Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Факультет електроніки та комп’ютерних технологій
Кафедра оптоелектроніки та інформаційних технологій

Пояснювальна записка
до курсової роботи
“ Конфіденційність цифрових підписів”

Виконав:
студент групи ФЕS-13
Безп’ятко Р. П.
Науковий керівник:
Свелеба С. А.

Львів – 2023

Зміст

1. Вступ
2. Теоретичні особливості поняття цифрового підпису
   2.1 Поняття цифрового підпису та сфера застосування
   2.2 Характеристика особливостей застосування цифрового підпису
3. Забезпечення конфіденційності цифрових підписів
   3.1 Алгоритми шифрування цифрових підписів
   3.2 ЦЕП на основі алгоритму
   3.3 RSA Система захисту даних на базі методу шифрування RSA (відкритий ключ)
   3.4 Алгоритми шифрування цифрових підписів
4. Література

ВСТУП

Актуальність. Одним із важливих засобів отримання послуг аутентифікації є цифровий підпис. Дослідження електронних підписів нині набувають актуальності з виникненням квантового комп'ютера.

Поява нових обчислювальних платформ, таких як хмарні обчислення, IoT, вимагає прийняття все більшої кількості стандартів безпеки, що, в свою чергу, вимагає впровадження різноманітного набору криптографічних примітивів. На рівні обчислювальної платформи видно різноманітність можливостей обчислювальної техніки, починаючи від високоефективних (у режимі реального часу) віртуалізованих середовищ, таких як хмарні обчислювальні ресурси та програмно визначені мережі, до сильно обмежених ресурсів платформ IoT, щоб реалізувати бачення Інтернету речей .

Це створює труднощі при розробці та здійсненні нових стандартів криптографії в одному варіанті здійснення, оскільки обчислювальні платформи точно визначають цілі та обмеження.

Метою даної роботи є дослідження цифрових підписів та аналіз їх безпечності.

Об’єктом дослідження є цифровий підпис.

Предметом – алгоритми забезпечення безпеки цифрового підпису.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Дослідити теоретичні особливості поняття цифрового підпису.
2. Розглянути сферу застосування.
3. Проаналізувати програмно-технічний комплекс для захисту інформації
4. Підсумувати отримані результати.

Наукова новизна даної роботи полягає у тому, що зазнавши подальшого розвитку цифровий підпис спрямований на забезпечення безпеки даних, з застосуванням сучасних веб-технологій; уточнено поняття «цифровий підпис» та подано аналіз основних алгоритмів забезпечення безпеки даних.

Практичне значення одержаних результатів полягає у наступному:

- наведено класифікацію основних алгоритмів шифрування;
- розроблено систему захисту даних на базі методу шифрування RSA.

Достовірність теоретичних положень роботи підтверджується строгістю постановки задач, коректним застосуванням математичних методів під час доведення наукових положень, строгим виведенням аналітичних співвідношень, порівнянням результатів з відомими.

Структура та об'єм роботи. Робота складається із вступу, двох розділів, основних висновків по роботі, переліку посилань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСОБЛИВОСТІ ПОНЯТТЯ ЦИФРОВОГО ПІДПИСУ

1.1. Поняття цифрового підпису та сфера застосування

Цифровий підпис - це криптографічний засіб, що дозволяє переконатися у відсутності спотворень в тексті електронного документа, і, у відповідних випадках, ідентифікувати особу, яка створила такий підпис. У розвинених країнах світу цифровий підпис широко використовується [1].

Алгоритм використання складається з ряду операцій:

- генерується пара ключів: відкритий і закритий;
- відкритий ключ передається зацікавленій стороні (одержувачу документів, підписаних стороною, що згенерувала Ключі);
- відправник повідомлення шифрує його своїм закритим ключем і передає одержувачу по каналах зв'язку;
- одержувач розшифровує повідомлення за допомогою відкритого ключа відправника.

