Міністерство освіти і науки України
ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»
Кафедра комп'ютерної інженерії та електроніки

Григорів Віталій Богданович
Hryhoriv Vitalii

УДК 004

Спеціальність 123 «комп'ютерна інженерія»
(шифр та назва спеціальності)

Кваліфікаційна робота
на здобуття освітньо-кваліфікаційного рівня магістр
(бакалавр, спеціаліст, магістр)

Дослідження стійкості алгоритмів захисту аудіофайлів (відеофайлів, графіків) в інформаційних комунікаційних системах

Research of stability of algorithms of protection of audio files (video files, graphics) in information communication systems

Науковий керівник:
кандитат фізико-математичних наук, доцент
Запухляк Р. І.

Рецензенти:
д. ф.-м. н.,
проф. кафедри фізики і хімії твердого тіла
Салій Я. П.

Івано-Франківськ
2020

Формат	Зона	Поз.	Позначення	Найменування	К-ть	Прим.
			123. УДК 004	Пояснювальна записка	1	

Змн.	Арк.	№ докум.	Підпис	Дата	123. УДК 004		
Розробив		Григорів В. Б.			Специфікація	Літ.	Арк. 2 / Аркушів 1
Перевірив		Запухляк Р. І.					
Н. Контр.							
Затвердив							

АНОТАЦІЯ

Пояснювальна записка до магістерської кваліфікаційної роботи «Дослідження стійкості алгоритмів захисту аудіофайлів (відеофайлів, графіків) в інформаційних комунікаційних системах»: 69 ст., 44 рис., 12 табл., 10 джерел.

Об’єкт дослідження – алгоритми шифрування.

Мета роботи – розробка рекомендацій для забезпечення захисту передачі конфіденційної інформації в незахищеній мережі.

Методом дослідження є математичні алгоритми, які закладені в основу роботи розглянутих методів шифрування.

Робота складається з вступу, 4 розділів, висновку, списку використаних джерел інформації.

Ключові слова: шифрування, інформаційні системи, ключ.

					123. УДК 004			
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*				
Розробив		Григорів В. Б.			Анотація	*Літ.*	*Арк.*	*Аркушів*
Перевірив		Запухляк Р. І.					3	1
Н. Контр.								
Затвердив								

ABSTRACT

Explanatory note to the Master's Research Work " Research of stability of algorithms of protection of audio files (video files, graphics) in information communication systems": 69 pages, 44 figures, 12 tables, 10 references.

The object of research is encryption algorithms.

The purpose of the work is to develop recommendations to ensure the protection of the transmission of confidential information in an unsecured network. Method of research - statistical analysis, mathematical and simulation modeling with the use of computer technology.

The research method is mathematical algorithms, which are the basis of the considered encryption methods.

The work consists of an introduction, 4 chapters, a conclusion, a list of used sources of information.

Keywords: encryption, information systems, key.

ДВНЗ
«Прикарпатський національний університет імені Василя Стефаника»
Фізико-технічний факультет
Кафедра комп’ютерної інженерії та електроніки

Пояснювальна записка

до кваліфікаційної роботи
на тему:

«Дослідження стійкості алгоритмів захисту аудіофайлів (відеофайлів, графіків) в інформаційних комунікаційних системах»

					123. УДК 004		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Григорів В. Б.			.	Літ.	Арк. / Аркушів
Перевірив		Запухляк Р. І.			Пояснювальна записка		5 / 69
Н. Контр.							
Затвердив							

ПЕРЕЛІК ОСНОВНИХ СКОРОЧЕНЬ

PKI – Public Key Infrastructure;

ОС – Операційна система;

ПЗ – Програмне забезпечення;

DES – Data Encryption Standard;

PKI – Public Key Infrastructure;

AES – Advanced Encryption Algorithm;

DES – Data Encryption Standard;

ЦОС – цифрова обробка сигналів.

ЗМІСТ

ВСТУП

Зрозуміло, що в сучасному цивілізованому світі, в якому величезну кількість занять людей супроводжується комп'ютерною підтримкою, проблема безпеки комп'ютерних систем надзвичайно важлива. Збільшення кількості матеріалу у вигляді мультимедіа файлів і, як наслідок, зростаюча потреба в захисті матеріалів, представляє нові вимоги до технічних засобів, які можуть забезпечити такий захист. Ось чому в наш час професіонали повинні мати навички, якими можна скористатися для захисту комп'ютерних даних та розуміти проблему захисту інформаційних ресурсів.

Необхідність запровадження засобів криптографічного захисту інформації дозволить зберегти її конфіденційність під час введення, виведення, передачі, обробки та зберігання, а також протистояти її знищенню, крадіжці або спотворенню.

Метою роботи є розробка рекомендацій для забезпечення захисту передачі файлів.

Об’єктом дослідження є інформаційні комунікаційні мережі.

Предметом дослідження є дослідження алгоритмів шифрування.

РОЗДІЛ 1. ЕЛЕМЕНТАРНІ ШИФРИ ТА ЇХ ВЛАСТИВОСТІ

На сьогоднішній день справедливо розглядається один із найнадійніших методів захисту інформації – шифрування. Тому для захисту інформації її передають використовуючи криптографію - науку про методи безпеки, конфіденційність та надійність інформації. Майже щодня надходять повідомлення про корпоративні зломи мережі зловмисниками та промисловими шпигунами. У багатьох компаніях заходи безпеки закінчуються встановленням брандмаузера. Крім того, брандмаузери ускладнюють проникнення лише в мережу ззовні, але не може захистити від зростаючої кількості внутрішніх злочинів.

Тривалий час методи захисту інформації розроблялися лише державною владою, а їх здійснення розглядалося як виключне право держави. Однак в останні роки, з розвитком комерційної та ділової діяльності, кількість спроб отримати несанкціонований доступ до конфіденційної інформації зросла, а питання інформаційної безпеки стало центральною проблемою багатьох вчених та експертів з різних країн. В результаті цього процесу зросла потреба в захисті конфіденційної інформації. Захист інформації - це сукупність організаційно-технічних заходів та правових норм для запобігання шкоди інтересам власника даної інформації.

Для вирішення цієї проблеми потрібна система заходів, метою якої є застереження від несанкціонованого доступу. Тому, в свою чергу, створення систем захисту інформаційних ресурсів від зловмисників забезпечує інформаційну безпеку.

1.1. Класифікація шифросистем

Найважливішою властивістю будь-якої криптосистеми є криптостійкість, що характеризується її здатністю протидіяти криптоаналітичним атакам, що надає можливість уникнати в деяких допустимих межах можливості дешифрування зашифрованої інформації без знання ключа. Існує низка підходів до оцінки крип-

тостійкості, в залежності від комплексу умов, що полегшують криптоаналіз. Наведемо декілька з них:

- Середній час, необхідний для пошуку істинного ключа за допомогою повного перебору всіх існуючих варіантів ключів;
- Складність найкращого алгоритму розв'язування задачі розкриття ключа при наявності відкритого тексту і відповідного йому шифрованого;
- Складність найкращого алгоритму розв'язування задачі розкриття ключа з допомогою правильно підібраних пар шифрованих і відповідних їм відкритих текстів та інше.

Ці та інші умови в криптографії часто використовуються для виокремлення стійких і слабких криптосистем. Тобто, якщо криптосистема допускає розкриття ключа при даному комплексі умов, то така система вважається слабкою, в іншому випадку – стійкою. Зрозуміло, що при данних умовах розкриття ключа повинно здійснюватися в прийнятний час.

Криптографія з ключем тепер називається алгоритмом шифрування, в якому сам алгоритм стає широко відомим і доступним для кожного, але шифрування виконується на основі невеликої кількості інформації - ключа, що відомий лише одержувачу та відправнику повідомлення. Розмір криптографічного ключа становить від 56 до 4096 біт. Загальна схема процесу передачі повідомлень представлена на рис.1.1.

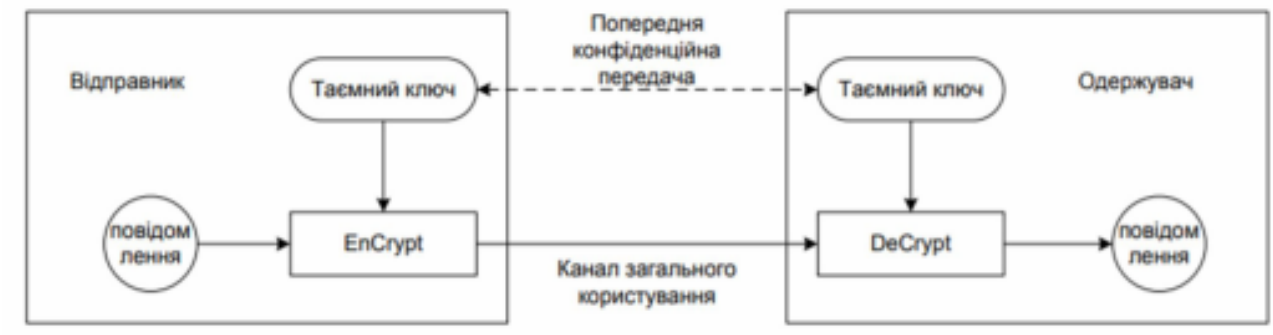


Рисунок 1.1 – Схема процесу передачі інформації повідомлення

Під інформаційною безпекою данних вважається цілісність, доступність та конфіденційність. До цього:

1. цілісність - це гарантія надійності та повної інформації та способи її обробки;
2. конфіденційність - це надання доступу лише до інформації авторизованому користувачеві;
3. доступність - це забезпечення доступу до інформації, а також можливості її використання.

1.2. Методи стеганографії

В теперішній час стеганографія використовується для захисту авторського права, приховання зв'язку, автентифікації, відстеження електронної пошти, додавання додаткової інформації, додавання підписів до зображення, захищення цілісністності зображення. Приклад використання прихованого з'єднання: організація резервного каналу, наприклад, для дипломатичних представництв, розташованих на територіях іноземних держав. На рис. 1.2. зображено загальні області застосування стеганографії.

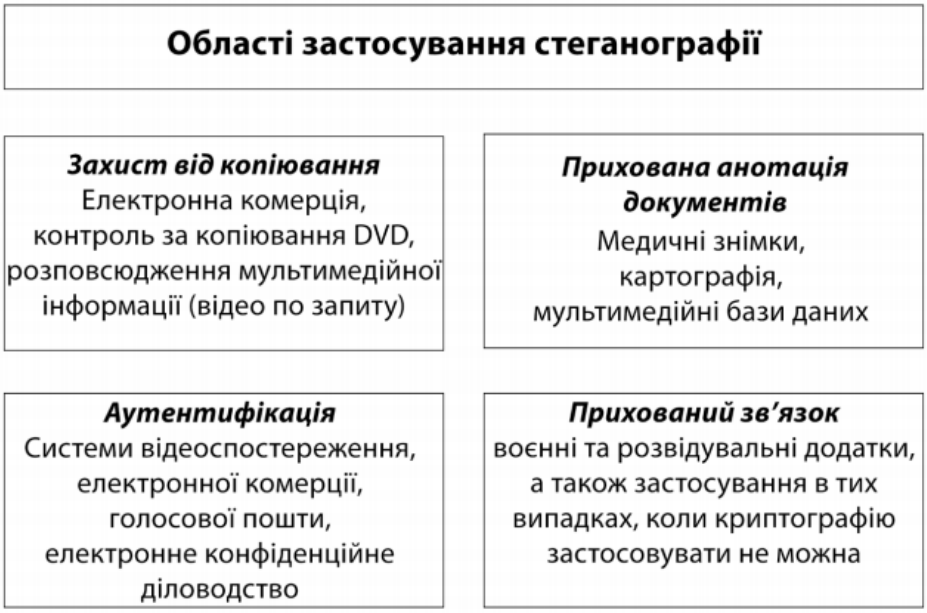


Рисунок 1.2 - Класифікація областей застосування стеганографії

Використання методів криптографії дозволяє сховати вміст конфіденційної інформації, але не може приховати сам факт його наявності або передачі. Методи стеганографії, спрямовані на засекречення самої присутності конфіденційної інформації. Як інформацію ви можете використовувати: текст, повідомлення, зображення тощо.

Стегоключ – це секретний ключ, необхідний для засекречення інформації. Залежно від рівня захисту в стегосистемі може бути один або кілька стегоключів. Як і в криптографії стеганографія поділяється на два типи: з відкритим та секретним ключем.

У системі з секретним ключем використовується ключ, який повинен бути ідентифікованим або перед обміном секретним повідомленням, або переданий через захищений канал.

У стеганосистемі з відкритим ключем для вбудовування та вилучення повідомлення використовують різні ключі, які передаються таким чином, що за допомогою розрахунків неможливо виробити один ключ незнаючи інший. Тому один ключ (відкритий) може передаватися вільно незахищеними каналами зв'язку. Крім того, ця схема добре працює при взаємній недовірі відправника та одержувача.

На сьогоднішній день існує три галузі застосування стеганографії: прослуховування даних (повідомлень), цифрові водяні знаки та заголовки.

Стеганографія може вирішити такі основні задачі захисту інформації:

- захист авторських прав власників електронних документів з допомогою нанесення на файли з цими документами (фото, аудіо або відео матеріали) спеціальної мітки;
- подолання управління мережевими ресурсами та систем моніторингу мережі;
- захист від несанкціонованого доступу до інформації;

- приховування конфіденційного програмного забезпечення (захистити його від використання незареєстрованими користувачами через приховування в мультимедійних файлах);

1.3. Методи криптографії

Криптографія є одиним з головних інструментів забезпечення секретності та цілісності інформація, авторизація, електронні платежі, оперативний контроль процесами управління та обробки даних. Найпоширенішим є захист даних у комп'ютерних мережах. Зазвичай це локальні мережі підприємств, які підключені до інтернету.

Звичайно, достатня довжина ключа та хороший метод шифрування дуже важливі. Розмір ключа вимірюється в бітах (двійковими цифрами). Чим більший ключ, тим більше часу потрібно для пошуку можливого значення, тим довше алгоритм працює.

Існує ряд алгоритмів шифрування даних, основні групи яких зображенні на рис.1.3.

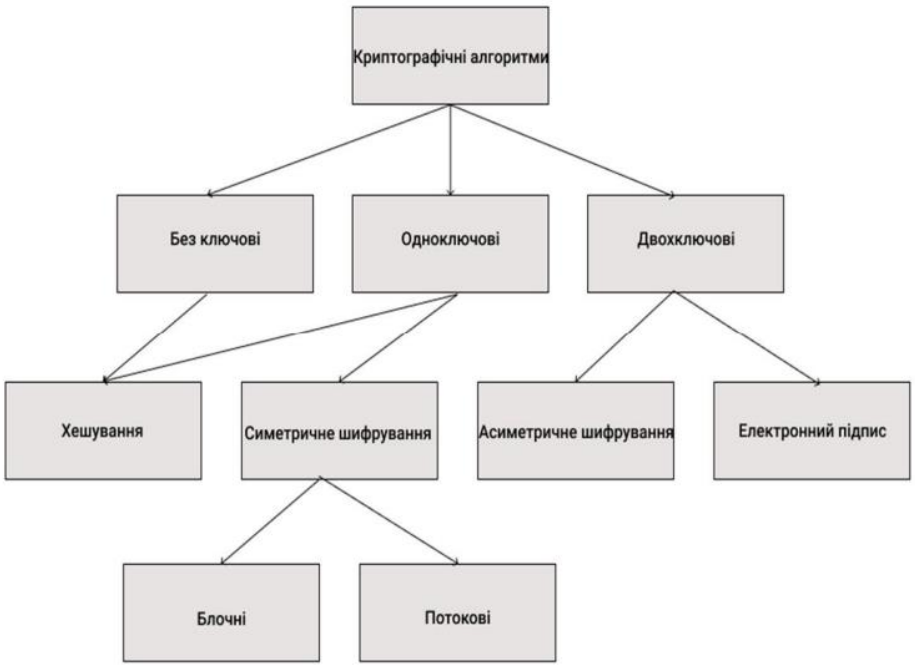


Рисунок 1.3 – Класифікація криптографічних алгоритмів

Часто використовується криптографічний захист інформації, тобто криптографія або шифрування. Шифрування - це процес обробки інформації за певним алгоритмом у нечитабельній формі для захисту від несанкціонованого перегляду або використання. В основі шифрування є два елементи: криптографічний алгоритм і ключ. За допомогою зміни ключа відбувається управління шифруванням. Саме шифрування забезпечує всі три аспекти безпеки даних користувача: доступність, конфіденційність та цілісність.

