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:
   - **a)** число – идентификатор алгоритма;
   - **b)** сокращённое название алгоритма;
   - **c)** полное название алгоритма;
   - **d)** класс алгоритма (определяется по идентификатору): алгоритм шифрования, хэширования, цифровой подписи, обмена ключами и т. д.;
   - **e)** 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);
   - **f)** длина ключа по умолчанию (кроме алгоритмов хэширования – в их работе ключи не используются);
   - **g)** минимально возможная длина ключа (кроме алгоритмов хэширования – в их работе ключи не используются);
   - **h)** максимально возможная длина ключа (кроме алгоритмов хэширования – в их работе ключи не используются);
   - **i)** 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.