



Національний технічний університет України

«Київський політехнічний інститут»

Фізико технічний інститут

Кафедра математичних методів захисту інформації

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

Лабораторна робота №4

Тема: “Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації”

Виконали:

Корж Нікіта ФІ-12мн

Тафтай Анастасія ФІ-12мп

Мазур Анастасія ФІ-12мн

Перевірила

Селюх П.В.

Київ - 2021

Мета роботи: Отримання практичних навичок побудови гібридних криптосистем.

Завдання: Розробити реалізацію асиметричної криптосистеми у відповідності до стандартних вимог Crypto API або стандартів PKCS та дослідити стійкість стандартних криптопровайдерів до атак, що використовують недосконалість механізмів захисту операційної системи.

Хід роботи

Стандарти криптографії з відкритим ключем (Public-Key Cryptography Standards, PKCS) розроблені компанією RSA Data Security Inc.

Компанія Google анонсувала проект **Wycheproof** в 2016 році, в рамках якого був підготовлений інструментарій для виявлення в різних реалізаціях алгоритмів шифрування недоробок та невідповідностей з очікуваною поведінкою.

На момент 2016 року у **Wycheproof** реалізовано понад 80 тестів, що перевіряють на наявність більше 40 видів помилок у реалізаціях алгоритмів RSA, DSA, ECDH та Diffie-Hellman, таких як некоректний вибір констант для побудови еліптичної кривої, повторне використання параметрів у схемах формування цифрових підписів, різні види атак на AES-EAX, AES-GCM, DH, DHIES, DSA, ECDH, ECDSA, ECIES та RSA.

Зокрема, інструментарій може використовуватись для перевірки криптопровайдерів на базі Java Cryptography Architecture, таких як **Bouncy Castle**.

Генерація ключів в **Bouncy Castle** відбувається відповідно до стандарту **PKCS # 14** - стандарт генерації псевдовипадкових чисел.

Архітектура

Було реалізовано клієнт серверний веб-додаток. Він підтримує функції створення користувачів разом з їх приватними та публічними ключами. Також створення повідомлення між існуючими користувачами. Під час створення отримується повідомлення, дістається публічний ключ отримувача по імені отримувача вказаному відправником, та за його допомогою воно шифрується і зберігається сервісом. Також користувачі можуть переглядати повідомлення в зашифрованому виді та дешифрувати за допомогою приватного ключа. Шифрування відбувається алгоритмом Ель Гамала.

Приклад роботи:

Створюємо користувачів Алісу та Боба і генеруємо їм ключі

- [Create User](#)
- [Create Message](#)
- [Messages](#)

Name

alice

Submit

Public Key

3078305006062B0E070201013046022100BB52012576EF464E7136BA992C986A8BDECD96E80F23E4E2423CFC4E48ABF20F02210091E223CA786CE4708424448D0116BFEBBCE43D6E690850181C05CF24A1DC405D03240002210092D8669040109A663D6483570ABD8A55F771326106BBC

Private Key

3079020100305006062B0E070201013046022100BB52012576EF464E7136BA992C986A8BDEC D96E80F23E4E2423CFC4E48ABF20F02210091E223CA786CE4708424448D0116BFEBBCE43D6E690850181C05CF24A1DC405D04220220513B05A716572926CCDB5590E98B413B3DD4355033

Name

bob

Submit

Public Key

3078305006062B0E070201013046022100BB52012576EF464E7136BA992C986A8BDECD96E80F23E4E2423CFC4E48ABF20F02210091E223CA786CE4708424448D0116BFEBBCE43D6E690850181C05CF24A1DC405D0324000221008E85510E12A49ED2DF735A23AC0E2BEB6E352DF5ED67E

Private Key

3079020100305006062B0E070201013046022100BB52012576EF464E7136BA992C986A8BDEC D96E80F23E4E2423CFC4E48ABF20F02210091E223CA786CE4708424448D0116BFEBBCE43D6E690850181C05CF24A1DC405D042202200F3A29F3426B79B161066014E3399E8905FEC870A53

Створюємо повідомлення від Аліси до Боба, яке шифрується і зберігається в зашифрованому виді:

- Create User
- Create Message
- Messages

Sender

alice

Receiver

bob

Message

hello bob!!!

Submit

Encrypted message

jdnW8f44vcbrezFEgftVrbuDDDH4wcMbCwF/2N9XPGCPY+JFbW4DYdaIR25drZE5SIHZFwR9oUrpUDR3AwsskQ==

Бачимо, що воно з'явилося в списку повідомлень:

- Create User
- Create Message
- Messages

Id	Sender	Receiver	Date
e5b62009-25cd-4123-93e0-f6d903db1ca3	alice	bob	2021-12-20

Вводимо приватний ключ отримувача - Боба, щоб дешифрувати повідомлення :

- Create User
- Create Message
- Messages

Id

e5b62009-25cd-4123-93e0-f6d903db1ca3

Date

2021-12-20

Sender

alice

Receiver

bob

Message

jdnW8f44vcbrezFEgftVrbuDDDH4wcMbCwF/2N9XPGCPY+JFbW4DYdaIR25drZE5SIHZFwR9oUrpUDR3AwsskQ==

Private Key To Decrypt

3079020100305006062B0E070201013046022100BB52012576EF4

Decrypt

Decrypted Message

hello bob!!!