Узагальнена криптографічна схема системи, що вимагає шифрування інформації, зображено на рис. 1.4.

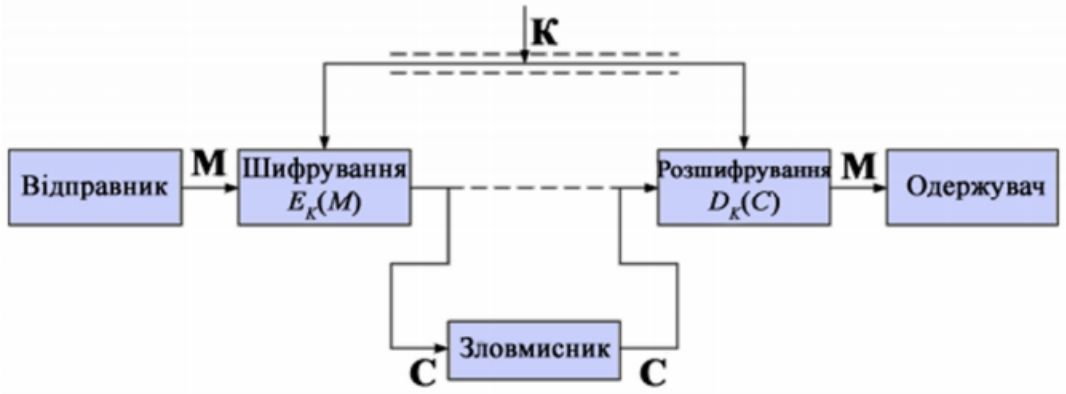


Рисунок 1.4 – Схема криптосистеми

Якщо однаковим ключем користуються і одержувач, і відправник інформації, то така система називається симетричною, системою з одним ключем, системою з секретним ключем або традиційна схема шифрування. Якщо одержувач і відправник використовують різні ключі (один загальнодоступний, а інший секретний), система називається асиметричною, системою з двома ключами або схема шифрування відкритого ключа.

Система шифрування даних використовує в основному два елементарні перетворення:

- заміна (біти вхідних даних всередині блоку заміняються).
- перестановка (біти вхідних даних всередині блоку міняються місцями);

Криптографічні алгоритми в основному використовуються для шифрування інформації та для забезпечення захисту даних та повідомлень від змін, підробки або спотворень. Поділяються сучасні криптографічні алгоритми шифрування даних на симетричні (з одним ключем для шифрування та дешифрування) та асиметричний (відкритий ключ). Асиметричні відповідно використовують відкритий (public) та секретний (private) ключі для шифрування та розшифровка.

1.3.1. Симетричне шифрування

Алгоритми шифрування та дешифрування даних широко поширені в комп'ютерних технологіях в системах приховування конфіденційної та комерційної інформація від неналежного використання стороньою особою. Симетрична криптографія досить поширена і широко використовуються для шифрування великих обсягів даних, таких як безперервні потоки інформації або файли. До винаходу схеми асиметричного шифрування було єдиним доступним способом – симетричне шифрування. Ключ від алгоритму повинен зберігатись в таємниці обома сторонами. Основою секретності цих алгоритмів є секретність симетричного ключа, який повинен бути відомий як одержувачу повідомлення, так і відправнику, без якого інформація являє собою лише набір символів, в яких немає сенсу.

Схема симетричного алгоритму шифрування зображена на рис. 1.5.

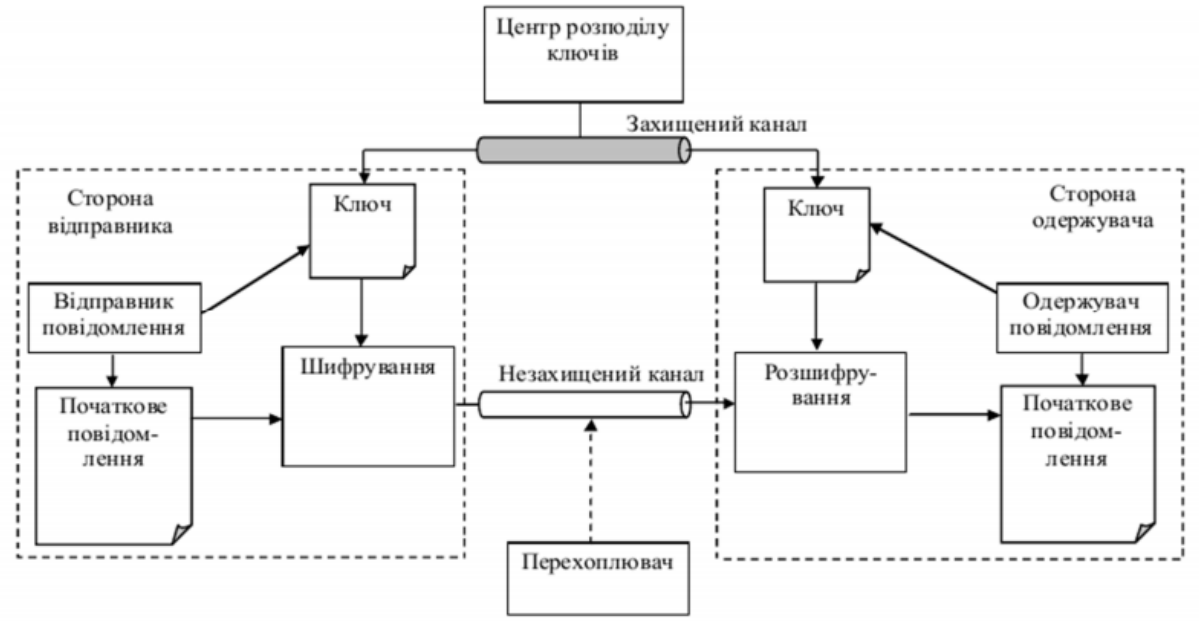


Рисунок 1.5 – Схема симетричного шифрування.

Застосування шифрування з використанням симетричних ключів може бути високоефективним, тому користувачі не відчувають значних затримок в часі в результаті дешифрування та шифрування. Алгоритми симетричного шифрування забезпечує певний рівень автентифікації, тому що інформація, яка є зашифрована одним симетричним ключем не може дешифроватися будь-яким іншим симетричним ключем. Тож до того часу, поки симетричний ключ зберігається в секреті двостороньо, кожна сторона може бути впевнена, що ділиться інформацією з іншою, до того часу, поки розшифровані повідомлення матимуть сенс.

Сучасні симетричні алгоритми криптостійкі та швидкі. Алгоритм **AES** (Advanced Encryption Standard), відомий як симетричний алгоритм блочного шифрування, розроблений Вінсентом Рейменом. Довжина блоку складає 128 біт, довжина ключа може бути 128, 192 і 256 біт.

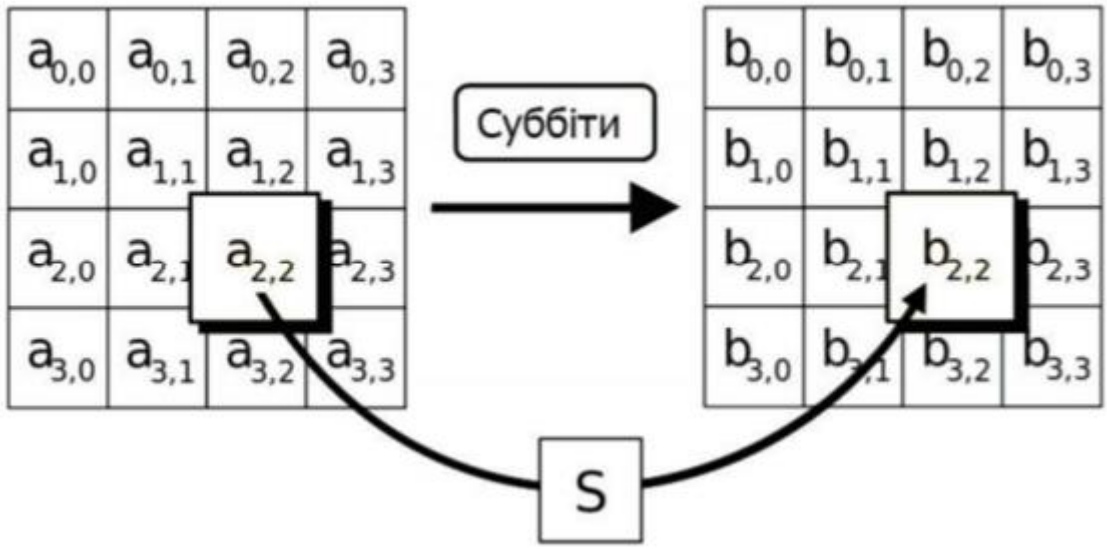


Рисунок 1.6 - Схема підстановки в алгоритмі AES
з використанням S-боксів

Прийнято, що ключ, який використовуємо у системі AES, довжина якого складає 128-біт – це надійний захист. При деяких недоліках AES, захищену цим алгоритмом інформацію зламати практично нереально.

Сила симетричного шифрування часто описується в довжині ключів, що використовуються для виконання шифрування: загалом, чим довший ключ, тим вищий рівень захисту. Різні шифри можуть потребувати ключів різноманітної довжни для отримання одного рівня захищеності.

В основному для симетричних алгоритмів шифрування потрібно менше обчислення, ніж для асиметричних. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох сторін передачі інформації. Оскільки ключі можуть бути перехоплені, їх потрібно часто змінювати і передавати захищеними каналами розповсюдження. Також недоліком є те, що секретний ключ повинен бути відомий і одержувачу, і відправнику. З одного боку, це створює нову проблему розподілу ключів. З іншого боку, одержувач залежно від наявності зашифрованих та розшифрованих повідомлень не зможе довести, що він отримав це повідомлення від конкретного відправника, адже він міг сгенерувати таке повідомлення самостійно. Цей недолік надає даному методу властивість до неможливісті

використовувати їх для підтвердження авторства, бо ключ відомий кожній із сторін.

Переваги:

- вивченість;
- для порівнянної стійкості необхідна менша довжина ключа;
- простота реалізації (за рахунок більш простих операцій);
- швидкодія.

Недоліки:

- складність управління ключами у великій мережі. Це означає квадратичне збільшення кількості пар ключів, які повинні генеруватися, передаватися, зберігатися та знищуватися в мережі. Мережа з 10 абонентами потребує 45 ключі;
- складність обміну ключами. Потрібно вирішити проблему безпечної передачі ключів кожному абоненту, оскільки секретний канал необхідний для передачі кожного ключа обом сторонам.

1.3.2. Асиметричне шифрування

Цей вид шифрування інформації має назву шифруванням на основі інфраструктури відкритих ключів (PKI – Public Key Infrastructure). Тому що, в процесі використання даного типу криптографічного шифрування і дешифрування інформації використовують різні ключі – відкритий і закритий.

Перший ключ – відкритий або публічний. Відповідно до його назви, можна зрозуміти, що в нього є можливість бути переданим іншим користувачам. І насправді ним потрібно ділитися. Адже відкритий ключ застосовується для перевірки цифрових підписів і шифрування повідомлень.

Приватний (закритий) ключ - це ваш особистий секретний ключ, який використовується для розшифровки повідомлень та створення цифрових підписів.

Як випливає з назви, цей ключ слід тримати в таємниці від сторонніх людей та у безпеці.

Асиметричні методи шифрування вимагають використання двох ключів. Один з них, відкритий (його можна опублікувати разом з іншою загальнодоступною інформацією про користувача), що використовується для зашифрування, інший (секретний, відомий лише отримувачу інформації) – для дешифрування.

Тому прочитати зашифрований текст можна лише тоді, коли відомий ключ для розшифровки. Отже, ключ шифрування може бути відомий усім користувачам мережі.

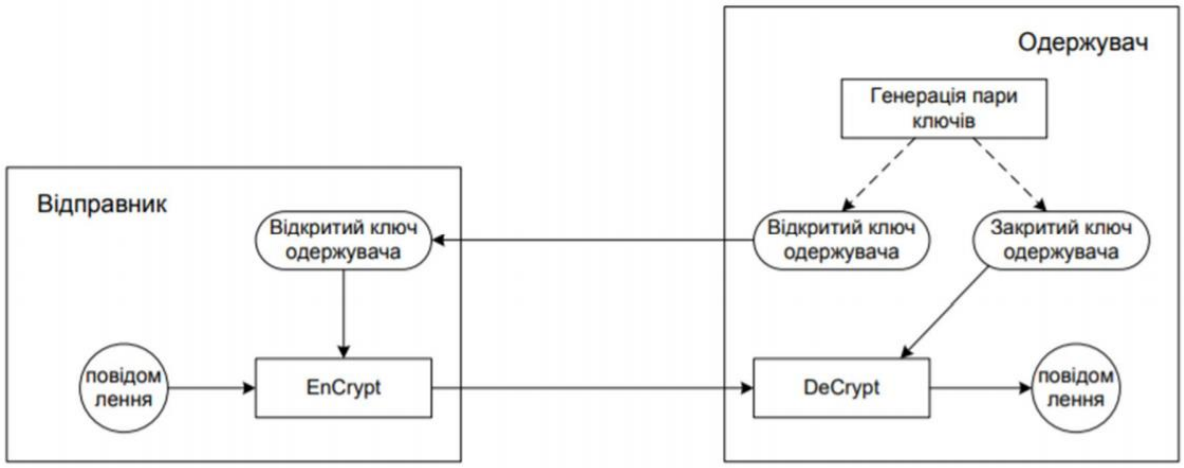


Рисунок 1.7 – Асиметричне шифрування

Найвідомішими асиметричними криптографічними системами є криптосистема на основі еліптичних кривих, системи RSA, El Gamal та.

Асиметричний тип шифрування найчастіше використовуються для:

- передачі секретного ключа симетричного шифрування через відкриту мережу (відправник шифрує цей ключ загальнодоступним ключем одержувача, який зможе розшифрувати отримане повідомлення лише своїм секретним ключем);
- системи електронного цифрового підпису для захисту електронних документів.

Асиметричні методи шифрування вирішили важливе завдання спільного формування секретних ключів. Хоча асиметричні методи шифрування не можуть в повній мірі замінити симетричні методи по даних причинах:

- необхідність використовувати значно довший ключ шифрування для забезпечення однакової криптографічної міцності шифру;
- тривала процедура шифрування та дешифрування.

Майте на увазі, що процеси асиметричного шифрування дуже повільні. Наступною критерією шифрів є схема їх обробки інформаційного потоку. Згідно нього симетричні криптографічні алгоритми поділяються на дві категорії: поточні та блочні шифри. Поточний шифр має змогу обробляти інформацію побітно. Ця схема дуже зручна в послідовних каналах зв'язку, де процес передачі інформації може зупинитися у будь-який час, а потім продовжитися далі. Перетворення даних можна застосовувати лише з інформацією, яка має визначений обсяг даних. Розмір блоку сьогодні дорівнює 64, 128 або 256 біт. Поточні шифри впроваджуються однаково як програмно, так і апаратно, але блочні шифри частіше реалізовано програмо, саме тому воно набуло значно ширшого поширення.

Визначення ступення стійкості криптографічної системи захисту інформації є одним з основних питань. Стійкість криптографічної системи захисту інформації – це її здатність чинити опір атакам на захищену інформацію.

1.3.3. Алгоритми шифрування

Криптосистема **DES** (Data Encryption Standard) є хорошим прикладом криптоалгоритму, який розроблений відповідно до принципів розсіювання та переміщення. Шифр був розроблений співробітником IBM X. Фейстелем у 1976 році. Після ряду змін та вдосконалень, внесених агентством Національної безпеки США (NSA), криптосистема DES була прийнята в якості національного стандарту шифрування даних.

Наведемо етапи шифрування DES:

- До блока відкритого тексту застосовується початкована фіксована перестановка IP (initial permutation), яка задається ключем К1;
- 64-бітний блок розділяють на ліву L_0 і праву R_0 половини по 32 біта;
- До отриманих половин застосовують 16 раундів перестановки і заміни по ключам K_i(i=1, 2, … ,16), які виробляються генератором псевдовипадкових чисел за заданим ключем K_2. На кожному і-му раунді компоненти правої і лівої половин блоку міняють місцями і до правої половини додається функція шифрування, яка залежить від значення правої половини блоку, отриманому на попередньому раунді, і значення ключа K_i, виробленому генератором псевдовипадкових чисел, тобто $f(R_{i-1}, K_2)$. Звичайно така функція визначається як додавання компонентів по модулю 2 (mod 2);
- До лівої L_{16} і правої R_{16} половин, які отримано після шістнадцятого раунду перестановки і заміни, застосовують операцію конкатенації і отримують 64- бітний блок;
- До 64-бітного блоку застосовують зворотну перестановку IP^{-1}. Результатом є зашифрований блок тексту.

