Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра комп'ютерної інженерії

ПРОГРАМНА СИСТЕМА РОЗПІЗНАВАННЯ ЦИФРОВОГО ПІДПИСУ

Доповідь по дипломній роботі

Спеціальність 6.050102 - «Комп'ютерна інженерія»

Студента групи 406з: Нікітіна Сергія Олександровича

Керівник: д.т.н., професор **Гожий Олександр Петрович**

Актуальність роботи

Проблема збереження та використання електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є ***Електронний цифровий підпис*** (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Програми електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні. Тому тема дипломної роботи є ***актуальною*** у сучасних умовах.

Призначення Електронного Цифрового Підпису

- Ідентифікація особистості.
- Дистанційна ідентифікація.
- Сучасний спосіб підпису документів.
- Можливість безпечної ідентифікації.
- Юридичне підтвердження особистості.

Мета, об’єкт та предмет дослідження

- ***Мета* роботи** - вдосконалення процесу ідентифікації підпису, завдяки модифікації алгоритму розпізнавання цифрового підпису.
- ***Об’єкт:*** процес модифікації та вдосконалення алгоритму розпізнавання цифрового підпису на основі алгоритму DSA.
- ***Предмет* :** алгоритми в системах ідентифікації цифрового підпису.
- ***Практичне значення*** результатів дипломної роботи полягає розробки програмної системи цифрового підпису, яка дозволяє створювати цифровий підпис та ідентифікувати його, за допомогою актуальних алгоритмів.

Завдання роботи:

- Дослідити сучасні схеми створення електронного цифрового підпису та провести порівняльний аналіз найбільш поширених схем.
- За результатами аналізу виявити фактори, що впливають на швидкодію, та запропоновано модифікований алгоритм.
- Підібрати апаратні компоненти для ефективної роботи програмної системи розпізнавання цифрового підпису;
- Розробити програмну систему розпізнавання цифрового підпису.
- Проаналізувати засоби для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса».

РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ
Аналітичний огляд електронних ключів

Назва ключа	 Електронний ключ "Кристал-1"	 Електронний ключ "Алмаз-1К"
Швидкість шифрування	Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257 - 100 мс. Швидкість формування спільного секрету Діффі-Гелмана в гр.т. еліптичної кривої, поле 571 - 800 мс.	Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257 - 300 мс. Швидкість формування спільного секрету Діффі-Гелмана в гр.т. еліптичної кривої, поле 571 - 2100 мс.
Характеристики	– генерацію особистих та відкритих ключів для алгоритму ЕЦП; – генерацію особистих та відкритих ключів для протоколу розподілу ключів; – генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора; – зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД; – формування і перевірку ЕЦП; – обчислення хеш-функції; – розподіл ключових даних на основі асиметричного протоколу розподілу; – контроль цілісності і працездатності.	

