Задача № 4
Криптографические хеш-функции

Материал для программной реализации криптографических хеш-функций содержится в каталоге HASH. Обзор хеш-функций приведен в файле RF2018-hash.pdf (это фрагмент из новой книжки Рябко Б. Я., Фионова А. Н.; из-за особенностей бесплатной программы извлечения в нем не пропечатались тире). В каталоге есть официальные документы и реализации для отечественной хеш-функции ГОСТ Р 34.11-2012 и американской хеш-функции SHA-3 (FIPS 202, Keccak). Однако для большинства студентов разобраться в официальных реализациях будет сложно. Поэтому предложены также упрощенные варианты программ, описанные ниже.

ГОСТ Р 34.11-2012 в простейшем виде (без оптимизаций) реализован в каталоге hGOST. Там, в частности, есть пример программы test.cpp, показывающий, как интегрировать хеш-функцию в свое приложение. Пример не нуждается в особых комментариях. Все файлы необходимо скопировать в рабочий каталог. Файл gost3411-2012-core.c – добавить в проект (в командную строку компилятора).

Для SHA-3 (равно как и других известных хеш-функций) можно воспользоваться простой библиотекой, содержащейся в каталоге hash-library. Она в обязательном порядке требует C++. Например, для интегрирования в свое приложение SHA-3 достаточно взять два файла – sha3.h и sha3.cpp. Техника использования кода описана в комментариях внутри файла sha3.h.

Задание

1. Выбрать одну понравившуюся хеш-функцию и интегрировать ее в приложение для передачи файла в зашифрованном виде по сети, как это требуют протоколы выработки секретного ключа. Сравнить время вычисления хеш-функции с временем выполнения других операций в протоколе.