Даний алгоритм шифрування можна розглянути як блок-схему:

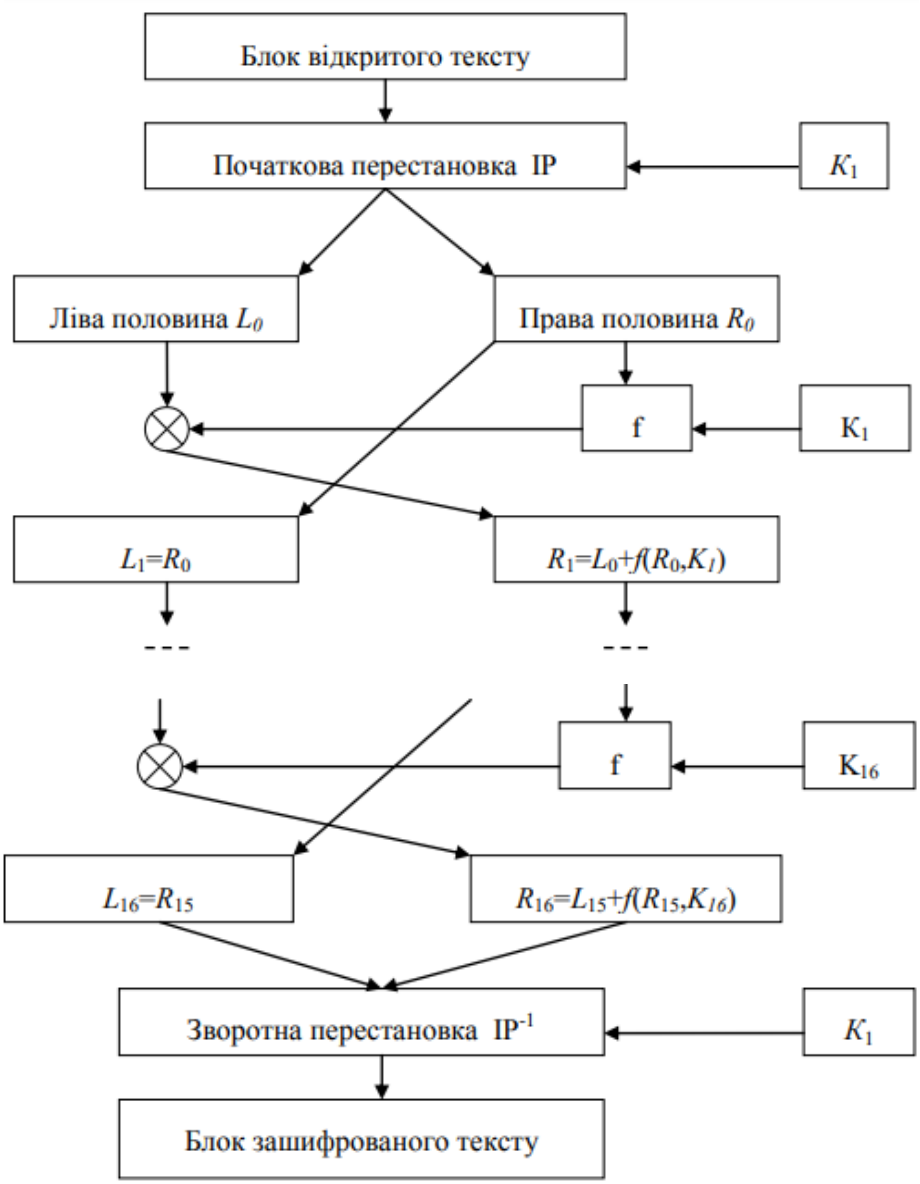


Рисунок 1.8 – Блок-схема криптосистеми DES

Основні переваги алгоритму DES:

- Висока стійкість алгоритму шифрування;
- Швидкодія обробки інформації забезпечується відносною простотою алгоритму;
- При зашифровці повідомлення одним пакетом, ви можете використовувати інший для розшифровки того ж повідомлення;

У криптографії, **Camellia** - це симетричний ключ блочного типу шифрування, із розміром блоку 128 біт та розмірами ключів 128, 192 та 256 біт. Camellia

вважається надійним, сучасним шифром. Немає відомих успішних атак, які б послабили значно шифр.

Первинний аналіз алгоритму Camellia був виконаний його розробниками. Була продемонстрована стійкість алгоритму до лінійного і диференціального криптоаналізу, а також до використання зрізаних і неможливих диференціалів, зсувними атакам і ряду інших атак. Перші відгуки відомих експертів про алгоритм Camellia також були вкрай позитивними. Зокрема, була відзначена виключно висока криптостійкість Camellia.

Ще одним видом криптосистеми є **прозорий**. Це алгоритм, працюючи у фоновому режимі драйвером фільтра, зашифровує та розшифровує дані без участі користувача та стежить за всіма зверненнями.

Прозора функція шифрування забезпечує швидку та зручну роботу з засекреченими даними одночасно для кількох користувачів. Коли файли створюються та редагуються процеси шифрування та дешифрування проводяться автоматично. Для роботи із захищеними документами співробітники компанії не повині володіти ніякими навичками у цій галузі криптографії, вони не повинні вживати жодних додаткових дій для розшифровки або шифрування секретних файлів.

Прозоре шифрування працює за таким принципом. Для шифрування файлу використовується випадково сформований симетричний ключ, який захищається відкритим асиметричним ключем користувача. Якщо користувач хоче внести зміни до зверненого файлу, прозорий драйвер шифрування розшифровує симетричний ключ за допомогою закритого ключа користувача, а потім, використовуючи симетричний ключ, розшифровує файл.

Якщо користувачів багато, а сам засекречений файл знаходиться не на ПК, а на віддаленому сервері, то у кожного користувача повинна бути своя персональна унікальна ключова пара до даного засекреченого файлу. Адже він один і той самий для кожного користувача. В таких випадках використовуються так звані цифрові конверти.

Як видно з рис. 1.9, цифровий конверт містить дані, зашифровані за допомогою випадково сформованого симетричного ключа, а також декілька копій

цього симетричного ключа, захищених відкритими асиметричними ключами кожного користувача. Примірників буде стільки, скільком користувачам буде надано доступ до захищеної папки.

Рисунок 1.9 – Схема прозорого шифрування

Принцип роботи прозорого драйвера шифрування полягає в тому, що коли користувач звертається до файлу, він перевіряє наявність сертифіката (відкритого ключа) у списку дозволених. Якщо так, то із закритим ключем цього користувача розшифровується та симетрична копія ключа, яка була зашифрована відкритим ключем даного користувача. Якщо в цей користувач не перебуває в даному списку, йому буде відмовлено в доступі.

Наведемо основні переваги криптографії:

- цілісність даних. Використовуються криптографічні хеші для підтримання цілісності повідомлень;
- автентифікація. Повідомлення, підписані цифровим підписом або зашифровані приватними ключами, підтверджують особистість;
- конфіденційність. Захищеність від несанкціонованого доступу;

- перевірка достовірності.

1.3.4. Метод ЕЦП

При обміні електронними документами через комп'ютерну мережу значно зменшуються витрати на обробку та зберігання документів, їх пошук прискорюється. Але з іншого боку, використовується проблема автентифікації автора електронного документа та самого документа, а саме встановлення дійсності автора та відсутності змін в отриманому електронному документі.

Захист від можливих зловмисних атак і є метою автентифікації. Наведемо декілька видів можливих атак:

- маскарад – користувач Х, від імені користувача А, відправляє документ користувачу Б;
- підміна – користувач Б формує чи змінює документ і вказує, що отримав його від користувача А;
- активний перехват – користувач, підключається до мережі, перехоплює документи та змінює їх;
- повтор – користувач Х повторює раніше відправлений документ, який користувач А відпраавляв користувачу Б.

Такі зловмисні дії можуть завдати значної шкоди банківським та комерційним струтурам, державним підприємствам та інше.

Електронний цифровий підпис - це один із видів електронного підпису, який отримується завдяки криптографічному перетворенню набору електронних даних, який логічно поєднується або додається до цього набору та дозволяє ідентифікувати користувача, який підписав його, й підтвердити цілісність. Електронний цифровий підпис сформовується за допомогою закритого ключа, а перевіряється за допомогою відкритого.

Підписувач - це особа, яка легально управляє приватним ключем від імені особи, яку вона представляє або від особистого імені, накладає електронний цифровий підпис на створенний електронний файл.

Приватний ключ - параметр криптографічного алгоритму, доступний лише підписувачу.

Відкритий ключ – параметр криптографічного алгоритму, доступний всім користувачам, які є у сфері користування електронного цифрового підпису.

Документ, який підтверджує, що даний відкритий ключ належить підписувачу, видається центром сертифікації ключів і має назву сертифікат відкритого ключа.

Електронний цифровий підпис - порівняно невелика кількість додаткових даних, які передаються разом з текстом, який підписується. ЕЦП сформована на оборотності асиметричних шифрів, взаємозв'язку змісту повідомлення, пари ключів та самого підпису. Якщо змінити хоча б один з цих елементів, то стане неможливим підтвердження справжності цифрового підпису. Таким чином, електронний документ набуває юридичного значення завдяки електронному цифровому підпису.

ЕЦП має дві основні процедури:

- процедура формування цифрового підпису;
- процедура перевірки цифрового підпису.

Для проведення першої процедури використовується приватний ключ, а для процедури перевірки цифрового підпису – використовується відкритий ключ. Цифрові підписи часто використовують асиметричну криптографію. Хоча, вони і вирішують різні завдання: асиметричне шифрування – забезпечує конфіденційність повідомлення, ЕЦП – автентичність відправника та цілісність повідомлення. Електронний документ,який містить в собі ЕЦП, підтверджує цілістність переданих данних та відповідає за автентифікацію відправника.

Для ведення фінансових операцій можна використовувати електронні підписи, також їх часто використовують для розповсюдження програмного забезпе-

чення, формування бюджетних та податкових звітів, а також для виявлення фальсифікацій.

ЕЦП зазвичай містить додаткові дані, з допомогою яких ідентифікується підписаний документ. Такі дані додаються до документа до самого визначення ЕЦП, що забезпечує їхню цілісність. Кожний підпис, який розміщений у файлі містить:

- ім’я відкритого ключа;
- дату підписа;
- дані про особу, яка підписала;
- термін дії ключа підпису;
- і сам цифровий підпис.

1.4. Висновки

У першому розділі розглядаються методи шифрування даних та їх особливості. Сформовано основні переваги криптографії як методу захисту конфіденційної інформація. Основні недоліки симетричного і асиметричного алгоритму: якісні симетричні алгоритми є швидшими за якісні асиметричні алгоритми; недоліком симетричних алгоритмів є те, що потрібно мати секретний ключ по обидва боки передачі інформації. Наведено основну інформація про алгоритми шифрування, які будуть використовуватися в магістерській.

РОЗДІЛ 2. ПРОГРАМА ДЛЯ ШИФРУВАННЯ ФАЙЛІВ

CyberSafe Top Secret – це програмне забезпечення з підтримкою криптографії, яка забезпечує захист ваших даних від несанкціонованого доступу. Функціонал CyberSafe надає можливість вирішити безліч варіантів завданнь в галузі інформаційної безпеки. Основні фунціїї даної програми описано нижче:

- цифровий підпис. Функція створення цифрових підписів на файли із використанням закритого ключа, а також перевірка підпису за допомогою відкритого ключа;
- сертифікаційний центр. Додаток CyberSafe Certificate Authority надає можливість для зберігання, створення та обробки сертифікатів, який використовується для шифрування електронної пошти;
- прозоре шифрування. Функція, яка надає можливість зручної роботи з зашифрованими файлами – всі операції з розшифруванням та шифруванням файлів виконуються автоматично.
- шифрування файлів. Функція, яка надає можливість шифрувати будь-який файл або декілька файлів для зберіганя на персональному комп'ютері або пересилання іншим користувачам. Шифрування може виконуватися на основі відкритих ключів (PKI) або з використанням пароля. Дешифрувати файли можна лише з допомогою комп'ютера на якому встановлено CyberSafe;

2.1. Огляд та принцип роботи програми: CSTS

CyberSafe Top Secret – програма захисту даних, яка використовує найсучаніші на сьогоднішній день алгоритми шифрування (RSA, AES, тощо). Це програмне забезпення має чудовий функціонал, що дозволяє працювати з програмою у всіх сферах роботи з інформацією: захист електронної інформації, захист конфіденційної пошти, перевірка та створення ЕЦП.

CyberSafe Top Secret базується на інфраструктурі відкритих ключів (PKI – Public Key Infrastructure). Можливості програми: створення зашифрованого віртуального диску будь-якого розміру, шифрування розділів жорсткого диска та зашифрування файлів на комп'ютері користувача. Функції CyberSafe дозволяють керувати ключами та сертифікатами.

Переваги даної програми:

- відмінною рисою від інших програм є власний сервер відкритих ключі для обміну та публікації ключами;
- функція, яка надає можливість прозорого шифрування;
- програма має можливість підписувати файли та підтримує функцію перевірки електронно-цифрового підпису;
- драйвер CyberSafe дозволяє працювати в мережі, яка надає можливість реалізації корпоративного шифрування;
- користувач має можливість обмежити доступ до зашифрованих файлів іншим додаткам. Здійснення такої функції надає система довірених додатків;
- включаючи двофакторну автентифікацію – користувач отримує можливість організувати надійніший захист;

2.2. Створення сертифікату

Для того, щоб створити сертифікат користувача, потрібно перейти до відповідного розділу: Сертифікати та ключі → Особисті ключі → Створити.

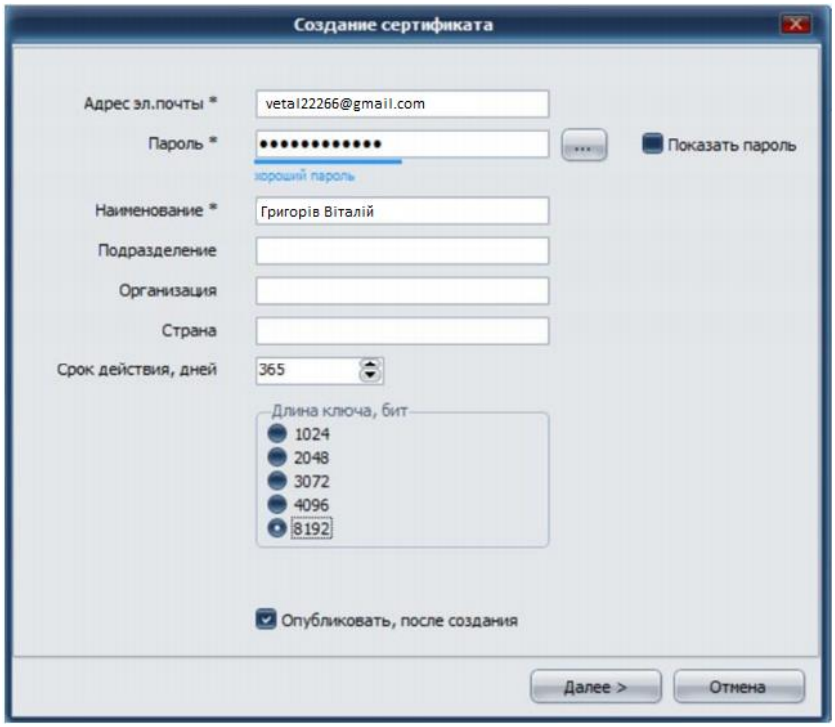


Рисунок 2.1 – Створення сертифікату

Обов’язкові поля відмічені символом *. У полі *Адреса ел. пошти*, потрібно ввести свою дійсну адресу електронної пошти – куди буде надісланий код, який необхідний для того, щоб опублікувати сертифікат на сервері CyberSafe.

Програма сгенерує приватний ключ сертифікату користувача, він буде захищений паролем, який прийде на пошту; цей пароль потрібно буде ввести, при включені папки, яка буде захищена функціями прозорого шифрування, або, якщо потрібно, експортувати приватний ключ в окремий файл.

Після цього проходить процес генерування ключів сертифіката, по закінченню якого на вказану вами електрону пошту буде надіслано код підтвердження, який потрібно ввести у поле зображене на рис. 2.2. Після цього ваш сертифікат буде опубліковано на сервері програми.