Суть в тому, що тільки власник закритого ключа, тобто відправник повідомлення, може створити зашифроване повідомлення, при розшифровці якого вихідний текст виходить за допомогою відкритого ключа. Для цього неможливо використовувати відкритий ключ. Шифрування використовується для забезпечення конфіденційності (секретності) повідомлення [1].

Для шифрування повідомлення використовується пара відкритого і закритого ключів, така ж, як і для формування ЕЦП. Для шифрування повідомлення (можливо, вже підписаного ЕЦП) використовується відкритий ключ адресата, і отримане зашифроване повідомлення може бути розшифровано тільки самим адресатом з використанням його закритого ключа. Навіть відправник, який щойно зашифрував повідомлення, не може його розшифрувати. Таким чином, приватний ключ відправника використовується для підпису повідомлення, а відкритий ключ одержувача використовується для шифрування [2].

Відповідно, одержувач використовує свій закритий ключ для розшифровки, а відкритий ключ відправника - для перевірки автентичності. ЕЦП і шифрування повідомлень можуть використовуватися як спільно, так і окремо, на розсуд користувача. Наприклад, наказ директора організації повинен бути підписаний за допомогою ЕЦП для підтвердження його справжності, але не повинен бути зашифрований.

Сертифікат ключа підпису служить для додаткового захисту відкритого ключа (підтвердження приналежності відкритого ключа конкретному користувачеві), в разі компрометації закритого ключа Сертифікат відкликається, термін дії становить 1 рік, після закінчення якого Сертифікат автоматично потрапляє в категорію недійсних і потрібен новий сертифікат. Для захисту інформації, що міститься в сертифікаті, використовується ЕЦП центру сертифікації (СС).

Прийнято класифікувати захист даних криптографічними методами в залежності від місця застосування шифрування: - рівень програми; - рівень файлової системи; - мережевий рівень; захист на рівні програми є оптимальною в тому сенсі, що цінність даних і ризики, пов'язані з порушеннями інформаційної безпеки, спочатку формулюються на рівні програми. Незважаючи на те, що з загальної точки зору сервер баз даних можна розглядати як додаток по відношенню до операційної системи, як правило, бізнес-логіка знаходиться вище, не тільки над таблицями і стовпцями, а й над призначеними для користувача схемами. SED-хороший приклад [2].

Як правило, документ існує разом з його електронною реєстраційною карткою. У процесі обробки документа до нього приєднується ряд інших об'єктів - резолюції, пов'язані з ними завдання, затвердження та погоджень. У цьому контексті управлінський документ-це записана історія виникнення, обробки та прийняття рішення щодо управлінської події. Повноваження щодо прийняття рішень є найбільш важливим ресурсом підприємства і повинні відповідним чином контролюватися.

При створенні завдання також необхідно мати на увазі єдність цілей інформаційної безпеки, визначених у вигляді тріади:

-цілісність;

- конфіденційність;

- доступність.

Електронний цифровий підпис в основному відповідає цілям захисту цілісності, а шифрування - цілям захисту конфіденційності. Цю відмінність слід мати на увазі, незважаючи на загальну технологічну базу для цих завдань - архітектуру відкритих ключів [6 С. 37-39]. Призначення та застосування електронного цифрового підпису електронний підпис призначений для ідентифікації особи, яка підписала електронний документ, і є повноцінною заміною (аналогом) власноручного підпису у випадках, передбачених законом [2].

Використання електронного підпису дозволяє:

- захист від змін (підробка) документа: гарантія виявлення підробки при перевірці цілісності робить підробку недоцільною в більшості випадків;

- неможливість відмови від авторства. Оскільки створити правильний підпис можна, тільки знаючи закритий ключ, і він повинен бути відомий тільки власнику, власник не може відмовитися від свого підпису під документом;

-доказове підтвердження авторства документа: оскільки створити правильний підпис можна, тільки знаючи закритий ключ і він повинен бути відомий тільки власнику, власник пари ключів може довести своє авторство підпису під документом.

