Одеський коледж комп’ютерних технології «Сервер»

Звіт з практичної роботи №5

З предмету «Технології захисту інформації»

Тема : «Сучасне використання електронно-цифрового підпису та його застосування в Україні»

Виконував :

Студент групи К21.1

Машков Володимир

Одеса 2024

ВСТУП

У сучасному цифровому світі питання безпеки і достовірності інформації набуває критичного значення. Мільйони транзакцій, контрактів, угод і документів щодня обробляються в електронній формі. Водночас стає все більш актуальною потреба в забезпеченні того, що ці документи залишаються автентичними, цілісними та захищеними від сторонніх змін. Одним із ключових інструментів для вирішення цієї задачі є електронно-цифровий підпис (ЕЦП).

ЕЦП гарантує ідентифікацію автора документа, а також надійний захист від несанкціонованих змін після його підписання. У зв’язку з поширенням електронного документообігу, потреба в надійному та безпечному підписанні документів зростає. Саме тому використання ЕЦП стає важливою складовою правових і бізнесових процесів у багатьох країнах, включно з Україною, де це регулюється національними стандартами, такими як ДСТУ 3008.

СУЧАСНІ АЛГОРИТМИ СТОВРЕННЯ ЕЦП

На поточний момент, існує багато методів та алгоритмів створення електронного цифрового підпису. Далі буде наведено декілька із них та описано їх :

1. RSA (Rivest-Shamir-Adleman)

Алгоритм RSA є одним із найстаріших і найбільш випробуваних у криптографічному світі. Його стійкість до взлому забезпечується використанням складних математичних операцій, заснованих на факторизації великих чисел. У процесі створення електронного підпису за допомогою RSA використовуються приватний ключ для шифрування хешу документа та публічний ключ для верифікації підпису. Алгоритм забезпечує надійність навіть для документів, що мають велике значення, як, наприклад, банківські операції або важливі правові угоди.

Приклад використання RSA:

* Банківські установи, під час обробки транзакцій через інтернет-банкінг, часто застосовують RSA для забезпечення безпеки передачі даних і підтвердження дій користувачів.
* У корпоративних середовищах RSA використовується для захисту електронної пошти та важливих комунікацій між працівниками.

1. DSA (Digital Signature Algorithm)

DSA був спеціально розроблений для використання в електронно-цифрових підписах, і його схвалено Національним інститутом стандартів і технологій США (NIST). Цей алгоритм вважається ефективнішим для створення підписів, однак верифікація займає більше часу порівняно з RSA. DSA добре підходить для випадків, коли важлива швидкість підпису документа, але перевірка підпису може відбуватися пізніше, наприклад, у державних реєстрах.

1. ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA — це сучасна еволюція алгоритмів цифрового підпису, яка забезпечує підвищену ефективність завдяки використанню еліптичних кривих. Завдяки цьому алгоритм може створювати надійні підписи з використанням коротших ключів, що підвищує ефективність і знижує витрати на обчислення. ЕCDSA вважається ідеальним вибором для мобільних додатків та пристроїв з обмеженими ресурсами.

Прикладом використання ECDSA – є сучасні криптовалютні системи, такі як Bitcoin і Ethereum, використовують ECDSA для підтвердження транзакцій, що гарантує високу надійність операцій у децентралізованих мережах.

Схема роботи ЕЦП

Схема роботи ЕЦП полягає в забезпеченні автентичності та цілісності документа між підписантом і одержувачем. Цей процес ділиться на дві фази: підписання та верифікація.

1. Підписання

* Підписант генерує пару криптографічних ключів: приватний і публічний.
* Приватний ключ використовується для підписання документа, створюючи цифровий підпис.
* Підписант передає документ разом із цифровим підписом і публічним ключем іншій стороні.

1. Верифікація

* Одержувач документа використовує публічний ключ для перевірки підпису.
* Якщо підпис дійсний, це підтверджує, що документ не зазнав змін з моменту підписання, і що він дійсно був підписаний власником приватного ключа.

Ця схема є основою роботи багатьох сучасних систем електронного документообігу і широко використовується в правовому та фінансовому секторах.

На рисунку 1.1 наведено діаграму цього процессу для алгоритму шифрування та дешифрування від відправника до отримувача.

Изображение выглядит как диаграмма, текст, План, Технический чертеж

Автоматически созданное описание

Рисунок 1.1 – схема роботи електронно-цифрового підпису DSS

Сторона отправителя: в подходе DSS из сообщения генерируется хэш-код, а следующие входные данные передаются функции подписи:

* Хэш-код.
* Случайное число «k», сгенерированное для данной конкретной подписи.
* Закрытый ключ отправителя, т.е. PR(a).
* Глобальный открытый ключ (который представляет собой набор параметров для принципов взаимодействия), т. е. PU(g).

Эти входные данные для функции предоставят нам выходную подпись, содержащую два компонента – 's' и 'r'. Таким образом, исходное сообщение, объединенное с подписью, отправляется получателю.

Сторона получателя: на стороне получателя выполняется проверка отправителя.Генерируется хэш-код отправленного сообщения. Существует функция проверки, которая принимает следующие входные данные :

* Хэш-код, сгенерированный получателем.
* Компоненты подписи «s» и «r».
* Открытый ключ отправителя.
* Глобальный открытый ключ.

