Практическое занятие №12

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ДЛЯ РЕАЛИЗАЦИИ

ПРИЛОЖЕНИЙ, ИСПОЛЬЗУЮЩИХ СИММЕТРИЧНОЕ

И АССИМЕТРИЧНОЕ ШИФРОВАНИЕ,

С ПРИМЕНЕНИЕМ БИБЛИОТЕКИ

SYSTEM.SECURITY.CRYPTOGRAPHY

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель:** изучить модель криптографии .NET Framework, основ-

ные классы и структуры данных, разработать приложение для шиф-

рования файлов, использующих симметричные и ассиметричные

алгоритмы шифрования.

**Теоретические сведения**

В .NET Framework присутствует пространство имен для

выполнения криптографических операций под названием

System.Security.Cryptography. Данное пространство имен предостав-

ляет криптографические службы, включающие безопасное кодиро-

вание и декодирование данных, а также другие операции, такие как

хеширование сообщений, генерация случайных чисел и проверка

подлинности сообщений. Данная библиотека предоставляет доступ

для использования различных реализаций алгоритмов, в основном

это программные интерфейсы CryptoApi (CAPI) и Cryptography Next

Generation API (CNG API). Помимо этого, для некоторых алгорит-

мов возможно использование реализаций на основе OpenSSL.

CryptoAPI – интерфейс программирования приложений, кото-

рый обеспечивает разработчиков Windows-приложений стандарт-

ным набором функций для работы с криптопровайдером. Входит в

состав операционных систем Microsoft. Большинство функций

CryptoAPI поддерживается, начиная с Windows 2000.

Cryptography Next Generation API стала долгосрочной заменой

CAPI. Данный набор интерфейсов поддерживает все алгоритмы, пред-

лагаемые CAPI, а также другие алгоритмы, перечисленные в своде пра-

вил Suite B Агентства национальной безопасности США. Данный интер-

фейс поддерживает следующие длины ключей или размерность хеша:

– RSA от 512 до 16 384 бит с шагом 64 бит;

– DH – от 512 до 16 384 бит с шагом 64 бит;

– DSA – от 512 до 1024 бит с шагом 64 бит;

– ECDSA – P-256, P-384, P-521 (NIST Curves);

– ECDH – P-256, P-384, P-521 (NIST Curves);

– MD2 – 128 бит;

– MD4 – 128 бит;

– MD5 – 128 бит;

– SHA1 – 1160 бит;

– SHA256 – 256 бит;

– SHA384 – 384 бит;

– SHA512 – 512 бит.

**Условие задания:**

1. Ознакомиться с созданием криптографического приложения.
2. Выполнить шифрование, дешифрование и хеширование своей фамилии по алгоритмам RSA и MD5.
3. Сохранить ключи, зашифрованные и захешированные данные в файлы.
4. Через Hex-редактор отобразить эти данные.
5. Реализовать проверку целостности сообщения и хеша по примеру ЭЦП, продемонстрировать результат при изменениях.

**Исполнительная часть**

**Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

****

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Результат выполнения:**

**Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

Использованные источники

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.