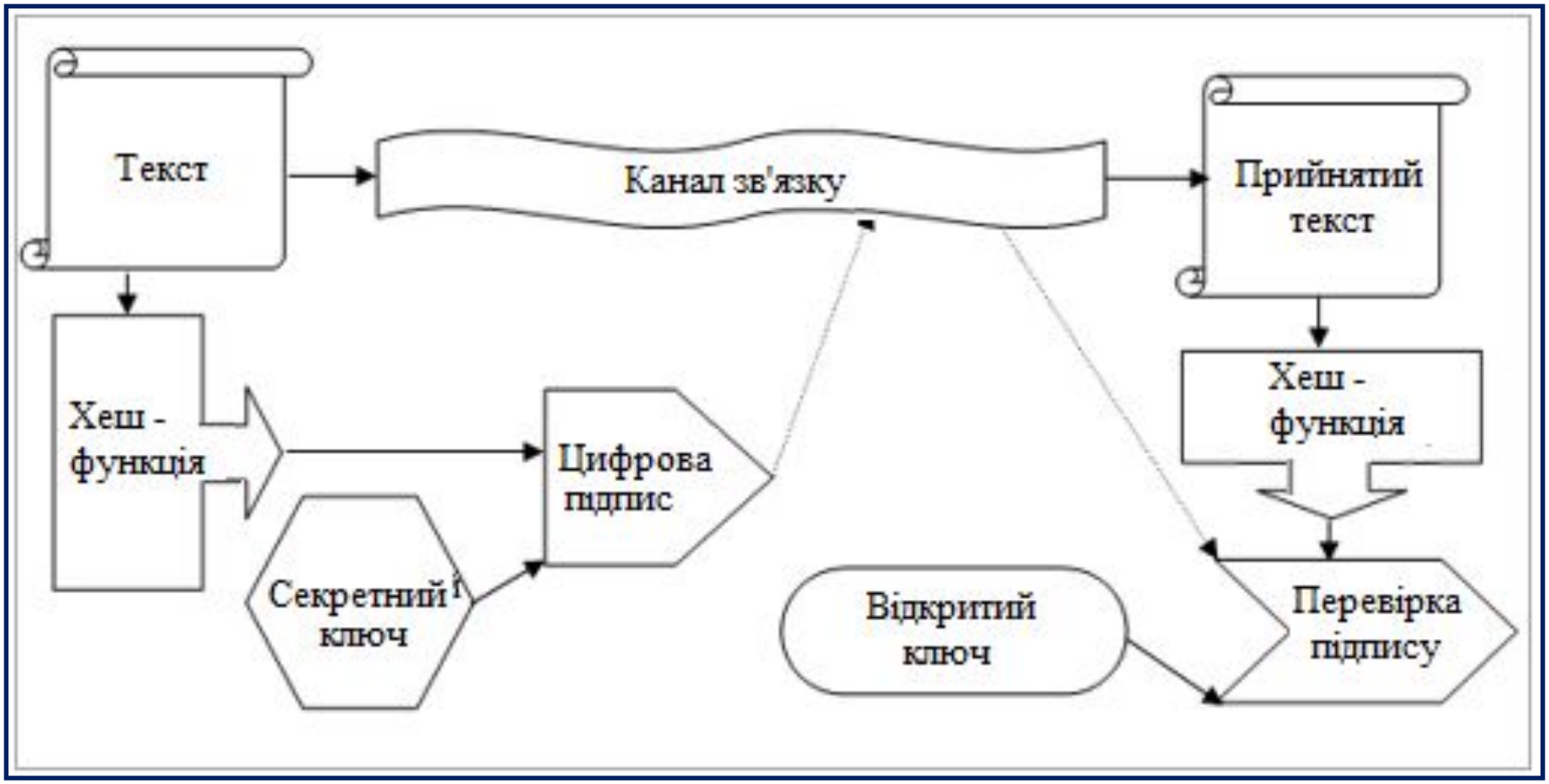
Аналітичний огляд електронних ключів
(подовження)

Назва ключа	 Електронний ключ "Кристал-1"	 Електронний ключ "Алмаз-1К"
Характеристики	Електронний ключ реалізує наступні криптографічні алгоритми та протоколи: – шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки); – ЕЦП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом); – хешування за ГОСТ 34.311-95; протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).	
Форм фактор	ЕК виконаний у вигляді малогабаритного знімного USB-пристрою. Конструктивно ЕК виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та зовнішній вигляд виробу. На друкованій платі встановлюються електроні компоненти ЕК та USB-з'єднувач типу A-plug (виделка).	

