная разработчиком стандарта и ориентированная на 8-битовую обработку, содержится в файле 28147_14.c (с хедерами 28147_14.h и table.h). Эту программу будем называть «код InfoTeCS». В документе BRU.pdf (англ.) описан метод ускорения шифра, основанный на предварительно вычисленных таблицах. Все эти документы были прокомментированы на лекциях.

Задание

1. На основе кода InfoTeCS построить приложение, которое воспроизводит контрольные примеры из стандарта. Рекомендуется исключить из кода лишние проверки и печать промежуточных значений. Целесообразно также укрупнить отдельные функции, чтобы минимизировать количество вызовов. Процедуру расширения ключа можно оставить без изменений.

2. Оптимизировать код InfoTeCS для простых 8-разрядных микроконтроллеров путем исключения таблицы умножения (table.h) и замены её алгоритмической реализацией (умножение полиномов ниже 8-й степени с коэффициентами в $\mathbb{F}_2$ по модулю $x^8 + x^7 + x^6 + x + 1$). Проверить правильность на контрольном примере.

3. Оптимизировать код InfoTeCS для 32-разрядных процессоров путем реализации табличных вычислений по методу из BRU.pdf.

4. Провести сравнение по времени (по числу циклов процессора) процедур зашифрования и расшифрования блока для всех трех вариантов программы.

5. Разработать приложение для передачи файла в зашифрованном виде по сети с ключом шифрования, полученным по протоколу MQV.