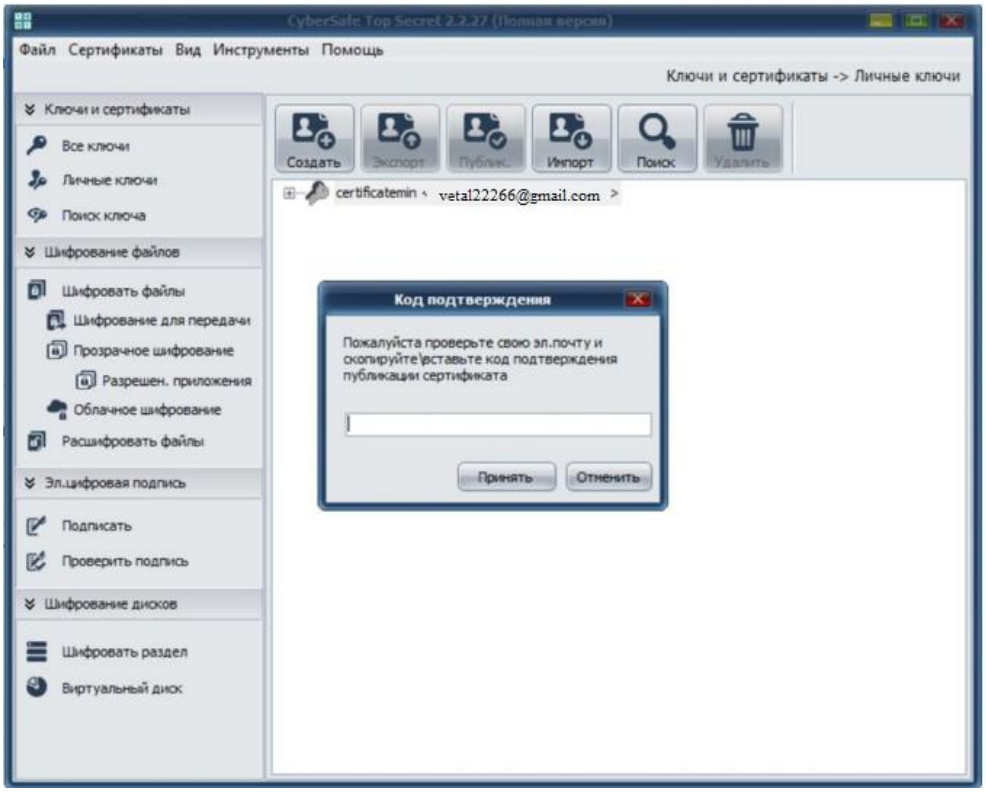


Рисунок 2.2 – Підтверджена публікація сертифікату

Після того, як пароль був підтверджений, процедура публікації сертифікату рахується завершеною. Кінцевий результат можна побачити на рисунку 2.3.

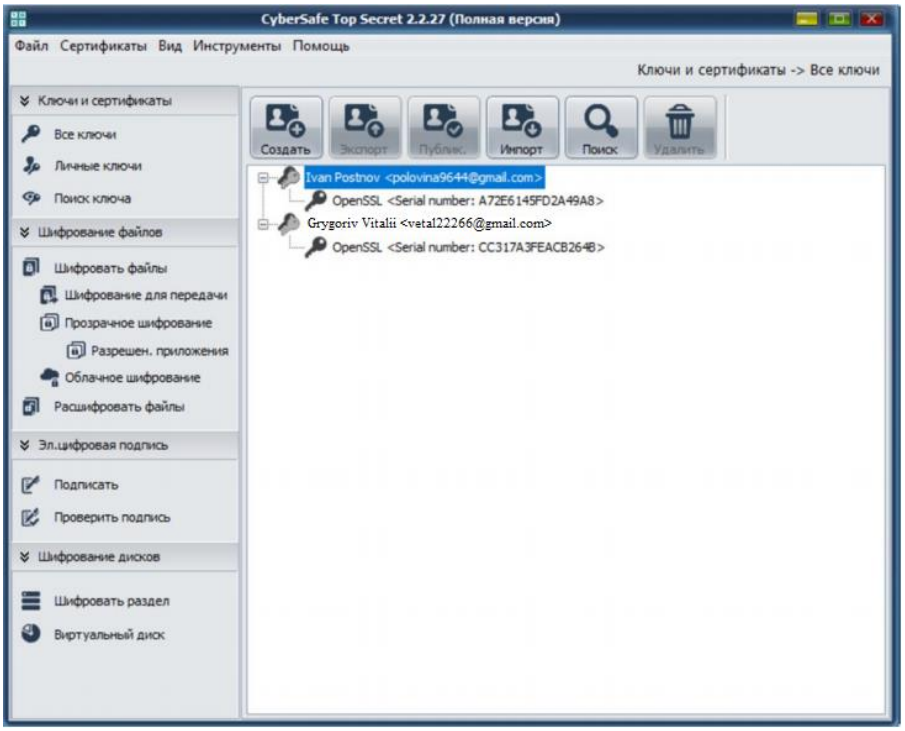


Рис.2.3 – Опубліковані сертифікати

Час створення сертифікату з більшою довжиною ключа (192 біт) становив 1хв. 05 секунд, з меншою довжиною ключа (124 біт) становив 35 сек.

2.3. Алгоритми шифрування

2.3.1. Шифрування файлів

Для захисту файлів від доступу сторонніми користувачами часто використовують шифрування. Шифрування файлів є корисним: для забезпечення конфіденційного зберігання на власному комп'ютері або для відправки іншому користувачу.

За допомогою CyberSafe ви можете шифрувати файли для їхнього передавання іншим користувачам трьома способами: використовуючи шифрування паролем, на основі сертифікатів (ключі), або створити зашифрований zip-архів, який сам розпаковується.

Якщо ви хочете зашифрувати файли для їх подальшої відправки іншим користувачам, вони будуть зашифровані за допомогою відкритих ключів користувачів, яким ви і будете відправляти ці файли. Для виконання даних дій ви повині мати зв’язву сертифікатів користувачів в CyberSafe. Якщо у вас немає сертифікату будь-якого користувача, то ви можете, за допомогою функції пошуку, спробувати знайти його на сервері відкритих ключів CyberSafe по електронній пошті користувача.

Також можна визначити дві важливі особливості програми: систему довірених додатків та двофакторну авторизацію. У налаштуваннях програми є можливість встановити двофакторну автентифікація або автентифікацію за допомогою пароля.

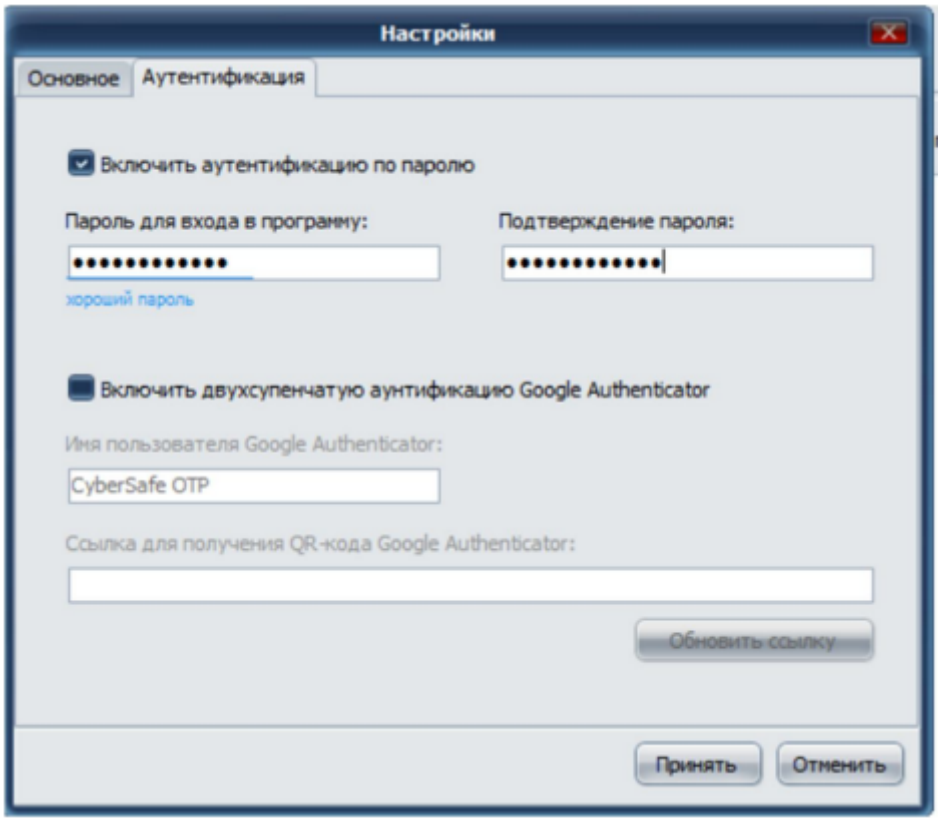


Рисунок 2.4 – Автентифікація користувача

2.3.2. Шифрування на основі ключів (сертифікатів)

Часто даний тип шифрування використовується:

- коли ви не хочете повідомляти пароль надісланого файлу;
- для того, щоб забезпечити найвищий рівень захисту файлів;
- для шифрування файлів для подальшого особистого користування, а також для обмінюватися файлами з користувачами, у яких є в наявності програма CyberSafe на комп'ютері і ви маєте на зв'язці відкриті ключі даних користувачів;

З метою зашифрування файлу для його подальшої безпечної передачі, користувач повинен вибрати *Шифрування файлу → Шифрування для передачі одержувачам*:

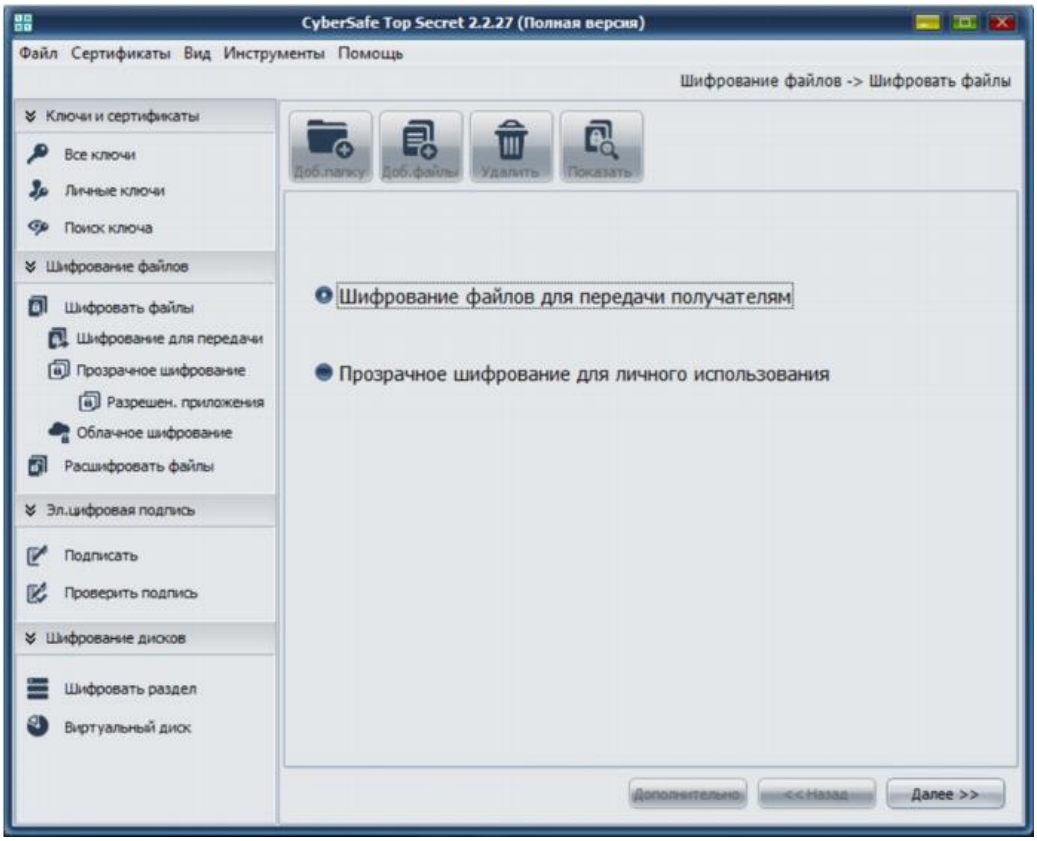


Рисунок 2.5 – Вкладка Шифрування файлів

Далі добаляємо файл, який потрбіно зашифрувати рис. 2.6.

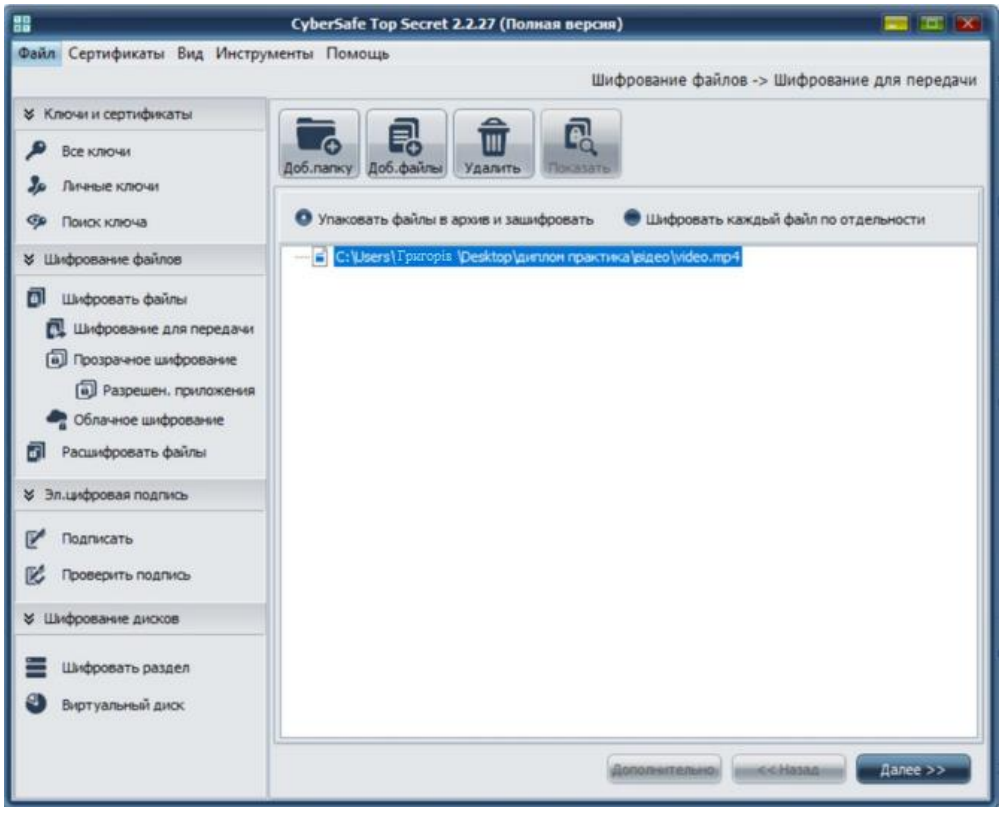


Рисунок 2.6 – Обраний файл

В наступному вікні вибираємо *Зашифрувати файли ключами одержувачів* та вибираємо *Далі:*

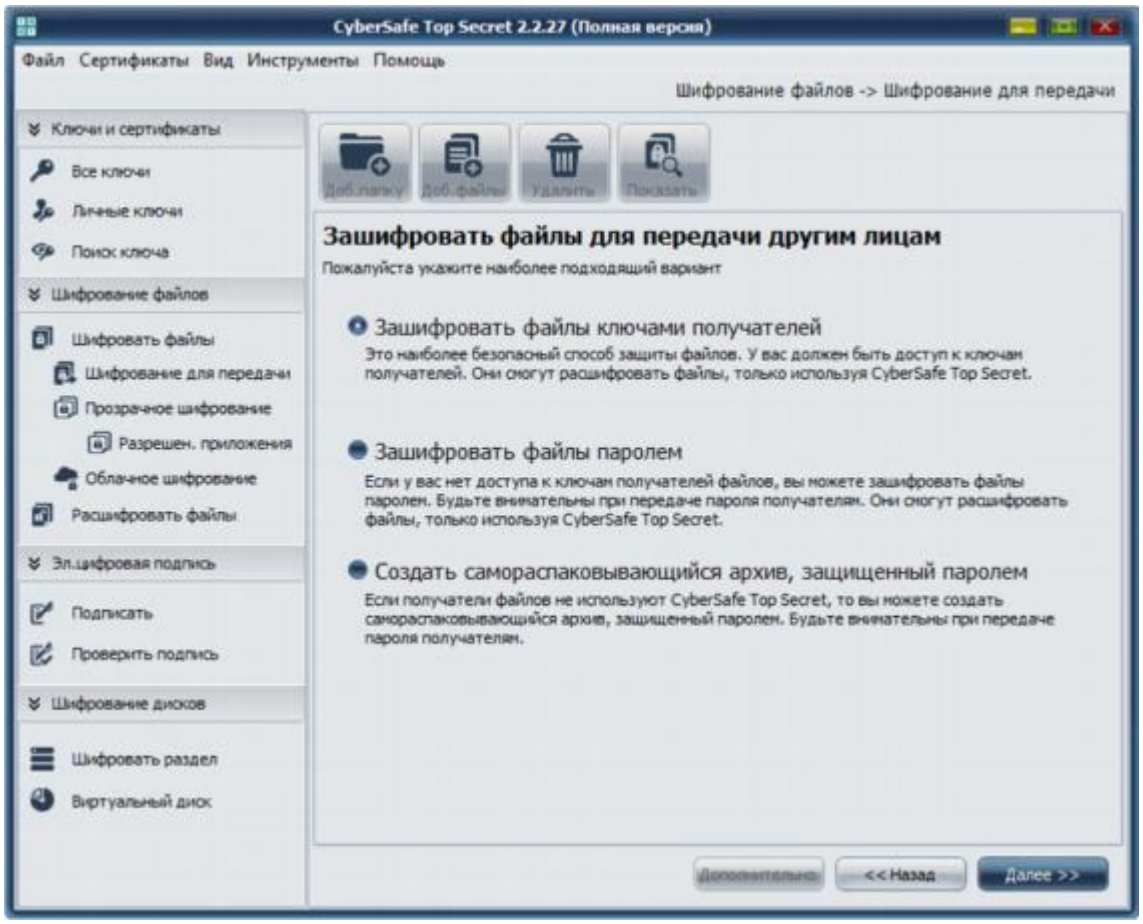


Рисунок 2.7 – Варіанти шифрування

Далі зі списку вибираємо користувачів, ключами яких ми будемо зашифровувати файли.