Аналітичний огляд криптомодулів

Назва криптомодуля	 Криптомодуль "Гряда-61"	 Мережний криптомодуль "Гряда-301"
Основні функції	• автентифікацію ЕОМ при доступі до модуля; • генерацію особистих та відкритих ключів для алгоритму ЕЦП та протоколу розподілу ключів; • генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора; • зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД; • обчислення хеш-функції, формування і перевірку ЕЦП; • розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних; • контроль цілісності і працездатності вбудованого програмного забезпечення та ін.	• автентифікацію ЕОМ при доступі до модуля; • генерацію особистих та відкритих ключів для алгоритму ЕЦП та протоколу розподілу ключів; • генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора; • зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД; • обчислення хеш-функції, формування і перевірку ЕЦП; • розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних; • контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

Схема формування асиметричного ЕЦП



Алгоритм створення відкритого та секретного ключів RSA

Опис операцій	Приклад
Обираються два випадкових простих числа p та q	$p = 11, q = 7$
Обчислюється їх модуль $n = p*q$	$n = 11 * 7 = 77$
Обчислюється значення функції Ейлера від числа n: $\varphi(n) = (p-1)(q-1)$.	$\varphi(n) = (11-1)*(7-1) = 60$
Обирається ціле число e ($1 < e < \varphi(n)$), взаємно просте зі значенням функції $\varphi(n)$. Зазвичай у якості e беруть прості числа.	$1 < 7 < 60$ $e = 7$
Обчислюється число d, мультипликативно зворотне до числа e по модулю $\varphi(n)$,тобто число, що задовольняє умові: $d\,e \equiv 1 \pmod{\varphi(n)}$	$7 * d \equiv 1 \bmod 60$ $d = 43$
Ключ (e) є відкритим ключем. Набір $P = (e, n)$ надається.	(7, 77)
Ключ (d) відіграє роль секретного ключа та тримається у секреті.	(43)

Алгоритм створення відкритого та секретного ключів El Gamal

Опис операцій	Приклад
Генерується випадкове просте число p	$p = 23$
Обирається довільне ціле число g, що є первісним коренем по модулю p.	$g = 5$
Обирається довільне ціле число x так, що $1 < x < p$	$x = 7$
Обчислюється $y = g^x \bmod p$	$y = 5^7 \bmod 23$
Трійка (p, g, y) надається у якості відкритого набора	(23, 5 17)
(x) відіграє роль секретного ключа та держиться у секреті	(7)

Алгоритм створення відкритого та секретного ключів DSA

Опис операцій	Приклад
Вибір хеш-функції $H(x)$. Для використання алгоритму необхідно, щоб повідомлення, що підписується, було числом.	У нашому випадку повідомлення pt є число 15, тому використовувати хеш-функцію необов'язково.
Вибір простого числа q, розмірність якого в бітах співпадає з розмірністю в бітах значень хеш-функцій $H(x)$ або повідомлення.	$q = 1_3$
Вибір простого числа p, такого, що $(p - 1)$ ділиться на q.	$p = 2_7$
Вибір числа g такого, що його мультиплікативний порядок по модулю p дорівнює q. Для його обчислення можна скористатися формулою $g = h^{(p-1)/q} \bmod p$, де h – деяке довільне число, $h \in (1; p - 1)$ таке, що $g \neq 1$.	$h = 2$ $g = 2^{27/13} \bmod 27$
Вибір секретного ключа x, з умовою, що $x \in (0, q)$. (x) зберігається в секреті.	$x = 8; 8 \in (0, 13)$
Обчислення відкритого ключа по формулі $y = g^x \bmod p$, набір (p, q, g, y) надається.	(7)

Порівняння алгоритмів електронного цифрового підпису

Алгоритм	*Ключ*	*Призначення*	*Коментарі*
RSA	До 4096 біт	Шифрування та ЕЦП	Засновано на трудностях задачі факторізації великих чисел, один з перших асиметричних алгоритмів. Включено до багатьох стандартів.
El Gamal	До 4096 біт	Шифрування та ЕЦП	Засновано на задачі обчислення дискретних логарифмів у кінцевому полі, дозволяє швидко генерувати ключі без зниження стійкості. (Використовується в алгоритмі DSA- стандарту DSS)
DSA	До 1024 біт	ЕЦП	Засновано на трудності задачі дискретного логарифмування у кінцевому полі. У США є стандартом. Використовується для секретних та несекретних комунікацій. Розробник АНБ

