*Лабораторная работа №4*

**Электронная подпись**

Цель работы: ознакомиться с принципами работы и алгоритмами, используемыми для создания электронной подписи. Разработать консольное приложение, позволяющее сгенерировать и проверить цифровую подпись для файла.

Задание:

1. Разработать консольное приложение, осуществляющее основные этапы ЭП:
   1. генерацию ключа подписи
   2. подпись данных
   3. проверку подписи

Приложение должно обладать функционалом выбора алгоритма ЭП из следующего списка:

* RSA-SHA256
* RSA-SHA512
* DSA
* ECDSA
* ГОСТ 34.10-2018 - опционально

1. Для каждого алгоритма измерить время, необходимое для формирования ключа, подписания и проверки подписи файла размером 2мб. Для тех, кто не может или не хочет так:  
   dd if=/dev/urandom of=urandom\_test count=2048 bs=1024  
   ссылка на [файл для тестов](https://drive.google.com/file/d/0B9BryOu65ov2OGNodkVnS29CRDQ/view?usp=sharing&resourcekey=0-FMZLBq_rB6Of9crdm5CmOg).

Результаты можно представить в виде таблицы или диаграммы.

Требования к консольному приложению

Консольное приложение должно иметь три режима:

* генерация ключа подписи и ключа для проверки подписи
* подпись файла
* проверка подписи

Консольное приложение должно принимать на вход следующие аргументы:

* режим работы
* алгоритм для подписи
* имя/имена файлов для ключей
* имя файла для подписи/проверки подписи
* имя файла для результата

О реализации приложения

Выбор языка не ограничен.

Формат хранения ключей в данном случае является спорным вопросом. К примеру, Node.js [поддерживает](https://nodejs.org/api/crypto.html#crypto_class_sign) использование ключей как в бинарном виде, так и в формате PEM. По умолчанию предлагаю использовать бинарный формат хранения ключей, чтобы не зависеть от платформы. Если в выбранных вами средствах нет возможности использования ключей в бинарном виде - обратитесь ко мне в телеграм (@a\_robingood) и мы решим, что с этим делать.

Также возможно, что у вас не будет какого-либо из алгоритмов подписи, хотя я постарался выбрать наиболее популярные. В остальных случаях порядок действий следующий:

* более внимательное чтение документации,
* поиск решений на [stackoverflow](http://stackoverflow.com/) и [github](http://github.com)
* в случае отсутствия возможности - воспользоваться другими средствами или реализовать возможность самостоятельно и, возможно законтрибьютить свое решение. *Если кого-то все-таки посетит идея сделать патч и помочь сообществу - это вполне тянет на курсовую работу.*

Контрольные вопросы

1. Электронная подпись. Определение.
2. Виды ЭП
3. Преимущества и недостатки ЭП на симметричных алгоритмах шифрования
4. Преимущества и недостатки ЭП на асимметричных алгоритмах шифрования
5. Классификация ЭП
6. Алгоритмы ЭП