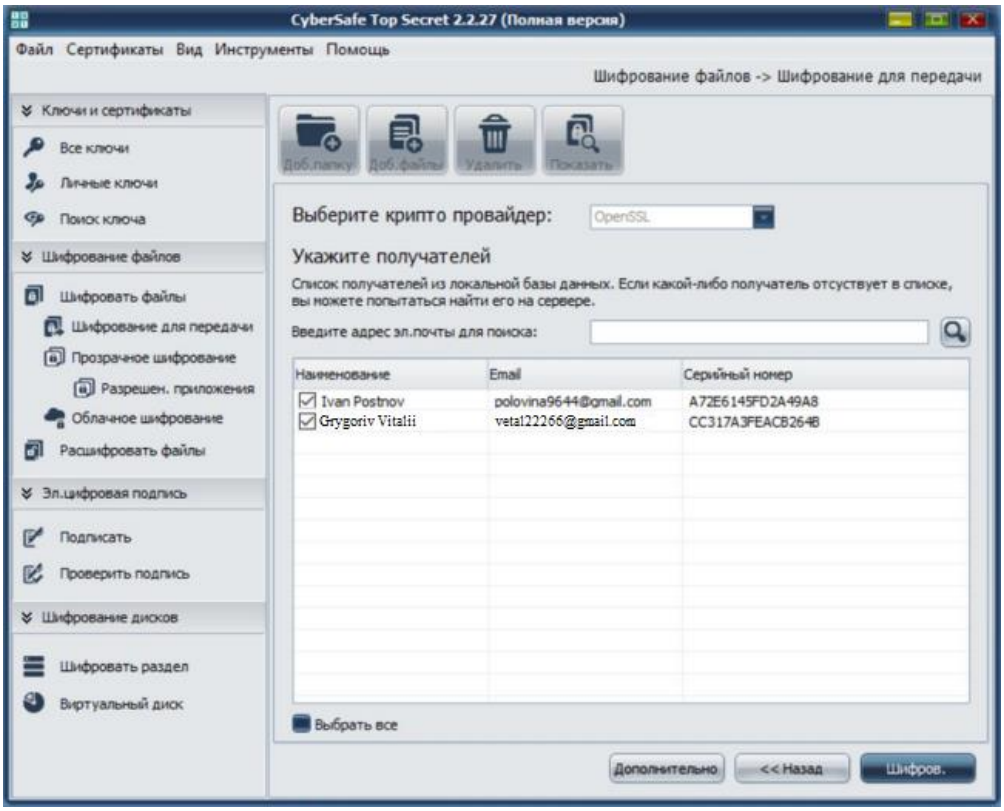


Рисунок 2.8 – Список доступних користувачів

Перед натисканням кнопки *Шифрувати*, коли у вас є вибір методу шифрування (пароль, на основі сертифікатів або зашифрований архів), ви можете скористуватися додатковими функціями у вікні додаткових налаштувань натиснувши *Додатково*:

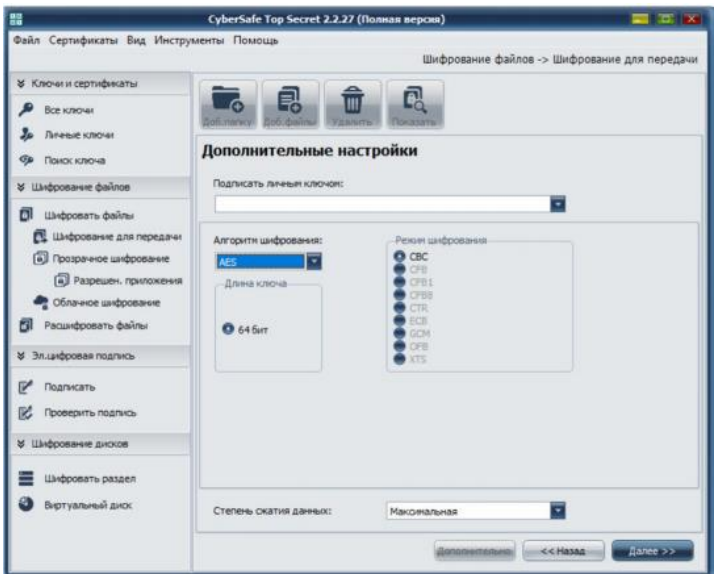


Рисунок 2.9 – Вікно додаткових налаштувань

У даному вікні ви маєте змогу:

- вказати наскільки ви хочете стиснути файл;
- змінити алгоритм шифрування за замовчуванням, довжина ключа;
- вибрати приватний ключ для цифрового підпису файлу (у разі шифрування відкритим ключем);

Процес шифрування розпочнеться, як тільки клацнете *Шифрувати*. По завершенню процедури буде дане вікно:

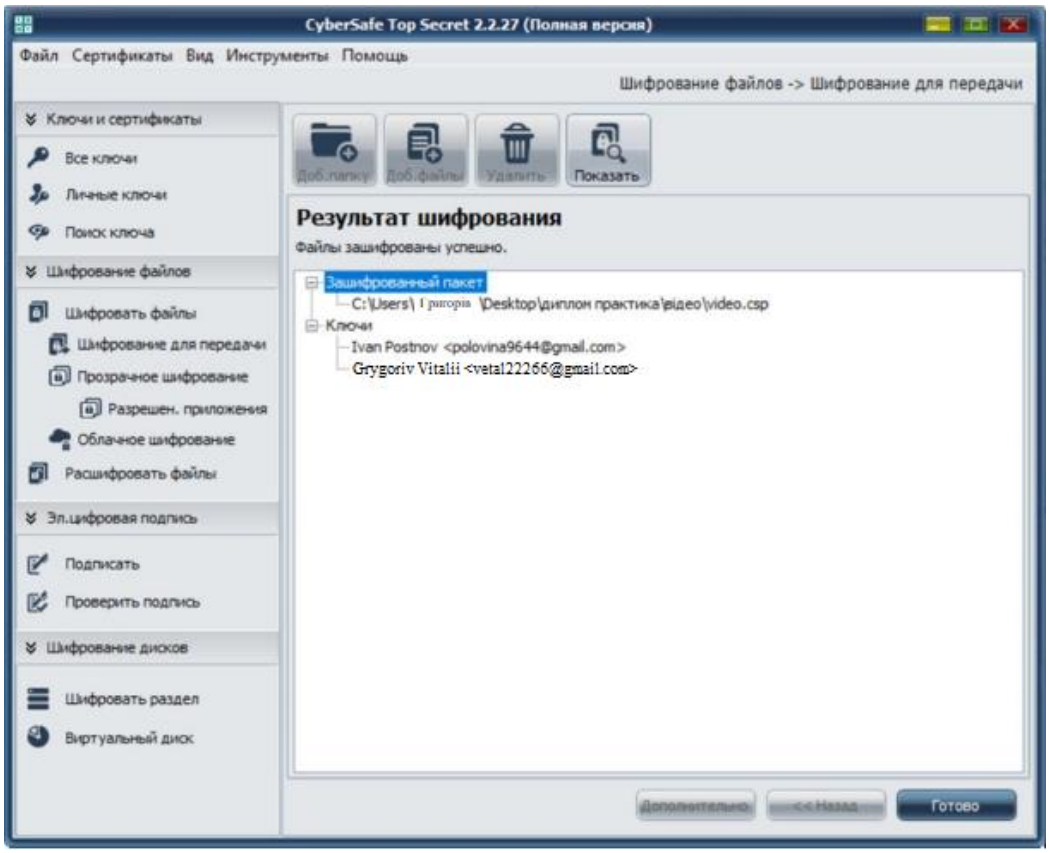


Рисунок 2.10 – Результат шифрування

Як тільки необхідні файли будуть зашифровані, вони можуть бути відправленими іншим користувачам. Після отримання файлів користувач розшифровує їх з використанням програми CyberSafe та його приватного ключа. Файли мають змогу розшифрувати всі отримувачі, чиї відкриті ключі ви використовували коли шифрували. В результаті кожен користувач отримує однаковий файл.

Якщо ви надсилаєте файл іншому користувачеві, зашифруйте його на основі відкритих ключів - найкраще рішення, яке прийнято вибирати першим можливим, якщо вам потрібен найвищий рівень безпеки й ви володієте всім для цього необхідним. Цей метод шифрування має змогу шифрувати дані з довжиною асиметричного ключа аж до 256 біт.

2.3.3. ЕЦП – електроний цифровий підпис

Ви також можете використовувати програму для електронного підпису файлу та перевірки цих підписів. Якщо вам потрібно створити цифровий підпис, тоді перейдіть до *Електронний цифровий підпис → Підпис*. Коли файл вибраний вам буде запропонований варіант *шифрування файлів ключами одержувачів*.

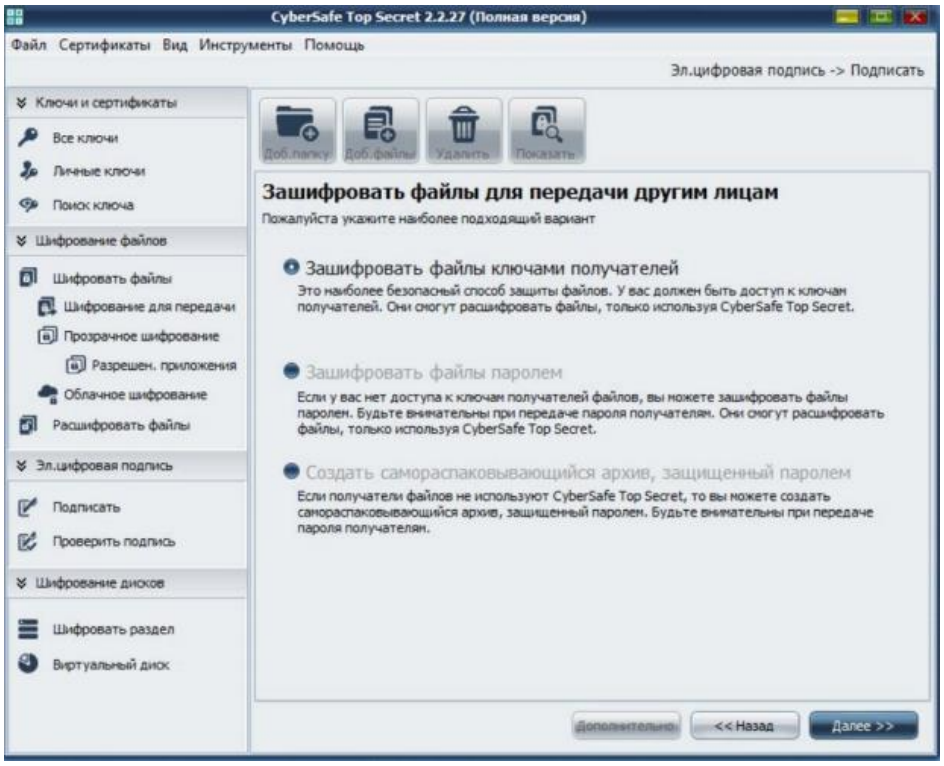


Рисунок 2.11 – ЕЦП

Як тільки ви оберете ключі одержувачів, які будуть мати можливість доступу до зашифрованого файлу, потрібно вибрати приватний ключ для цифрового підпису файлу, довжину ключа, алгоритми шифрування та стиснення файлів.

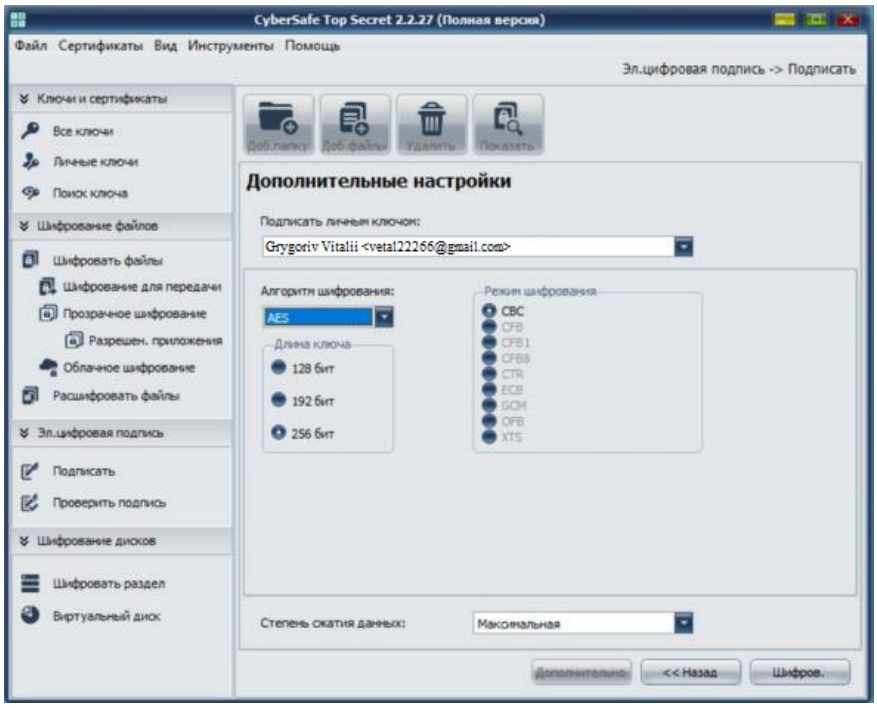


Рисунок 2.12 – Вкладка меню з даним типом шифрування

Ви повинні підтвердити електронний цифровий підпис перед шифруванням файлу за допомогою пароля сертифікату. Після підтвердження пароля, шифрування файлів розпочнеться автоматично.