РОЗРОБКА ПРОГРАМНОЇ ЧАСТИНИ

Діаграма варіантів використання

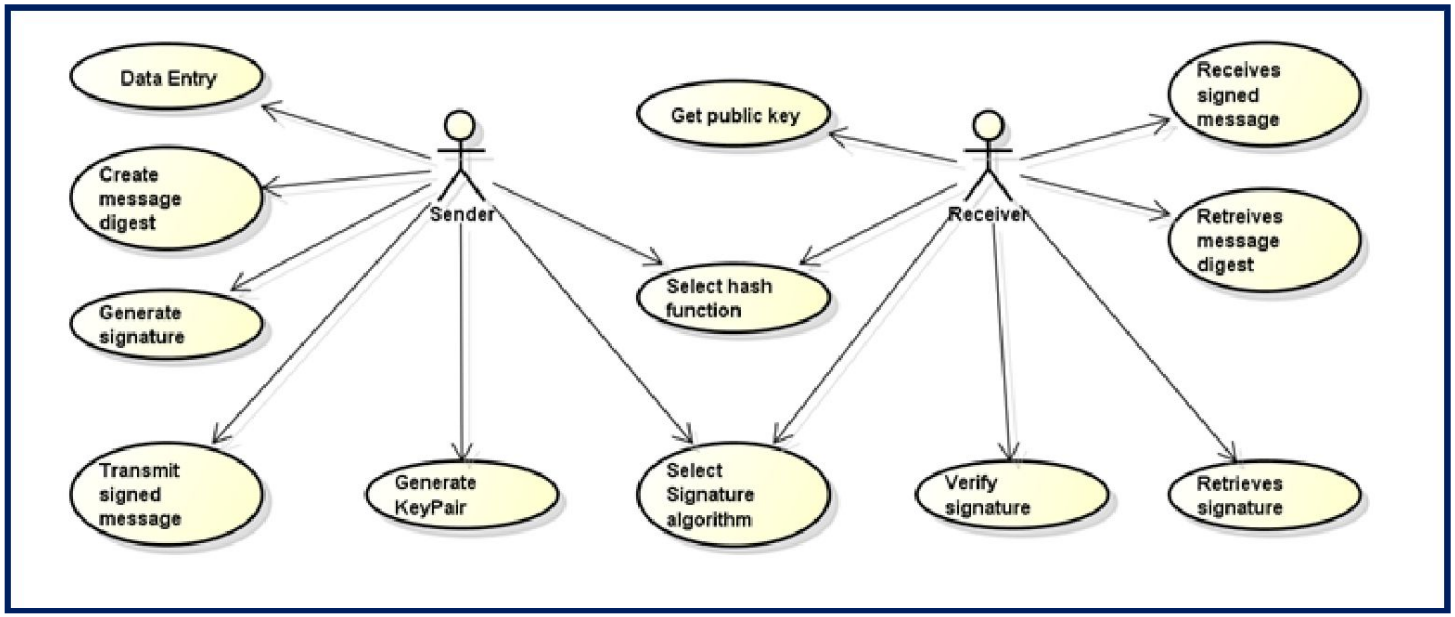


