Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна работа №1
з дисципліни
«Методи реалізації криптографічних
механізмів»
Тема:
« Вибір бібліотеки для реалізації Web-сервісу електронного цифрового підпису»

Виконав
Студент групи ФІ-22мн
Русєв Денис
Перевірив
Кудін А.М.

Київ-2023

Електро́нний цифрови́й пі́дпис (ЕЦП) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Цифрові підписи можна використовувати для розповсюдження повідомлення у формі відкритого тексту, коли одержувачі повинні ідентифікувати та перевірити відправника повідомлення. Підписання повідомлення не змінює повідомлення; він просто генерує рядок цифрового підпису, який можна з'єднати з повідомленням або передати окремо. Цифровий підпис — це короткий фрагмент даних, зашифрований закритим ключем відправника. Розшифровка даних підпису за допомогою відкритого ключа відправника доводить, що дані були зашифровані відправником або кимось, хто мав доступ до закритого ключа відправника.

Цифрові підписи генеруються за допомогою алгоритмів підпису відкритого ключа. Закритий ключ генерує підпис, а відповідний відкритий ключ потрібно використовувати для перевірки підпису. Цей процес показано на наступній ілюстрації.

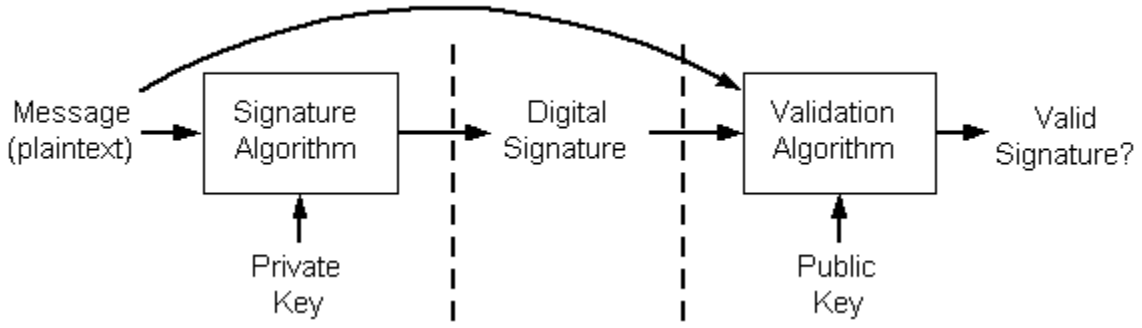
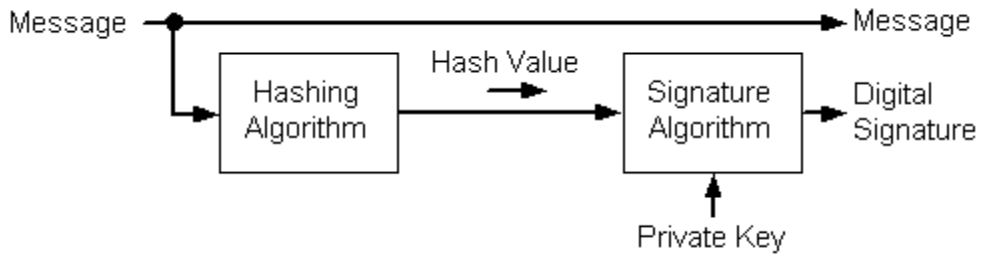