Выход функции проверки сравнивается с компонентом подписи 'r'. Оба значения будут совпадать, если отправленная подпись действительна, поскольку только отправитель с помощью своего закрытого ключа может сгенерировать действительную подпись.

АЛГОРИТМИ ШИФРУВАННЯ І ДЕШИФРУВАННЯ

Основною характеристикою ЕЦП є асиметричне шифрування, де шифрування і дешифрування використовують різні ключі. У випадку з RSA або ECDSA приватний ключ використовується для шифрування хешу документа, що створює цифровий підпис. Одержувач використовує публічний ключ для дешифрування і верифікації підпису.

Процес шифрування складається із :

* Підписант хешує документ за допомогою криптографічної хеш-функції (наприклад, SHA-256).
* Приватний ключ використовується для шифрування цього хешу, що і створює підпис

Процес дешифрування складається із :

* Одержувач використовує публічний ключ підписанта для дешифрування підпису.
* Розшифрований хеш порівнюється з хешем отриманого документа для перевірки цілісності та автентичності.

АКТУАЛЬНІ СИСТЕМИ ГЕНЕРАЦІЇ ПІДПИСУ ТА ПРОЦЕСС ЇХ СТВОРЕННЯ

Далі буде наведено найбільш поширенні стандарти шифрування електронно-цифрового підпису, та їх генерації, а саме :

OpenSSL - є одним із найпопулярніших інструментів для створення і верифікації цифрових підписів. Його універсальність, підтримка різних алгоритмів (RSA, DSA, ECDSA) і кросплатформенність роблять його зручним інструментом як для приватних осіб, так і для великих організацій.

GnuPG (Gnu Privacy Guard) — це відкритий стандарт, що підтримує асиметричне шифрування та підписування документів. Він широко використовується для захисту електронної пошти і шифрування файлів.

Далі буде наведено приклад із створення ЕЦП за допомогою OpenSSL :

1. Створення пари ключів:

Код :

openssl genpkey -algorithm RSA -out private\_key.pem -pkeyopt rsa\_keygen\_bits:2048

openssl rsa -in private\_key.pem -pubout -out public\_key.pem

1. Створення підпису:

Код :

openssl dgst -sha256 -sign private\_key.pem -out signature.sig document.txt

1. Перевірка підпису:

Код :

openssl dgst -sha256 -verify public\_key.pem -signature signature.sig document.txt

Цей процес є стандартним підходом до використання RSA для створення та перевірки ЕЦП, що дозволяє легко інтегрувати цю схему в будь-яку систему документообігу.

ЕЦП забезпечує високий рівень захисту за умови використання достатньої довжини ключів і сучасних алгоритмів шифрування. Зокрема, для RSA рекомендується використовувати ключі довжиною 2048 біт або більше, тоді як для ECDSA рекомендується мінімальна довжина ключів 256 біт. Проте з розвитком квантових обчислень існує можливість, що асиметричні алгоритми, такі як RSA, можуть стати вразливими, і тому все більше уваги приділяється квантово-стійким алгоритмам.

РЕАЛЬНІ ПРИКЛАДИ ВИКОРИСТАННЯ ЕЦП

Далі буде наведено приклади використання електронно-цифрового підпису у реальних сферах та секторах :

1. Державні послуги

В Україні система Дія активно використовує ЕЦП для забезпечення цифрових державних послуг. Завдяки цьому користувачі можуть підписувати електронні документи для отримання довідок, реєстрації підприємств, оформлення субсидій та інших послуг.

1. Банківський сектор

Банки активно використовують ЕЦП для підтвердження фінансових операцій в інтернет-банкінгу. Це дозволяє уникнути підробки підписів і забезпечити безпеку клієнтів при здійсненні переказів та підписанні електронних договорів.

1. Корпоративний документообіг

Багато великих компаній, як наприклад, Microsoft і Apple, використовують ЕЦП для внутрішнього обміну конфіденційними документами, договорами і звітами. Цифровий підпис гарантує, що документи, які пересилаються всередині організації, залишаються недоторканими та підписані відповідальними особами.

1. Криптовалютні транзакції

Криптовалюти, такі як Bitcoin і Ethereum, використовують ЕЦП на основі ECDSA для підтвердження та захисту транзакцій. Це дозволяє гарантувати, що операції виконуються тільки власником приватного ключа, а дані в блокчейні залишаються незмінними.

ВИСНОВОК

Електронно-цифровий підпис (ЕЦП) є надійним інструментом для забезпечення безпеки та автентичності електронних документів. У звіті було детально розглянуто сучасні алгоритми, які використовуються для створення ЕЦП, такі як RSA, DSA та ECDSA, а також схеми їх роботи. ЕЦП надає можливість ідентифікувати автора документа, гарантує, що документ не був змінений, і підтверджує його правовий статус. Використання таких систем, як OpenSSL та GnuPG, дозволяє реалізувати ЕЦП у різних сферах, зокрема у державному секторі, корпоративному середовищі та навіть у криптовалютних транзакціях.

Цифрова трансформація суспільства продовжує активно розвиватися, і використання ЕЦП стає невід'ємною частиною цього процесу. Завдяки сучасним алгоритмам та надійним системам, користувачі можуть бути впевнені в безпеці своїх даних і підписаних документів.