МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

**Практическое занятие №14**

**Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)»**

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

**Практическое занятие №14**

**Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/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

**Контрольные вопросы:**

1. Какие симметричные алгоритмы шифрования Вы знаете?

- Простая перестановка

- Одиночная перестановка по ключу

- Двойная перестановка

- Перестановка «Магический квадрат»

2) Какие ассиметричные алгоритмы шифрования Вы знаете?

• RSA (аббревиатура от Rivest, Shamir и Adelman, фамилий создателей алгоритма) — алгоритм, в основе которого лежит вычислительная сложность факторизации (разложения на множители) больших чисел. Используется и для шифрования данных, и для создания цифровых подписей.

• DSA (Digital Signature Algorithm, «алгоритм цифровой подписи») — алгоритм, основанный на сложности вычисления дискретных логарифмов. Используется для генерации цифровых подписей.

• Схема Эль-Гамаля — алгоритм, основанный на сложности вычисления дискретных логарифмов. Применяется как для шифрования, так и для создания цифровых подписей.

• Алгоритм Диффи-Хеллмана – протокол, позволяющий двум и более получить общий секретный ключ, с открытым каналом связи.

3) Основное назначение библиотеки System.Security.Cryptography?

Пространство имен System. Security. Cryptography открывает программный доступ к самым разнообразным криптографическим сервисам, с помощью которых приложения могут шифровать и дешифровать данные, обеспечивать их целостность, а также обрабатывать цифровые подписи и сертификаты.

4) Влияет ли размер ключа на криптостойкость алгоритма?

Чем больше размер ключа, тем, соответственно, больше времени требуется на переборки возможных значений, тем дольше работает алгоритм. Поэтому выбор оптимальной длины ключа - это вопрос баланса.

Минимальные размеры ключей для разных типов информации

|  |  |  |
| --- | --- | --- |
| Разновидность информации | Срок секретности | Длина ключа, бит |
| Военная тактическая | Минуты, часы | 56 |
| Объявления о выпуске новой продукции | Дни недели | 56-64 |
| Промышленные тайны | Месяца | 64 |
| Секрет водородной бомбы | Более 40 лет | 128 |
| Частная | Более 50 лет | 128 |
| Дипломатическая | Более 65 лет | 128 (не менее) |

Криптостойкость симметричных ключей оценивается просто. Например, если длина симметричного ключа составляет 40 бит (такое шифрование называют слабым), то для его реконструкции надо перебрать числа. Используя несколько современных передовых компьютеров, задачу можно решить быстрее, чем за сутки. Это недешевое, но вполне возможное мероприятие. Если длина ключа составляет 64 бита, то необходимо иметь сеть из нескольких десятков специализированных компьютеров, и задача решается в течение нескольких недель. Это крайне дорогостоящее мероприятие, но технически оно возможно при современном уровне развития техники. Сильным называют шифрование с длиной симметричного ключа 128 бит. На любом современном оборудовании реконструкция такого ключа занимает времени в миллионы раз больше, чем возраст Вселенной. Это технически невозможное мероприятие, если нет каких-либо дополнительных данных.

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

**Основные классы:**

‣ **Класс CSPParameters** – содержит параметры, передаваемые поставщику служб шифрования (CSP), который выполняет криптографические вычисления.

‣ **Класс RSACryptoServiceProvider** - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP).

‣ **Класс CryptoStream** – определяет поток, который связывает потоки данных с криптографическими преобразованиями.

‣ **Класс RijndaelManaged** – реализует симметричный алгоритм шифрования Rijndael. Поддерживаются ключи длиной 128, 192 и 256 бит.

**Вывод**: изучены модель криптографии .NET Framework, основные классы и структуры данных.