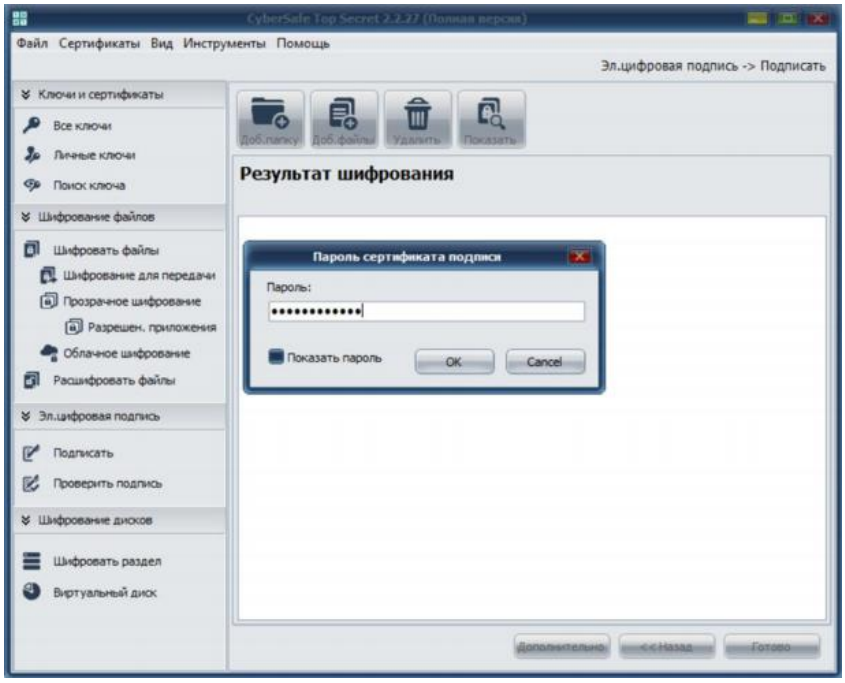


Рисунок 2.13 – Підтвердження ЕЦП

Коли шифрування завершено у розділі *Зашифрований пакет* відображатиметься шлях до файлів, які були зашифровані. Розділ *Ключі* буде вміщувати користувачів, відкриті ключі яких використовувалися для шифрування. Розділ *Підпис* міститеме сертифікат, приватний ключ якого було використано для створення цифрового підпису.

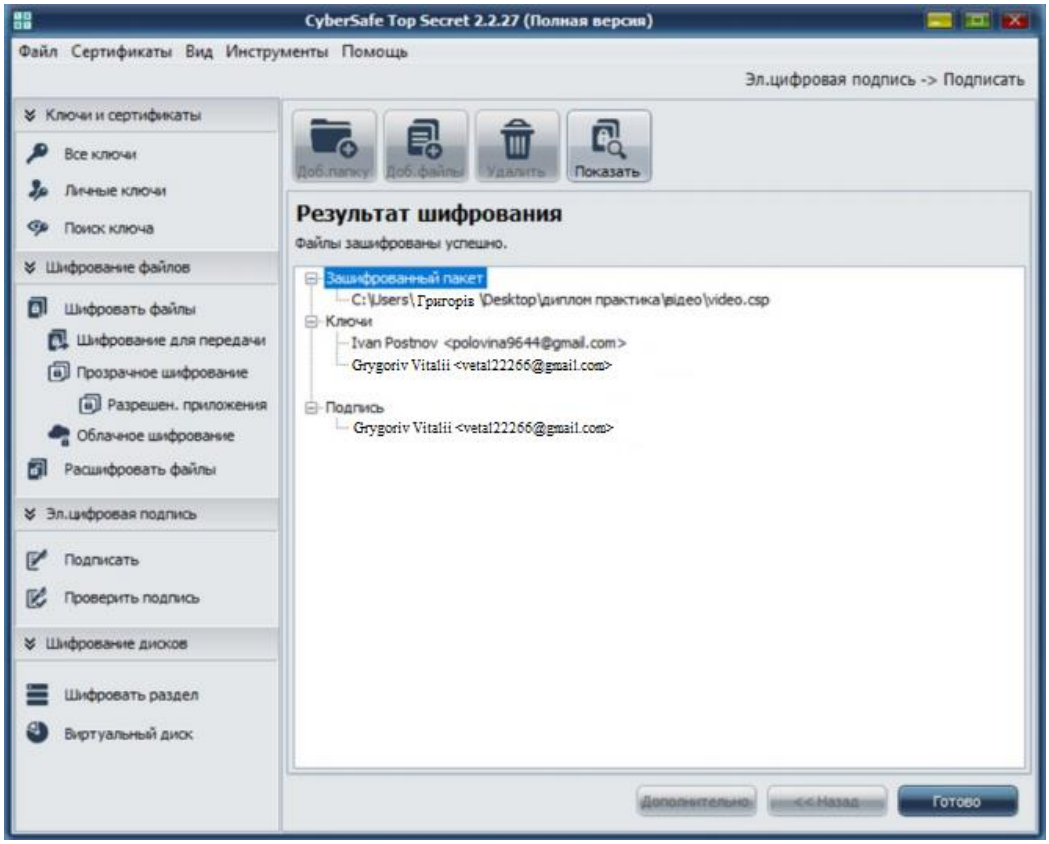


Рисунок 2.14 – Результат даного типу шифрування

2.4. Шифрування файлів

Шифрування інформації допомагає зберегти її конфіденційність, але в той же час привертає занадто багато уваги. Якщо користувач спробує приховувати дані за допомогою шифрування, тоді напевно щось в них є важливе. І тому іноді важливіше приховати саме існування інформації, ніж просто її зашифрувати.

На сьогоднішній день активно набирають популярності комбінаторні методи, які часто використовується в декодуваннях та кодуваннях різних типів інформації.

Для приховування файлу у графічний, текстовий формат чи звуковий файл, без особих зусиль та спеціальних знань, дозволяє стеганографія.

2.4.1. Процес шифрування зображення

Щоб зашифрувати зображення, вибираємо довжину ключа 128 біт, алгоритм шифрування AES і максимальну ступінь стиснення. Використовуємо приватний ключ, у якого мінімальна довжина складає 128 біт, для цифрового підпису.

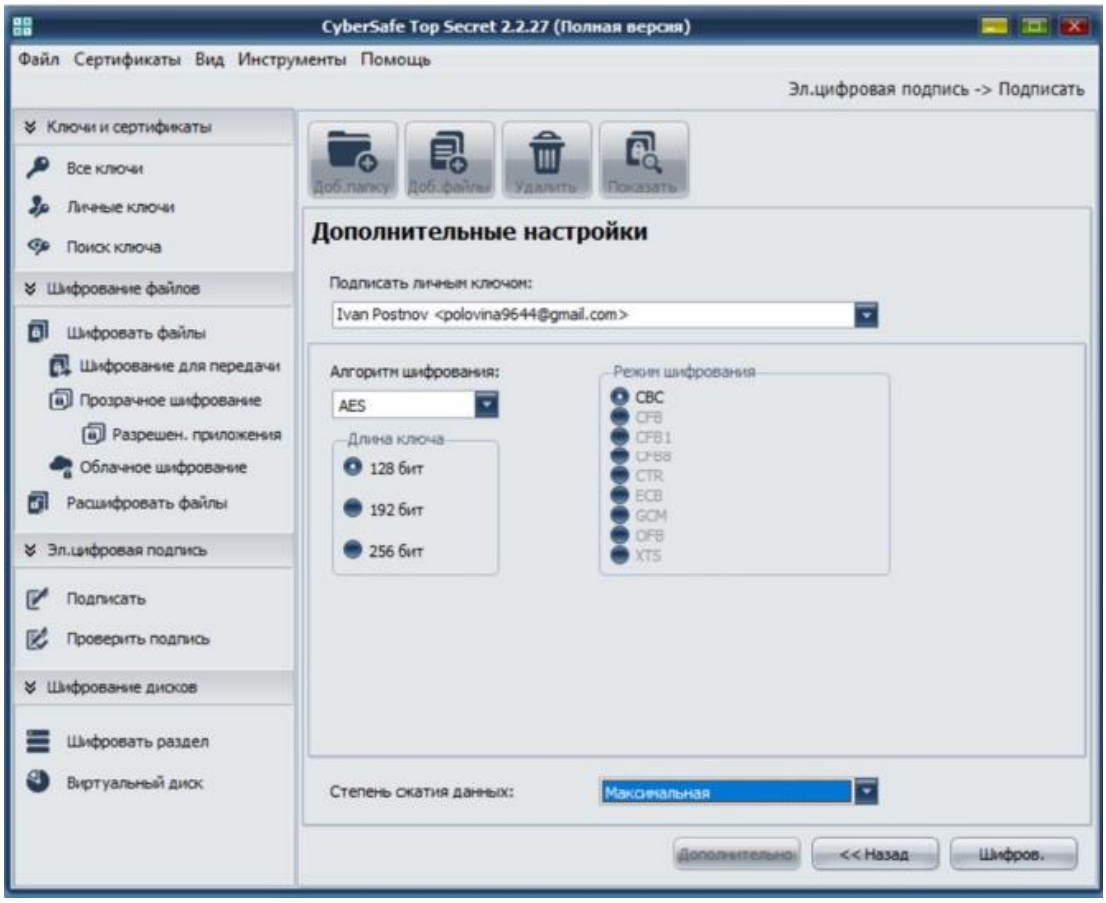


Рисунок 2.15 – Параметри шифрування

Розмір файлу 2,2 Мб. Час шифрування зображення – 7.16 секунд.

Нижче показано результати даного шифрування. Рисунок 2.21 зображує вигляд фотографії до шифрування, на рисунку 2.22 текстовий представлений документ з текстовою інформацією фотографії для шифрування.

Рисунок 2.16 – Зображення до шифрування

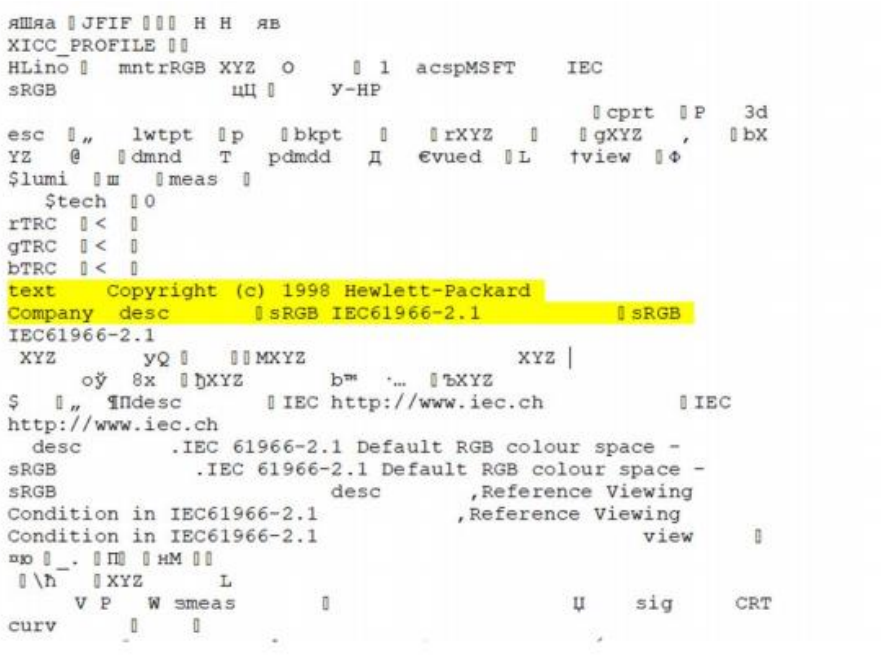


Рисунок 2.17 – Тестовава інформація зображення до Шифрування

Результат зашифрованого тесту інформації зображення можна побачити на рисунку 2.18.

Рисунок 2.18 – Результат шифрування

Вибрана інформація в зашифрованому документі показує зовсім інший номер локального ідентифікаційного ключа, тому що для шифрування зображення було створено електронний цифровий підпис, з допомогою сертифікату з мінімальною довжиною ключа (128 біт).

2.4.2. Процес шифрування звукового файлу

При різних типах шифрування аудіоінформація перетворюється на числову формулу і кодується в наборі нулів і відтворюється, та має деякий універсальний вигляд. Універсальність подання таких даних надає файлам додаткової переваги в посиленні криптографічної стабільністості алгоритмів шифрування, адже тяжко визначити яка саме інформація представлена в шифрі: текст, зображення, музика

або відео. Запропонований спосіб шифрування аудіоінформації можна використовувати для різних цілей, зокрема:

- приховання тематики розмови, яка ведеться і т.д. В даний час такий спосіб часто використовується в сучасних месенджерах (Viber, WhatsApp, Telegram та ін.).
- приховування самого змісту веденої розмови.

Наприклад, вибераємо аудіофайл, який має розширення .flac та розмір, якого складає 39 Мб. Відкриваємо даний файл з допомогою текстового редактора. На рисунку 2.19 зображено аудіофайл до шифрування.

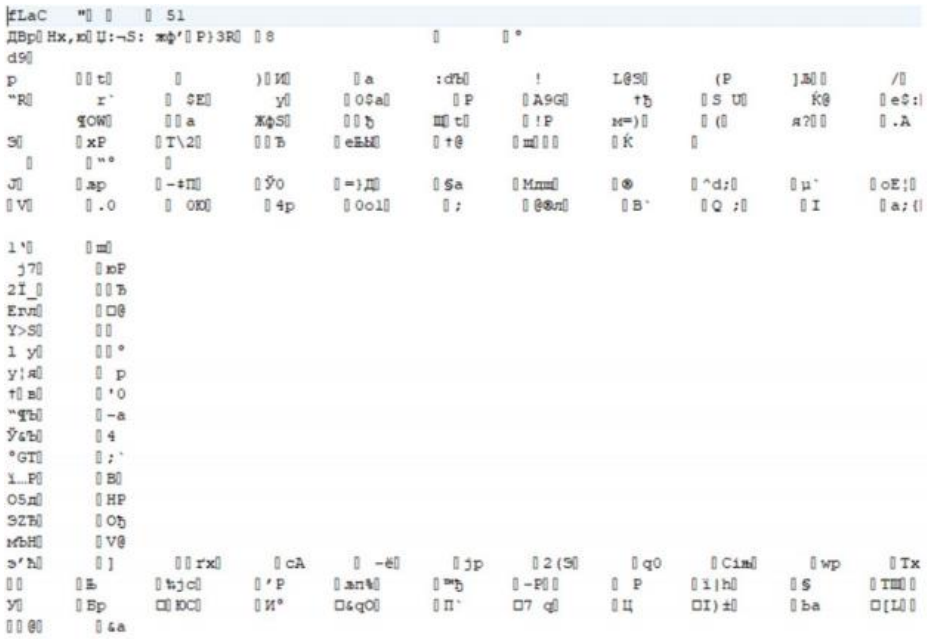


Рисунок 2.19 – Аудіофайл до шифрування

Використовуючи програми CSTS, ми шифруємо аудіофайл. Шифрувати його ми будемо за домогою алгоритма AES (128 біт) використовуючи метод ЕЦП з мінімальним ключем. Час шифрування аудіофайлу склав 26,34 секунди. Зашифрований файл відкриємо за допогою текстового редактора для порівняння з оригіналом рис.2.10.

Рисунок 2.20 – Зашифрований файл

По закінченню шифрування розмір файлу збільшився на 53 кб, одже даний аудіофайл захщено з допомогою ключа шифрування.

2.4.3. Процес шифрування відеофайлу

Щоб зашифрувати відеофайл, вибераємо алгоритм шифрування DES, режим шифрування – CBC, довжина ключа шифру становить 64 біти, і ступінь стиснення файлу – максимальний. Підписуємо даний файл власним ключем, довжина якого максимально становить – 256 біт.

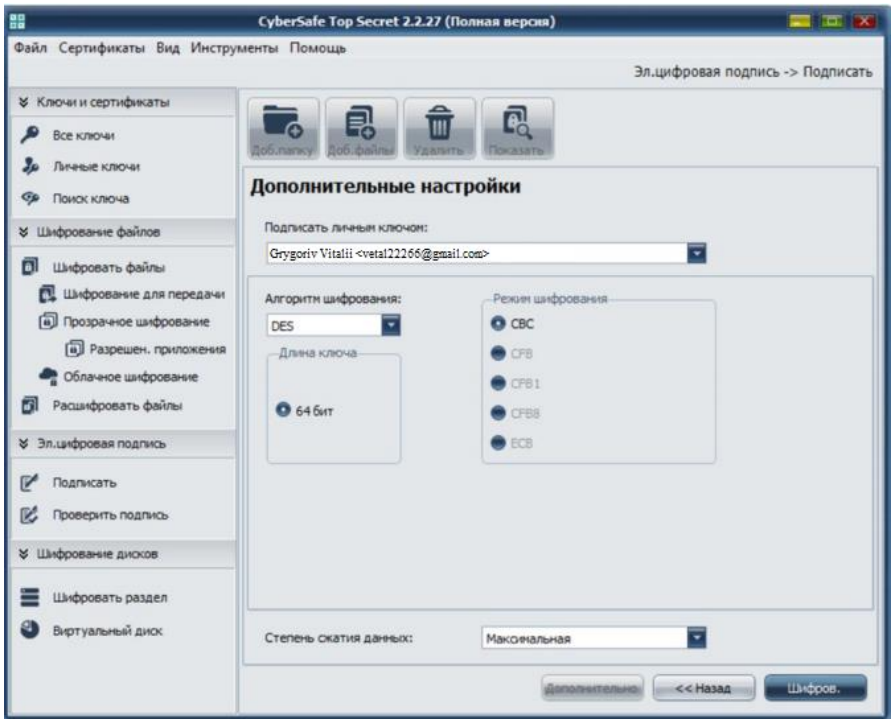


Рисунок 2.21 – Вікно з додатковими налаштуваннями

Файли зашифровано успішно. Шифрування тримало 37.92 сек. Данні після завершення процедури зображено на рис.2.22.

