МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І. С.
«____»_____ 2018 р.

ДИПЛОМНИЙ ПРОЕКТ БАКАЛАВРА
ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

«Програмний комплекс для отримання цифрового електронного підпису»

Освітньо-кваліфікаційний рівень – бакалавр
Напрям підготовки : 6.050102 « Комп'ютерна інженерія»

Керівник проекту:		Кардашук В. С.
	(підпис)	(ініціали, прізвище)
Консультант з охорони праці:		Критська Я. О.
	(підпис)	(ініціали, прізвище)
Студент:		Сандулов В. Ю.
	(підпис)	(ініціали, прізвище)
Група:		КІ-14 ад

Сєвєродонецьк-2018

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

Факультет інформаційних технологій та електроніки
Кафедра комп'ютерних наук та інженерії
Напрям підготовки 6.050102 – Комп'ютерна інженерія
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ
_____Скарга-Бандурова І. С.
"____" _____2018 р.

ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Сандулову Владиславу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): «Програмний комплекс для отримання цифрового електронного підпису»,

затверджена наказом по інституту від « 14 » травня 2018 р. №

2. Термін подання студентом закінченого проекту (роботи): 15.06.2018 р.

3. Початкові дані до проекту (роботи): матеріали переддипломної практики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці):

Розробити програмний комплекс для отримання цифрового електронного підпису.

Основна частина повинна містити постановку задачі, короткі теоретичні відомості, опис алгоритмів, використаних в процесі розроблення, програмне забезпечення, додатки.

5. Перелік графічного матеріалу (з точною вказівкою обов'язкових креслень): електронні плакати.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я. О., ст. викладач		

8. Дата видачі завдання: 15.05.2018 р.

Керівник _____

(підпис)

Завдання прийняв до виконання

_____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту	Строк виконання етапів	Примітка
1.	Отримання завдання, збір матеріалів	15.05.18 – 16.05.18	
2.	Огляд літератури й обґрунтування необхідності розроблення	15.05.18– 18.05.18	
3.	Розроблення технічного завдання	21.05.18 – 20.05.18	
4.	Визначення алгоритмів для отримання цифрового електронного підпису	26.05.18 – 28.05.18	
5.	Порівняльний аналіз алгоритмів	23.04.18 – 24.05.18	
6.	Розроблення програмного забезпечення	25.05.18 – 01.06.18	
7.	Охорона праці та безпека в надзвичайних ситуаціях	01.06.18 – 02.06.18	
8.	Оформлення пояснювальної записки	02.06.18 – 04.06.18	

Студент _____ Сандулов В. Ю..

(підпис) (прізвище та ініціали)

Керівник _____ Кардашук В. С.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту: 80 стор., 45 рис., 2 табл., 3 додатки, 32 посилань.

Мета роботи – розроблення програмного комплексу для отримання електронного цифрового підпису з використанням алгоритмів RSA та Ель Гамаля на основі інформації користувача та обраних алгоритмів кодування. З метою розроблення здійснено аналіз та механізм створення електронного цифрового підпису, порівняння симетричних та асиметричних криптосистем, визначені переваги асиметричної криптографії в створенні електронного цифрового підпису.

Проведено аналіз алгоритмів реалізації проекту, розглянуті обчислювальні аспекти вищенаведених алгоритмів.

Розроблений програмний комплекс для отримання ЕЦП по алгоритмам RSA та Ель Гамаля здійснює шифрування з обраними параметрами та зберігає ЕЦП на диску або зовнішньому носію. Програма володіє загально прийнятим інтуїтивно зрозумілим інтерфейсом та підписаними опціями, за замовчуванням сама обирає необхідне розширення файлу, що спрощує роботу з нею користувачів, що не володіють достатніми навиками роботи на персональному комп’ютері.

Розроблені заходи щодо охорони праці та безпеки у надзвичайних ситуаціях.

Ключові слова: *криптографія, електронний цифровий підпис, алгоритм, ключ, хеш-функція, верифікація, криптостійкість.*

Умови одержання роботи:

93406. м. Сєвєродонецьк, пр-кт Центральний, 59а, СНУ ім. В. Даля

ЗМІСТ

ВСТУП

Ухвалення рішень у всіх сферах життєдіяльності підприємства або організації все більшою мірою базується на інформаційних процесах. Аналіз цих процесів з подальшим виробленням управляючих рішень здійснюється на основі інформаційних моделей, побудованих на сучасних інформаційно-телекомунікаційних технологіях. Тому, захист інформації являє собою самостійну складову безпеки підприємства в цілому, значення якої з кожним роком зростає.

Інформаційний ресурс стає одним з головних джерел економічної ефективності підприємства. Фактично спостерігається тенденція, коли всі сфери життєдіяльності підприємства стають залежними від інформаційного розвитку, в процесі якого вони самі породжують інформацію і самі ж її споживають.

На сучасному етапі розвитку основними загрозами безпеці підприємства є загрози в сфері інформаційного забезпечення. Наслідками успішного проведення інформаційних атак можуть стати компрометація або спотворення конфіденційної інформації, нав'язування неправдивої інформації, порушення встановленого регламенту збору, обробки і передачі інформації, відмови і збої в роботі технічних систем, викликані навмисними і ненавмисними діями як з боку конкурентів, так і з боку інших груп користувачів. До однієї з найбільш важливий завдань в області безпеки підприємства слід віднести створення комплексної системи захисту інформації.

З розвитком інформаційних технологій зростає роль достовірності інформації, що передається по каналам зв’язку. Важливу роль в цій передачі відіграє ідентифікація користувачів на основі цифрового електронного підпису.

ЕЦП, відповідно до стандарту ISO 7498-2, є отримані в результаті криптографічного перетворення блоку даних дані, які дозволяють одержувачу

упевнитися в цілісності цього блоку і справжності джерела, а також забезпечує захист від підробки одержувача інформації.

ЕЦП (англ. digital signature) — вид електронного підпису, відповідно до стандарту ISO 7498-2, 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 особу, яка підписувала документ. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

ЕЦП як спосіб ідентифікації підписувача електронного документу, дозволяє однозначно визначати походження інформації (джерело інформації), що міститься у документі. Завдяки цьому ЕЦП є також надійним засобом розмежування відповідальності за інформаційну діяльність у суспільстві.

Метою бакалаврської роботи - розроблення програмного комплексу формування електронного підпису на основі інформації користувача та обраних алгоритмів кодування.

1 АНАЛІЗ ТА МЕХАНІЗМ СТВОРЕННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

1.1 Призначення та юридична значимість ЕЦП

ЕЦП призначений для використання фізичними та юридичними особами - суб'єктами електронного документообігу:

– для ідентифікації особи, яка підписує повідомлення (документ);

– для підтвердження цілісності даних в електронній формі [1].

Накладання ЕЦП завершує утворення електронного документа, надаючи йому юридичної сили. Юридична сила електронного документа з нанесеними одним або множинними ЕЦП та допустимість такого документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму (ст. 8 Закону України «Про електронні документи та електронний документообіг»).

Електронний цифровий підпис володіє також ще і політичними аспектами діяльності суб’єктів підприємницької діяльності, учасників ринку товарів та послуг.

Електронний цифровий підпис як засіб контролю походження і цілісності інформації є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави. Тому ЕЦП, зокрема, і інфраструктура відкритих ключів, у цілому, є стратегічною оборонною технологією, від якості й надійності реалізації якої залежить інформаційна безпека України.

Механізм створення ЕЦП полягає в накладенні за допомогою особистого ключа кодованої інформації та перевірки за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

За умови правильного зберігання власником секретного (особистого) ключа його підробка неможлива. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть миттєво виявлені.

Електронний цифровий підпис підтверджує достовірність і цілісність документа. Якщо в документ в процесі пересилки були внесені які-небудь зміни, нехай навіть зовсім незначні, то підміна виявиться. Сертифікат відкритого ключа містить персональну інформацію про власника, що дозволяє однозначно ідентифікувати автора документу.

Однією з додаткових можливостей при роботі з ЕЦП є послуга фіксації точного часу підписання документа ЕЦП відмітка точного часу. Відмітка точного часу при підписанні документу дозволяє точно ідентифікувати момент накладання підпису, причому змінити його значення згодом, навіть особою, яка наклала підпис, неможливо. Можливе лише повторне підписання з фіксацією нового часу. Точне значення часу, який використовується для формування відмітки точного часу, здійснюється апаратними засобами Центру сертифікації ключів шляхом синхронізації з джерелами точного часу з точністю до 1 секунди.

1.2 Основні поняття та механізм формування ЕЦП

В процедурі створення та подальшої обробки кодованої інформації вводять такі поняття як особистий ключ, відкритий ключ, сертифікат відкритого ключа.

Особистий ключ ЕЦП формується на підставі абсолютно випадкових чисел, що генеруються давачем випадкових чисел, а відкритий ключ обчислюється з особистого ключа ЕЦП так, щоб одержати другий з першого було неможливо.

Особистий ключ ЕЦП є унікальною послідовністю символів довжиною 264 біти, яка призначена для створення електронного цифрового підпису в

електронних документах. Працює особистий ключ тільки в парі з відкритим ключем. Особистий ключ необхідно зберігати в таємниці, адже будь-хто, хто дізнається його, зможе підробити ЕЦП

Документ підписується ЕЦП за допомогою особистого ключа ЕЦП, який існує в одному екземплярі тільки у його власника. Цьому особистому ключу відповідає відкритий ключ, за допомогою якого можна перевірити відповідність ЕЦП його власнику.

Відкритий ключ використовується для перевірки ЕЦП одержуваних документів (файлів). Відкритий ключ працює тільки в парі з особистим ключем. Відкритий ключ міститься в Сертифікаті відкритого ключа, і підтверджує приналежність відкритого ключа ЕЦП певній особі. Крім самого відкритого ключа, Сертифікат відкритого ключа містить в собі персональну інформацію про його власника (ім'я, реквізити), унікальний реєстраційний номер, термін дії Сертифікату відкритого ключа. З метою забезпечення цілісності представлених у Сертифікаті даних він підписується особистим ключем Центру сертифікації ключів. Сертифікат відкритого ключа може публікуватися на сайті відповідного центру сертифікації ключів відповідно до Договору про надання послуг ЕЦП для підприємства чи організації.

1.3 Процедура підписання електронного документу ЕЦП

При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних, так званий ЕЦП. Отримання цього блоку можна розділити на два етапи (рис. 1.1):

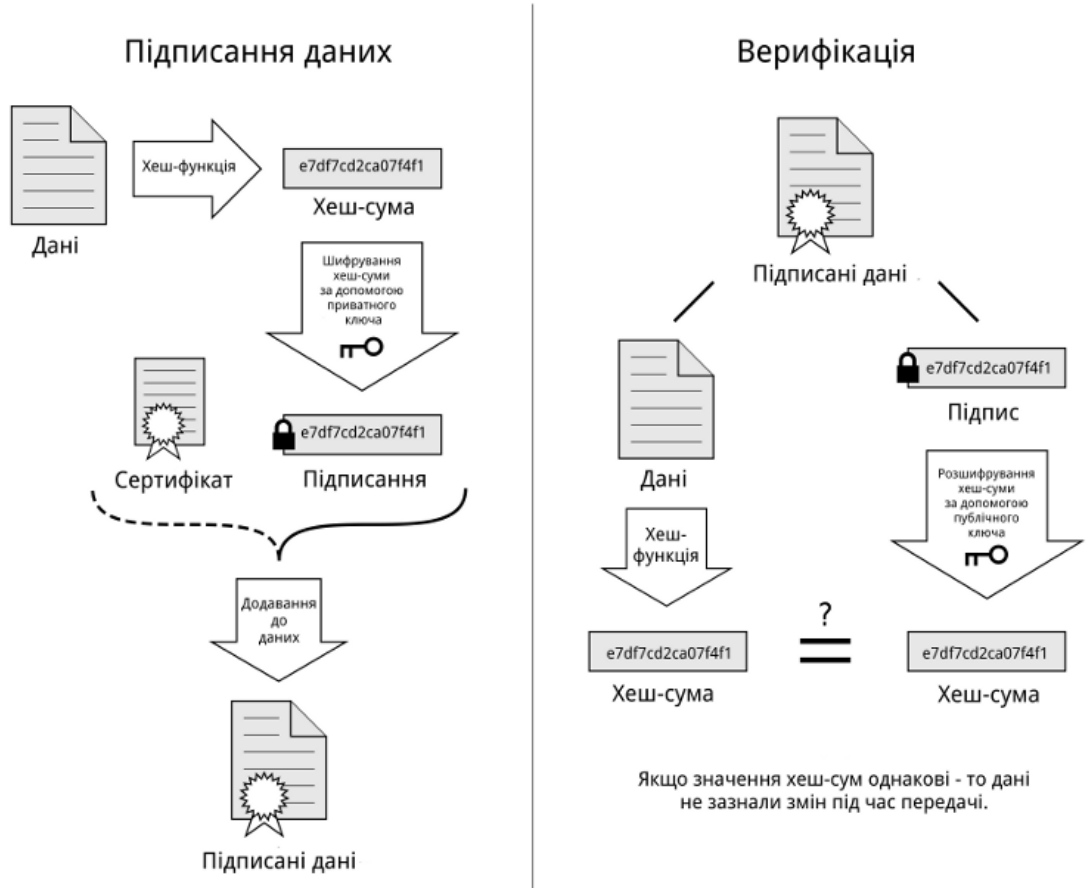


Рисунок 1.1 – Етапи ЕЦП

1. На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest).

Цей відбиток має такі особливості:

– фіксовану довжину, незалежно від довжини повідомлення;

– унікальність відбитку для кожного повідомлення;

– неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться при перевірці електронного цифрового підпису.

2. На другому етапі відбиток документу шифрується за допомогою програмного забезпечення і особистого ключа автора. Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна тільки використовуючи Сертифікат відкритого ключа автора.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документу.

Перевірка Електронного цифрового підпису одержаного документу проводиться декількома етапами:

На першому етапі адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.

За допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток.

При перевірці ЕЦП порівнюються відбитки початкового і одержаного документів. Результат перевірки — одна з відповідей: «вірний»/«невірний».

1.4 Термін валідності та вразливості ЕЦП

Відповідно до чинного законодавства, позначка часу не є обов'язковим атрибутом електронного документу, підписаного електронним цифровим підписом. Цей факт обмежує використання національного ЕЦП тільки для підпису документів, що валідні протягом дії сертифікату ЕЦП, яким було підписано документ. Зазвичай користувачі самі визначають термін валідності, якщо немає застережень. Зазвичай термін дії ЕЦП виданий сертифікованими центрами обмежується 1 або 2 роками використання і визначається при початковій реєстрації в центрах надання таких послуг.

Чинне законодавство не визначає особливості застосування ЕЦП, щодо документів, термін дії яких перевищує термін дії ЕЦП. Також не визначено статус підписаних документів, термін дії яких не закінчився, у разі компрометації ЕЦП. Це дозволяє реалізувати два види атак на ЕЦП:

1. Використання недійсного ЕЦП (скомпрометованого, або ЕЦП, термін дії якого закінчився) для підпису документів заднім числом;

Визнання підписаного документу без позначки часу, сертифікат якого на час перевірки підпису не діє, недійсним на підставі того, що неможливо встановити чи був документ підписаний дійсним ЕЦП, чи був підписаний заднім числом недійсним ЕЦП. Ця атака може супроводжуватись брехливою заявою про компрометацію ключа ЕЦП.

Ця вразливість позбавляє змісту такі послуги сертифікаційних центрів, як призупинення дії ЕЦП або реєстрація компрометації ключа ЕЦП.

Головною помилкою, що призвела до з'явлення вразливості, є сприйняття інфраструктури ЕЦП обмеженою відношеннями двох сторін, що перевіряють підпис на момент складання документу. При цьому не враховується роль арбітра при виникненні спорів, щодо підписаного документу. Тобто валідність підписаного документа розглядається у статиці, а має розглядатися у динаміці.

Атака підпису заднім числом може бути успішно змодельована з використанням чинного ЕЦП і сертифікованого програмного забезпечення переведенням системного годинника комп'ютера назад.

1.5 Порівняння симетричних та асиметричних криптосистем

В основному, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні. На практиці, це означає, що якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох боків передачі інформації. Так як ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

Переваги:

- швидкість (за даними Applied Cryptography - на 3 порядки вище);
- простота реалізації (за рахунок більш простих операцій);
- менша необхідна довжина ключа для порівнянної стійкості;
- вивченість (за рахунок більшого віку).

Недоліки:

1. Складність управління ключами у великій мережі. Це означає квадратичне зростання числа пар ключів, які треба генерувати, передавати, зберігати і знищувати в мережі. Для мережі в 10 абонентів потрібно 45 ключів, для 100 вже 4950, для 1000 - 499500 і т. д.

2. Складність обміну ключами. Для застосування необхідно вирішити проблему надійної передачі ключів кожному абоненту, тому що потрібен секретний канал для передачі кожного ключа обом сторонам.

3. Для компенсації недоліків симетричного шифрування в даний час широко застосовується комбінована (гібридна) криптографічний схема, де за допомогою асиметричного шифрування передається сеансовий ключ, що використовується сторонами для обміну даними за допомогою симетричного шифрування.

4. Важливою властивістю симетричних шифрів є неможливість їх використання для підтвердження авторства, так як ключ відомий кожній стороні.

1.6 Переваги асиметричної криптографії в створенні ЕЦП

Асиметрична криптографія або системи з відкритим ключем дозволяють зашифрувати повідомлення для конкретного адресата без попереднього обміну ключами, тобто зашифрувати лист, телефонну розмову тощо з незнайомою людиною таким чином, що перехопити ключ до шифру принципово неможливо. Їх суть полягає в тому, що кожний користувач генерує два ключі, які пов’язані деяким співвідношенням. Один ключ функціонує відкрито, інший є таємним. Текст шифрується відкритим ключем адресата. Процес дешифрування можна здійснити тоді, коли відомий таємний ключ. Дану систему можна використовувати як самостійний засіб захисту, так і при розподілі ключів, а також як засіб аутентифікації, тобто, асиметрична

криптографія дозволяє підтвердити, що повідомлення передане власником конкретного ключа і ніким іншим.

Надійність захисту інформації забезпечується не таємністю алгоритмів, а передусім математичними фактами (алгоритмічною нерозв'язністю визначених математичних задач).