Залежно від деталей визначення документа, такі поля, як "автор", "внесені зміни", "тимчасова мітка" і т.д., можуть бути підписані По суті, ЕЦП-це певна послідовність символів, яка виходить в результаті певного перетворення вихідного документа (або будь-який інший інформації) за допомогою спеціального програмного забезпечення. ЕЦП додається при пересиланні до вихідного документа. Будь-яка зміна вихідного документа робить ЕЦП недійсною.

На практиці ЕЦП унікальна для кожного документа і не може бути перенесена на інший документ; неможливість підробки електронного цифрового підпису забезпечується дуже великим обсягом математичних

обчислень, необхідних для її вибору. Таким чином, при отриманні документа, підписаного ЕЦП, одержувач може бути впевнений в авторстві і незмінності тексту цього документа. Електронний цифровий підпис використовується для підтвердження авторства та незмінності інформації (електронного документа). В системі електронних торгів постачальник, який подав цінову пропозицію або заявку на участь в тендері, зобов'язується поставити товари або послуги на умовах, зазначених у його пропозиції. Будучи підписаним ЕЦП, дана пропозиція набуває юридичного значення і тягне за собою відповідальність відповідно до законодавства [1].

Таким чином, замовник в системі електронних торгів має справу з реальними пропозиціями, виконання яких гарантовано законом. ЕЦП використовується в наступних випадках:

- для електронних торгів: постачальник може підписати заявку з використанням ЕЦП на аукціоні, і це гарантує юридичну значимість його пропозиції, Замовник може підписати заявку з використанням ЕЦП, розміщену в системі електронних торгів.

Використання електронного цифрового підпису не змінює порядок підписання договорів та інших документів, встановлений законом для вчинення правочинів у письмовій формі. Висновки по розділу Електронний цифровий підпис (ЕЦП) - послідовність символів, отримана в результаті криптографічного перетворення вихідної інформації (криптографічний захист інформації заснована на функціональному перетворенні інформації і використовується для приховування змісту інформації), яка дозволяє підтвердити цілісність і незмінюваність вихідної інформації. ця інформація, а також її авторство.

Цифровий підпис-це кінцева Цифрова послідовність, яка залежить від самого повідомлення або документа і від секретного ключа, відомого тільки суб'єкту підпису, призначеного для встановлення авторства. Оскільки цифровий підпис заснований на криптосистемі з відкритим ключем, необхідно мати пару ключів - секретний і відкритий. Секретний ключ використовується для формування цифрового підпису, тому його потрібно зберігати в таємниці. А відкритий ключ використовується для перевірки відповідності підпису

документу, тому він повинен бути опублікований, наприклад, у загальнодоступному каталозі. електронний захист цифровий підпис

1.2. Характеристика особливостей застосування цифрового підпису

Цифрові підписи засновані на криптографії з відкритим ключем, також відомій як асиметрична криптографія. Використовуючи алгоритм відкритого ключа, такий як Rivest-Shamir-Adleman або RSA, генеруються два ключі, створюючи математично пов'язану пару ключів: один приватний та один відкритий .

Цифрові підписи працюють за допомогою двох криптографічних ключів з відкритим ключем, що забезпечують взаємну автентифікацію. Для шифрування та дешифрування особа, яка створює цифровий підпис, використовує приватний ключ для шифрування даних, пов'язаних із підписом. Єдиний спосіб розшифрувати ці дані - за допомогою відкритого ключа підписувача [4].

Якщо одержувач не може відкрити документ за допомогою відкритого ключа підписувача, це вказує на наявність проблеми з документом або підписом. Саме так здійснюється аутентифікація цифрових підписів.

Цифрові сертифікати, які також називаються сертифікатами відкритого ключа, використовуються для перевірки того, що відкритий ключ належить емітенту. Цифрові сертифікати містять відкритий ключ, інформацію про його власника, дати закінчення терміну дії та цифровий підпис емітента сертифіката. Цифрові сертифікати видаються довіреними сторонніми центрами сертифікації (CAS), такими як DocuSign або GlobalSign, наприклад. Сторона, що відправляє документ, і особа, що підписує його, повинні погодитися використовувати даний центр сертифікації .