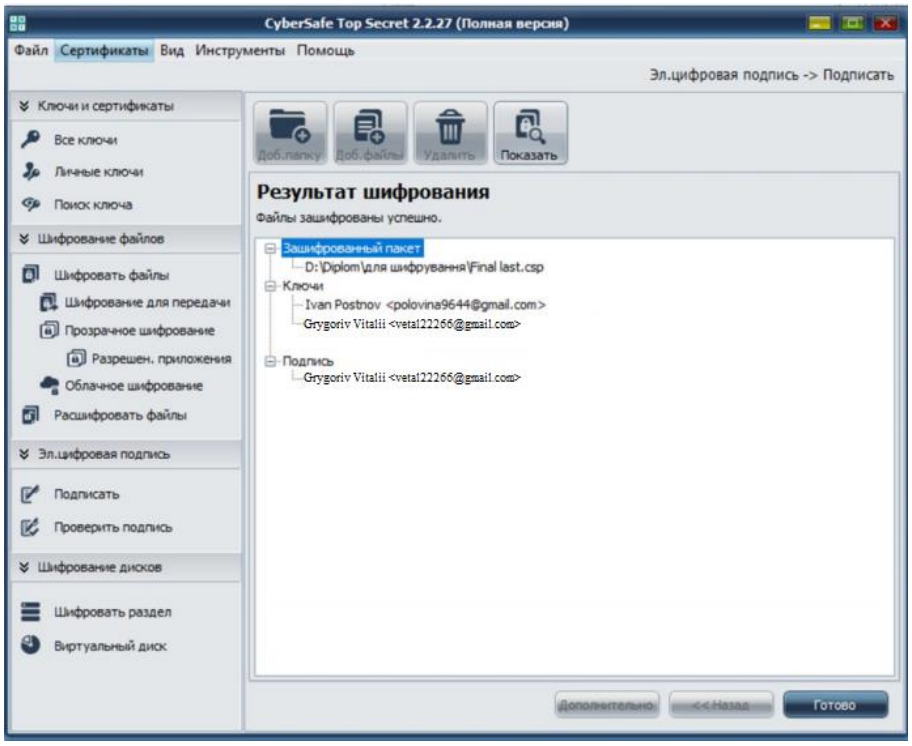


Рисунок 2.22 – Дані шифрування

Відеофайл до шифрування, відкритий за домогою текстового редактора, зображено на рисунку 2.23.

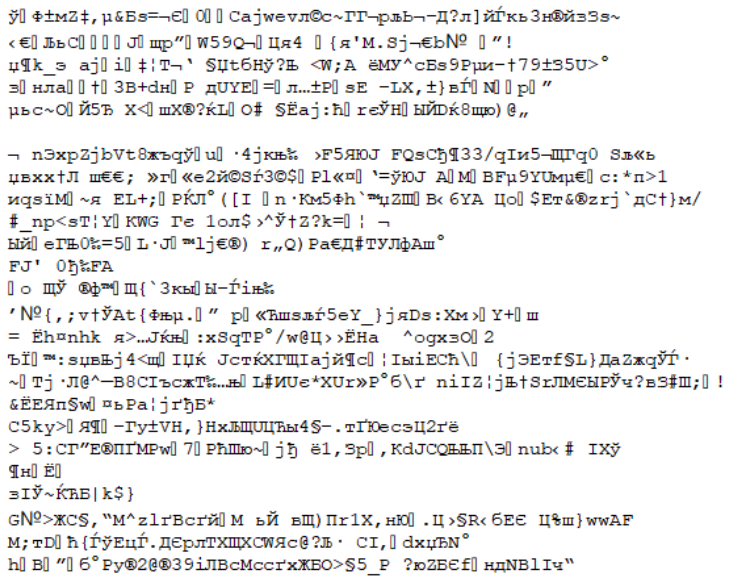


Рисунок 2.23 – Відеофайл до шифрування

На рис. 2.24 вже можна побачити відеофайл у зашифрованому вигляді з електронним цифровим підписом.

Рисунок 2.24 – Готовий зашифрований відеофайл

Після шифрування розміру відеофайл складав 32,27 МБ, а до шифрування - 32,37 МБ – документ зменшився на 10 байт.

На рисунку 2.24 показано виділену текстову інформацію, яка вказує на наявність локального ідентифікаційного ключа, за його допомогою був створений електронний цифровий підпис(ЕЦП). В цій частині вказане ім'я, програма та електронна адреса сертифікату, який використовувався для шифрування відеофайлу.

2.5. Порівняння характеристик алгоритмів шифрування

Використовуючи діаграму ми можемо порівняти швидкості алгоритмів шифрування, користуючись різними методами шифрування та параметрами. Для цього буде користуватися відеофайлом, розмір якого складає 77,3 Мб і ми використовуємо різні типи шифрування:

- метод ЕЦП;
- шифрування файлу паролем;
- метод шифрування файлу використовуючи відкриті ключі користувачів.

Діаграми дають можливість порівняння результати алгоритмів шифрування на час між собою. Max comp.– максимальне стиснення файлів, в свою чергу min comp. – мінімальне стиснення. Вертикальна вісь графіка – це час шифрування файлів. По горизонталі – алгоритми шифрування, що використовується в ході проведення експерименту з максимальнимим та мінімальними довжинами ключів.

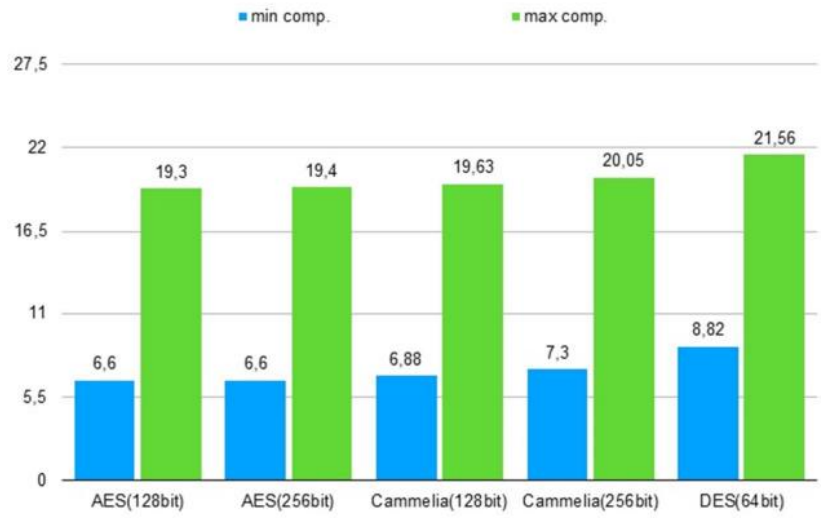


Рисунок 2.25 – Метод шифрування ЕЦП

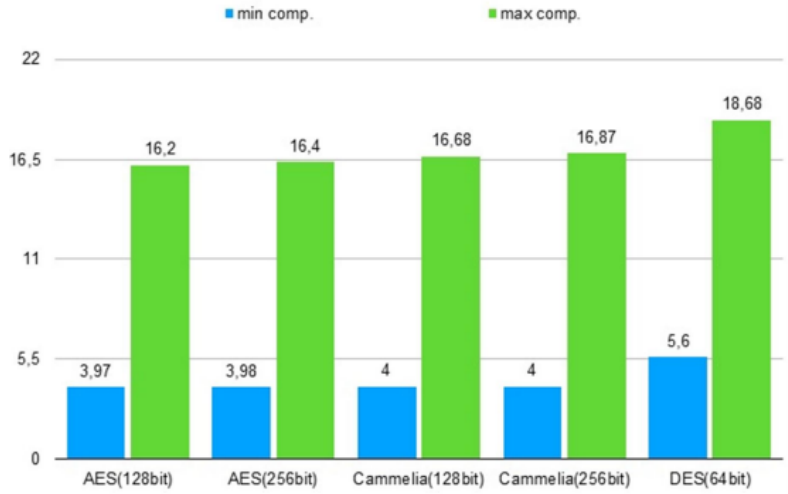


Рисунок 2.26 – Шифрування паролем

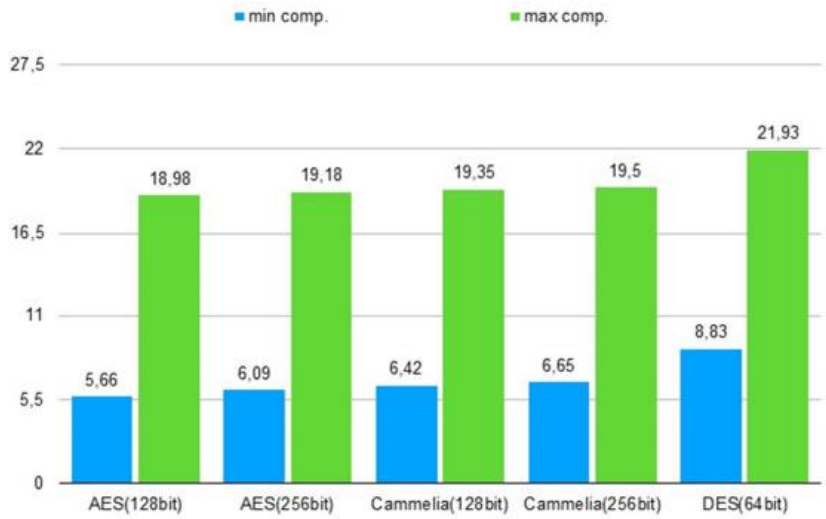


Рисунок 2.27 – Шифрування відкритими ключами користувачів

Діаграма надає нам можливість побачити, що метод шифрування AES з довжиною ключа 128 біт є найнадійнішим та найкращим алгоритмом з тих, які представлено на рисунках 2.25-2.27.

2.6. Висновки

В даному розділі було оглянуто принцип роботи програми CyberSafe, де використовуються сучасні алгоритми шифрування. Було показано практичне застосування основних методів шифрування різних типів файлів та показані переваги у використанні програми.

На основі результатів аналізу було зроблено висновок про те, що представлені алгоритми є зручними при використовувані їх для шифрування аудіо-, відеофалів, зображення та текстових документів для підвищення безпеки даних. По закінченню аналізу було обрано найбільш надійний та швидкий алгоритм – AES (128 біт).

РОЗДІЛ 3. ВІДПРАВЛЕННЯ ЗАШИФРОВАНИХ ФАЙЛІВ ПО КОМУНІКАЦІЙНИХ СИСТЕМАХ

Для того, щоб перевірити ефективність шифрування було проведено дослідження, сенс якого полягає в підрахунку пакетів переданих даних перед шифруванням і після.

Передавати ми будемо декілька типів даних: відео (m2ts), зображення (.jpg), аудіо (.flac) та текстовий файл. Будемо використовувати файли до шифрування та після, для шифрування використали алгоритми (AES, DES, Camellia) з мінімальними та максимальними довжинами ключів. Надаємо перевагу методу шифрування ЕЦП з мінімальною довжиною ключа сертифікації.

В подальшому будемо використовувати три способи передачі інформації по комунікаційних системах:

- захищена передача даних на основі VPN;
- захищена передача даних на основі зміни IP (браузер Tor);
- незахищена передача даних (використовуючи відкритий http);

3.1. Захищена передача даних на основі VPN

Щоб передати зашифрований файл ми застосовуємо VPN для захищеної передачі даних. Для цього ми будемо використовувати програму для шифрування мережевого трафіку NordVPN.

NordVPN – це додаток, задача якого полягає в захисті інформації, використовуючи шифрування Інтернет-з'єднання. Шифрування з'єднання: 256-біт AES.

З допогою даної програми IP-адресу було змінено рисунок 3.1. Перевірити вже змінену адресу ми можемо на веб-сайті https://2ip.ua.

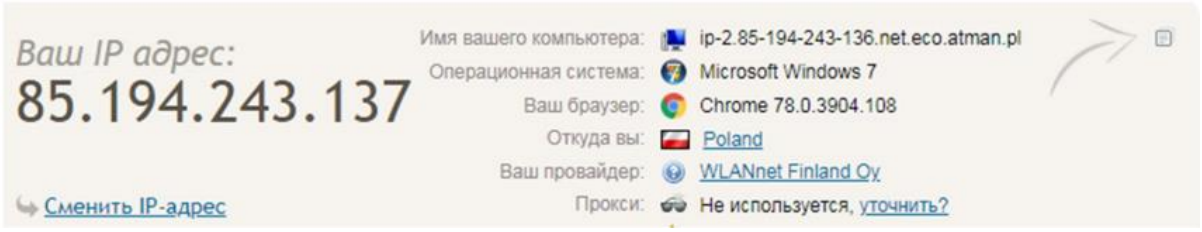


Рисунок 3.1 – Змінена IP-адреса з використанням програми NordVPN

Для відслідковування передачі пакетів зашифрованого файлу будемо використовувати програму PingPlotter – зручна та проста у використані програма для Windows, яка призначена для відстеження маршруту між вашим IP та будь-якою адресою, яка буде вказана користувачем, це може бути будь-який конкретний провайдер, сайт, або сервер. Даний продукт буде постійно збирати та зберігати інформацію про пакети, які було втрачено під час пересилання, після чого користувач може проаналізувати їх та вирішити ці проблеми.

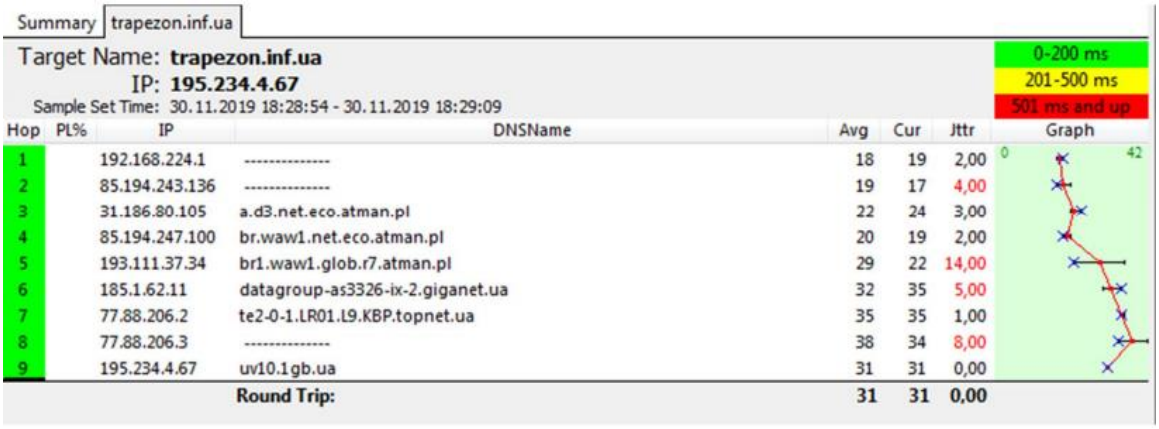


Рисунок 3.2 – Відстеження передачі даних

3.2. Захищена передача даних на основі зміни IP (браузер Tor)

Для зміни IP-адреси мережі, з якої будемо передавати наші дані, використаємо програму Tor. Даний продукт надає можливість для анонімного мережевого з’єднання з властивістю захисту від прослуховування. Має представлення ано-

німної мережі віртуальних тунелів, що забезпечує передачу даних у зашифрованому форматі.

Перший етап: заходимо у браузер Tor та, змінивши IP-адресу, створюємо нову ланку передачі на сайт.

Другий етап: перевіряємо змінену адресу, використовуючи сайт https://2ip.ua.

