Лабораторная работа №2

*Выберите любой криптопровайдер из тех, что установлены в вашей системе. (Лично я советую вы­бирать провайдеры от Microsoft, потому что провайдеры других производите­лей могут ра­ботать не так, как значится в спецификации.)*

Напишите программу, которая за один запуск выводит на экран все нижеуказанные сведе­ния о выбранном криптопровайдере:

1. тип реализации криптопровайдера (программный, аппаратный, смешанный и т. д.);
2. версия криптопровайдера;
3. список всех криптоалгоритмов, которые поддерживает провайдер. Для каждого алго­ритма в списке нужно вывести следующую информацию:
   1. число – идентификатор алгоритма;
   2. сокращённое название алгоритма;
   3. полное название алгоритма;
   4. класс алгоритма (определяется по идентификатору): алгоритм шифрования, хэши­ро­ва­ния, цифровой подписи, об­мена ключами и т. д.;
   5. тип алгоритма (тоже определяется по идентификатору: для симметричного алго­ритма шифрования – блочный или пото­ко­вый шифр, для алгоритма цифровой под­писи или ключевого обмена – схема RSA или схема DSS);
   6. длина ключа по умолчанию (кроме алгоритмов хэширования – в их работе ключи не используются);
   7. минимально возможная длина ключа (кроме алгоритмов хэширования – в их рабо­те ключи не используются);
   8. максимально возможная длина ключа (кроме алгоритмов хэширования – в их ра­бо­те ключи не используются);
   9. протоколы, которые поддерживает данный алгоритм (если он вообще их поддер­жи­вает), например IPSec, PCT v1, SSL v2, SSL v3, TLS v1 и т. д.
4. инкрементный шаг при изменении длины ключа в алгоритме цифровой подписи;
5. инкрементный шаг при изменении длины ключа в алгоритме ключевого обмена.