Наприклад, лист, зашифрований за декілька хвилин на дешевому персональному комп'ютері, для "зламу" зажадає багатьох днів, а то і років, роботи самих потужних суперкомп'ютерів, якими володіють державні силові структури.

Стандарти ЕЦП наведені в табл. 1.1

Таблиця 1.1 – Стандарти ЕЦП

№ п/п	Тип цифрового підпису	Стандарт
1	RSA схема	ISO 9796, 11166
2	DSA схема	NIST MD-20899
3	DSA подібная схема	ГОСТ 34.10-94
4	Ель-Гамаля	–
5	Діффі-Хелмана	–

Наведені стандарти припускають несиметричну схему формування і перевірки цифрового підпису. Для виконання цих процедур використовуються різні ключі. Для установки цифрового підпису - т. зв. конфіденційні, а для перевірки цифрового підпису - відкриті ключі. Тому додатково з цими схемами використовуються стандарти для роботи з відкритими ключами, наприклад, стандарт для угоди про ключі Діффі-Хелмана (X9.42).

Основна задача проекту полягає в розробленні програмного комплексу створення ЕЦП на основі алгоритмів асиметричного шифрування з

використанням мови програмування C++ та середовища налаштування Microsoft Visual Studio Net/

Висновки до розділу 1

У першому розділі розглянуто призначення та юридична значимість ЕЦП. Підкреслено, що накладання ЕЦП завершує процес утворення електронного документа, надаючи йому юридичної сили. Електронний цифровий підпис як засіб контролю походження і цілісності інформації є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави.

В процедурі створення, механізму формування ЕЦП та подальшої обробки кодованої інформації вводять такі поняття як особистий ключ, відкритий ключ, сертифікат відкритого ключа.

Визначені процедура підписання електронного документу, термін валідності та вразливості, переваги асиметричної криптографії в створенні ЕЦП.

На основі проведеного огляду визначені задачі розроблення.

2 АЛГОРИТМИ ФОРМУВАННЯ ЦИФРОВОГО ЕЛЕКТРОННОГО ПІДПИСУ

2.1 Загальна класифікація алгоритмів та порівняння асиметричних та симетричних алгоритмів

На рисунку 2.1 наведена загальна класифікація криптографічних алгоритмів.

Рисунок 2.1 – Класифікація криптографічних алгоритмів

Алгоритми з відкритим ключем (звані також асиметричними алгоритмами) розроблені таким чином, що ключ, використовуваний для зашифрування, відрізняється від ключа розшифрування. Більш того, ключ розшифрування не може бути (принаймні протягом розумного інтервалу часу) розрахований по ключу зашифрування. Такі алгоритми називають алгоритмами з відкритим ключем, тому що ключ зашифрування може бути

відкритим: хто завгодно може використовувати цей ключ для зашифрування повідомлення, але розшифрувати повідомлення може тільки конкретна людина, яка знає ключем розшифрування. У таких системах ключ зашифрування часто називають відкритим ключем, а ключ розшифрування – закритим ключем. Закритий ключ іноді називають секретним ключем, але щоб не було плутанини з симетричними алгоритмами, цей термін використовується в даній роботі. Припустимо, що К1 – деякий відкритий ключ (для зашифрування), а К2 – відповідний закритий ключ (для розшифрування), тоді зашифрування з відкритим ключем К1 позначається як: Ек1(М)=С, а розшифрування з відповідним закритим ключем К2 позначається як: Dк2(С)=М.

Схематично зашифрування та розшифрування при використанні асиметричних криптографічних алгоритмів зображені на рисунку 2.2.

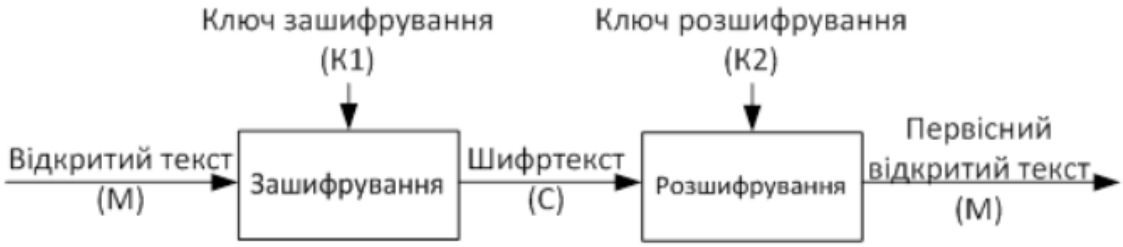


Рисунок 2.2 – Операції зашифрування та розшифрування в асиметричних криптосистемах

Слід зауважити, що ключі К1 та К2 не обов’язково мають бути різними, але в тому випадку, коли вони співпадають, втрачається багато переваг алгоритма з відкритим ключем.

Іноді повідомлення зашифровуються закритим ключем, а розшифровуються – відкритим ключем. Такий метод використовують для цифрового підпису. Ці операції, відповідно, позначають як: Ек2(М)=С, Dк1(С)=М.

Від часу винайдення криптографії з відкритим ключем було запропоновано безліч криптографічних алгоритмів з відкритими ключами . Багато з них не є стійкими. А з тих, які є стійкими, багато непридатних для практичної реалізації . Або вони використовують дуже великий ключ, або розмір отриманого шифртексту набагато перевищує розмір відкритого тексту. Небагато алгоритмів є і безпечними, і практичними. Зазвичай ці алгоритми засновані на одній з важких проблем. Деякі з цих безпечних і практичних алгоритмів підходять тільки для розподілу ключів. Інші підходять для шифрування (і для розподілу ключів). Треті корисні тільки для цифрових підписів.

Тільки три алгоритми добре працюють як при шифруванні, так і для цифрового підпису: RSA (RSA абревіатура від прізвищ Rivest, Shamir и Adleman - Рональд Рівест, Аді Шамір и Леонард Адлеман - Массачусетський технологічний институт) — криптографічний алгоритм з відкритим ключем, який базується на обчислювальній складності задачі факторизації великих цілих чисел.

Усі ці алгоритми повільні. Вони зашифровують і розшифровують дані набагато повільніше, ніж симетричні алгоритми. Зазвичай їх швидкість недостатня для шифрування великих обсягів даних.

Гібридні криптосистеми дозволяють прискорити події: для шифрування повідомлення використовується симетричний алгоритм з випадковим ключем, а алгоритм з відкритим ключем застосовується для шифрування випадкового сеансового ключа.

Симетричні алгоритми, які іноді називають умовними алгоритмами, це ті, в яких ключ зашифрування може бути розрахований з ключа розшифрування, і навпаки. У більшості симетричних алгоритмів ключі зашифрування і розшифрування ті самі . Ці алгоритми, також звані алгоритмами з секретним ключем або алгоритмами з єдиним ключем, вимагають, щоб відправник і одержувач погодили використовуваний ключ перед початком передачі секретних повідомлень. Захист, що забезпечується симетричним алгоритмом

визначається ключем; розкриття ключа означає, що хто завгодно зможе зашифрувати і розшифрувати повідомлення. Поки повідомлення, що передаються, повинні залишатися таємними, ключ повинен зберігатися в секреті.

Якщо припустити, що К – ключ, що використовується у деякому симетричному криптографічному алгоритмі, тоді зашифрування і розшифрування з використанням симетричного алгоритму позначається як: Ек(М)=С, Dк(С)=М.

Схематично зашифрування та розшифрування при використанні симетричних криптографічних алгоритмів зображені на рисунку 2.3.

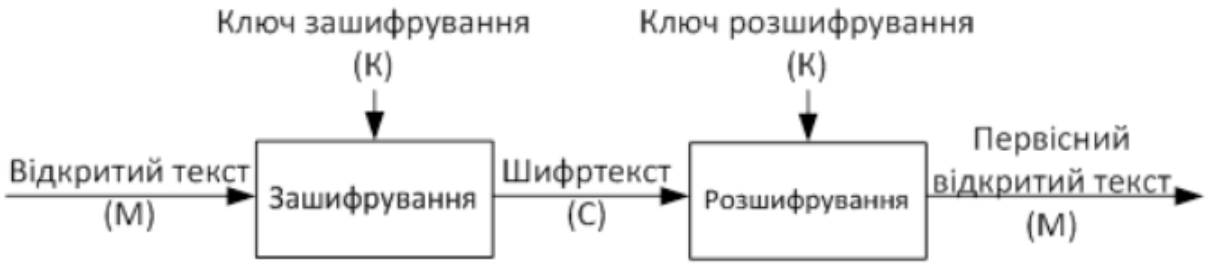


Рисунок 2.3 – Операції шифрування та розшифрування в симетричних алгоритмах

Симетричні алгоритми поділяються на дві категорії. Одні алгоритми обробляють відкритий текст побітово (іноді побайтово), вони називаються потоковими алгоритмами або потоковими шифрами. Інші працюють з групами бітів відкритого тексту. Групи бітів називаються блоками, а алгоритми - блоковими алгоритмами або блоковими шифрами.

2.2 Теоретичні основи асиметричного шифрування

Основи криптографії з відкритими ключами були висунуті Уітфілдом Діффі (Whitfield Diffie) і Мартіном Хеллманом (Martin Hellman), і незалежно

Ральфом Меркле (Ralph Merkle). Їх внеском у криптографію було переконання, що ключі можна використовувати парами - ключ шифрування і ключ дешифрування - і що може бути неможливо отримати один ключ з іншого (рис. 2.4).

Рисунок 2.4 – Спрощена схема асиметричного шифрування

Діффі і Хеллмана вперше представили цю ідею на Національної комп'ютерної конференції 1976р., згодом була опублікована їх основна робота "New Directions in Cryptography" ("Нові напрямки в криптографії").

Свою назву алгоритми з відкритим ключем отримали завдяки тому, що ключ шифрування не потрібно тримати в таємниці. Будь-хто може ним скористатися, щоб зашифрувати своє повідомлення, але тільки володар відповідного секретного ключа розшифрування буде в змозі прочитати це шифрування повідомлення.

Алгоритми шифрування з відкритим ключем засновані на використанні односпрямований функцій. Ці функції мають наступну властивість: при заданому значенні аргументу x відносно просто обчислити значення функції y = f (x), однак знаходження x, відповідного заданому значенню y, надзвичайно важко, точніше, пов'язане з надмірно великим об'ємом обчислень, які

неможливо реалізувати за доступний проміжок часу. Прикладом односпрямованої функції може послужити наступна ступенева функція:

$$y = f(x) = A^x mod\ (n), \qquad (2.1)$$

де x і n - надмірно великі числа,

A - довільне число з інтервалу [2, n - 2].

При заданому значенні x відносно просто обчислити значення y, тоді як для обчислення значення x = f -1 (x) буде потрібно дуже великий обсяг обчислень.

Але, використовуючи односпрямовану функцію, повідомлення розшифрувати неможливо. Тому в криптографії з відкритим ключем використовуються односпрямовані функції (рис. 2.5).

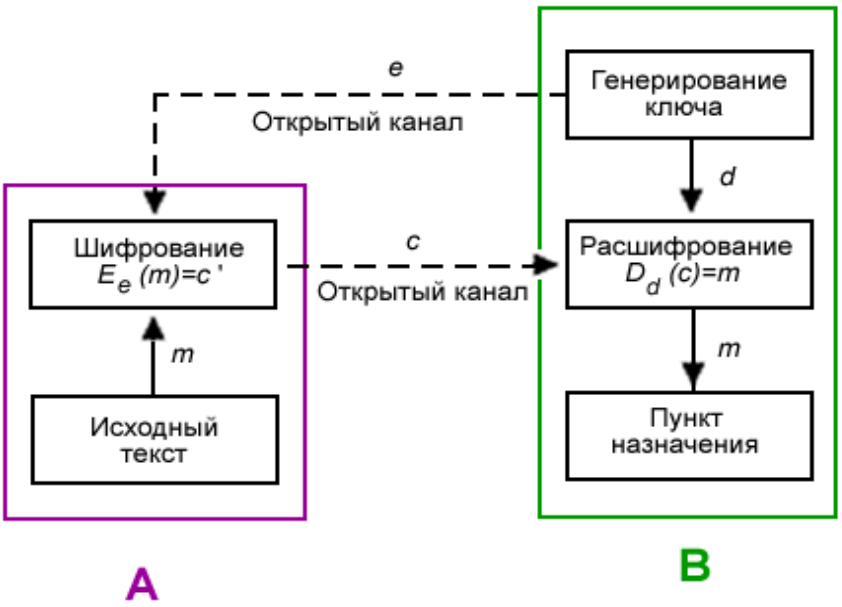


Рисунок 2.5 – Схема шифрування з відкрити ключем

На відміну від інших односпрямованих функцій, дані функції володіють специфічною властивістю, що при знанні певної інформації, обчислення x = f-1 (x) стає легко реалізованим.

Для того, щоб гарантувати надійний захист інформації, до криптосистемам з відкритим ключем пред'являються наступні вимоги.

1. Перетворення вихідного тексту повинно бути умовно незворотним і виключати її відновлення на основі відкритого ключа.

2. Визначення закритого ключа на основі відкритого також повинно бути неможливим на сучасному технологічному рівні.

2.3 Загальні вимоги до транспортного кодування

У деяких системах передачі інформації потрібно, щоб потік містив лише певні символи ASCII кодів. Однак, вихідний потік криптоалгоритму має дуже високу рандомізацію і в ньому зустрічаються з однаковою ймовірністю всі 256 символів. Для подолання цієї проблеми використовується транспортне кодування.

Оскільки системи шифрування даних часто використовуються для кодування текстової інформації: листування, рахунків, платежів електронної комерції, і при цьому криптосистема повинна бути абсолютно прозорою для користувача, то над вихідним потоком криптосистеми часто проводиться транспортне кодування, то є додаткове кодування (не шифрування!) Інформації виключно для забезпечення сумісності з протоколами передачі даних.

Вся справа в тому, що на виході криптосистеми, байт може приймати всі 256 можливих значень, незалежно від того чи був вхідний потік текстовою інформацією чи ні. А при передачі поштових повідомлень багато систем орієнтовані на те, що допустимі значення байтів тексту лежать в більш вузькому діапазоні: всі цифри, знаки пунктуації, абетка латиниці плюс, можливо, національної мови. Перші 32 символи набору ASCII служать для спеціальних цілей. Для того, щоб вони і деякі інші службові символи ніколи не з'явилися у вихідному потоці використовується транспортне кодування.

2.4 Обчислювальні аспекти алгоритму RSA

Алгоритми RSA є класикою асиметричної криптографії. У ньому в якості незворотнього перетворення відправки використовується зведення цілих чисел у великі ступені за модулем.

Алгоритм RSA стоїть біля витоків асиметричної криптографії. Він був запропонований трьома дослідниками –математиками: Рональдом Рівестом (R. Rivest), Аді Шамір (A. Shamir) та Леонардом Адльманом (L. Adleman) в 1977-78 роках.

Першим етапом будь-якого асиметричного алгоритму є створення пари ключів: відкритого та закритого, та поширення відкритого ключа користувачам, що приймають участь в обміні інформацією.

Насправді операції зведення в ступінь великих чисел досить трудомісткі для сучасних процесорів, навіть якщо вони проводяться за оптимізованими за часом алгоритмами. Тому зазвичай весь текст повідомлення кодується звичайним блоковим шифром (набагато більш швидким), але з використанням ключа сеансу, а от сам ключ сеансу шифрується якраз асиметричним алгоритмом за допомогою відкритого ключа одержувача і поміщається в початок файлу.

Сьогодні алгоритм RSA активно реалізується як в окремих криптографічних продуктах, наприклад, в програмі PGP, так і в якості вмонтованих засобів у популярне прикладне програмне забезпечення, наприклад, в браузерах Інтернет від Microsoft і Netscape. Слід зазначити, що алгоритм шифрування RSA є доступним для будь-кого (рис. 2.6).

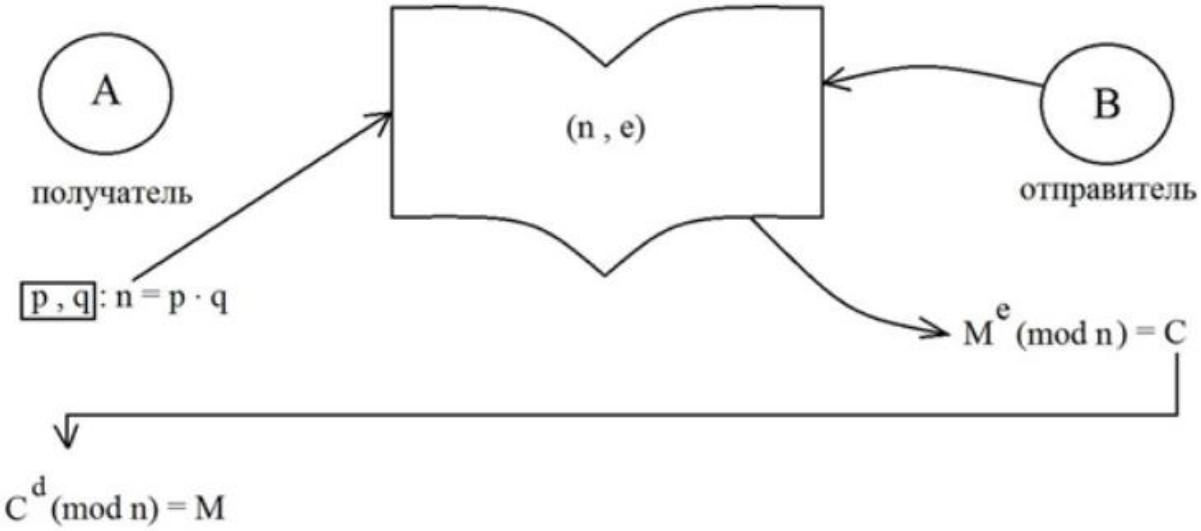


Рисунок 2.6 – Схема алгоритму RSA

PGP (англ. Pretty Good Privacy) — комп'ютерна програма, також бібліотека функцій, що дозволяє виконувати операції шифрування і цифрового підпису повідомлень, файлів та іншої інформації, поданої в електронному вигляді, у тому числі прозоре шифрування даних на запам'ятовуючих пристроях, наприклад, на твердому диску. Програма була написана Пилипом Цимерманом в 1991 році.

RSA став першим алгоритмом придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних програмних продуктів.

Алгоритм RSA складається з 4 етапів:

– генерації ключів;
– шифрування;
– розшифрування;
– розповсюдження ключів.