Технологія цифрового підпису вимагає, щоб усі сторони були впевнені, що особа, яка створює зображення підпису, зберігає секретний ключ у таємниці. Якщо хтось інший має доступ до приватного ключа підпису, ця сторона може створити шахрайські цифрові підписи від імені власника приватного ключа [2].

Цифрові підписи мають наступні переваги:

Безпека. Можливості безпеки вбудовані в цифрові підписи, щоб гарантувати, що юридичний документ не буде змінений і підписи будуть законними. Функції безпеки включають асиметричну криптографію, персональні ідентифікаційні номери (PIN-коди), контрольні суми та циклічні перевірки надмірності (CRCS), а також перевірку CA та постачальника довірчих послуг (tsp).

Тимчасова мітка. Це дозволяє вказати дату та час цифрового підпису і корисно, коли терміни мають вирішальне значення, наприклад, при біржових торгах, видачі лотерейних квитків і судових розглядах [1].

Визнаний у всьому світі і відповідний законодавству. Стандарт інфраструктури відкритих ключів (PKI) забезпечує безпечне створення та зберігання ключів, створених постачальником. Оскільки цифрові підписи стають міжнародним стандартом, все більше країн приймають їх як юридично обов'язкові.

Економія часу. Цифрові підписи спрощують трудомісткі процеси фізичного підписання документів, їх зберігання та обміну, дозволяючи підприємствам швидко отримувати доступ до документів і підписувати їх.

Економія коштів. Організації можуть перейти на безпаперовий формат і заощадити гроші, раніше витрачені на фізичні ресурси, час, персонал та офісні приміщення, які використовуються для управління документами та їх транспортування.

Позитивний вплив на навколишнє середовище. Зменшення використання паперу також зменшує кількість фізичних відходів, що утворюються при використанні паперу, та негативний вплив транспортування паперових документів на навколишнє середовище.

Простежуваність. Цифрові підписи створюють контрольний журнал, який спрощує ведення внутрішнього обліку для підприємств. Оскільки все записується та зберігається цифровим способом, користувач, який підписує документи вручну, має менше можливостей помилитися або помістити щось не туди.

Для створення цифрового підпису використовується програмне забезпечення для підпису, таке як програма електронної пошти, яке забезпечує односторонній хеш електронних даних, що підлягають підпису.

Хеш-це рядок букв і цифр фіксованої довжини, що генерується алгоритмом. Для шифрування хешу використовується закритий ключ творця цифрового підпису. Зашифрований хеш-разом з іншою інформацією, такою як алгоритм хешування, - це цифровий підпис.

Причиною шифрування хешу замість усього повідомлення чи документа є те, що хеш-функція може перетворити довільний вхід у Значення фіксованої довжини, яке зазвичай набагато коротше. Це економить час, оскільки хешування відбувається набагато швидше, ніж підписання.

Значення хешу унікальне для хешованих даних. Будь - яка зміна даних - навіть зміна одного символу-призводить до іншого значення. Цей атрибут дозволяє іншим користувачам використовувати відкритий ключ підписувача для розшифровки хешу для перевірки цілісності даних.

Якщо розшифрований хеш збігається з другим обчисленим хешем тих самих даних, це доводить, що дані не змінилися з моменту їх підписання. Але, якщо два хеші не збігаються, дані або були якимось чином змінені та скомпрометовані, або підпис був створений за допомогою приватного ключа, який не відповідає відкритому ключу, представленому підписувачем. Це сигналізує про проблему автентифікації [2].

