Лабораторная работа № 5
Асимметричная криптография

Базовое задание (8 *баллов, дата сдачи* $\leq$ *03.06.2021*).

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. (1+4 балла, дата сдачи $\leq$ *03.06.2021*). Реализовать ЭЦП RSA с длиной модуля n ($n=pq$) не менее 512 бит.

– 2. (1+4 *балла, дата сдачи* $\leq$ *03.06.2021*). Реализовать трехсторонний протокол Диффи-Хеллмана.