Рисунок 1 - Діаграма варіантів використання

Діаграма класів

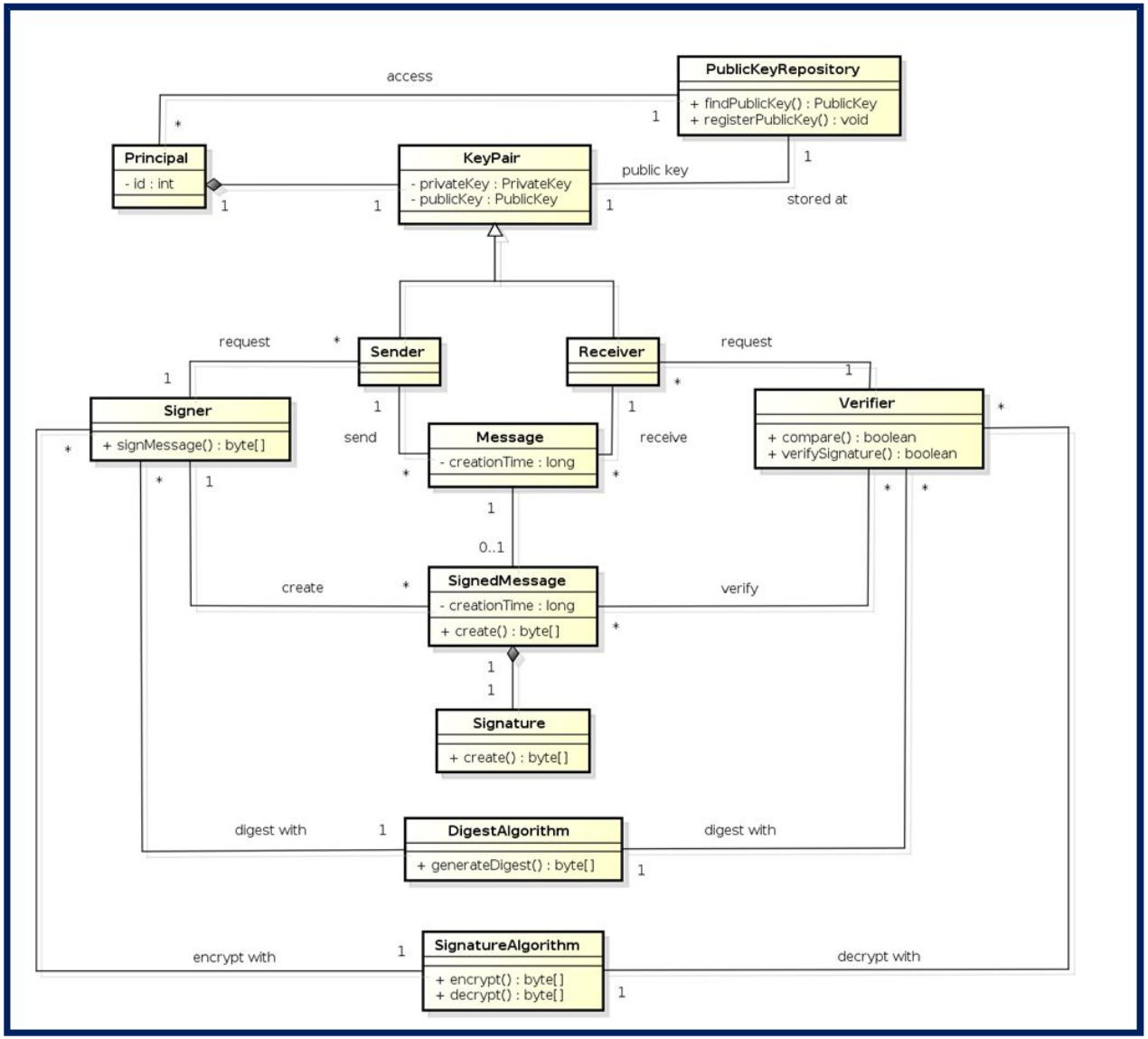