Розділ 3 Забезпечення конфіденційності цифрових підписів

3.1. Алгоритми шифрування цифрових підписів

Алгоритми шифрування поділяють на асиметричні (з відкритим, публічним ключем) та симетричні (з приватним, секретним ключем, одноключові). Алгоритми шифрування, що називаються симетричними базуються на принципі того, що і відправники, і одержувачі користуються однаковим 13 ключем. Таємний ключ повинен триматися в секреті і передаватись так, щоб запобігти його перехоплення. В разі якщо таємний ключ захищений, при розшифруванні повідомлення автоматично автентифікація

відправника, тому що саме він є власником ключа, за яким можливо зашифрувати інформацію і саме отримувач має ключ, за допомогою якого можна дешифрувати повідомлення. Оскільки відправники та одержувачі є єдиними користувачами, які мають цей симетричний ключ, при спробі скористатись несанкціоновано ключем, буде скомпрометовано взаємодія лише цих двох користувачів. Безпека цього типу системи шифрування залежить від збережності захищеності ключа, що використовується в алгоритмі шифрування, а не від зберігання в секреті алгоритму. Зазвичай симетричний варіант ЕЦП передбачає присутність в системі третьої сторони – «арбітра», який виступає довіреною стороною обох користувачів. Аутентифікація документу визначається самим факт зашифрування його секретним ключем і передача арбітру. Використовується рідко, тому що ефективних алгоритмів не існує. Переваги симетричного методу генерування електронного цифрового підпису: - криптостійкість симетричних схем має високі показники за рахунок стійкості блочних шифрів, що використовується. Їх надійність також достатньо досліджена; - якщо стійкість шифру недостатня, його легко замінити іншим. Недостатки симетричних методів для створення ЕЦП: - необхідно підписувати кожен з бітів інформації, що значно збільшує підпис (він часто буває на порядок довшим за довжину документу); - створені для підпису ключі можна використати лише один раз, тому що після підпису розсекречується половина секретного ключа. Будь-які криптосистеми, в основі роботи яких лежить використання закритого ключа, безпосередньо залежать від ступеня секретності цих даних.

Алгоритми шифрування, які називають асиметричними (або шифрування з публічним ключем), відмінно від асиметричних схем, використовують два ключі - секретний ключ (secret key или private key) і відкритий ключ (public key), створені таким чином, що їх послідовне застосування до інформаційного об’єкту не змінює цей об’єкт. Ці ключі різні і не можуть бути отримані один від одного, не дивлячись на те, що вони згенеровані разом. Для зашифрування використовується лише відкритий ключ, для декодування використовується тільки секретний ключ. Розшифровка коду без знання секретного ключа – це

надмірно складна задача. Зокрема, задача розрахунку секретного ключа по відомому відкритому ключу є практично нерозв'язною. Основною перевагою шифрування з публічним ключем є простий механізм передачі ключів. При з’єднанні каналом зв'язку передається лише відкритий ключ. Це дозволяє використовувати звичайний канал для цього і виключає потребу спеціального каналу безпеки для пересилання ключа. В асиметричної моделі побудови ЕЦП є свої недостатки: - асиметричні схеми ЕЦП базуються, як і асиметричне шифрування, на обрахунково складних задачах (задача дискретного логарифмування або задача факторизації); - криптостійкість алгоритмів шифрування з відкритим ключем поки що не доведена строго математично; - для покращення криптостійкості необхідно робити довжину ключів більшою. Саме криптосистеми з відкритими ключами широко застосовуються для генерування електронн-цифрового підпису (ЕЦП). Цифрові підписи, базовані 15 на асиметричних методах шифрування, дозволяють одержувачу перевірити повідомлення на автентичність джерела інформації (іншими словами, автора інформації), а також перевірити, чи змінилася інформація, в процесі передачі адресату. Тому цифрові підписи є засобом аутентифікації та контролю цілісності даних.

3.2. ЦЕП на основі алгоритму RSA

ЦЕП на основі алгоритму RSA може бути складеним наступним чином:

1. Відправник шифрує повідомлення за допомогою публічного ключа отримувача.

2. Отримувач отримує зашифроване повідомлення та використовує свій приватний ключ для розшифрування його.

3. Якщо отримувач хоче відповісти на повідомлення, він шифрує його за допомогою публічного ключа відправника.

4. Відправник отримує зашифровану відповідь та використовує свій приватний ключ для розшифрування її.

5. Цей процес може продовжуватися далі для кількох отримувачів та відправників.

