**Написать работу по данным и требованиям в файлах заказа**. Уникальность от 30% с проверкой по бесплатной версии антиплагиат ру, заимствование из одного источника не более 25%. Антиплагиат нужен реальный, без технических поднятий, замены букв, символов, переносов и прочего, такое не пройдет проверку. **Если есть вопросы по работе**, их можно оперативно обсудить в заказе.

Алгоритмы шифрования. Суть в исследовании и сравнении алгоритмов ЭЦП. Необходимо реализовать и сравнить эффективность, построить графики по полученным результатам. В коде не нужно использовать специальные библиотеки, то есть чтобы было видно по алгоритму что и как вычисляется.

Реализовать два приложения на C++ в VS (2019) для постановки и проверки электронной цифровой подписи.

1. ЭЦП по ГОСТ Р 34.10.-1994 для сжатия файла использовать хэш-функцию ГОСТ Р 34.11-1994

2. ЭЦП по ГОСТ Р 34.10-2012, для сжатия файла использовать хэш-функцию ГОСТ Р 34.11-2012

Меню приложений:

****

При постановке подписи – на вход подается файл txt с текстом, пользователь вводит имя нужного файла, на выходе – ЭЦП должна сохраниться в отдельный файл (.txt). При проверке – выбрать файл с документом (.txt) и с ЭЦП (.txt) из нужной директории, на выходе сообщение с результатом проверки.

Если подпись верна – вывести сообщение «Подпись верна. Файл не был изменен»

Если подпись не верна – «Файл был изменен!»

Отдельно реализовать программный код для сравнения эффективности алгоритмов. Необходимо сравнить длину ключей (открытых, закрытых), генерируемых алгоритмами. Сравнить время выработки хэш-функции. Сравнить время 1.генерации ключей, 2.постановки подписи, 3.проверки подписи.

В отдельном файле .doc описать полученные результаты. Для сравнения ключей – таблица с полученными результатами. Для сравнения хэш-функций построить график зависимости времени работы (100 повторов) от длины текста в байтах. Для сравнения времени работы процессов построить график зависимости времени работы (100 повторов) от ГОСТа. Примеры ниже на скринах. Описать технические характеристики компьютера, на котором было произведено исследование.
Объем пояснительной записки на усмотрение автора.