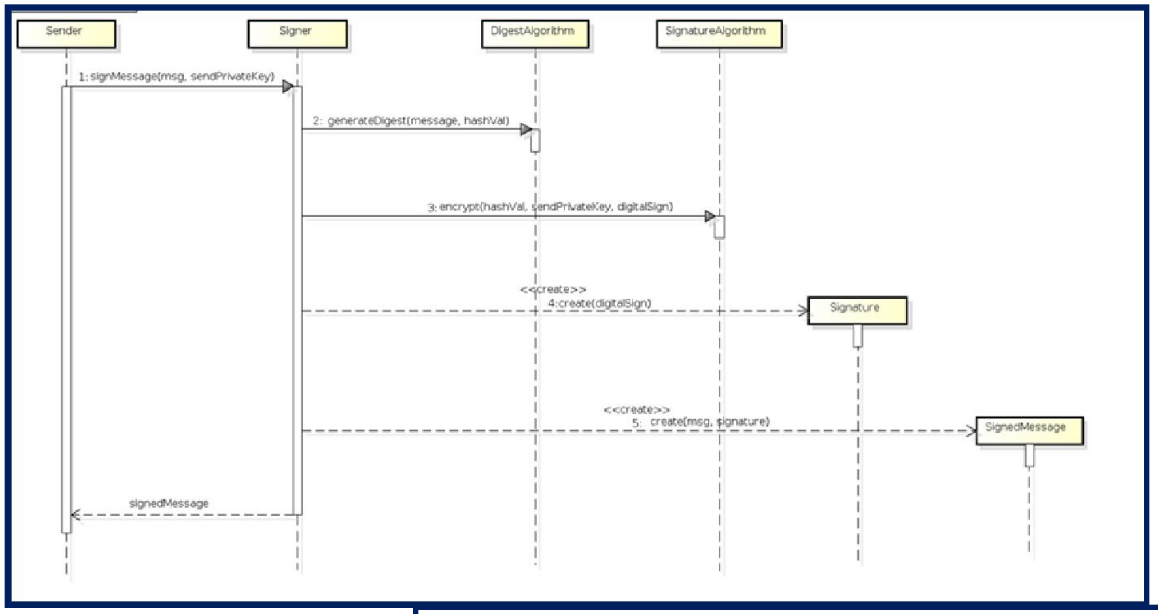
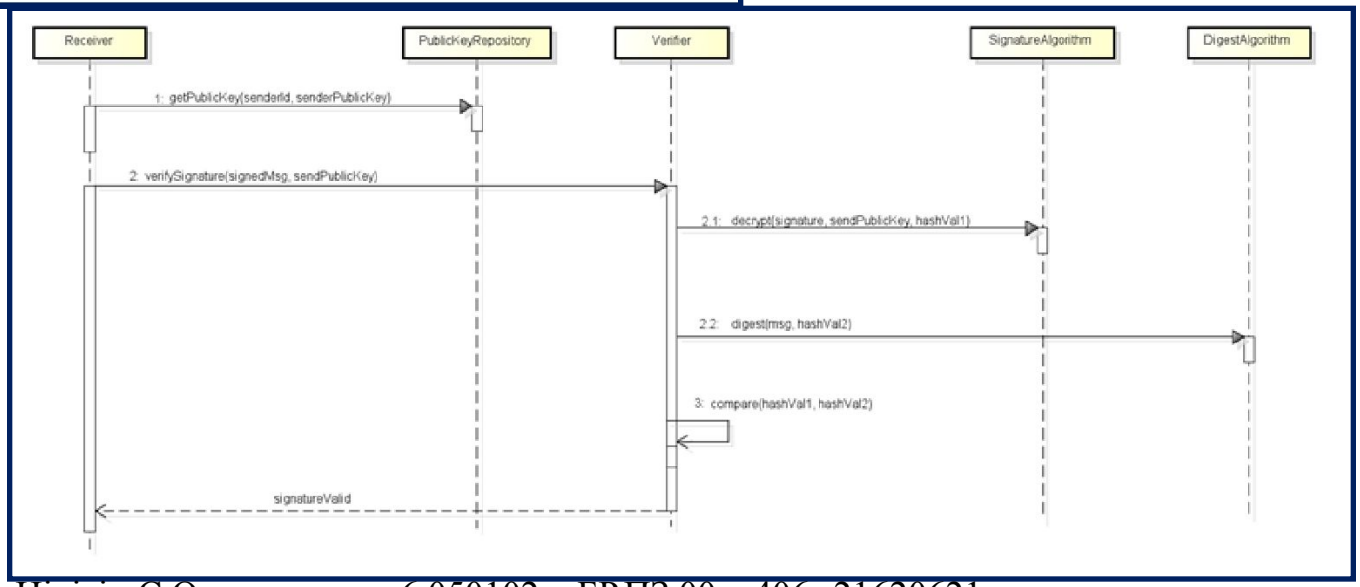