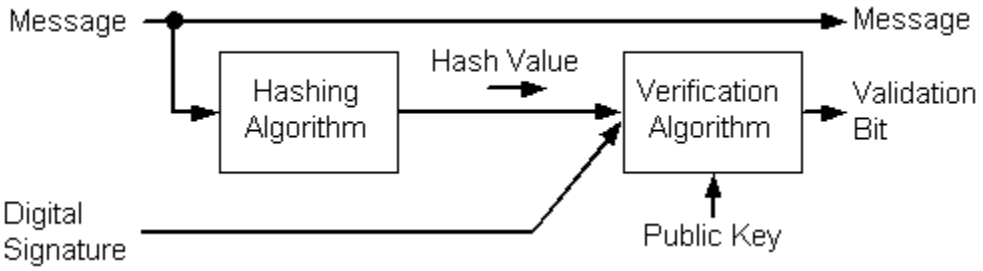
Рис. 1

Створення цифрового підпису з повідомлення складається з двох кроків. Перший крок передбачає створення хеш-значення (також відомого як дайджест повідомлення) з повідомлення. Потім це хеш-значення підписується за допомогою закритого ключа підписувача. Нижче наведено ілюстрацію етапів створення цифрового підпису.



Pic. 2

Для перевірки підпису потрібні як повідомлення, так і підпис. По-перше, хеш-значення має бути створено з повідомлення так само, як створено підпис. Потім це хеш-значення перевіряється на відповідність підпису за допомогою відкритого ключа підписувача. Якщо хеш-значення та підпис збігаються, ви можете бути впевнені, що повідомлення дійсно є тим, яке підписав первісно, і що воно не було змінено. Наступна схема ілюструє процес перевірки цифрового підпису.



Pic. 3

Хеш-значення складається з невеликої кількості двійкових даних, зазвичай близько 160 біт. Це створюється за допомогою алгоритму хешування. Деякі з цих алгоритмів перераховані далі в цьому розділі.

Усі хеш-значення мають такі властивості, незалежно від використовуваного алгоритму:

- Довжина хеш-значення визначається типом використовуваного алгоритму, і її довжина не змінюється залежно від розміру повідомлення. Найпоширеніша довжина хеш-значення становить 128 або 160 біт.

- Кожна пара неідентичних повідомлень перетворюється на зовсім інше хеш-значення, навіть якщо два повідомлення відрізняються лише одним бітом. Використовуючи сучасні технології, неможливо виявити пару повідомлень, які перетворюються на однакове значення хешування, не порушуючи алгоритм хешування.
- Кожного разу, коли певне повідомлення хешується за тим самим алгоритмом, створюється те саме хеш-значення.
- Усі алгоритми хешування є односторонніми. Враховуючи хеш-значення, неможливо відновити оригінальне повідомлення. Насправді жодна з властивостей вихідного повідомлення не може бути визначена лише за допомогою хеш-значення.

Для реалізації Web-сервісу електронного цифрового підпису мною було обрана бібліотека **CryptoLib®V.3.**

CryptoLib®V.3 — багатоцільова криптографічна бібліотека, сертифікована Державною службою спеціального зв'язку та захисту інформації України що підтримує міжнародні та українські криптографічні стандарти. Призначена для криптографічного захисту інформації з використанням кваліфікованого електронного підпису.

CryptoLib®V.3 є набором бібліотек і допоміжного програмного забезпечення, призначеного для шифрування і/або формування і перевірки електронного підпису. Отриманий за допомогою CryptoLibV3 електронний підпис додається до первинних даних і забезпечує їх цілісність, а також надає можливість ідентифікації особи, що підписує. Бібліотека розроблена для різних мов програмування, архітектур та операційних систем.

Основні функції

Криптографічна бібліотека може використовуватися в різноманітних додатках, для генерації та перевірки електронного підпису, шифрування даних, двофакторної автентифікації, забезпечення захищеного каналу зв'язку, управління ключами та сертифікатами (наприклад, генерація, видалення тощо).

Генерація електронного підпису

Криптографічна бібліотека може генерувати удосконалений / кваліфікований електронний підпис (УЕП/КЕП) на програмні або апаратні носії ключової інформації (сумісні з PKCS # 11).

Перевірка електронного підпису

Криптографічна бібліотека експортує функціональність для перевірки різних форматів електронних підписів та перевірки сертифікатів X.509. Процедура перевірки включає перевірку шляху сертифіката та перевірку стану через OCSP (Інтернет-протокол статусу сертифіката) або CRL (Список відкликаних сертифікатів).