Учреждение образования

«Белорусский государственный технологический университет»

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Студентки 2 курса 1 группы ФИТ

Шимчёнок Елизаветы Константиновны

**2022 г.**

**Цель работы:** изучить модель криптографии .NET Framework, основные классы и структуры данных.

**Ответы на вопросы**

1. Какие симметричные алгоритмы шифрования Вы знаете?

В симметричном шифровании один и тот же ключ используется как для шифрования, так и для дешифрования. В этом методе исходное сообщение преобразуется в нераспознаваемое сообщение, которое невозможно идентифицировать. Это преобразованное сообщение называется зашифрованным текстом. Это делается с помощью ключа и алгоритма шифрования. На принимающей стороне зашифрованный текст преобразуется обратно в исходное сообщение с использованием того же ключа и алгоритма дешифрования.

Поскольку обе стороны используют один и тот же ключ, симметричное шифрование намного быстрее. С другой стороны, ключ должен быть доступен для расшифровки сообщения. Поэтому для передачи ключа требуется защищенный канал. В целом, симметричное шифрование является простым методом и не требует много времени для завершения. RC4, AES, DES, 3DES - это некоторые распространенные алгоритмы симметричного шифрования.

1. Какие ассиметричные алгоритмы шифрования Вы знаете?

Асимметричное шифрование использует два ключа для шифрования и дешифрования. Эти два ключа называются закрытым ключом и открытым ключом. Он использует открытый ключ для шифрования и закрытый ключ для расшифровки. Открытый ключ доступен для стороны, которая хочет отправить сообщение. Закрытый ключ принадлежит владельцу сообщения. Сообщение, которое зашифровано открытым ключом и алгоритмом шифрования, может быть дешифровано с использованием алгоритма дешифрования и соответствующего закрытого ключа соответствующего открытого ключа.

В целом, асимметричное шифрование обеспечивает большую безопасность данных. С другой стороны, использование двух ключей делает асимметричное шифрование трудоемким и более сложным. Алгоритм Диффи-Хеллмана и RSA - это некоторые распространенные алгоритмы асимметричного шифрования.

1. Основное назначение библиотеки System.Security.Cryptography?

Предоставляет криптографические службы, включая безопасное кодирование и декодирование данных, а также множество других операций, таких как хэширование, генерация случайных чисел и проверка подлинности сообщений.

1. Влияет ли размер ключа на криптостойкость алгоритма?

Размер ключа измеряется в битах (двоичных разрядах). Чем он больше, тем, соответственно, больше времени необходимо на перебор возможных значений, но и тем продолжительнее работает алгоритм.

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

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

Класс CspParameters представляет параметры, которые можно передавать управляемым криптографическим классам, использующим службы шифрования (CSP), с помощью интерфейса Microsoft Cryptography API (CAPI).

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

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

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