Рисунок 2 - Діаграма класів

Діаграми послідовності





Приклад роботи програми

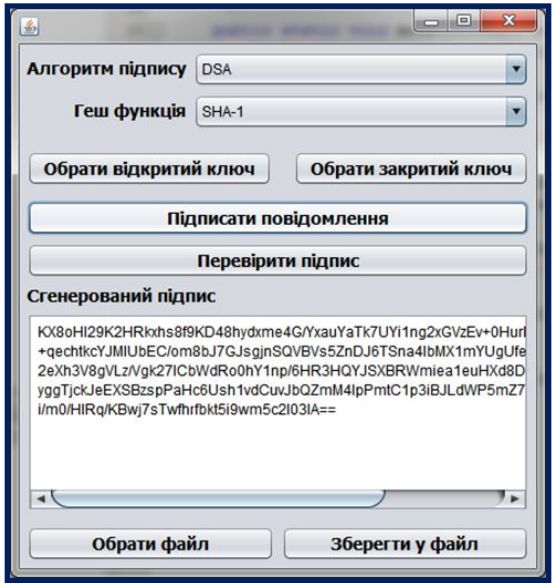


Рисунок 3 - Створення цифрового підпису повідомлення

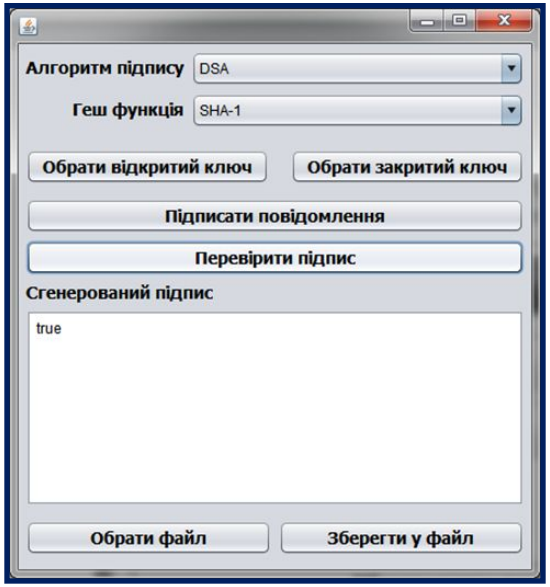


Рисунок 4 - Перевірка підпису

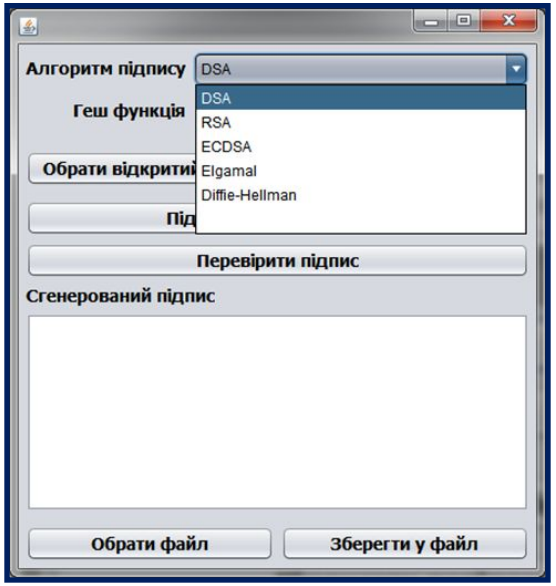


Рисунок 5 - Обрання алгоритму підпису

Приклад роботи програми (подовження)

