Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Валдайцев А. Д.

ФИТ 2 курс 5 группа

Преподаватель: Берников В. О.

Минск 2022

**Практическое занятие №14**

**Тема «****Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки System.Security.Cryptography»**

**Цель:** Изучить модель криптографии .NET Framework, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования.

**Задания для выполнения**

1) Какие симметричные алгоритмы шифрования Вы знаете?

Простая перестановка, одиночная перестановка по ключу, двойная перестановка по ключу, магический квадрат Дюрера, шифр Цезаря, ширф Трисемуса, шифр Плейфера, шифр Виженера, двойной квадрат Уинстона.

2) Какие ассиметричные алгоритмы шифрования Вы знаете?

RSA, алгоритм Диффи-Хеллмана, алгоритм Эль-Гамаля.

3) Основное назначение библиотеки System.Security.Cryptography?

Классы в пространстве имён [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography) управляют множеством сведений о криптографии. Некоторые из них являются оболочками для реализации операционных систем, а другие — исключительно управляемыми реализациями. Позволяют создать открытые и закрытые ключи, электронные подписи, ассиметрично шифровать файлы и сообщения через безопасные потоки, используя последние разработки в этой сфере, а также переопределять абстрактные классы для создания собственных реализаций алгоритмов.

4) Влияет ли размер ключа на криптостойкость алгоритма?

Да.

5) Назовите основные классы библиотеки System.Security.Cryptography?

Иерархия классов:

- класс типа алгоритма, например SymmetricAlgorithm или HashAlgorithm. Это абстрактный уровень;

- класс алгоритма, является производным от класса типа алгоритма, например RC2 или SHA1. Это абстрактный уровень;

- реализация класса алгоритма, который является производным от класса алгоритма, например RC2CryptoServiceProvider или SHA1Managed. Это уровень реализации алгоритма.

Основные классы:

CryptoStream – производный от класса Stream поток, который связывает потоки данных с криптографическими преобразованиями;

CSPParameters – параметры, передаваемые поставщику служб шифрования (CSP), который выполняет криптографические вычисления;

RSACryptoServiceProvder – шифрование и дешифрование с помощью алгоритма RSA;

RSAParameters - стандартные параметры для алгоритма RSA (значения d, e, n, p, q и т.д.).