На рис. 2.7 схематично зображена ілюстрація роботи алгоритму RSA.

Рисунок 2.7 – Робота алгоритму RSA

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

Розповсюдження ключів полягає в тому, що абонент А передає свій відкритий ключ (n, e) абоненту Б через надійний, але не обов'язково секретний маршрут. Секретний ключ d ніколи не розповсюджується.

Для того, щоб згенерувати пари ключів виконуються такі дії:

1. Вибираються два великі прості числа p і q приблизно 512 біт завдовжки кожне

2. Обчислюється їх добуток $n=p\cdot q$.

3 .Обчислюється функція Ейлера $(n)=(p-1)\cdot(q-1)$.

4. Вибирається ціле число e таке, що $1<e<\varphi(n)$ та e взаємно просте з $\varphi(n)$.

За допомогою розширеного алгоритму Евкліда знаходиться число *d* таке, що

$d = e^{-1} \cdot mod\ \varphi(n).$

Число *n* називається модулем, а числа *e* і *d* – відкритою й секретною експонентами відповідно. Пари *n* та *e* є відкритою частиною ключа, а *n* та *d* – секретною. Числа *p* і *q* після генерації пари ключів можуть бути знищені, але в жодному разі не повинні бути розкриті.

RSA може використовуватися не тільки для шифрування, але й для цифрового підпису. Підпис *S* повідомлення *m* обчислюється з використанням секретного ключа за формулою:

$$S = m^d \cdot mod\ n \qquad (2.2)$$

Для перевірки правильності підпису потрібно переконатися, що виконується рівність:

$$m = s^e \cdot mod\ n \qquad (2.3)$$

Як виявилося, теорія асиметричного шифрування дозволяє значно простіше вирішувати проблему інформаційної безпеки - перевірку справжності автора повідомлення. Для вирішення цієї проблеми за допомогою симетричної криптографії була розроблена дуже трудомістка і складна схема. У той же час за допомогою, наприклад, того ж алгоритму RSA створити алгоритм перевірки дійсності автора та незмінності повідомлення надзвичайно просто, використовуючи вирази 2.2, 2.3.

Важливий аспект реалізації RSA - обчислювальний. Покажемо реалізацію алгоритму RSA на прикладі**.**

1. Етап генерації ключів:

– оберемо 2 простих числа, наприклад, $p = 3537$ *та* $q = 2579$;

– обчислимо модуль двох чисел: $n = p \cdot q = 3537 \cdot 2579 = 9173503$;

– обчислимо функцію Ейлера $\varphi(n) = (p-1) \cdot (q-1) = 9167368$;

– оберемо відкриту експоненту, наприклад, $e=3$;
– обчислимо секретну експоненту: $d= e^{-1} \cdot mod\ \varphi(n);\quad d = 6111579;$
– опублікуємо відкритий ключ $\{e, n\} = 3, 9173503$;
– збережемо закритий ключ $\{d, n\} = 6111579, 9173503$.

2. Етап шифрування:

– оберемо текст для шифрування, наприклад, m = 111111;
– обчислимо шифротекст: $c = E(m) = m^e \cdot mod\ n = 111111^3 \cdot 9173503 = 4051753;$
– проведемо розшифрування:

$$m = D(c) = cd \cdot mod\ n = 4051753\ 6111579 \cdot 9173503 = 111111.$$

Таким чином, робота алгоритму завершена.

Як видно з наведено прикладу робота алгоритму обтяжена обчисленням чисел великої розрядності, операціями множення, зведення в ступінь та ділення. Такі операції накладають велике навантаження на обчислювальні ресурси (рис. 2.8).

Як висновок, можна рекомендувати реалізацію даного алгоритму тільки для реалізації ЕЦП та генерації ключів. Для звичайних завдань рекомендується розмір ключа в 1024 біта, а для особливо важливих завдань - 2048 біт. Для реалізації шифрування звичайного текстового фрагменту алгоритм до застосування не рекомендується.

2.5 Швидкість роботи алгоритму RSA

Як при шифруванні і розшифруванні, так і при створенні і перевірці підпису, алгоритм RSA у своїй сутності складається з операції піднесення в ступінь, яке виконується як ряд множень.

У практичних додатках для відкритого ключа зазвичай обирається відносно невеликий показник, а часто групи користувачів використовують один і той же відкритий показник, але кожен з різним модулем. Якщо відкритий показник незмінний, вводяться деякі обмеження на головні

співмножники (фактори) модуля. При цьому шифрування даних йде швидше, ніж розшифрування, а перевірка підпису — швидше, ніж підписання.

Якщо k — кількість бітів у модулі, то зазвичай в алгоритмах, що використовуються для RSA, кількість кроків, необхідна для виконання операції з відкритим ключем, пропорційна k^2, кількість кроків для операцій секретного ключа — k^3, кількість кроків для операції створення ключів — k^4.

Методи «швидкого множення» — наприклад, методи основані на швидкому перетворенні Фур'є — виконуються меншою кількістю кроків. Проте вони не набули широкого поширення через складність програмного забезпечення, а також тому, що з типовими розмірами ключів вони фактично працюють повільніше. Однак продуктивність та ефективність програм і обладнання, які реалізовують алгоритм RSA, швидко збільшується.

Алгоритм RSA набагато повільніший, ніж DES та інші алгоритми блокового шифрування. Програмна реалізація DES працює швидше принаймні в 100 разів і від 1,000 до 10,000 — в апаратній реалізації (в залежності від конкретного пристрою). Завдяки проведенню розробок, швидкість алгоритму RSA, ймовірно, прискориться, але одночасно прискориться і робота алгоритмів блокового шифрування.

2.6 Обчислювальні аспекти алгоритму Ель Гамаля

Схема Ель-Гамаля (ElGamal) – криптосистема з відкритим ключем, заснована на труднощі обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Схема Ель-Гамаля лежить в основі колишніх стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

Схема була запропонована Тахером Ель-Гамалем в 1985 р. Ель-Гамаль розробив один з варіантів алгоритму Діффі-Геллмана. Він удосконалив систему Діффі-Геллмана і отримав два алгоритми, які призначені для

шифрування і для автентифікації. На відміну від RSA алгоритм Ель-Гамаля не запатентований і, тому, став дешевшою альтернативою, оскільки не потрібна оплата внесків за ліцензію. Вважається, що алгоритм потрапляє під дію патенту Діффі-Геллмана.

Як і у алгоритмі RSA, робота по алгоритму Ель Гамаля складається з етапів генерації ключів, шифрування та розшифрування (рис. 2.8).

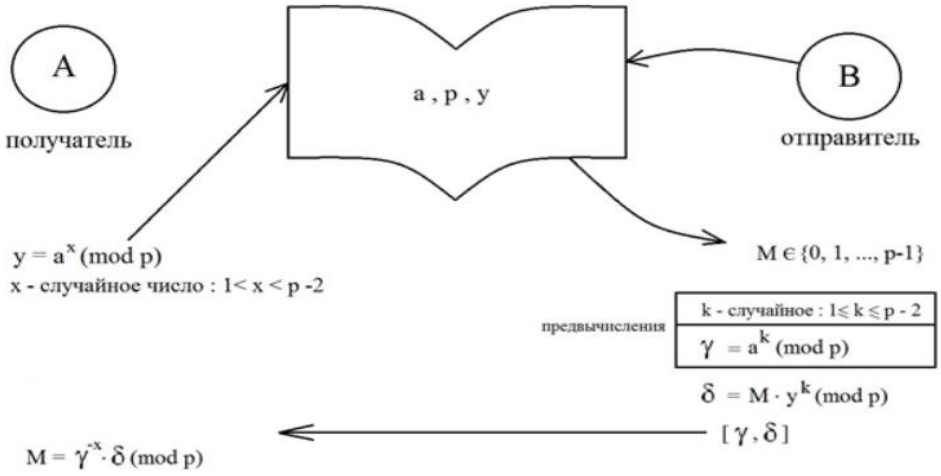


Рисунок 2.8 – Схема алгоритму Ель Гамаля

2.6.1 Шифрування по алгоритму Ель Гамаля

Припустимо що потрібно зашифрувати повідомлення M=5.

Здійснимо генерацію ключів:

Нехай $p=11$, $q=2$. Виберемо $x=8$ – випадкове ціле число x таке, що $1<x<p$.

Обчислимо $y=g^x \cdot mod\ p$, $y= 28 \cdot mod\ 11 = 3$.

Отже, відкритим є трійка чисел $(p, g, y) = (11, 2, 3)$, а закритим ключем – число $x=8$.

Вибираємо випадкове ціле число k таке, що $1 < k < (p - 1)$. Нехай $k=9$.

Обчислюємо число $a=g^k \cdot mod\ p = 2^9 \cdot mod\ 11 = 512 \cdot mod\ 11 = 6$.

Обчислюємо число $b=y^k \cdot M \cdot \mathrm{mod}\ p=3^9 \cdot 5 \cdot \mathrm{mod}\ 11=19683 \cdot 5 \cdot \mathrm{mod}\ 11= 9$.

Отримана пара чисел (a, b) = (6, 9) – є шифротекст.

2.6.2 Розшифрування

Необхідно отримати повідомлення *M=5* за відомим даними шифротекста *(a, b)=(6, 9)* і закритому ключу *x=8*.

Обчислюємо *M* за формулою: $M=b(ax)\text{-}1 \cdot b \cdot mod\ p = 9(6^8)^{-1} \cdot mod\ 11 = 5$.

Отримали вхідне повідомлення *M=5*.

2.6.3 Реалізація алгоритму Ель-Гамаля в режимі цифрового підпису

При роботі в режимі електронного підпису методом Ель Гамаля передбачається наявність фіксованої хеш-функції *h( )*, значення якої лежать в інтервалі *(1,p-1)*.

Для підпису повідомлення *M* виконуються наступні операції:

Обчислюється дайджест (в криптографії хеш-суму іноді також називають дайджестом повідомлення) *M: m=h(M)*.

Вибирається випадкове число 1<k<p-1 взаємно просте з *p-1* і обчислюється

$r=gk \cdot mod\ p$.

Обчислюється число $s \equiv (m\text{-}xr \cdot r)k\text{-}1 \cdot mod\ (p\text{-}1)$. (≡ – знак еквівалентності).

Підписом повідомлення *M* є пара *(r, s)*.

Перевірка підпису полягає в наступному.

Знаючи відкритий ключ *(p, g, y)* підпис *(r, s)* повідомлення *M* перевіряється наступним чином:

Перевіряється виконання умов: *0<r<p* і *0<s<p-1*. Якщо хоча б одна з них не виконується, то підпис вважається невірним.

Обчислюється дайджест *m = h (M)*.

Підпис вважається вірним, якщо виконується порівняння: $y^r \cdot r^s \equiv g^m \cdot mod\ p$.

При перевірці цифрового підпису адресат повідомляє, що знову вираховує хеш-функцію $m = h\ (M)$ прийнятого по каналу тексту M, після чого за допомогою відкритого ключа відправника перевіряє, чи відповідає отриманий підпис обчисленому значенню хеш-функції (рис 2.9).

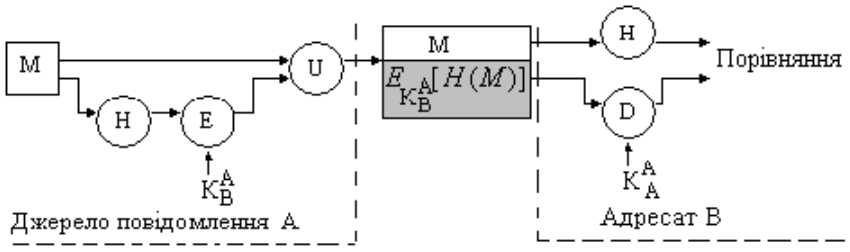


Рисунок 2.9 – Схема реалізації цифрового підпису по алгоритму Ель Гамаля

2.7 Порівняння алгоритмів RSA та Ель-Гамаля

В таблиці 2.1 наведені порівняльні характеристики алгоритмів RSA та Уль Гамаля

Таблиця 2.1 – Порівняльні характеристики алгоритмів RSA та Ель Гамаля

Алгоритм	Ключ	Призначення	Крипостійкість, MIPS	Примітки
RSA	До 4096 біт	Шифрування і підпис	$2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на труднощі завдання факторизації великих чисел; один з перших асиметричних алгоритмів. Включений до багатьох стандартів
Ель Гамаля	До 4096 біт	Шифрування і підпис	При однаковій довжині ключа криптостійкості рівна RSA, тобто $2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на важкій задачі обчислення дискретних логарифмів в кінцевому полі; дозволяє швидко генерувати ключі без зниження стійкості. Використовується в алгоритмі цифрового підпису DSA-стандарту DSS

Висновки до розділу 2

У другому розділі розглянута загальна класифікація алгоритмів криптографічного перетворення інформації, проведено порівняння асиметричних та симетричних алгоритмів кодування, детально розглянуто теоретичні основи асиметричного шифрування, загальні вимоги до транспортного кодування.

З метою розроблення програмного забезпечення проведений аналіз обчислювальних аспектів алгоритмів RSA та Ель Гамаля в режимах створення електронного цифрового підпису, проведений порівняльний аналіз даних алгоритмів з метою їх подальшого використання.

3 РОЗРОБЛЕННЯ ПРОГРАМНОГО КОМПЛЕКСУ НА ОСНОВІ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Програмний комплекс отримання цифрового підпису на основі алгоритмів RSA та Ель Гамаля реалізований на мові програмування С++ в середовищі Microsoft Visual Studio Net 2017 (додаток А). Розмір файлу *ESign.exe* – 88 Кбайт.

3.1 Програмна реалізація отримання цифрового підпису на основі алгоритму RSA

Підготовчі операції для отримання ЕЦП складаються з декількох етапів:

1. Створення ключа. Для реалізації цього етапу потрібно в будь-якому текстовому редакторі задати ключ (числа від 0 до 9) та зберегти його на жорсткому диску або зовнішньому носію в форматі *.txt.* Розмір ключа довільний. У нашому прикладі розмір ключа 9 байт (72 біта) (рис. 3.1).

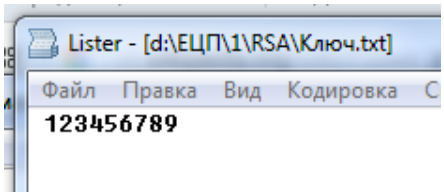


Рисунок 3.1 – Створення ключа

2. Генерація закритого та відкритого ключів. На цьому етапі генерується закритий (keysPr – приватний) та відкритий ключ (keysPb – публічний). Для цього необхідно на головній формі натиснути кнопку «Налаштування даних» (рис. 3.2), обрати ключ попереднього етапу і на його основі створити вищезгадані ключі.

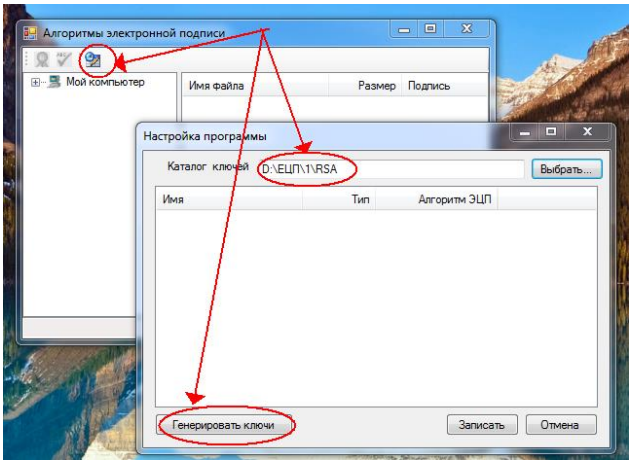
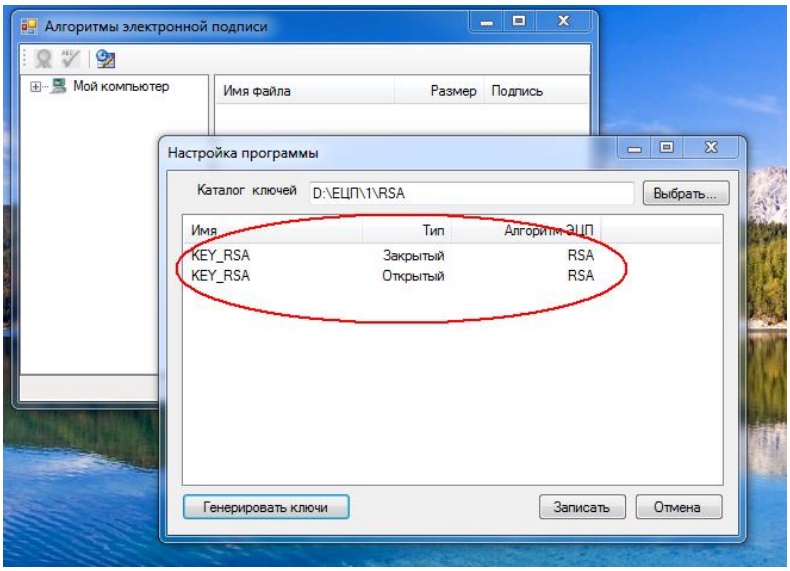


Рисунок 3.2 – Генерація ключів

Створені ключі (закритий і відкритий) зберігаються в тій же директорії, що і загальний ключ (рис. 3.3,а,б).



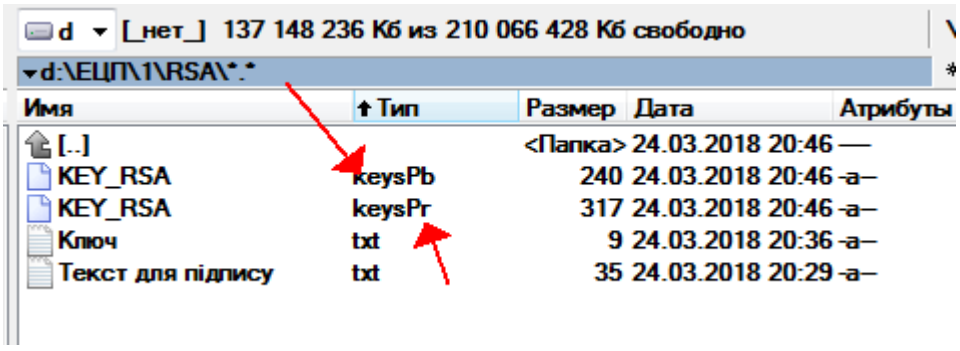


Рисунок 3.3,а – Структура відкритого (*.keysPb*) та закритого (*.keysPr*) ключів

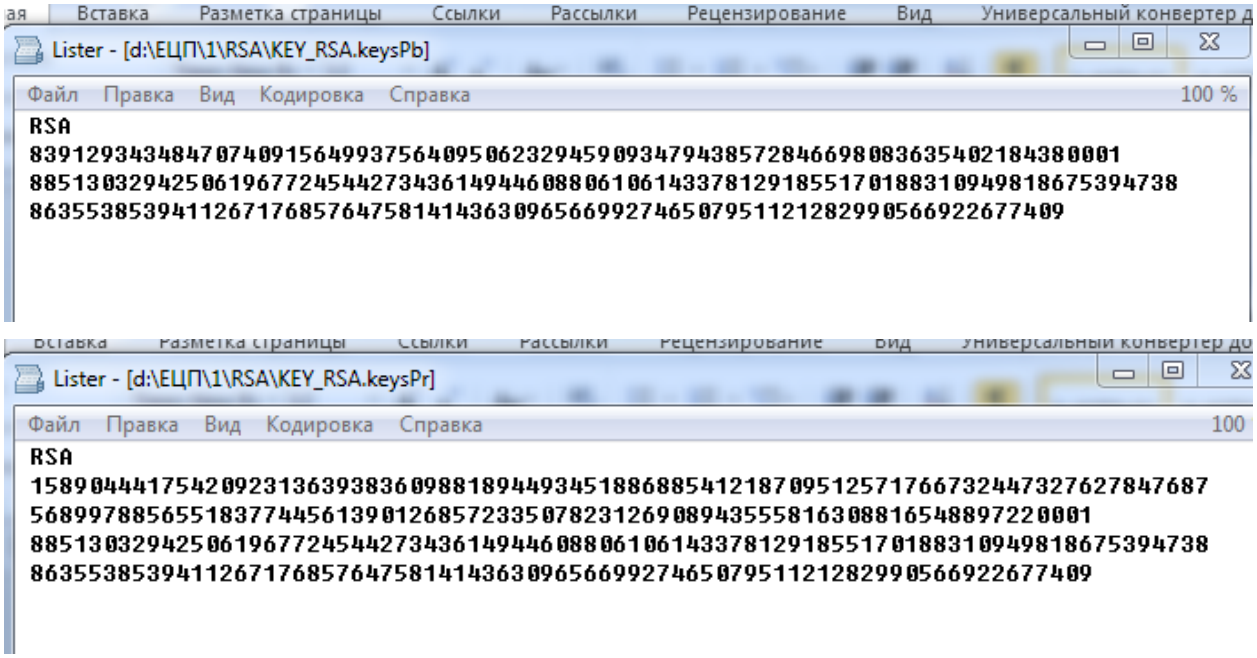
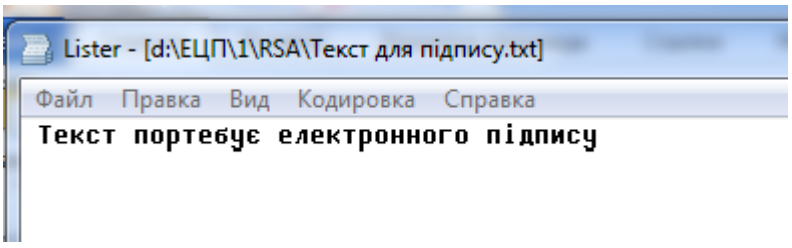


Рисунок 3.3,б – Структура відкритого (*.keysPb*) та закритого (*.keysPr*) ключів

Як видно з рисунка 3.3, довжина закритого ключа більше довжини відкритого ключа.

3. Вибір параметрів підпису та накладення ЕЦП на обраний текст. Для виконання цього етапу необхідно створити (обрати раніше створений) текст для підпису в форматі *.txt* , натиснути кнопку «Підписати файл» та підписати файл за допомогою закритого ключа (рис. 3.4).



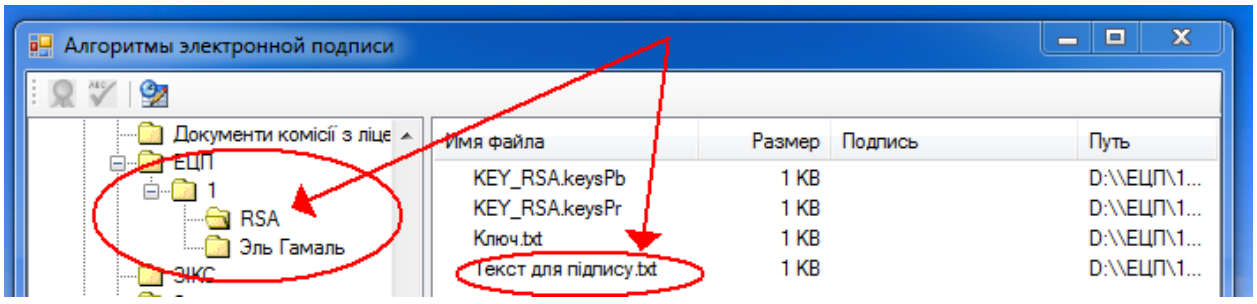


Рисунок 3.4,а – Обрання файлу для підпису з використання закритого ключа

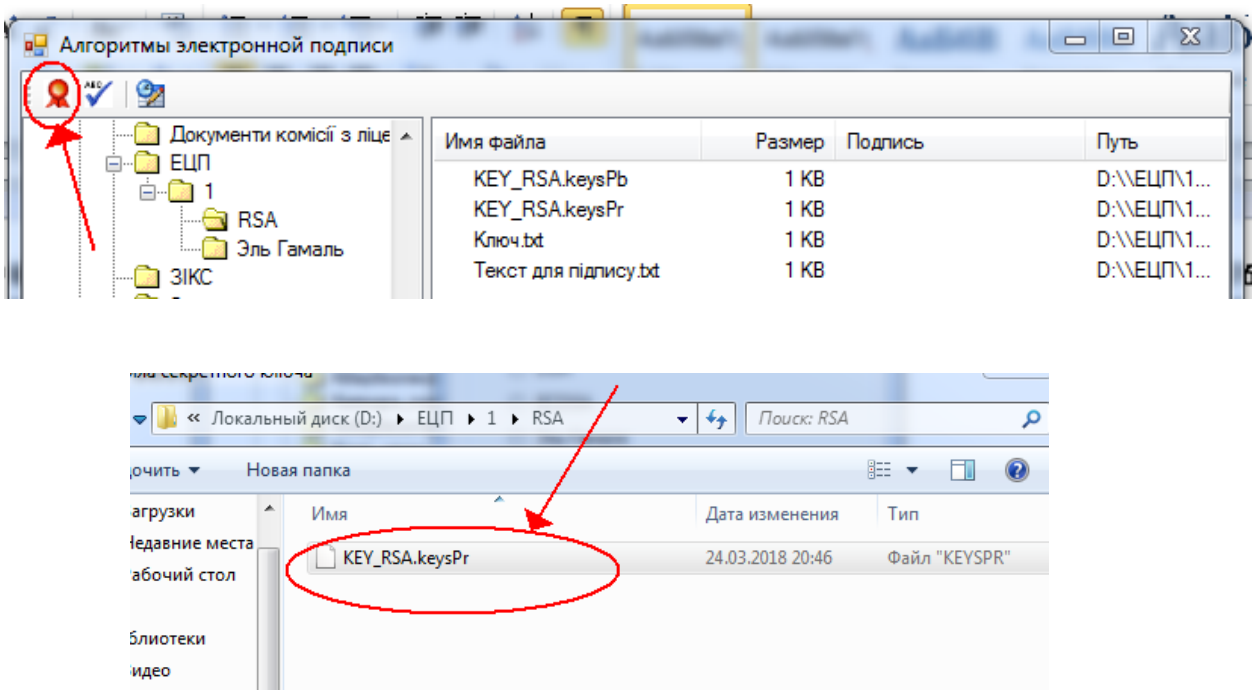


Рисунок 3.4,б – Обрання файлу для підпису з використання закритого ключа

Вибір параметрів підпису з використанням закритого ключа наведено на рис. 3.5.

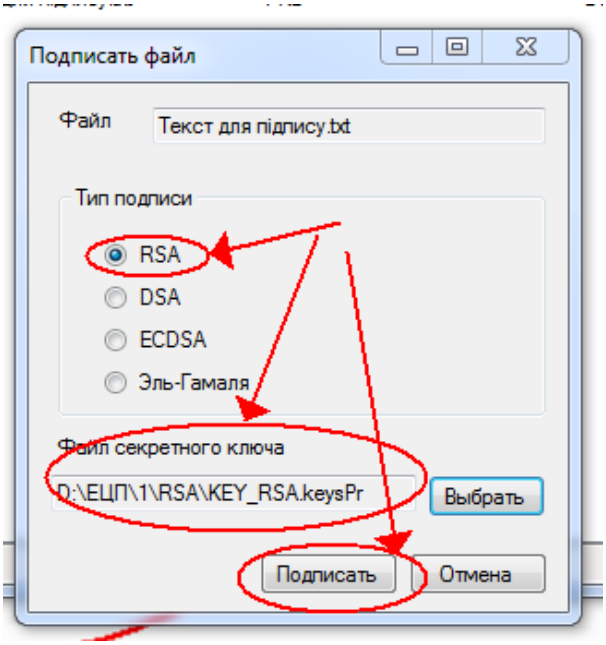


Рисунок 3.5 – Вибір параметрів підпису

4. Збереження файлу, підписаного ЕЦП. Після підпису створюється файл з розширенням *.sign* (рис. 3.6).

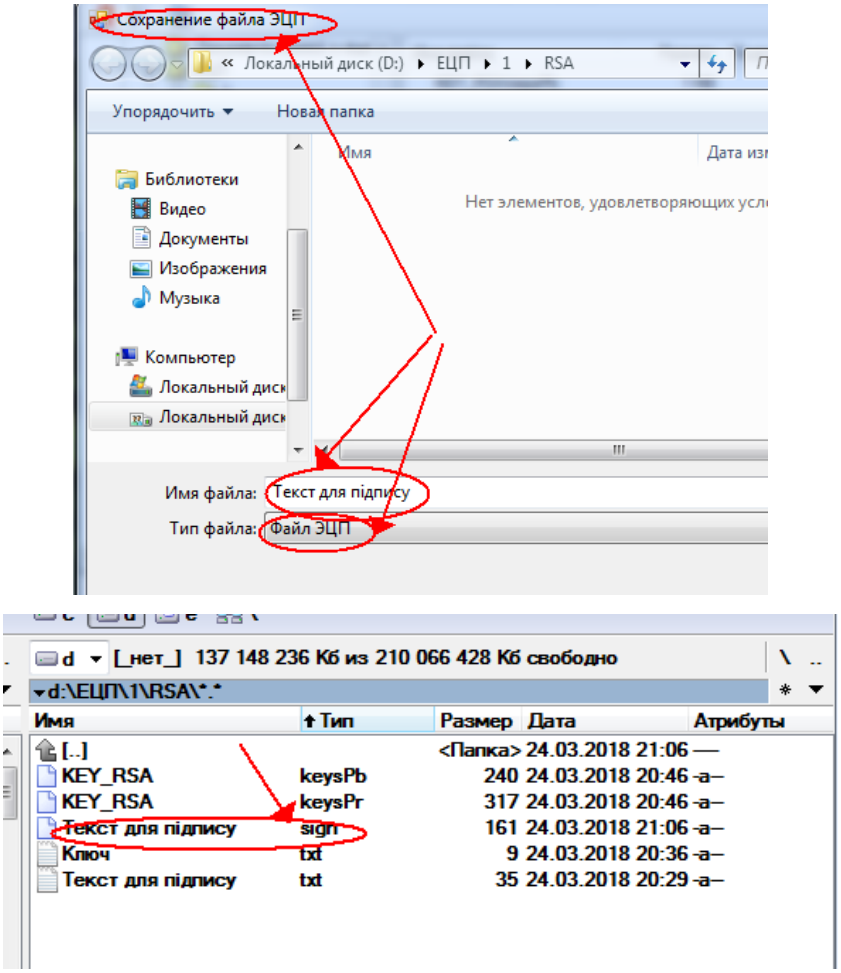


Рисунок 3.6 – Збереження підписаного ЕЦП файлу

Структура файлу *Текст для підпису.sign* наведена на рис. 3.7.

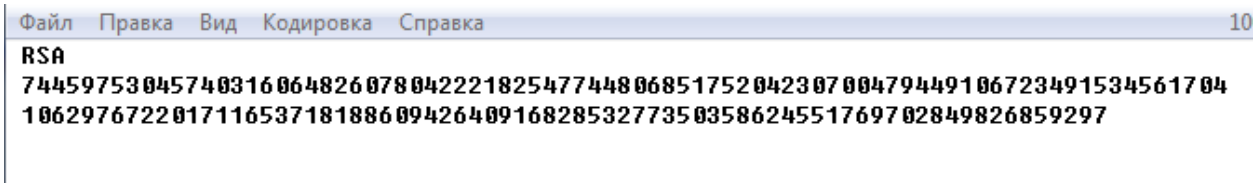


Рисунок 3.7 – Структура файлу *Текст для підпису.sign*

Підпис файлу (документу) завершено.

5. Етап перевірки ЕЦП. Для виконання перевірки ЕЦП на головному екрані меню програми обрати файл тексту для підпису, файл відкритого ключа та файл ЕЦП та натиснути кнопку «Перевірити підпис» (рис. 3.8).

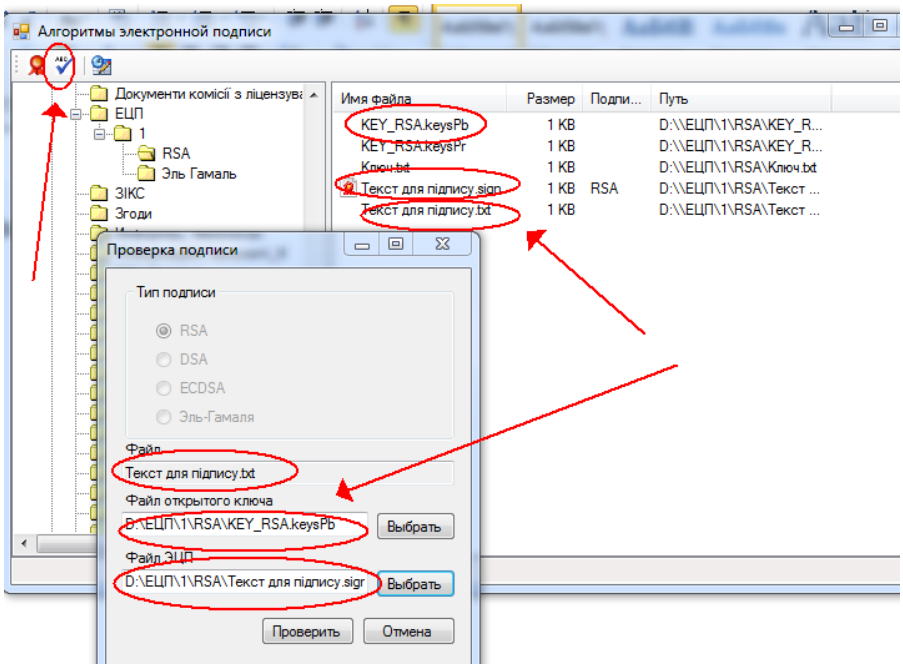


Рисунок 3.8 – Перевірка ЕЦП

При правильності ЕЦП програма видає повідомлення «ОК», що свідчить про відповідність ЕЦП оригіналу (рис. 3.9). В іншому випадку програма видає помилку.

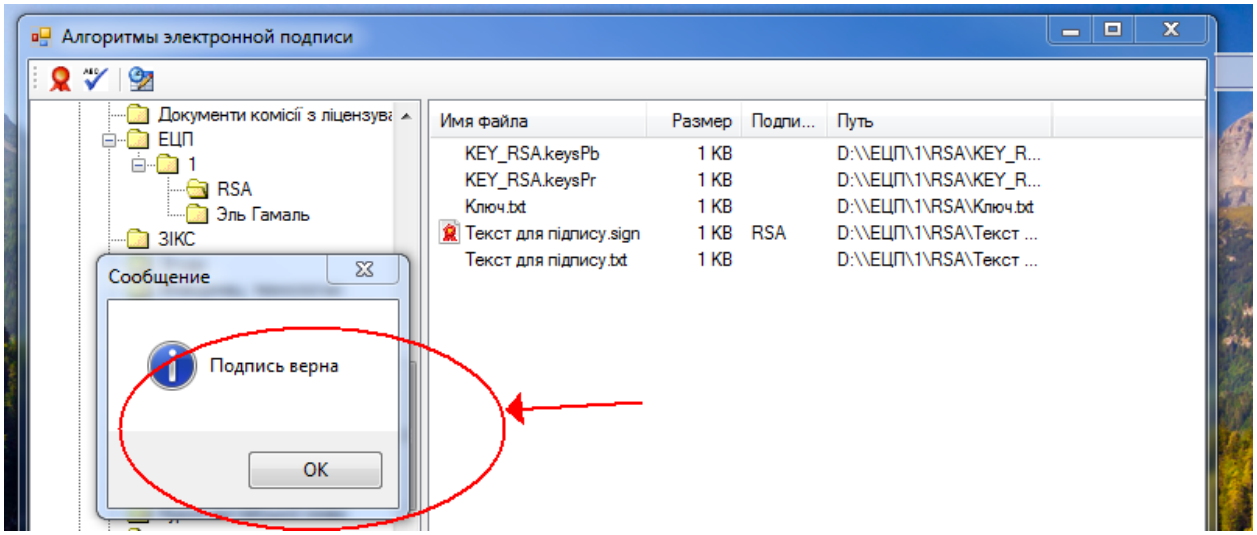


Рисунок 3.9 – Перевірка правильності ЕЦП

3.2 Програмна реалізація отримання цифрового підпису на основі алгоритму Ель Гамаля

Етапи створення ЕЦП на основі алгоритму Ель Гамаля аналогічні етапам по алгоритму RSA, що були детально описані у попередньому розділі. Тому, обмежимось коротким описом процедури отримання ЕЦП на основі алгоритму Ель Гамаля:

1. Для алгоритму Ель Гамаля оберемо довільний за розміром ключ, що відрізняється від ключа, обраного по алгоритму RSA (рис. 3.10).

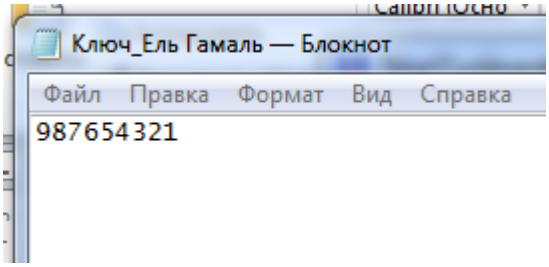


Рисунок 3.10 – Ключ для алгоритму Ель Гамаля

2. Як і в попередньому випадку, на його основі ключа *987654321*, використовуючи 256-бітне перетворення отримаємо відкритий та закритий ключі по алгоритму Ель Гамаля (рис. 3.11.)

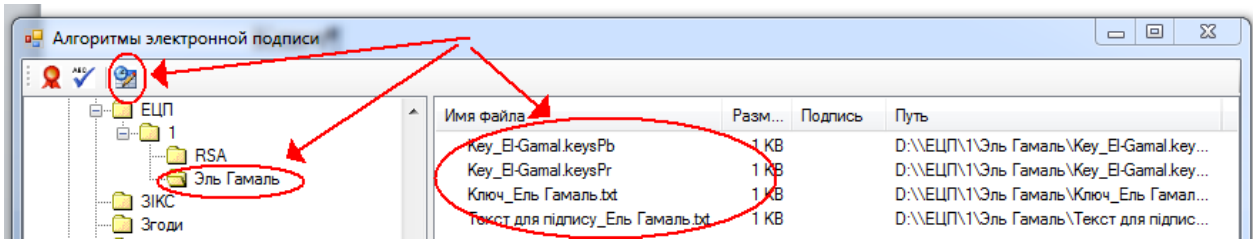


Рисунок 3.11 – Отримання закритого та відкритого ключів по алгоритму Ель Гамаля

3. Отримаємо ЕЦП по алгоритму Ель Гамаля (рис. 3.12).

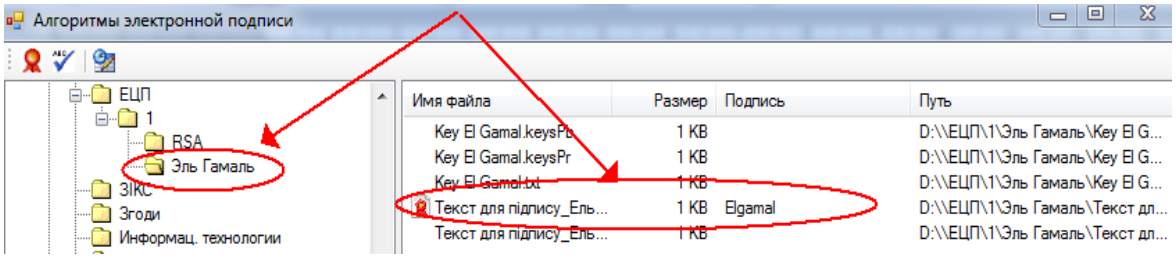


Рисунок 3.12 – Електронний підпис по алгоритму Ель Гамаля

Структура ЕЦП по алгоритму Ель Гамаля наведена на рис. 3.13.

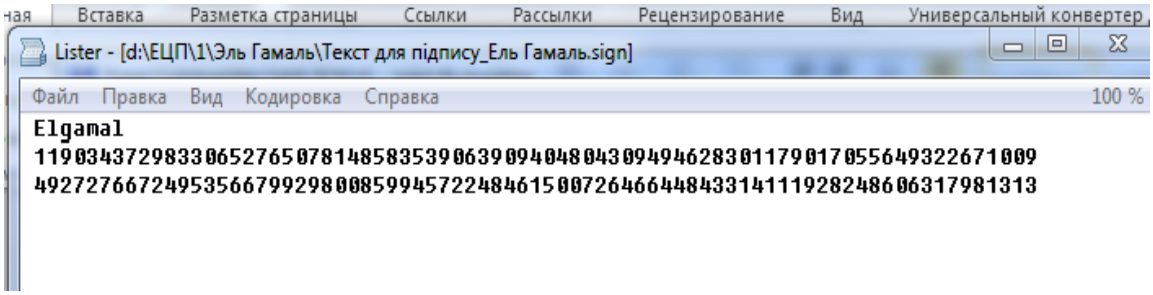


Рисунок 3.13 – Структура ЕЦП по алгоритму Ель Гамаля

4. Перевірка ЕЦП по алгоритму Ель Гамаля наведена на рис. 3.14.

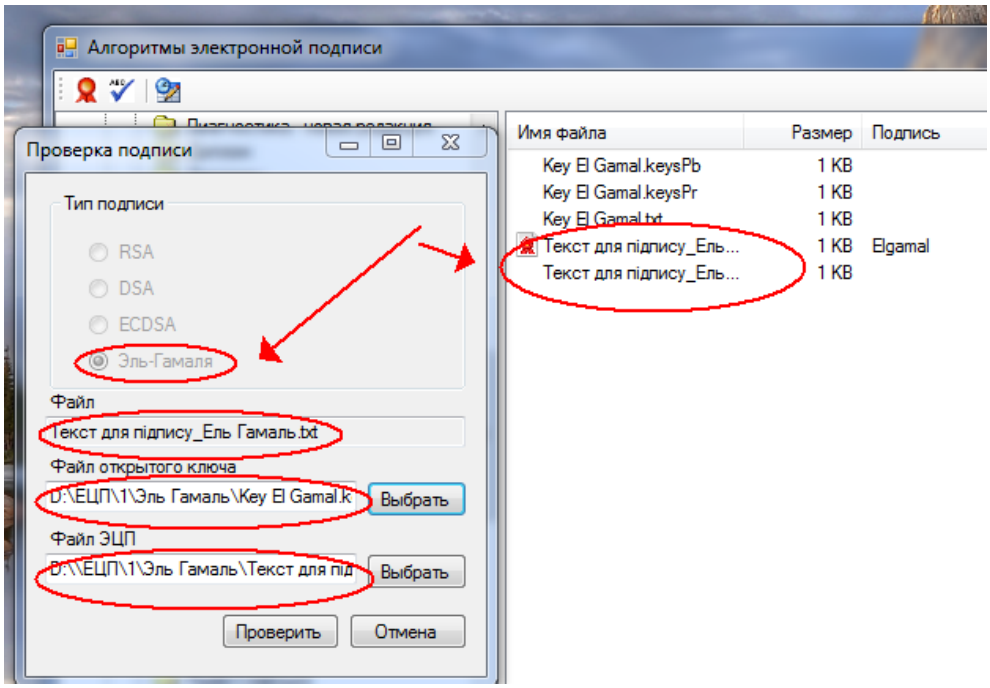


Рисунок 3.14,а – Перевірка ЕЦП по алгоритму Ель Гамаля

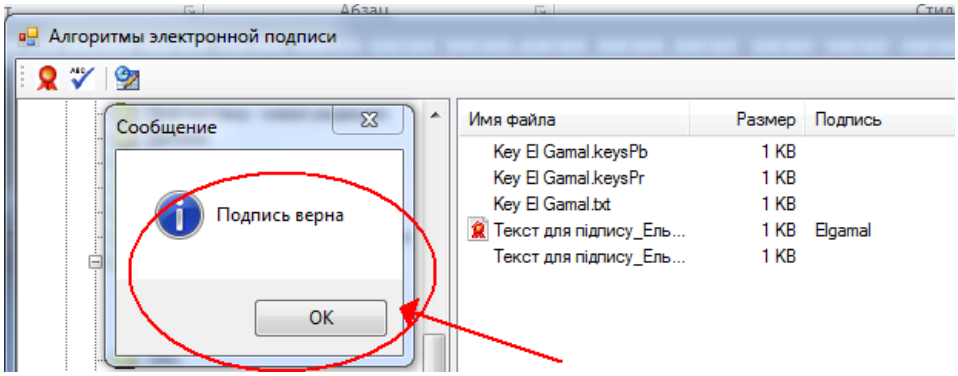


Рисунок 3.14,б – Перевірка ЕЦП по алгоритму Ель Гамаля

Висновки до розділу 3

У третьому розділі здійснено розроблення програмного комплексу для отримання ЕЦП по алгоритмам RSA та Ель Гамаля. Програма здійснює шифрування з обраними параметрами та зберігає ЕЦП на диску або зовнішньому носію. Програма володіє загально прийнятим інтуїтивно зрозумілим інтерфейсом та підписаними опціями, за замовчуванням сама обирає необхідне розширення файлу, що спрощує роботу з нею користувачів, що не володіють достатніми навиками роботи на персональному комп’ютері.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці.

4.2 Аналіз стану умов праці та вимоги до приміщення

Робота над створенням дипломного проекту проходитиме в приміщенні відповідної установи (компанії, підприємстві тощо). Для даної роботи

достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером. ГПКетричні розміри приміщення зазначені в таблиці 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об’єм, $м^3$	75

Згідно з ДСН 3.3.6.042-99 розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м [20]. Отже, дане приміщення цілком відповідає зазначеним нормам. Для зручності спільної роботи з іншими працівниками (обговорення ідей, з’ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов’язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування. Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.3 Вимоги до організації робочого місця

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця [21] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність в таблиці 4.2.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	**Фактичне значення**	**Нормативне значення**
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно-поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Приміщення кабінету знаходиться на четвертому поверсі *чотирьох* поверхової будівлі і має об’єм 75 м^3, площу — 25 м^2. У цьому кабінеті обладнано 10 місць праці укомплектованих ПК.

Температура в приміщенні протягом року коливається у межах 18–24°C, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум на робочому місці знаходиться на рівні 50 дБА. Система

вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет має бути оснащений переносним вуглекислотним вогнегасником ВВК-5.

Наявна аптечка для надання долікарської допомоги, а також у кабінеті роблять вологе прибирання та щоденно провітрюють приміщення.

4.4 Навантаження та напруженість процесу праці

Під час виконання робіт використовують ПК та периферійні пристрої, що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв через кожну годину роботи.

4.5 Аналіз небезпечних та шкідливих факторів при роботі на персональному комп'ютері

Роботу, пов'язану з електронно-обчислювальними машинами (далі - ПК) з відео дисплейними терміналами (далі - ВДТ), у тому числі на тих, які мають робочі місця, обладнані ПК з ВДТ і периферійними пристроями (далі - ПП), виконують із забезпеченням виконання правил охорони праці під час експлуатації електронно-обчислювальних машин, які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ПК з ВДТ і ПП [24]. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема ПК та периферійні пристрої.

Робочі місця мають відповідати вимогам цих Правил та Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [21].

Це передбачає, що визначена виробнича діяльність пов'язана з наявністю певної кількості небезпечних та/або шкідливих виробничих факторів. Тому у

першій частині цього підрозділу за результатами аналізу повинні бути визначені такі фактори.

Робота ПК та периферійних пристроїв супроводжує виділення багатьох хімічних речовин, зокрема озону, оксидів нітрогену та аерозолів (високодисперсних частинок тонера). Для прикладу, за умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом яких може бути принтер, сканер та ін.), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

4.6 Пожежна безпека

Пожежна безпека при застосуванні ПК забезпечується:

– системою запобігання пожежі,

– системою протипожежного захисту,

– організаційно-технічними заходами.

Приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння [31]. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

– ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт. або ОП-10 – 1 шт;

– повсть 1 1 м2, кошму 2×1,5 м2 або азбестове полотно 2×2 м2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки

приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ПК, є:

– поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420 ˚С,

– полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335˚С, температура самозаймання 530 ˚С,

– склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

– пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

– деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255 ℃, температура самозаймання 399 ˚С.

Для відводу теплоти від ПК діє система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь-якій точці приміщень ВЦ.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відносяться до пожежонебезпечної зони класу П-IIа [31]. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

– іскри і дуги короткого замикання;

– електрична іскра при замиканні і розмиканні ланцюгів;

– перегріви від тривалого перевантаження,

– відкритий вогонь і продукти горіння,

– наявність речовин, нагрітих вище за температуру самозаймання,

– розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

– несправність електроустановки;

– конструктивні недоліки устаткування;

– коротке замикання в електричних мережах;

– запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол. [29].

Для захисту від дії небезпечних і шкідливих чинників пожежі передбачається застосування промислового протигаза, що фільтрує, з коробкою марки «В» із сірою відміткою забарвлення – захист від неорганічних газів (хлор, фтор, бром, сірководень, сірковуглець, хлорциан, галогени), а цей фільтр не захистить від СО (тобто від чадного газу).

4.7 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три-провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного

провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.8 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають ДСН 3.3.6.042-99 і наведені в таблиці 4.3 [20].

Таблиця 4.3 – Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату:

температури, відносної вологості й рухливості повітря у відповідності до санітарних норм мікроклімату виробничих приміщень. Рівні позитивних і негативних іонів у повітрі мають відповідати до ДСН 3.3.6.042-99 [20]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі користувача, з метою його провітрювання. Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів мікроклімату. Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.9 Освітлення робочого місця

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

У приміщенні, де розташовані ПК передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2015 [22]. Джерелом

природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє СНіП і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2 + b^2} \cdot S_b = (1/8 \div 1/10) \cdot S_n \quad (4.1)$$

де S_b S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2

$S_{вік} = 1/8 \cdot 25 = 3{,}125$ м^2

Приймаємо 2 вікна площею S = 1,6 м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *N* виробляється по формулі (4.2):

$$N = E \cdot S \cdot Z \cdot K / F \cdot U \cdot M \quad (4.2)$$

Де *E* – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м2; S = 25 м2;

Z – поправочний коефіцієнт світильника (для стандартних світильників Z = 1.1 - 1.3) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм.

Підставивши числові значення у формулу (3.1), отримуємо:

$$n = (300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5) / (5400 \cdot 0{,}575 \cdot 2) \approx 2$$

Приймаємо освітлювальну установку, яка складається з 3-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

Потужність електроосвітлювальної установки з урахуванням місцевого освітлення визначається за формулою:

$$N=(n \cdot W+(0{,}1 \div 0{,}2) \cdot n \cdot W) / 1000 \qquad (4.3)$$

де n– розрахункова кількість ламп для освітлення даного приміщення;

W – потужність однієї лампи, Вт;

(0,1÷0,2) – додаткова потужність для ламп місцевого освітлення, Вт

$$N = (2 \cdot 160 + (0{,}1 \div 0{,}2) \cdot 2 \cdot 160)/1000 = 0{,}48 \text{ кВт}$$

Висновки до розділу 4

У даному розділі проведений аналіз умов праці, шкідливих та небезпечних чинників. Визначено параметри і характеристики приміщення

для роботи над дипломним проектом, заходи, які потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для роботи. Приведені рекомендації щодо організації робочого місця, електробезпеки та пожежної безпеки. Наведені розміри приміщення та значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці, рекомендації з охорони праці, техніки безпеки при роботі на комп’ютері.

ВИСНОВКИ

У вступі до дипломного проекту визначена актуальність ЕЦП як способу ідентифікації підписувала електронного документу, що дозволяє однозначно визначати походження інформації (джерело інформації), що міститься у документі та мета проекту. Зазначен, що ЕЦП є надійним засобом розмежування відповідальності за інформаційну діяльність.

У першому розділі розглянуто призначення та юридична значимість ЕЦП. Підкреслено, що накладання ЕЦП завершує процес утворення електронного документа, надаючи йому юридичної сили. Електронний цифровий підпис як засіб контролю походження і цілісності інформації є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави.

В процедурі створення, механізму формування ЕЦП та подальшої обробки кодованої інформації вводять такі поняття як особистий ключ, відкритий ключ, сертифікат відкритого ключа. Визначені процедура підписання електронного документу, термін валідності та вразливості, переваги асиметричної криптографії в створенні ЕЦП. На основі проведеного огляду визначені задачі розроблення.

У другому розділі розглянута загальна класифікація алгоритмів криптографічного перетворення інформації, проведено порівняння асиметричних та симетричних алгоритмів кодування, детально розглянуто теоретичні основи асиметричного шифрування, загальні вимоги до транспортного кодування.

З метою розроблення програмного забезпечення проведений аналіз обчислювальних аспектів алгоритмів RSA та Ель Гамаля в режимах створення електронного цифрового підпису, проведений порівняльний аналіз даних алгоритмів з метою їх подальшого використання.

У третій частині здійснено розроблення програмного комплексу для отримання ЕЦП по алгоритмам RSA та Ель Гамаля. Програма здійснює шифрування з обраними параметрами та зберігає ЕЦП на диску або зовнішньому носію. Програма володіє загально прийнятим інтуїтивно зрозумілим інтерфейсом та підписаними опціями, за замовчуванням сама обирає необхідне розширення файлу, що спрощує роботу з нею користувачів, що не володіють достатніми навиками роботи на персональному комп’ютері.

У четвертому розділі проведений аналіз умов праці, шкідливих та небезпечних чинників. Визначено параметри і характеристики приміщення для роботи над дипломним проектом, заходи, які потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для роботи. Приведені рекомендації щодо організації робочого місця, електробезпеки та пожежної безпеки. Наведені розміри приміщення та значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці, рекомендації з охорони праці, техніки безпеки при роботі на комп’ютері

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про електронний цифровий підпис». Стаття 4.
2. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин // – М: ДМК Пресс, 2012. – 592 с.
3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах / В. Ф. Шаньгин // Серия: Высшее образование; Учебное пособие. – М: Форум, Инфа-М, 2010. – 592 с.
4. Тимошенко А. А. Защита информации в специализированных информационно-телекоммуникационных системах / Тимошенко А. А. // – К: НТУУ «КПИ», ФТИ, 2010. – 252 с.
5. Грибунин В. Г. Комплексная система защиты информации на предприятии / В. Г. Грибунин, В. В. Чудовский // Учебное пособие. Серия: Информационная безопасность. – М: Академия, 2009. – 159 с.
6. Хореев П. Б. Методы и средства защиты информации в компьютерных системах / П. Б. Хореев // Серия: Высшее профессиональное образование. – М: Академия, 2008. – 256 с.
7. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / Шаньгин В. Ф. // Учебное пособие. – М.: ИД «Форум»: ИНФРА-М, 2008. – 416 с. ил. – (Профессиональное образование).
8. Мельников В. П. Информационная безопасность и защита информации / В. П. Мельников, С. А. Клейменов, А. М. Петраков // Серия: Информатика и вычислительная техника; 4-е издание. – М: Академия, 2008. – 332 с.
9. Варлатая С. К. Аппаратно-программные средства и методы защиты информации / Варлатая С. К., Шаханова М. В. // Владивосток: ДВГТУ, 2007. – 318 с.
10. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина // – М: Гелиос АРВ, 2007. – 320 с.

11. Безбогов А. А. Методы и средства защиты компьютерной информации // Серия: Информатика и компьютерная техника. – Таганрог: ТГТУ, 2006. – 120 с.
12. Болотов А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых // А. А. Болотов, С. Б. Гашков, А. Б. Фролов // – М: КомКнига, 2006. – 280 с.
13. Коханович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Коханович // Серия: Высшее профессиональное образование. – М: МК-Пресс, 2005. – 281 с.
14. Рябко Б. Я. Криптографические методы защиты информации / Рябко Б.Я., Фионов А.Н. // Учебное пособие для вузов. – М: Горячая линия – Телеком, 2005. – 229 с.: ил.
15. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В., Шаньгин В.Ф. // – М.: Изд. ДМК, 2002. – 424 с.
16. ДБН В.2.5-28:2015 Природнє і штучне освітлення.
17. Закон України Про забезпечення санітарного та епідемічного благополуччя населення.
18. НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві».
19. НПАОП 0.00-4.12-05. «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці».
20. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».
21. ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».
22. ДБН В.2.5-28:2015 «Природнє і штучне освітлення».
23. Закон України «Про забезпечення санітарного та епідемічного благополуччя населення».

24. НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно- обчислювальних машин».
25. НПАОП 0.00-8.24-05 «Перелік робіт з підвищеною небезпекою».
26. НАПБ А. 01.001-2004 «Правила пожежної безпеки України».
27. НПАОП 40.1-1.21-98 Правила безпечної експлуатації електроустановок споживачів.
28. ГОСТ 12.1.018-93 ССБТ. Пожаро взрыво безопасность статического электричества. Общие требования.
29. ГОСТ 12.1.044-89 Система стандартов безопасности труда. Пожаро взрывоопасность веществ и материалов.
30. ГОСТ 12.1.030-81 ССБТ. Электробезопасность. Защитное заземление. Зануление.
31. НАПБ Б.03.002-2007. «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».
32. НПАОП 40.1-1.01-97. Правила безпечної експлуатації електроустановок

Додаток А

Лістинг програми реалізації алгоритму RSA

```
// RSA.cpp : RSA.
//

#include "stdafx.h"
#include <iostream>
#include <ctime>
#include <cstdlib>
#include <iomanip>
using namespace std;

////////////////////////////////////////////////////////////////////
//Алгоритм "решето Сундарама". Выбирает все простые числа
//до заданного (случайно сгенерированного).
int sundaram(int n)
{
int *a = new int [n], i, j, k;
memset(a, 0, sizeof(int) * n);
for(i = 1; 3*i+1 < n; i++)
{
for(j = 1; (k = i+j+2*i*j) < n && j <= i; j++)
a[k] = 1;
}
//Выбирает из списка простых чисел ближайшее к заданному.
for(i = n-1; i >= 1; i--)
if(a[i] == 0)
{
return (2 * i + 1);
break;
}
delete [] a;
}
////////////////////////////////////////////////////////////////////
//Алгоритм Евклида. Алгоритм для нахождения наибольшего
//общего делителя двух целых чисел. Используется для проверки
//чисел на взаимопростоту.
int gcd(int a, int b)
{
int c;
while (b)
{
```

```
c = a % b;
a = b;
b = c;
}
return abs(a);
}
//////////////////////////////////////////////////////////////////
int main()
{
cout << "Please wait... Key generation procces." << endl << endl;
// Генерация двух чисел и выбор двух простых чисел.
srand( (unsigned)time( NULL ) );
int p = rand()%100;
int q = rand()%100;
int p_simple = sundaram(p);
int q_simple = sundaram(q);
//Находим число n.
unsigned int n = p_simple*q_simple;
//Генерация числа d и проверка его на взаимопростоту
//с числом ((p_simple-1)*(q_simple-1)).
int d, d_simple = 0;
while (d_simple !=1)
{
d = rand()%100;
d_simple = gcd (d, ((p_simple-1)*(q_simple-1)));
}
//Определение числа e, для которого является истинным
//соотношение (e*d)%((p_simple-1)*(q_simple-1))=1.
unsigned int e = 0, e_simple = 0;
while (e_simple !=1)
{
e += 1;
e_simple = (e*d)%((p_simple-1)*(q_simple-1));
}
//Сгенерированные ключи.
cout << '{' << setw(12) << e << ',' << setw(12) << n << '}' << " - Open key"
<< endl;
cout << '{' << setw(12) << d << ',' << setw(12) << n << '}' << " - Secret key"
<< endl << endl;
//Ввод шифруемых данных.
const int MAX = 20;
char *Text = new char [MAX];
cout << "Please enter the Text. Use <Enter> button when done." << endl;
cin.get(Text, MAX);
```

```
//Массив для хранения шифротекста.
unsigned int *CryptoText = new unsigned int [MAX];
unsigned int *Tdecrypt = new unsigned int [MAX];
//Получение из введённых данных десятичного кода ASCII и
//дальнейшее его преобразование по формуле ci = (mj^e)%n.
int b = 301;
int c;
cout << endl << setw(5) << "Text" << setw(6) << "ASCII"
<< setw(20) <<"CryptoText/Block#" << setw(14)
<< "ASCIIdecrypt" << setw(14) << "Text decrypt" << endl
<< "------------------------------------------------------------" << endl;
for (int j = 0; j < MAX; j++)
{
c = 1;
unsigned int i = 0;
int ASCIIcode = (static_cast<int>(Text[j]))+b;
while (i<e)
{
c = c*ASCIIcode;
c = c%n;
i++;
}
CryptoText[j] = c;
b+=1;
}
//Расшифровка полученного кода по формуле mi = (ci^d)%n
//и перевод его в десятичный код ASCII.
b = 301;
int m;
for (int j = 0; j < MAX; j++)
{
m = 1;
unsigned int i = 0;
while (i<d)
{
m = m*CryptoText[j];
m = m%n;
i++;
}
m = m-b;
Tdecrypt[j] = m;
b+=1;
}
for (int j = 0; j < MAX; j++)
```

```
{
cout << setw(5) << Text[j] << setw(6) << static_cast<int>(Text[j]) << setw(20)
<< CryptoText[j] << setw(14) << Tdecrypt[j] << setw(14) <<
static_cast<char>(Tdecrypt[j]) << endl;
}
delete [] Text;
delete [] CryptoText;
delete [] Tdecrypt;
return 0;
}

int _tmain(int argc, _TCHAR* argv[])
{
return 0;
}
```

Додаток Б

Лістинг програми реалізації алгоритму Ель Гамаля

```
// El_Gamal.cpp : // Алгоритм Эль Гамаля.

#define _CRT_SECURE_NO_WARNINGS
#include <fstream>
#include <iostream>
#include <cstdlib>
#include <ctime>
#include <string>

#pragma hdrstop      // Предоставляет дополнительный элемент управления по именам файлов предварительной компиляции и над местоположением на котором сохраняется состояние компиляции

 using namespace std;

int power(int a, int b, int n){// a^b mod n
    int tmp=a;
    int sum=tmp;
    for(int i=1;i<b;i++){
        for(int j=1;j<a;j++){
            sum+=tmp;
            if(sum>=n){
                sum-=n;
            }
        }
        tmp=sum;
```

```
    }
    return tmp;
}
int mul(int a, int b, int n){// a*b mod n
    int sum=0;

    for(int i=0;i<b;i++){
        sum+=a;
    if(sum>=n){
            sum-=n;
        }
    }
  return sum;
}
 void crypt(int p,int g,int x, string inFileName,string outFileName){
setlocale( LC_ALL,"Russian" );
     ifstream inf(inFileName.c_str());   //Формирует массив строк  И возвращает
указатель на него.
    ofstream outf(outFileName.c_str());
    cout<<"Введите p,g,x\n";
    cin>>p>>g>>x;
    int y=power(g,x,p);
    printf("Открытый ключ (p,g,y)=", setlocale(LC_ALL, "Russian"));
    cout<<""<<"("<<p<<","<<g<<","<<y<<")"<<endl;
    cout<<"Закрытый ключ x="<<x<<endl;
    cout<<"Введите текст который необходимо зашифровать\n";
    while(inf.good()){
        int m=inf.get();
        if(m>0){
            cout<<(char)m;
```

```
            int k=rand()%(p-2)+1; // 1 < k < (p-1)
            int a= power(g,k,p);
            int b= mul(power(y,k,p),m,p);
            outf<<a<<" "<<b<<" ";
        }
    }
  cout<<endl;
        inf.close();
    outf.close();
}
 void decrypt(int p,int x,string inFileName,string outFileName){
       ifstream inf(inFileName.c_str());
    ofstream outf(outFileName.c_str());
    setlocale( LC_ALL,"Russian" );
    cout<<"\nДешифрованый текст:"<<endl;
     while(inf.good()){
        int a=0;
        int b=0;
        inf>>a;
        inf>>b;
         if(a!=0&&b!=0){
              int deM=mul(b,power(a,p-1-x,p),p);// m=b*(a^x)^(-1)mod p =b*a^(p-1-
x)mod p
            char m=static_cast<char>(deM);
            outf<<m;
            cout<<m;
        }
    }
    cout<<endl;
    inf.close();
```

```
    outf.close();
}
 int main(){
    srand(time(NULL));
    setlocale( LC_ALL,"Russian" );
    int p=0,g=0,x=0;
    crypt(p,g,x, "input.txt","outsh.txt");
    decrypt(p,x, "outsh.txt","outdesh.txt");
    system("pause");
    return 0;
}
```

Додаток В

Презентація

Рисунок В1 – Слайд 1

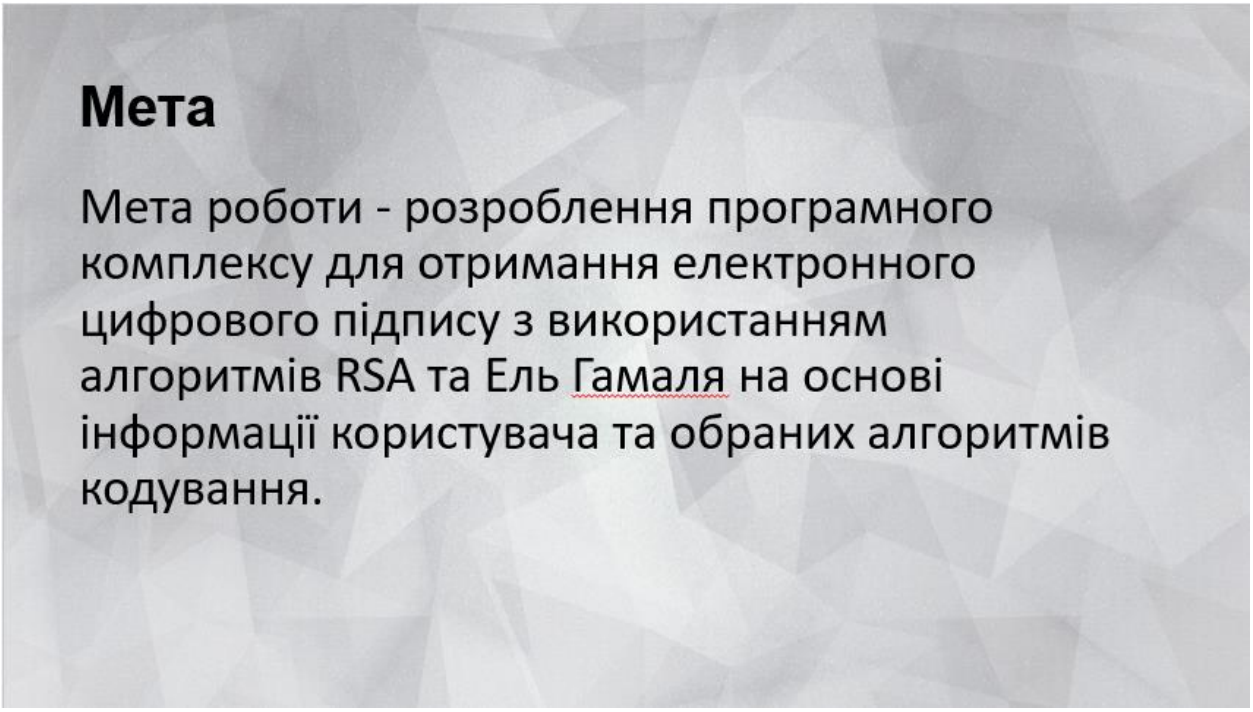


Рисунок В2 – Слайд 2

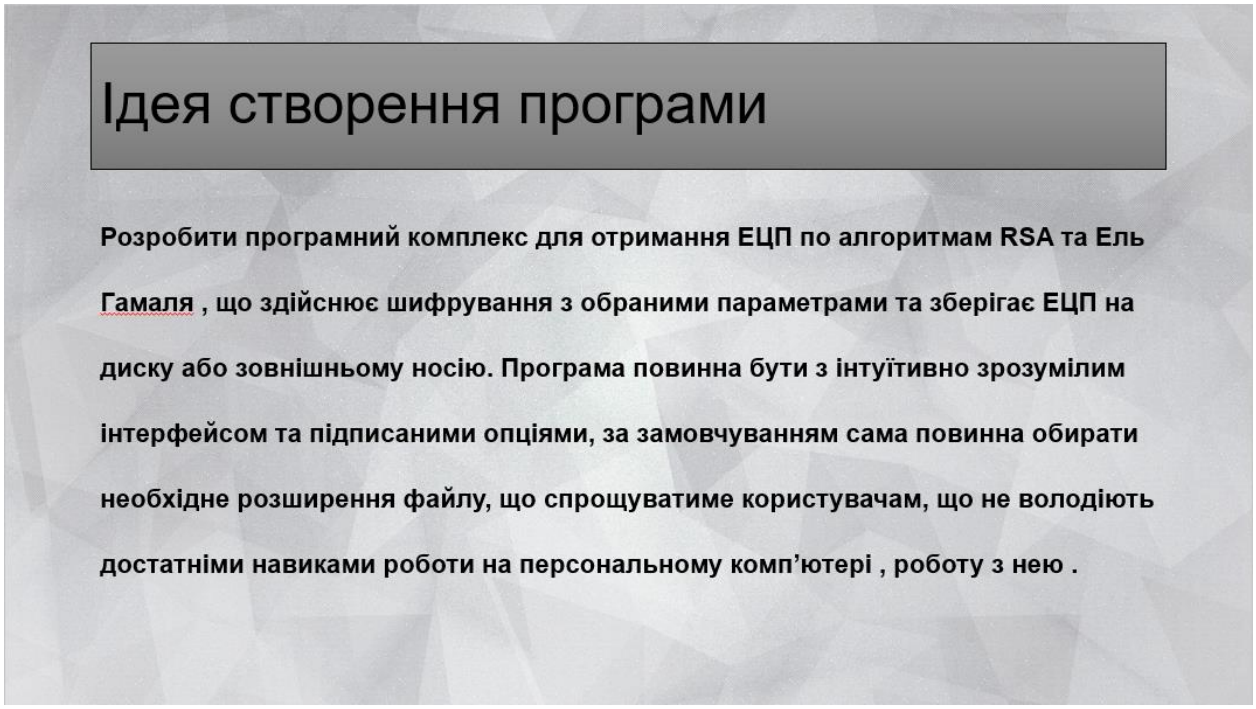


Рисунок В3 – Слайд 3

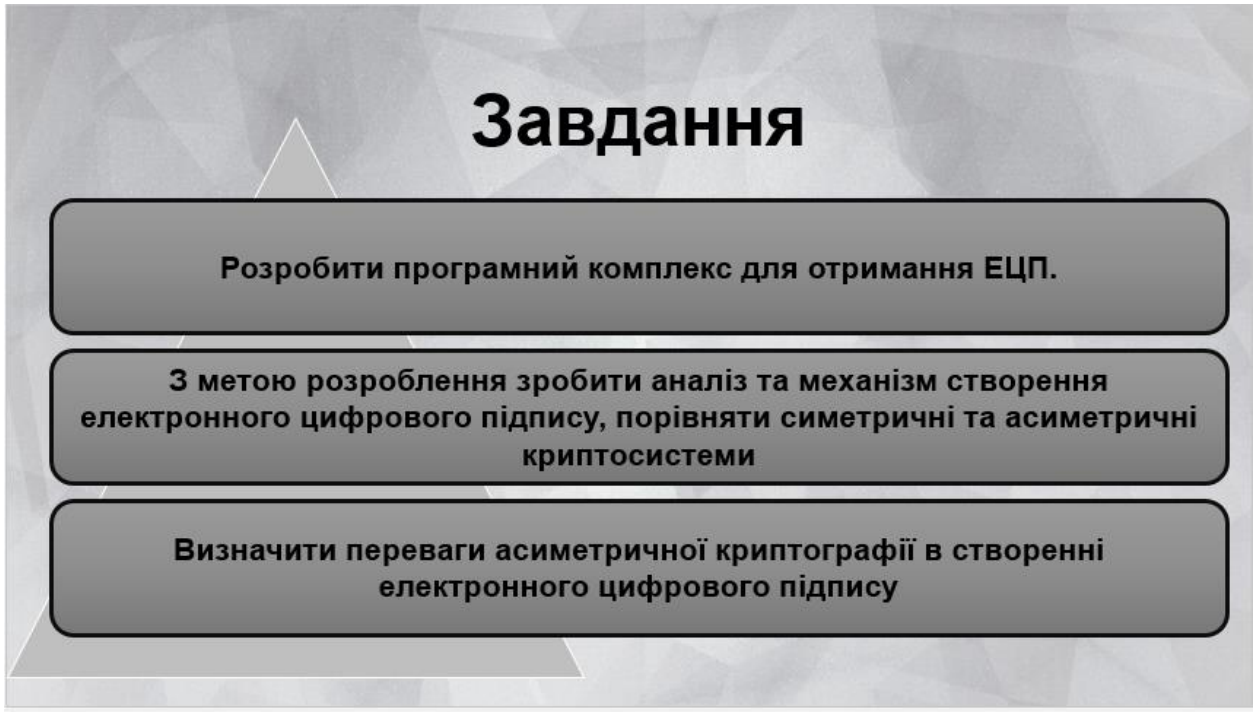


Рисунок В4 – Слайд 4

Рисунок В5 – Слайд 5

Рисунок В6 – Слайд 6

Порівняння асиметричних та симетричних алгоритмів

1. Операції шифрування та розшифрування в симетричних алгоритмах

2. Операції шифрування та розшифрування в асиметричних криптосистемах

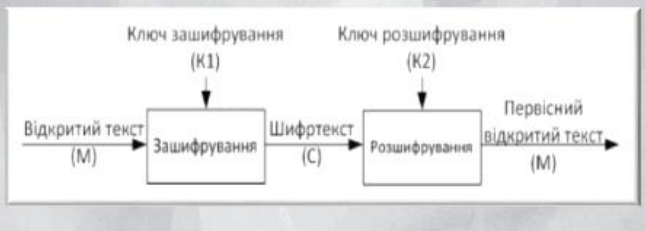


Рисунок В7 – Слайд 7

Порівняння характеристики алгоритмів RSA та Ель-Гамаля

Алгоритм	Ключ	Призначення	Крипостійкість, MIPS	Примітки
RSA	До 4096 біт	Шифрування і підпис	$2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на труднощі завдання факторизації великих чисел; один з перших асиметричних алгоритмів. Включений до багатьох стандартів
Ель Гамаля	До 4096 біт	Шифрування і підпис	При однаковій довжині ключа криптостійкості рівна RSA, тобто $2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на важкій задачі обчислення дискретних логарифмів в кінцевому полі; дозволяє швидко генерувати ключі без зниження стійкості. Використовується в алгоритмі цифрового підпису DSA-стандарту DSS

Рисунок В8 – Слайд 8

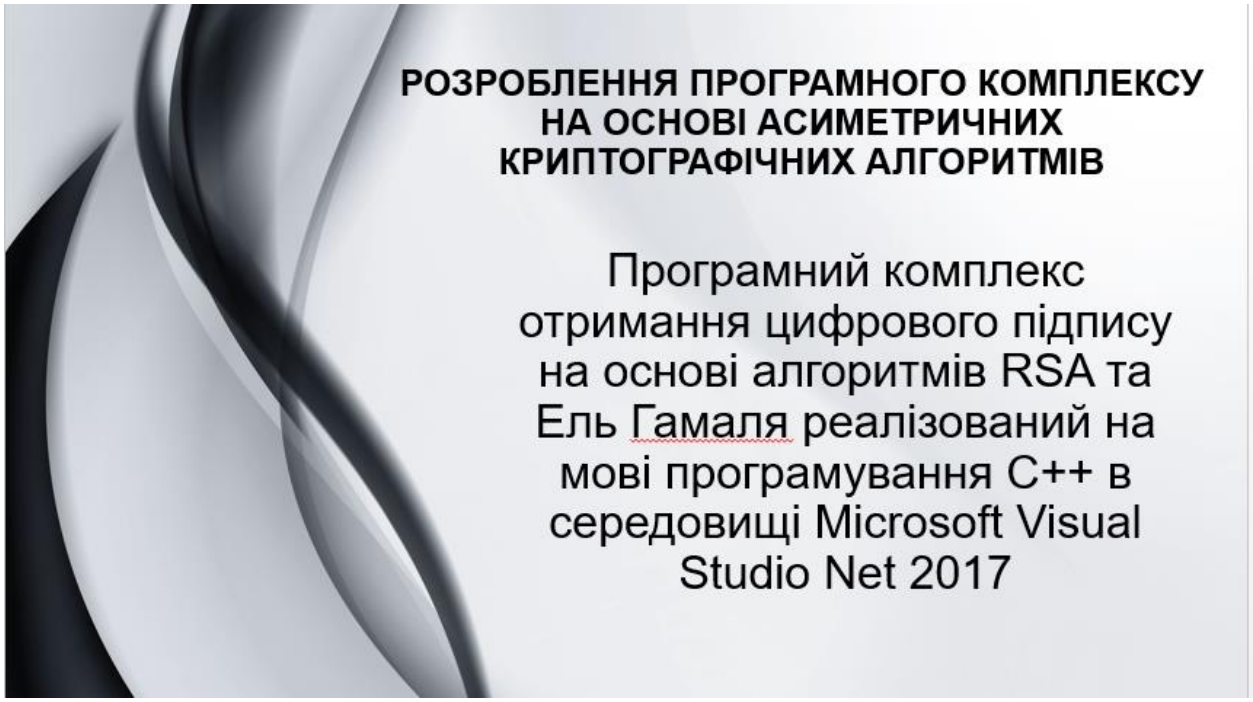


Рисунок В9 – Слайд 9

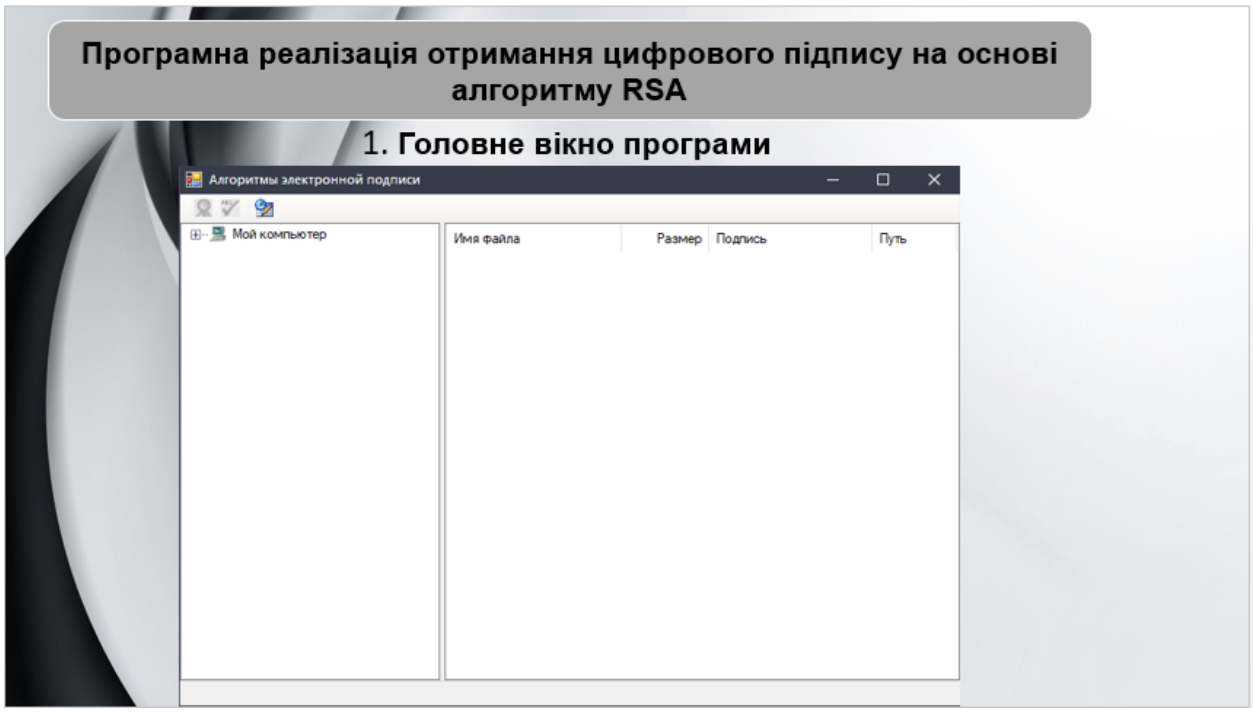


Рисунок В10 – Слайд 10

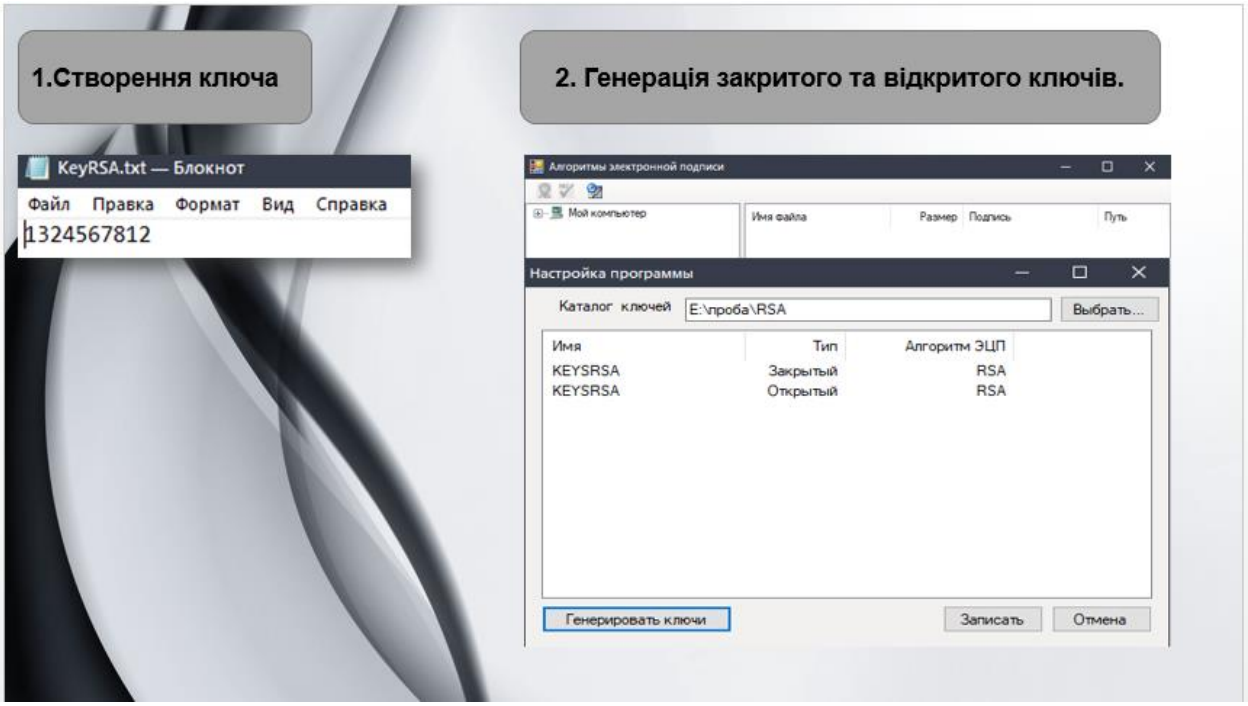


Рисунок В11 – Слайд 11

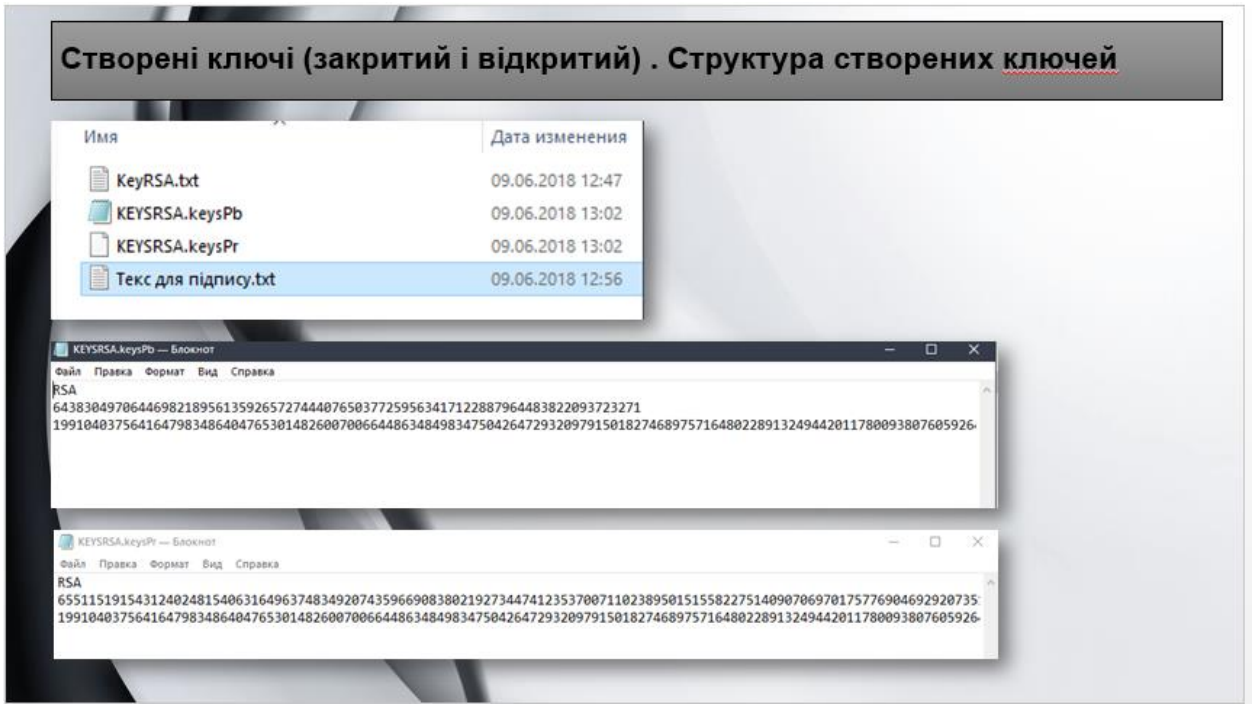


Рисунок В12 – Слайд 12

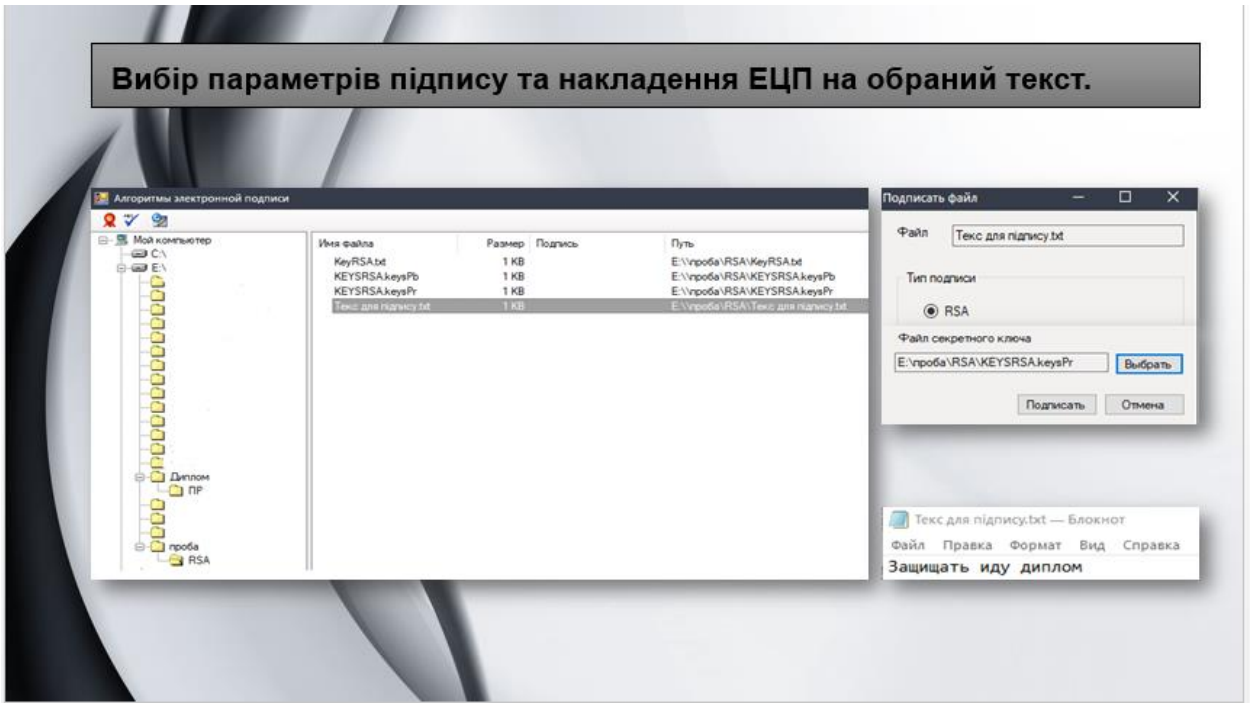


Рисунок В13 – Слайд 13

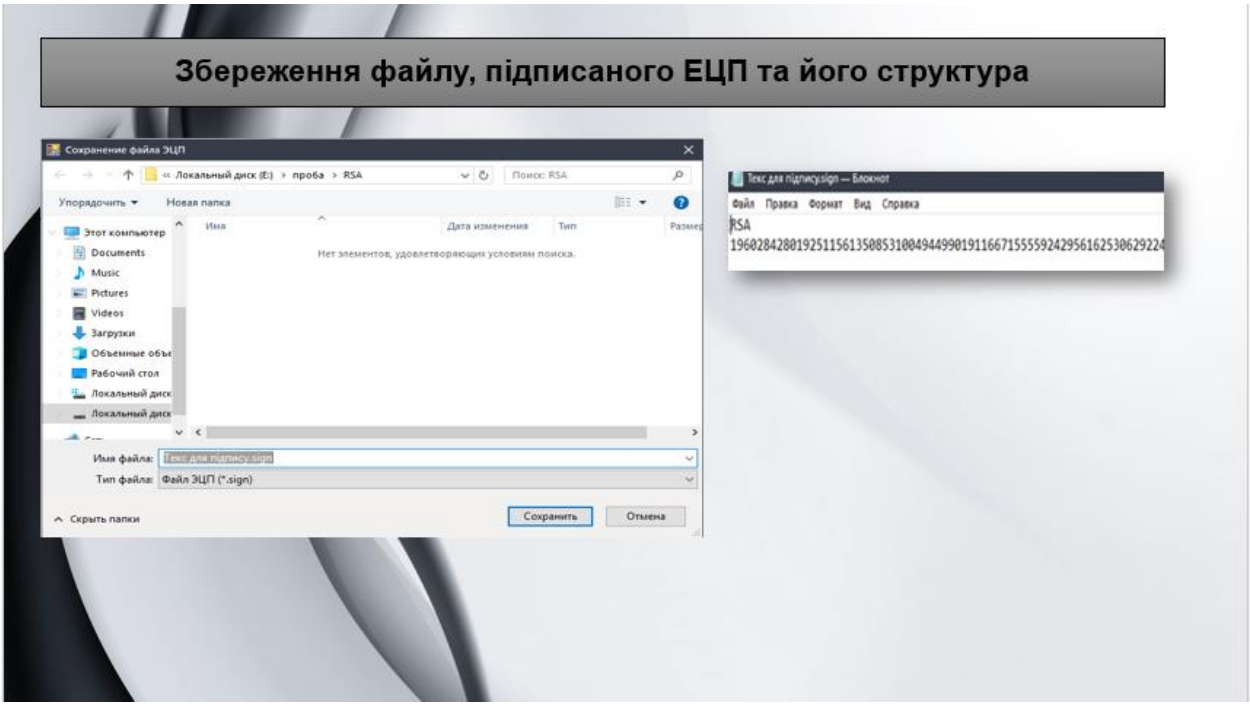


Рисунок В14 – Слайд 14

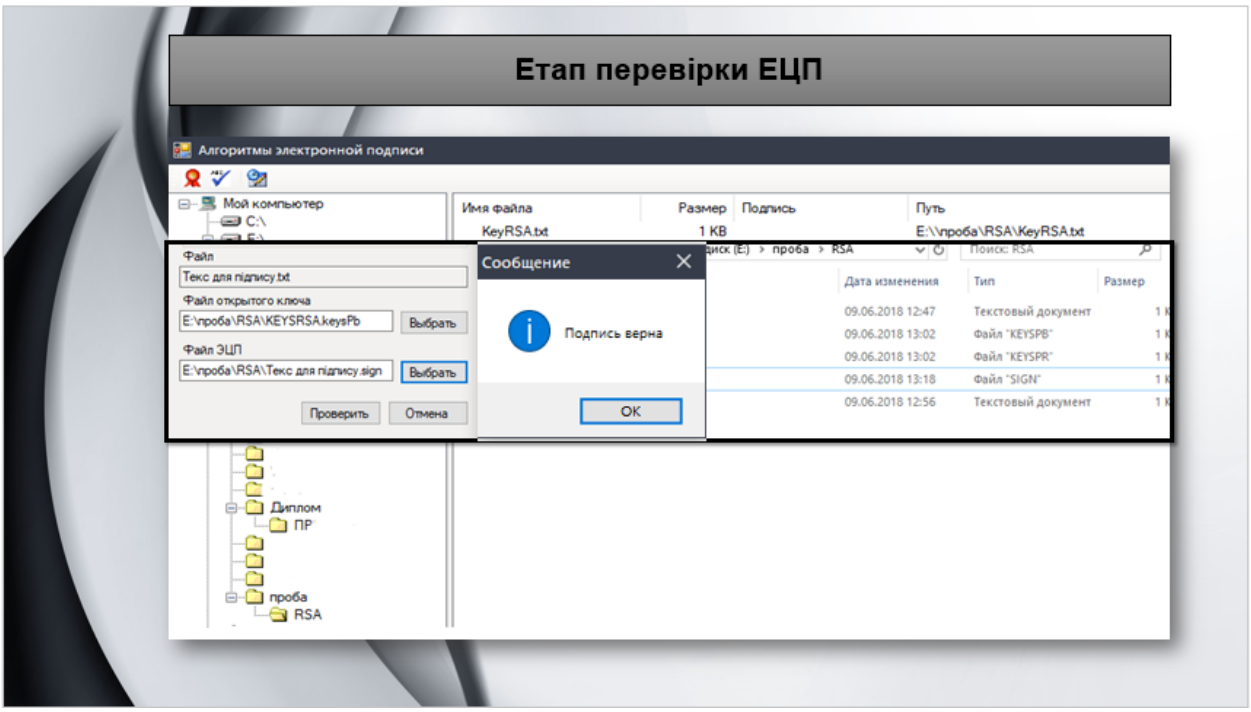


Рисунок В15 – Слайд 15

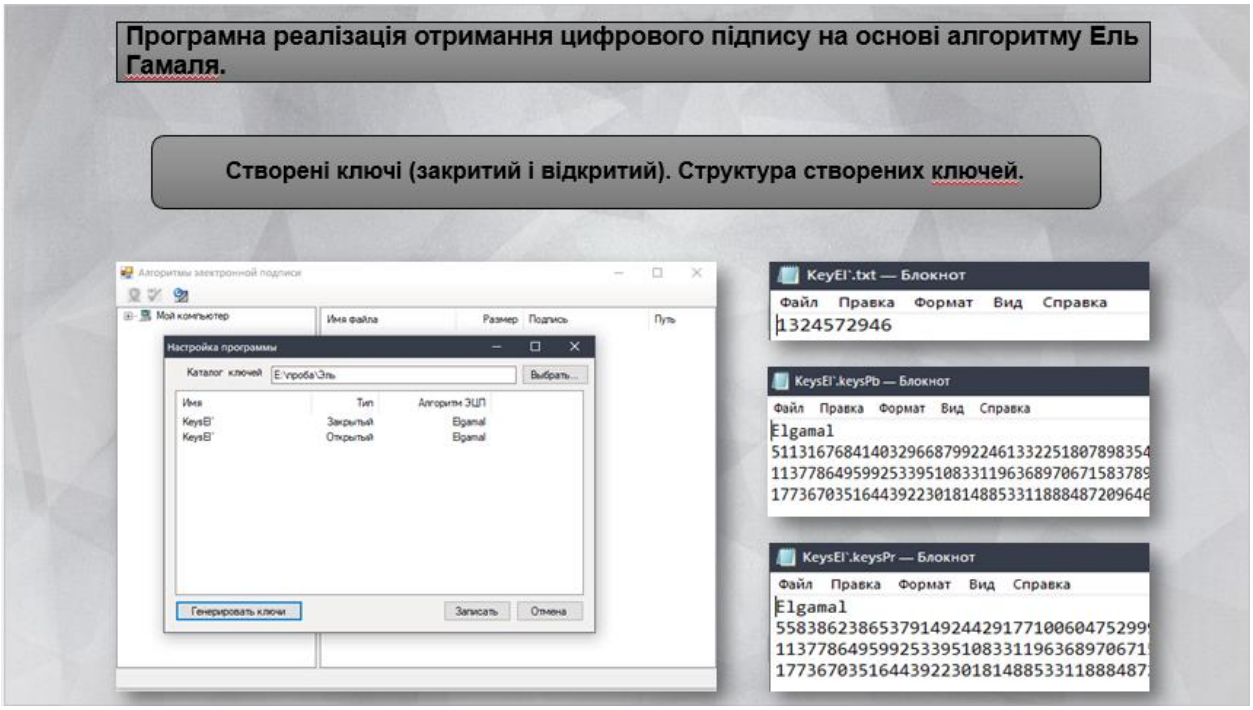


Рисунок В16 – Слайд 16

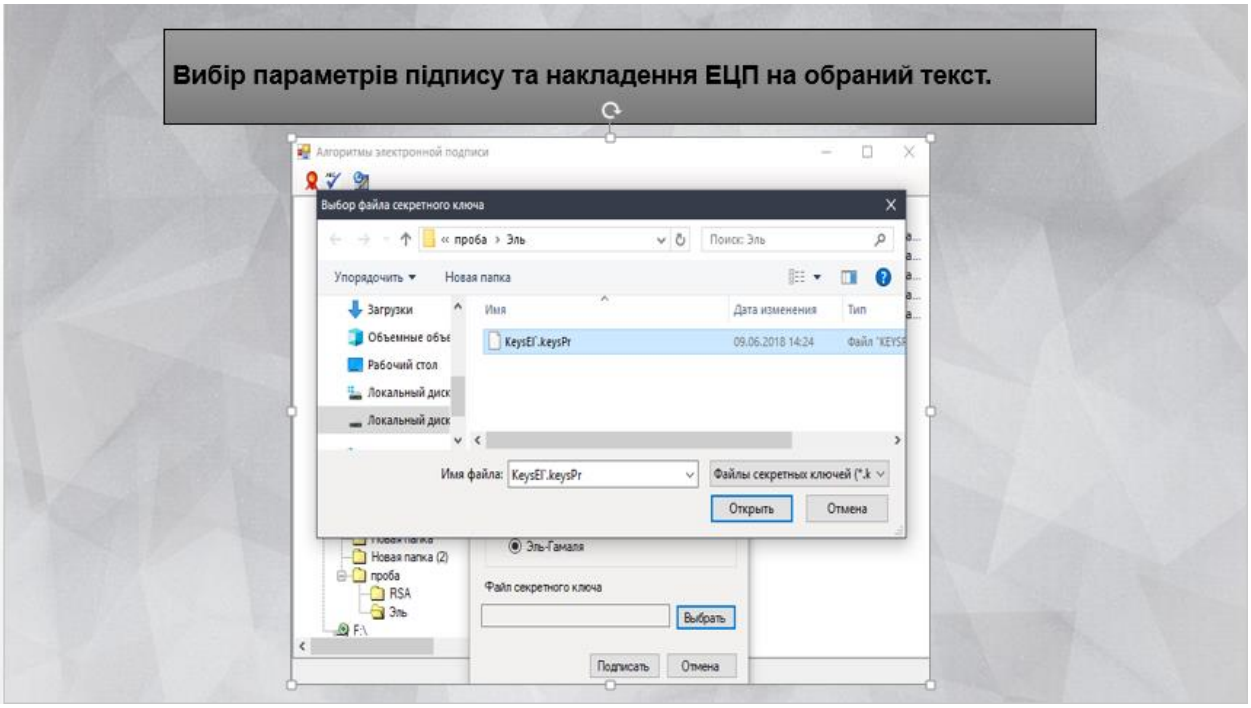


Рисунок В17 – Слайд 17

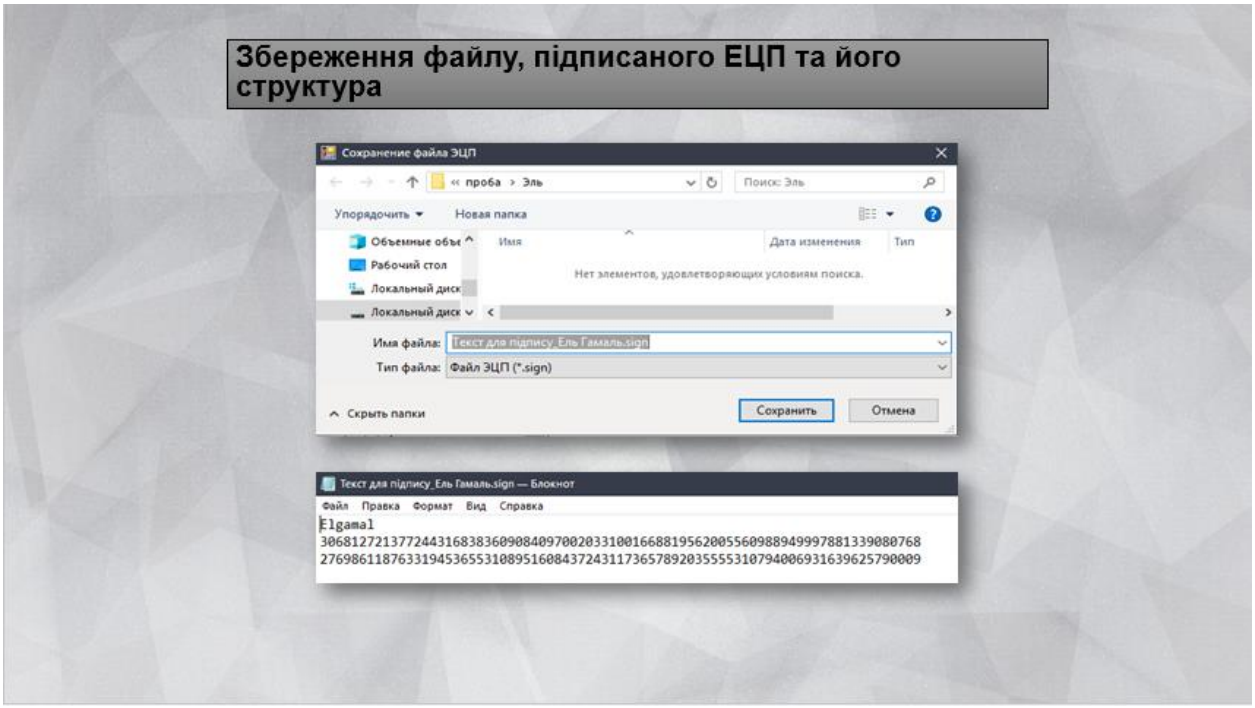


Рисунок В18 – Слайд 18

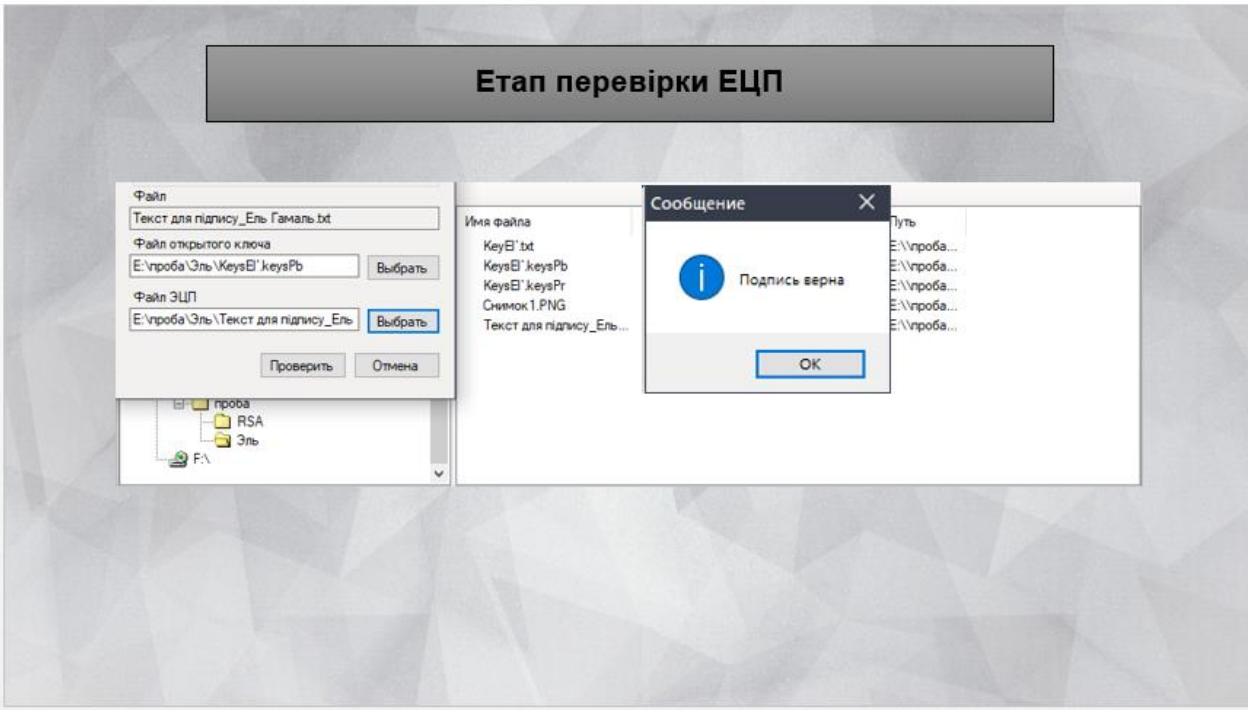


Рисунок В19 – Слайд 19

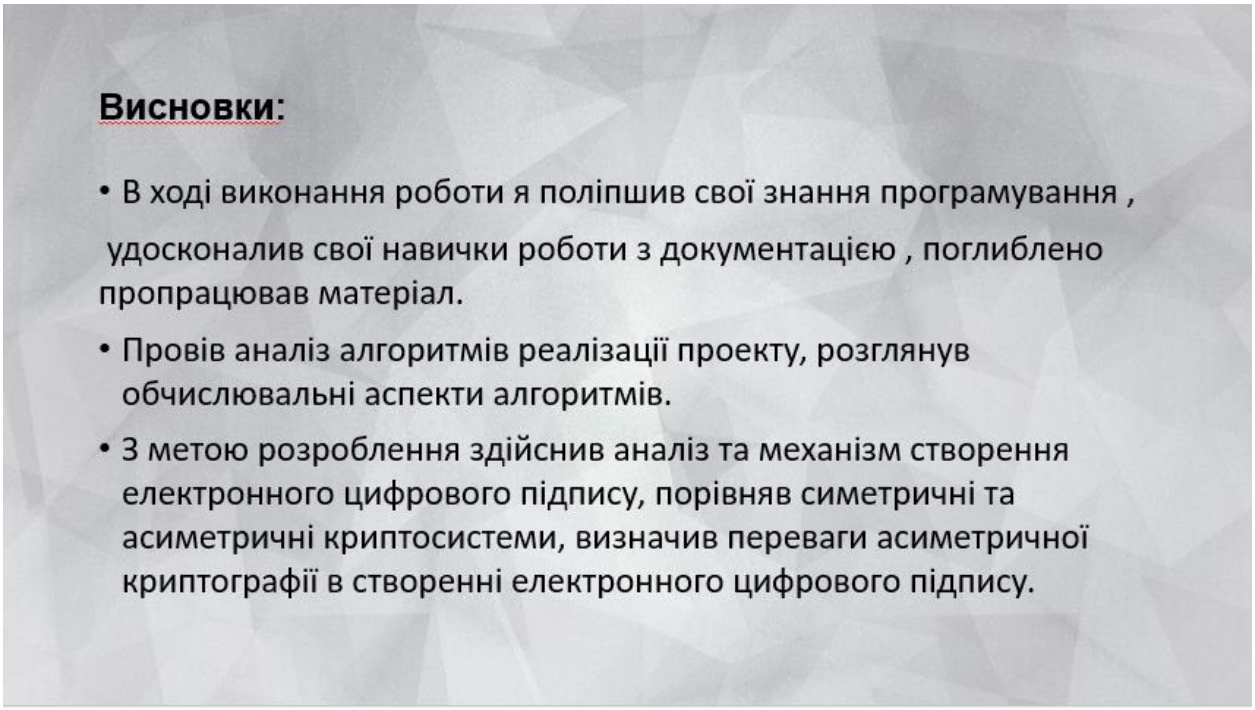


Рисунок В20 – Слайд 20

Рисунок В21 – Слайд 21