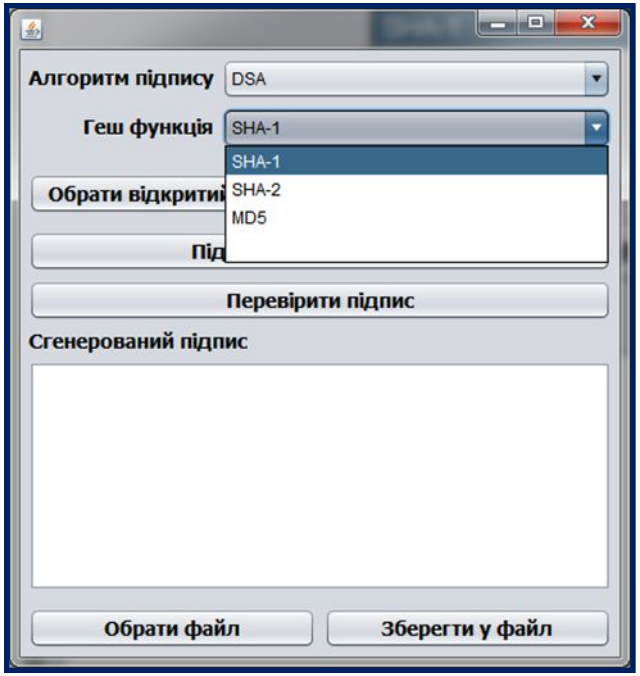


Рисунок 6 - Обрання алгоритму хеш-функції

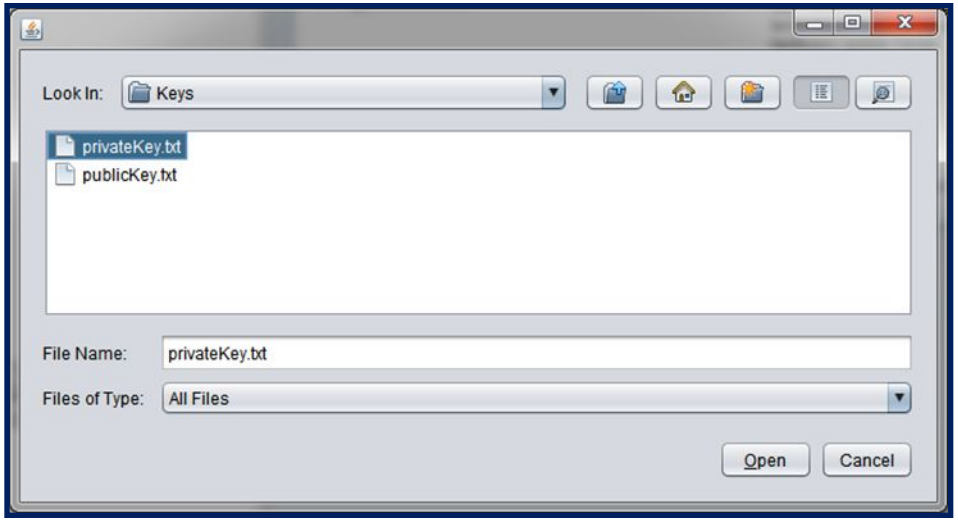


Рисунок 7 - Обрання відкритого/закритого ключа

ВИСНОВКИ

- На основі проведеного аналітичного огляду сучасних схеми створення електронного цифрового підпису, виявлене основні вимоги до програмної системи розпізнавання цифрового підпису.
- За результатами аналізу виявлене фактори, що впливають на швидкодію алгоритму, що є основою програмної системи. Запропоновано та реалізовано оптимізований алгоритм розпізнавання цифрового підпису.
- Здійснено підбір компонентів апаратної частини для ефективної роботи програмної системи розпізнавання цифрового підпису.
- Розроблено програмна система розпізнавання цифрового підпису, що виконує такі функції: створення цифрового підпису повідомлення, перевірка підпису, обрання алгоритму підпису, обрання алгоритму хеш-функції, обрання відкритого/закритого ключа.
- У спеціальному розділі з охорони праці наведено аналіз засобів для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса».