**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)**»**

**Контрольные вопросы:**

**Какие симметричные алгоритмы шифрования Вы знаете?**

1. **Какие ассиметричные алгоритмы шифрования Вы знаете?**
2. **Основное назначение библиотеки System.Security.Cryptography?**
3. **Влияет ли размер ключа на криптостойкость алгоритма?**
4. **Назовите основные классы библиотеки System.Security.Cryptography?**
5. **Какие симметричные алгоритмы шифрования Вы знаете?**

.NET использует поточно-ориентированный подход для реализации алгоритмов симметричного шифрования и хэширования. Основой такого подхода является класс CryptoStream, производный от класса Stream. Все основанные на потоках криптографические объекты поддерживают единый стандартный интерфейс (CryptoStream) для управления своими частями, ответственными за передачу данных. Благодаря тому, что все эти объекты построены на основе стандартного интерфейса, можно сцеплять вместе различные объекты (например, за объектом, реализующим хэширование, поставить объект, реализующий шифрование) и выполнять ряд операций над данными без использования промежуточных хранилищ данных. Поточная модель также позволяет строить объекты на основе меньших объектов. Например, связанные вместе алгоритмы шифрования и хэширования можно рассматривать как единый поточный объект, несмотря на то, что он может быть построен на основе набора некоторых поточных объектов.

1. **Какие ассиметричные алгоритмы шифрования Вы знаете?**

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP). Позволяет выполнить экспорт, импорт данных ассиметричной пары ключей. Поддерживаются ключи длиной от 384 до 16384 бит с приращениями по 8 бит, если установлен Microsoft Enhanced Cryptographic Provider, и ключи длиной от 384 до 512 бит с приращениями по 8 бит, если установлен Microsoft Base Cryptographic Provider.

1. **Основное назначение библиотеки System.Security.Cryptography?**

В .NET классы в [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography) пространстве имен управляют множеством сведений о криптографии. Некоторые из них являются оболочками для реализации операционных систем, а другие — исключительно управляемыми реализациями. При создании экземпляра одного из классов, реализующих алгоритмы шифрования, ключи создаются автоматически с целью удобства использования, а принятые по умолчанию значения свойств призваны обеспечить максимальную защищенность.

1. **Влияет ли размер ключа на криптостойкость алгоритма?**

Да

1. **Назовите основные классы библиотеки System.Security.Cryptography?**

CryptoStream, CSPParameters, RSACryptoServiceProvder, RijndaelManaged