Лабораторная работа № 5
Асимметричная криптография

Базовое задание (7 *баллов, дата сдачи* ≤ *02.06.2022*).

Реализовать ЭЦП RSA (подпись и проверка подписи), используя при этом хэш-функцию из лабораторной работы № 4.

Дополнительные задания (принимаются при условии, что сдано основное задание, *i*-ое дополнительное задание принимается при условии, что сданы дополнительные задания 1,..., *i*–1, *i* = 2, 3,...).

– 1. (*2 балла, дата сдачи* ≤ *26.05.2022*) Реализовать генерацию простого числа $p > 2^{128}$, реализовать критерий проверки простоты числа (на ваш выбор).

– 2. (1 + 5 баллов, *дата сдачи* ≤ *19.05.2022*). Реализовать ЭЦП RSA с модулем $n = pq$ таким, что $p > 2^{128}$, $q > 2^{128}$, секретный ключ $d > 2^{128}$. Всю длинную арифметику необходимо реализовать самостоятельно.