ЦЕП на основі алгоритму RSA дозволяє забезпечити безпеку даних та захист від несанкціонованого доступу до них. Це особливо важливо у випадку передачі конфіденційної інформації, такої як фінансові та медичні дані.

ЦЕП на основі алгоритму RSA Ідея використання алгоритму шифрування RSA полягає в тому, що якщо Степан отримує повідомлення від Марти, він хоче переконатися, що воно насправді від Марти, а не від Зоряни. Якщо Зоряна може видавати себе за Марту та надсилати повідомлення Степану, прикидаючись Мартою, то це здається поганою справою. На щастя, RSA визначає просту схему цифрового підпису. Це не обов'язково найкращий підхід до цифрових підписів, але він підходить, адже це свого роду доведення концепції, хоча й слабкі сторони у ньому також присутні. Для використання цифрових підписів RSA і Марта, і Степан повинні мати ключі RSA. Для них нам потрібно визначити функції шифрування та дешифровки. Припустимо, що функція шифрування повідомлень Марти — eA, а її функція дешифровки — dA. Щоб зашифрувати відкрите текстове повідомлення т для відправки Марті, Степан обчислює c = eA(т). Щоб розшифрувати c, Марта обчислює dA(c), так що dA(c) = dA(eA(m)) = т. Аналогічно, нехай функція шифрування Степана буде ев, а функція дешифровки — dB. 10 Тепер припустимо, що Марта хоче надіслати повідомлення т Степану, і вона хоче ще підписати його, щоб Степан міг не тільки розшифрувати його, але й переконатися, що його надіслала Марта, а не Зоряна. Марта спочатку обчислює зашифрований текст c = ев(т). Потім вона обчислює л = c/A(c), підписаний зашифрований текст, і надсилає я Степану. Цей алгоритм дій відомий як протокол 1111111 (шифрування, а потім підпис). Щоб розшифрувати повідомлення, Степан спочатку обчислює c = eA(з), а потім обчислює т = cIв(c).

3.3. Система захисту даних на базі методу шифрування RSA (відкритий ключ)

Відкритий ключ відомий всім користувачам, які можуть відправляти зашифровані повідомлення за допомогою цього ключа. Закритий ключ використовується тільки власником, який може розшифрувати отримане повідомлення з використанням цього ключа.

При шифруванні повідомлення за допомогою RSA спочатку обирається два прості числа p та q, які використовуються для обчислення модуля n = p*q. Потім вибирається число e, яке буде відкритим ключем, і виконується обчислення числа d - закритого ключа, що задовольняє умову e*d = 1 mod ((p-1)*(q-1)).

Для шифрування повідомлення M використовується формула C = M^e mod n, де C - зашифроване повідомлення. Для розшифрування повідомлення використовується формула M = C^d mod n.

RSA є досить надійним методом шифрування, але його безпека може бути порушена, якщо зловмисник зможе отримати закритий ключ. Тому важливо забезпечити безпеку зберігання закритого ключа, наприклад, зашифрувавши його ще одним методом шифрування або зберігши на фізичному носії з обмеженим доступом.

3.4 Вразливості алгоритму RSA

Спроба зламати ЕЦП фактично обмежується зламом алгоритму шифрування. У випадку спроби зламу шифру RSA існує декілька теоретичних та практичних способів. Найбільш ефективним способом є пошук секретного ключа, який відповідає доступному відкритому ключу. Таким чином, зловмисник може підроблювати підписи та прочитати абсолютно всі повідомлення, зашифровані публічним ключем. Така атака може бути виконана шляхом знаходження основних множників загального модуля p і q. На підставі p, q і n (загальний показник) зловмисник може легко обчислити дробовий показник d. Як уже було зазначено, складність полягає в пошуку цих множників. Безпека RSA напряму залежить від факторингу (розкладу на множники), що є майже невиконуваним завданням, для якого немає ефективного рішення. Насправді, задача відтворення приватного ключа однакова за складністю з проблемою пошуку множників модуля: можна використати d для знаходження співмножників n. А також навпаки, можна застосувати n для знаходження d. Слід зазначити, що вдосконалення комп'ютерних технологій не зменшить криптостійкість від RSA, якщо ключі будуть достатньої довжини. Фактично, модернізація обладнання тільки

