НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №3
«Реалізація основних асиметричних криптосистем»

Підгрупа 1С

Виконали:
студенти групи ФІ-22мн
Бондаренко Андрій
Гузей Дмитро
Яценко Артем

Перевірила:
Байденко П. В.

Київ – 2022

Мета роботи: Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

Постановка задачі: дослідити можливість реалізації одного з чотирьох криптографічних протоколів: розділення секрету, сліпого цифрового підпису, несуперечливого цифрового підпису та розподілу ключів для симетричної криптосистеми за допомогою різних асиметричних алгоритмів (не менше як двох) та порівняти їх ефективність за обраним критерієм.

Хід роботи

Несуперечливий цифровий підпис (NRD) - це криптографічний механізм, який запобігає запереченню відповідальності того, хто підписує документ. Насправді процес підтвердження несуперечливості полягає в тому, щоб захистити не підставне заперечення авторства. Відповідальність за підписаний документ відхиляється тільки тоді, коли суб'єкт не може довести його автентичність.

Для того, щоб забезпечити несуперечливість цифрового підпису, необхідно використовувати два ключі: публічний ключ та приватний ключ. Публічний ключ призначається для підтвердження авторства підпису, а приватний ключ використовується для підписання документа. Підписаний документ може бути захищений проти неправдоподібного заперечення авторства, оскільки приватний ключ не може бути відновлений з публічного ключа.

Існує декілька основних принципів, які лежать в основі несуперечливості цифрових підписів. Перш за все, суб'єкт повинен мати доступ до приватного ключа, а його приватний ключ повинен бути доступним тільки для нього. Також потрібно, щоб суб'єкт мав доступ до цифрової інформації, яку він підписує. Третім принципом є точність підписаного документа, що означає, що документ повинен бути точно підписаний і не підлягати змінам.

Останнім принципом є незалежність підпису, яка означає, що підпис повинен бути

незалежним від кого-небудь іншого. Це означає, що суб'єкт має можливість підписати документ без залежності від будь-якого іншого суб'єкта.

Найбільш розповсюдженим прикладом несуперечливості цифрового підпису є процес підтвердження платежу. У цьому випадку суб'єкт має доступ до свого приватного ключа, який використовується для підписання платіжного поручення. Поручення підписується приватним ключем, а після цього публікується на публічний блокчейн. Для підтвердження автентичності поручення використовуються публічні ключі.

Іншим прикладом може бути застосування несуперечливого цифрового підпису для аутентифікації користувача. У цьому випадку користувач підписує логін та пароль з допомогою приватного ключа, а публічний ключ використовується для підтвердження автентичності логіна та пароля. Після того, як користувач був аутентифікований, система дозволяє йому доступ до ресурсів, захищених його приватним ключем.

У симетричних системах криптографії несуперечність часто досягається за допомогою асиметричних алгоритмів, які використовують пару ключів, один для підпису, а інший для перевірки. Два найпоширеніші асиметричні алгоритми для цифрових підписів - RSA та алгоритм еліптичної кривої (ECDSA).

RSA - це широко використовуваний алгоритм цифрового підпису, який базується на математичних властивостях великих простих чисел. Він використовує відкритий ключ для перевірки та закритий ключ для підписання. Підписи RSA мають відносно великий розмір і можуть бути відносно повільними в обчисленні, особливо для великих повідомлень.

ECDSA, з іншого боку, є алгоритмом цифрового підпису, який базується на математиці еліптичних кривих. Він також використовує відкритий ключ для перевірки і закритий ключ для підписання. Підписи ECDSA, як правило, коротші і швидше обчислюються, ніж підписи RSA.

Порівнюючи ефективність RSA і ECDSA, слід враховувати кілька факторів. Одним з важливих факторів є довжина підпису. Підписи ECDSA, як правило, коротші за підписи RSA, що робить їх більш ефективними в ситуаціях, коли пропускна здатність або простір для зберігання даних обмежені.

Іншим фактором, який слід враховувати, є час, необхідний для підписання або перевірки повідомлення. ECDSA, як правило, швидший за RSA як для підписання, так і для перевірки, особливо для великих повідомлень.

Нарешті, рівень безпеки, що забезпечується алгоритмом, також є важливим фактором, який слід враховувати. RSA вважається більш безпечним, ніж ECDSA при однаковому розмірі ключа. Однак, підписи ECDSA, як правило, більш безпечні, ніж підписи RSA при однаковій довжині підпису.

Висновок: ми дослідили можливість реалізації криптографічного протоколу несуперечливого цифрового підпису за допомогою асиметричних алгоритмів RSA та ECDSA порівняли їх ефективність за довжиною підпису, часом та рівнем безпеки. RSA і ECDSA є загальновживаними алгоритмами цифрового підпису, які можуть бути використані для досягнення стійкості до відмови в системах симетричної криптографії. Підписи RSA відносно великі і повільні в обчисленні, в той час як підписи ECDSA, як правило, коротші і швидші. Вибір між цими двома алгоритмами буде залежати від конкретних вимог програми і компромісу між довжиною підпису, часом обчислення і рівнем безпеки.