Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ Лабораторна робота №4 Тема: “ Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації.”

Виконали:

Студенти групи ФІ-12мн

Мітрофанова Еліна

Морозюк Анастасія

Гетьман Дмитро

Перевірила:

Селюх П.В.

Мета роботи: Дослідження стікості криптопровайдерів, стандартів CryptoAPI, PKCS.

Хід роботи

.NET Framework включает набор криптографических сервисов, расширяющих сервисы Windows через CryptoAPI.

Простір імен System.Security.Cryptography відкриває програмний доступ до найрізноманітніших криптографічних сервісів, за допомогою яких програми можуть шифрувати та дешифрувати дані , забезпечувати їх цілісність, а також обробляти цифрові підписи та сертифікати.

Стандарт PKCS # 7 описує загальний синтаксис для даних, до яких може застосовуватися *Шифрування* , наприклад *цифрові підписи* та *цифрові конверти* .

Розглянемо деякі класи даного стандарту

- Cms Signer Class - Представляє потенційного підписувача для підписаного повідомлення
- Клас ContentInfo представляє структуру даних CMS/PKCS #7.

Пространство имен Cryptography содержит базовый класс HashAlgorithm и производные классы, поддерживающие алгоритмы MD5, SHA1, SHA256, SHA384 и SHA512.

Чем больше хеш, тем надежнее алгоритм и тем труднее его взломать. Все эти алгоритмы реализованы в двух версиях: на основе управляемого и неуправляемого кода.

Чтобы вычислить дайджест, нужно просто создать экземпляр класса алгоритма хеширования и вызвать его перегруженный метод ComputeHash.

Більш того, існуть класи, які допомогають дуже швидко реалізувати деякі криптосистеми. Наприклад, RSACryptoServiceProvider. Виконує асиметричне шифрування та розшифровку за допомогою реалізації алгоритму RSA , що надається постачальником служб шифрування (CSP).

Цей клас має методи для шифрування, розшифрування, підпису, веріфікації. Дуже часто для генерації сеансового ключа використовують інший клас – AES.

Проаналізувавши літературу пов’язану з даними криптопровайдерами, було виявлено, що вони є достатньо стійкими, а також прискорють час розробки програмного продукту. Аналогічні провайдери існують у бібліотеці Bounce

Custle, але на наш суб’єктивний погляд, System.Security.Cryptography є більш зручною пр використанні.

Висновок : отже, під час виконання роботи було розглянуто пространство імен System.Security.Cryptography та стандарт PKCS # 7. Також, було проаналізовано основні методи та влистовості найпопулярніших криптопровайдерів.