Задание по практикуму на ЭВМ №2. 319 группа. 2017 год.

Описание задания.

Необходимо реализовать хэш функцию из семейства хэш функций SHA.

БЫРЕЕВА АНАСТАСИЯ АНДРЕЕВНА – SHA-512

ЕФРЕМОВ СТЕПАН СЕРГЕЕВИЧ – SHA-256

ЖАНДАРОВИЧ НИКИТА ИГОРЕВИЧ - SHA-512

КАСЬКОВ НИКИТА РОДИОНОВИЧ - SHA-512

КАШТАНОВ АЛЕКСЕЙ АЛЕКСЕЕВИЧ - SHA-512

КОЛЕНИКОВА ВЕРА АНДРЕЕВНА - SHA-256

КОНЮХОВ СЕРГЕЙ АНДРЕЕВИЧ - SHA-256

Входные параметры:

Параметры передаются в качестве аргументов командной строки:

--path=<path_file>

Где <path_file> - путь до файла с исходными данными.

Структура файла следующая:

INPUT=0923ABCD74380

Данный пример носит справочный характер, а не является тестовыми данными.

Выходные параметры:

На выходе должен быть получен файл следующего вида:

INPUT=0923ABCD74380

OUTPUT=2491AD6723440

Список литературы:

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

Требования к реализации:

1. Необходимо разработать библиотеку, реализующую функционал по заданному программному интерфейсу, и разработать утилиту модульного тестирования всего функционала библиотеки.

2. Программа должна быть написана на языке C++

3. Корректная обработка всех возможных ошибок и входных данных

4. Прохождение всех контрольных примеров из стандарта

5. Код должен быть комментирован, читаем, без «магических чисел»!!!

Сроки приема задания:

Сдача задания состоится 19.04.2017, о времени договоримся ближе к делу. Необходимо будет на предоставленных мною файлах с тестовыми данными продемонстрировать правильность работы программы, а также знание и владение кодом.