**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

отчет

**по лабораторной работе №8**

**по дисциплине «Криптография и защита информации»**

Тема: Изучение цифровой подписи

|  |  |  |
| --- | --- | --- |
| Студент гр. 8304 |  | Сергеев А.Д. |
| Преподаватель |  |  |

Санкт-Петербург

2021

**Цель работы.**

Исследовать алгоритмы создания и проверки цифровой подписи, алгоритмы генерации ключевых пар для алгоритмов цифрой подписи RSA, DSA, ECDSA и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

**Генераторы ключевых пар.**

Задание:

1. Перейти к утилите «*Digital Signatures/PKI->PKI/Generate…*».
2. Сгенерировать ключевые пары по алгоритмам *RSA-2048*, *DSA2048*, *EC-239*. Зафиксируйте время генерации в таблице.
3. С помощью утилиты «*Digital Signatures/PKI -> PKI/Display…*» вывести сгенерированный открытый ключ и сохранить соответствующий скриншот.

Описание алгоритмов генерации:

ррр

Таблица с фактическими временем генерации ключевых пар:

ррр

Скриншоты со значениями открытых ключей:

ррр

**Процессы создания и проверки цифровой подписи.**

Задание:

1. Открыть текст не менее 5000 знаков. Перейти к приложению *Digital Signatures/PKI -> Sign Document*…
2. Задайте хэш-функцию, и другие параметры цифровой подписи.
3. Создайте подпись ключами, сгенерированными в предыдущем задании. Зафиксируйте время создания цифровой подписи для каждого ключа.
4. Сохраните скриншот цифровой подписи с помощью приложения *Digital Signatures/PKI -> Extract Signature*.
5. Выполните процедуру проверки подписи *Digital Signatures/PKI -> Verify Signature* для случаев сохранения и нарушения целостности исходного текста. Сохраните скриншоты результатов.

Обобщенная схема создания и проверки цифровой подписи:

Ррр

Таблица с фактическими временем генерации цифровой подписи:

Ррр

Скриншоты со значениями цифровой подписи:

Ррр

Скриншоты с результатами проверки цифрой подписи:

Ррр

**Схемы цифровой подписи на эллиптических кривых.**

Задание:

1. Выполните процедуру создание подписи «*Digital Signatures/PKI -> Sign Document…*» алгоритмом *ECSP-DSA* в пошаговом режиме (*Display inter. results=ON*). Зафиксируйте скриншоты последовательности шагов.
2. Выполните процедуру проверки подписи *ECSP-DSA* для случаев сохранения и нарушения целостности исходного текста. Сохраните скриншоты результатов.
3. Проверить лекционный материал по *ECDSA*, выполнив создание и проверку подписи сообщения M (принять *M=h(M)*) приложением *Indiv.Procedures -> Number Theory… -> Point Addition on EC*.

Описание алгоритма формирования и проверки подписи ECDSA:

Ррр

Результаты (скриншоты) пошагового выполнения ECDSA в CrypTool 1. Сравнение лекционной версии и реализации:

Ррр

Результаты проверки лекционного материала по ECDSA с использованием приложения *Indiv.Procedures -> Number Theory… -> Point Addition on EC*:

Ррр

**Демонстрация процесса подписи в среде PKI.**

Задание:

1. Запустить демонстрационную утилиту «*Digital Signatures/PKI -> Signature Demonstration…*».
2. Получите сертификат на ранее сгенерированную ключевую пару RSA-2048.
3. Выполните и сохраните скриншоты всех этапов создания цифровой подписи документа.
4. Сохраните скриншот сертификата для проверки этой цифровой подписи.

Сравнение структуры сертификата (как в лекции) и сертификата из CrypTool 1.0:

Ррр

Схема процедуры подписания из CrypTool:

Ррр

**Подписание своего отчета.**

Задание:

1. Сконвертируйте отчет в формат pdf.
2. Экспортируйте ранее созданный сертификат ключевой пары *RSA Digital Signatures/PKI -> PKI/Generate… -> Export PSE(#PKCS12)*.
3. Откройте pdf-версию отчета и попытайтесь подписать с использованием этого сертификата.
4. Создайте собственный самоподписанный сертификат в среде Adobe Reader и используйте его для подписи отчета.
5. Сохраните скриншоты свойств подписи и сертификата.
6. Внесите изменения (маркеры, комментарии) в отчет и проверьте подпись.

Скриншот титульного листа с цифровой подписью:

Ррр

Скриншот титульного листа с цифровой подписью:

Ррр

Скриншот титульного листа с цифровой подписью:

Ррр

**Выводы.**

В ходе выполнения лабораторной работы были исследованы следующие шифры: RailFence, Vigenere и ADFGVX, а также получены навыки работы с ними вручную и с помощью специальных программ CrypTool 1 и CrypTool 2.

Шифр RailFence:

Это шифр перестановочного типа, его ключом являются два числа: количество строк в шифровальной таблице и смещение относительно ее начала. Шифр уязвим к атаке перебором, так как его ключом являются два числа, вариантов для подбора которых сравнительно не много. Вследствие этого не является криптографически стойким.

Шифр Vigenere:

Это шифр перестановочного типа, его ключом является строка-ключ (по сути представляющая из себя набор чисел – ключей шифра Цезаря). Шифр уязвим к атаке автокорреляционным методом с последующим статистическим и/или частотным анализом или простым перебором. Не является стойким, если для задачи взлома использовать описанные выше методы вместо полного перебора.

Шифр ADFGVX:

Это шифр комбинированного типа, его ключом является строка-ключ на стадии перестановки и (опционально) матрица подстановки на стадии замены. Шифр уязвим к атаке на основе знания части открытого текста (2х и более сообщений с одинаковыми частями или сообщений одинакового размера), заключающимся в определении перестановки биграмм и частотному анализу шифрующей матрицы. Без знания частей открытого текста является достаточно криптостойким за счет использования биграмм и перестановок.