Лабораторная работа №2

**Изучение криптографических алгоритмов.**

**Алгоритмы хэширования.**

Задание

1. Реализовать указанный преподавателем алгоритм хэширования.
2. Программа должна иметь интерфейс, в котором содержатся данные студента, вариант, справочная информация – алгоритм и его описание, возможности для сохранения и выбора обрабатываемого файла.
3. Отчет должен содержать вариант задания, блок-схему алгоритма, реализованного в программе, листинг программы с комментариями, расчет данных по одному циклу алгоритма.
4. Отчет и код программы с исполняемым кодом дополнительно представляются в электронном виде.
5. Обрабатываться должен файл любого формата(word,excel, графические форматы и т.д.), длиной не менее 1 кБ.
6. Для хэш-функций должны быть приведены результаты хэширования каких-либо значений, полученных в разрабатываемой программе, и результаты хэширования, рассчитанные с помощью общедоступных инструментов в сети «Интернет».
7. Ответить на вопросы преподавателя.

**Варианты:**

1. Хэш-функция MD4.
2. Хэш-функция MD5.
3. Хэш-функция SHA-1.
4. Хэш-функция ГОСТ Р 34.11 (в работе указать какая разновидность стандарта реализована).