Лабораторная работа №6

Для выполнения этой лабораторной работы рекомендуется сделать три программы, оформив их, например, как отдельные проекты в рамках одного решения: первая программа – для задания 1, вторая программа – для задания 2 и третья – для заданий 3 и 4.

1. Возьмите любой криптопровайдер, который поддерживает работу с цифровыми подписями (а они практически все её поддерживают), сгенерируйте ключевую пару для создания и проверки цифровой подписи (или воспользуйтесь готовой, которая была сгенерирована ранее) и экспортируйте открытый ключ этой пары в файл.

2. Выберите любой файл и создайте для него цифровую подпись, используя закрытый ключ вышеупомянутой пары. В качестве алгоритма хэширования для создания подписи можете взять любой хэш-алгоритм из числа тех, что поддерживаются вашим криптопровайдером. Полученную цифровую подпись сохраните в отдельном файле (не в том, где хранится открытый ключ).

3. Проверьте цифровую подпись у файла. Для этого импортируйте ключ для проверки подписи и саму подпись из файла и проведите необходимые операции.

4. Измените в исходном файле хотя бы один байт и проверьте цифровую подпись у файла ещё раз.