Лабораторна роботи № 3.

Тема: Реалізація основних асиметричних криптосистем.

Виконали: студенти групи ФІ-32мн Ємець Єлизавета, Звєрєв Сергій, Коваленко Дар'я

Для першого типу лабораторних робіт – 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.

Підгрупа 1В. Розподіл ключів.

Розподіл ключів - це процес передачі симетричного ключа від одного суб'єкта до іншого в спосіб, який забезпечує конфіденційність та цілісність ключа. Симетричні ключі використовуються для шифрування і розшифрування даних, і важливо забезпечити їх безпеку під час передачі.

Основні підходи до розподілу симетричних ключів включають такі методи:

1. Ручний обмін ключами: Цей метод включає фізичний обмін ключами між суб'єктами, які співпрацюють. Наприклад, особи можуть обмінюватися ключами особисто або поштою. Цей метод є найпростішим, але не завжди можливим або практичним, особливо в мережевих застосунках.

2. Розподіл ключів за допомогою асиметричного шифрування: В цьому методі одна сторона (наприклад, сервер) генерує пару ключів: публічний і приватний. Публічний ключ розповсюджується, а приватний ключ зберігається в таємниці. Коли інша сторона (клієнт) хоче встановити спільний симетричний ключ для комунікації з сервером, вона шифрує ключ за допомогою публічного ключа сервера і надсилає його. Сервер розшифровує отриманий ключ за допомогою свого приватного ключа. Цей метод забезпечує конфіденційність ключа під час передачі.

3. Протоколи обміну ключами: Протоколи, такі як протокол Діффі-Гельмана, дозволяють двом або більше сторонам безпечно домовитися про спільний симетричний ключ, навіть якщо всі вони спілкуються через незахищені канали. Протоколи цього типу гарантують конфіденційність ключа і можуть використовуватися для обміну ключами під час встановлення безпечного з'єднання.

4. Розподіл ключів за допомогою третьої довіри: У цьому випадку третя довірена сторона, яка відома як центр дистрибуції ключів (Key Distribution Center, KDC), відповідає за розподіл ключів між сторонами. Клієнт і сервер обирають спільний симетричний ключ, і KDC розподіляє цей ключ обом

сторонам. Цей метод використовується, наприклад, у протоколі Kerberos для аутентифікації та безпечного обміну даними.

5. Використання симетричних ключів для зашифровування інших симетричних ключів: Цей метод включає в себе використання симетричних ключів для зашифровування інших симетричних ключів перед їх розподілом. Це дозволяє безпечно обмінюватися ключами, зашифровуючи їх за допомогою інших ключів, які вже відомі сторонам.

Вибір методу розподілу ключів залежить від конкретних потреб та вимог безпеки вашого застосунку. Кожен метод має свої переваги та недоліки, і важливо розглянути контекст і потенційні загрози перед вибором правильного підходу.

Симетричний ключ - це криптографічний ключ, який використовується в симетричних криптосистемах для одночасного шифрування і розшифрування даних. Головна особливість симетричних ключів полягає в тому, що той самий ключ використовується як для зашифрування, так і для розшифрування інформації. Такий підхід відомий як "симетричне шифрування" або "секретний ключовий обмін".

Основні характеристики симетричних ключів:

1. Спільний ключ: Один і той самий ключ використовується як для шифрування, так і для розшифрування повідомлень між відправником і отримувачем. Це означає, що обидва боки повинні мати доступ до цього ключа.

2. Швидкодія: Симетричне шифрування зазвичай є набагато швидшим і менш обчислювально витратним порівняно з асиметричним шифруванням (де використовуються різні ключі для шифрування і розшифрування).

3. Ключова безпека: Забезпечення безпеки симетричних ключів вимагає безпечного обміну ключами між відправником і отримувачем. Якщо ключ потрапить у ненадійні руки, це може призвести до розкриття зашифрованих даних.

4. Використання: Симетричне шифрування застосовується для шифрування і розшифрування великої кількості даних, таких як текстові повідомлення, файли або комунікації в реальному часі.

Прикладами симетричних алгоритмів є Advanced Encryption Standard (AES), Data Encryption Standard (DES), і Triple DES (3DES).

Результати виконання:

```
Час розподілу ключа за допомогою ECC: 0.00090861320495605 47 сек
Час розподілу ключа за допомогою RSA: 0.04292178153991699 сек
Розмір зашифрованого ключа за допомогою ECC: 103 байт
Розмір зашифрованого ключа за допомогою RSA: 288 байт
```

На основі отриманих результатів можна зробити наступні висновки:

1. Час розподілу ключа: Розподіл симетричного ключа за допомогою ECC займає набагато менше часу (приблизно 0.0009 секунди) порівняно з RSA (приблизно 0.043 секунди). ECC дозволяє більш ефективно виконувати операції з криптографічними ключами.

2. Розмір зашифрованого ключа: Зашифрований ключ ECC має розмір 103 байти, в той час як зашифрований ключ RSA має розмір 288 байтів. Розмір ключа ECC набагато менший, що дозволяє зменшити обсяг передачі даних при обміні ключами.

3. Ефективність: За результатами, ECC виявляється більш ефективним для розподілу симетричних ключів порівняно з RSA. Він забезпечує швидший час виконання та менший обсяг передачі даних.

4. Безпека: Важливо враховувати, що безпека криптографічного протоколу не зводиться тільки до швидкості і розміру ключа. Обидва методи мають свої переваги і недоліки з точки зору безпеки. ECC вважається більш безпечним на практиці за однакової довжини ключа порівняно з RSA. Однак правильна і безпечна реалізація будь-якого криптографічного протоколу є надзвичайно важливою.

Отже, якщо швидкість та обсяг передачі даних мають велике значення для вашого випадку використання, ECC може бути більш підходящим варіантом для розподілу симетричних ключів. Однак завжди слід враховувати вимоги до безпеки та правильно виконувати реалізацію криптографічних протоколів.ча