підвищує надійність криптосистем. Наступним методом зламу RSA є знаходження методу обчислення кореня ступеня e з $mod\ n$. Так як $C = Me\ (mod\ n)$ (1.2), то коренем порядку e з $mod\ n$ є саме повідомлення M. Знайшовши корінь, можна відкривати шифровані повідомлення і підробити підписи навіть без знання закритого ключа. Така атака не є еквівалентом факторингу, але в даний час не існує відомих методів злому RSA таким чином. Однак у особливих випадках, коли багато пов'язаних між собою повідомлень шифрується на основі тих же показників відносно невеликих розмірів, є можливість відкрити повідомлення. Ці атаки є єдиним способом відтворити всі повідомлення, закодовані за допомогою цього шифру RSA. 28 Існують також інші типи атак, які дозволяють розшифровувати лише одне повідомлення і не дають змоги зловмисникам відкривати інші повідомлення, які зашифровані одним і тим же ключем. Також досліджено та проаналізовано можливість дешифрування тільки якоїсь частини зашифрованого повідомлення. Найпростішою атакою на конкретне повідомлення є атака з допущенням можливого відкритого тексту. Зловмисник, який має зашифрований текст, повинен допустити, що повідомлення має якийсь конкретний текст, після цього шифрує цей текст публічним шифром одержувача, і порівнює текст, що отримав з існуючим шифрованим текстом. Такий вид атаки можна передбачити способом додавання декільках рандомних бітів в кінці тексту. Інша атака на конкретне повідомлення використовується, коли користувач посилає однакове повідомлення трьом отримувачам відразу, кожен з яких має спільний індикатор e = 3. З цим знанням зловмисник має змогу перехопити цей текст і дешифрувати повідомлення M. Таку атаку можна передбачити знову ж таки шляхом введення декількох випадкових бітів до повідомлення, в цей раз при кожному шифруванні. Крім того, існує декілька атак на зашифрований текст (атаки на окремі відправлені тексти для підробки підписів), в яких зловмисник створює деякий шифрований текст і отримує результуючий відкритий текст, для прикладу, підвівши зареєстрованого користувача до розшифрування підставного повідомлення. Звичайно, є ті, хто не зосереджується не на самій криптосистемі, а на сприйнятливості всієї системи комунікації в цілому. Такі атаки не можна

вважати взломом RSA, так як вони не свідчать про слабкості алгоритму RSA, а про вразливість цієї реалізації. Наприклад, зловмисник може мати секретний ключ, якщо він зберігається без достатньої обережності. Слід зазначити, що для цілковитого захисту недостатньо роботи алгоритму RSA і заходів для захисту безпеки зі сторони математики, тобто використати ключ з достатньою довжиною, оскільки фактично атаки на 29 незахищені ланки системи взаємодії та генерації ключів RSA мають більший успіх

Література:

1. What is a digital signature? [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/digital-signature.
2. Криптографічний захист інформації [Електронний ресурс] // АТ "ІІТ" – Режим доступу до ресурсу: https://iit.com.ua//index.php?page=itemdetails&p=9&gtype=1&type=1&id=38.
3. Hohenberger S. Synchronized Aggregate Signatures from the RSA Assumption / Susan Hohenberger, Brent Waters // [Електронний ресурс] - Режим доступу: https://www.researchgate.net/publication/324109825_Synchronized_Aggregate SignaturesfromtheRSAAssumption
4. Ishida A. Proper Usage of the Group Signature Scheme in ISO/IEC 20008-2 / A. Ishida, Yu. Sakai, K. Emura, G. Hanaoka, K. Tanaka// 5 July 2019, (https://www.researchgate.net/publication/334331763_Proper_Usage_of_the_Gr oup_Signature_Scheme_in_ISOIEC_20008-2)