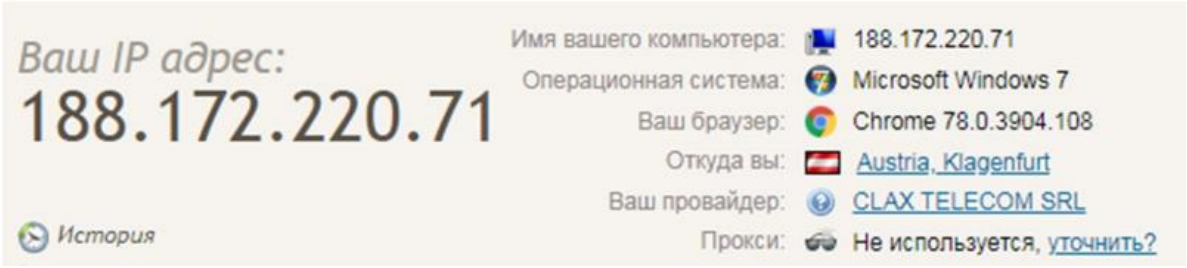
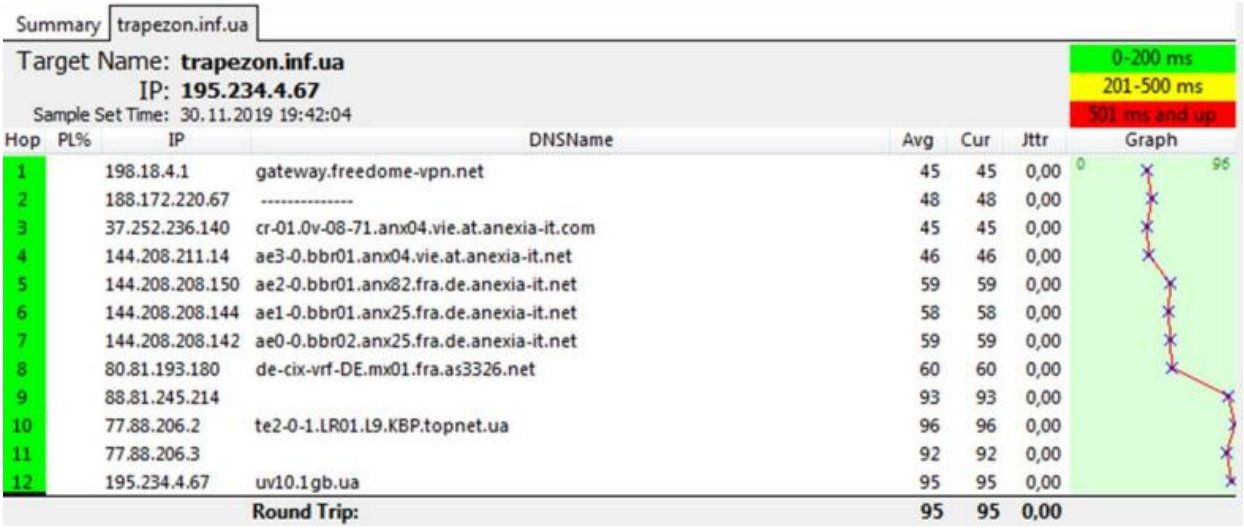


Рисунок 3.3 – Перевірка зміненого IP

Третій етап: коли IP-адреса змінено, заходимо у програму WinSCP для подальшої передачі файлу на сервер.

Четвертий крок: за домогою відомої нам програми PingPlotter ми будемо відслідковувати шлях нашого переданого файлу по мережі. На графіку будуть зображені точки, через які пройшов наш файл рисунок 3.4.



Hop	PL%	IP	DNSName	Avg	Cur	Jttr	Graph
1		198.18.4.1	gateway.freedome-vpn.net	45	45	0,00	
2		188.172.220.67	----------	48	48	0,00	
3		37.252.236.140	cr-01.0v-08-71.anx04.vie.at.anexia-it.com	45	45	0,00	
4		144.208.211.14	ae3-0.bbr01.anx04.vie.at.anexia-it.net	46	46	0,00	
5		144.208.208.150	ae2-0.bbr01.anx82.fra.de.anexia-it.net	59	59	0,00	
6		144.208.208.144	ae1-0.bbr01.anx25.fra.de.anexia-it.net	58	58	0,00	
7		144.208.208.142	ae0-0.bbr02.anx25.fra.de.anexia-it.net	59	59	0,00	
8		80.81.193.180	de-cix-vrf-DE.mx01.fra.as3326.net	60	60	0,00	
9		88.81.245.214		93	93	0,00	
10		77.88.206.2	te2-0-1.LR01.L9.KBP.topnet.ua	96	96	0,00	
11		77.88.206.3		92	92	0,00	
12		195.234.4.67	uv10.1gb.ua	95	95	0,00	
			Round Trip:	**95**	**95**	**0,00**	

Рисунок 3.4 – Шлях переданого файлу по мережі

3.3. Незахищена передача даних (використовуючи відкритий http)

Для подальшої передачі файлів будемо використовувати програму WinSCP. WinSCP – безкоштовний SFTP, FTP та SCP-клієнт з відкритим кодом. Головним завданням даної програми є забезпечення захищеного копіювання файлів між необхідними серверами, які мають можливість працювати з даними протоколами, та комп'ютером.

Використовуючи дану програму створимо підключення до сайту, який представлений FTP-сервером, на якому знаходиться папка для пересилання в неї файлів.

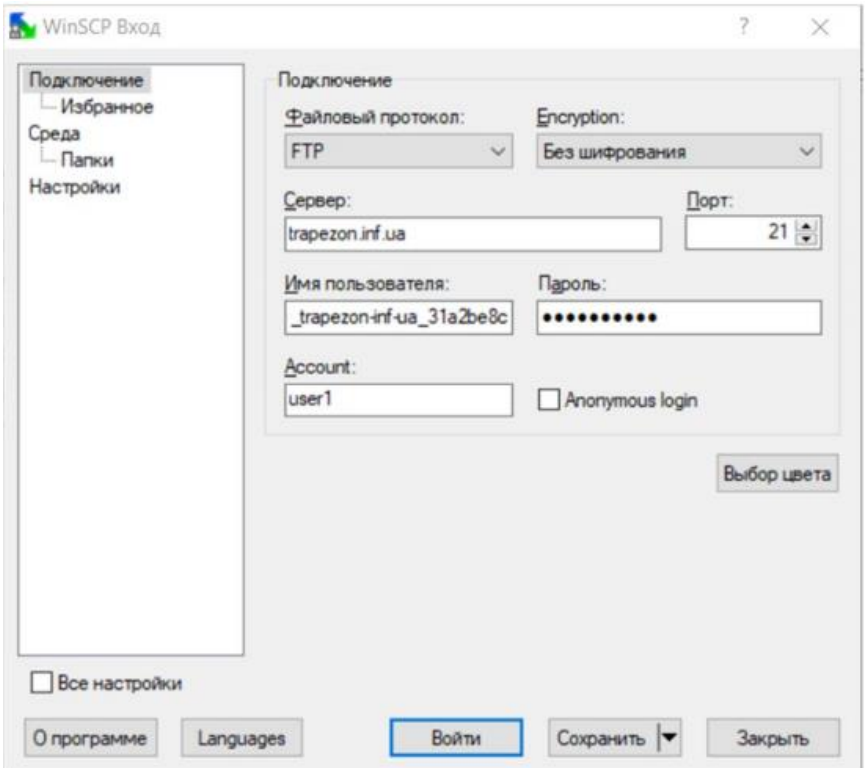


Рисунок 3.5 – Підключення до FTP-сервера

Після того як ми підключилися до FTP-сервера, знаходимо папку *files* та потрібний нам зашифрований файл. Саме в неї і буде відбуватися пересилання наших файлів.

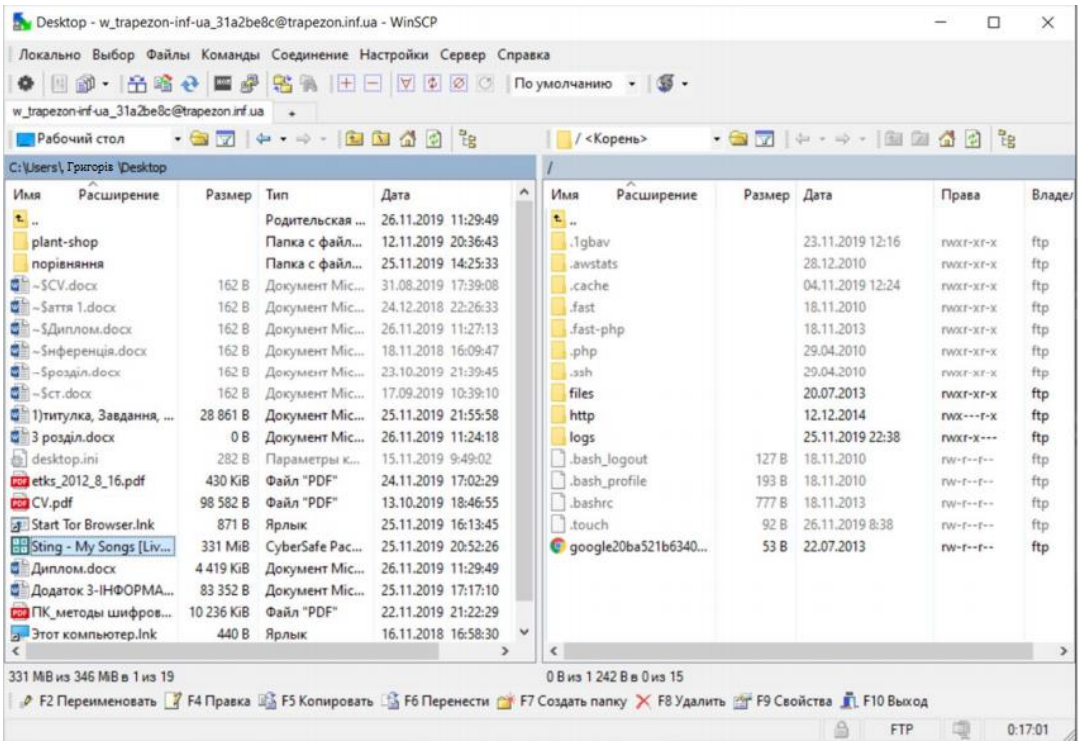


Рисунок 3.6 – Середовище FTP-сервера

Далі відкриваємо папку на сервері та передаємо туди наш зашифрований файл.

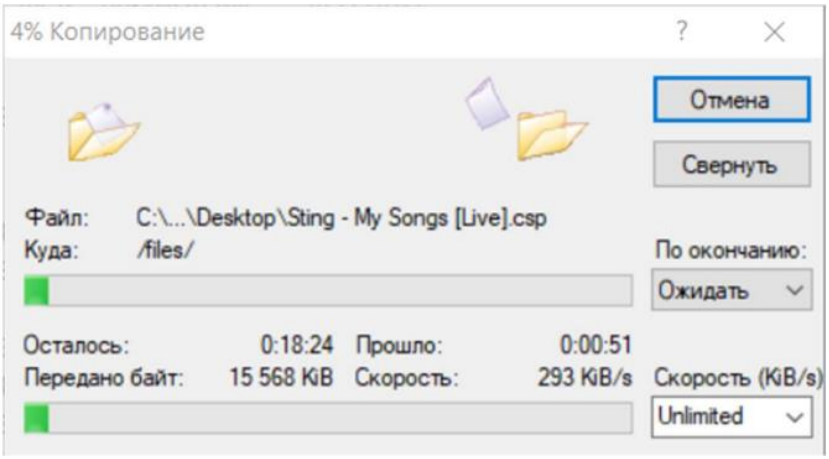


Рисунок 3.7 – Передача зашифрованого файлу

Програмою PingPlotter проведемо аналіз передачі пакетів файлу по мережі. Рисунок 3.8.

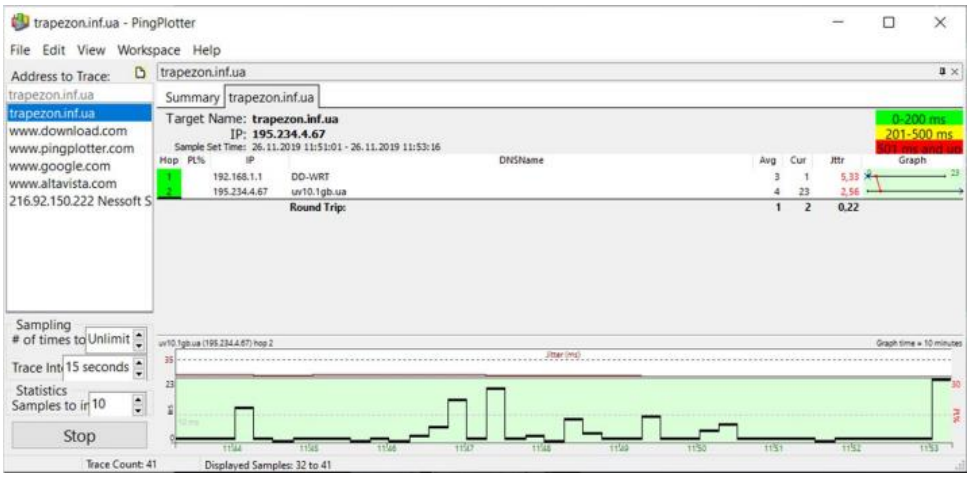


Рисунок 3.8 – Відстеження відправки

3.4. Порівняння кількості пакетів

Для того, щоб перевірити ефективність даного шифрування можна провести дослідження, суть якого полягає в підрахунку пакетів переданих даних після і до шифрування. В цьому нам допоможе програма URL Helper, яка підрахує кількість переданих пакетів даних при різних алгоритмах шифрування. Дані щодо переданих пакетів різних типів інформації до шифрування представлені в таблиці 3.1, а пакети які передавалися після шифрування різними алгоритмами представлені в таблиці 3.2.

Таблиця 3.1 – Кількість пакетів, які перенаправлюються до шифрування

Тип даних	Кількість пакетів, які перенаправлюються		
	Передача на основі VPN	Передача на основі IP (Tor)	Незахищена передача
Аудіо (.flac)	591987	667052	488100
Відео (.MOV)	195386	233623	159240
Зображення (jpg)	13763	14305	11162
Текстовий файл	7497	7867	6098

Таблиця 3.2 – Кількість переданих пакетів даних після шифрування при різних алгоритмах

Тип даних	Кількість пакетів, які перенаправлюються				
	Передача на основі VPN				
	AES 128bit	AES 256bit	Camellia 128bit	Camellia 256bit	DES 64bit
Аудіо	745231				
Відео	18473	18652	18745	18699	19124
Зображення	11169	11170	11166	11139	11146
	Передача на основі IP (Tor)				
Аудіо	752698				
Відео	247358	247567	247612	247589	2479458
Зображення	14151	14481	14689	18943	19916
	Незахищена передача				
Аудіо	488475	488586	489854	488863	488974
Відео	195874	196065	196258	195989	196265
Зображення	11169	11170	11166	11139	11146

3.5. Висновки

В даному розділі магістерської роботи було проаналізовано процес передачі зашифрованих даних по мережі. Як приклад було використано різні типи даних (аудіо, відео та зображення), які були зашифровані різними алгоритмами

шифрування (AES, Camellia та DES). При використанні відповідного програмного забезпечення, було проведено детальний аналіз передачі даних при використанні різних способів шифрування та перенаправлення даних. При передачі інформації по мережі було перевірено зміну кількості пакетів даних після та до шифрування.

РОЗДІЛ 4. РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

4.1. Опис ідеї проекту

Розділ містить економічне обґрунтування стартап-проекту «Secure mobile data transfer». Розділ має на меті ознайомлення з функціональними та економічними характеристиками майбутнього проекту, основними аспектами його реалізації та впровадження у використання.

Опис основної ідеї майбутнього стартап-проекту наведено в таблиці 4.1.

Таблиця 4.1–Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Secure mobile data transfer – це мобільний додаток за допомогою якого можна безпечно передавати різні типи інформації з автоматичним додаванням цифрового підпису.	Підвищення захисту та швидкості передачі файлів	Обмін даними в місцях без доступу до інтернета з використанням QR-коду або NFC-модуля, забезпечення захисту взаємодії між користувачами.

Для оцінювання конкурентноспроможності та складності і можливості виходу стартапу на ринок було виконано порівняння з потенційними конкурентами, до яких можуть бути застосована обрана характеристика. Опис до таблиці 4.2:

- W – слабка сторона;
- N – нейтральна сторона;
- S – сильна сторона.

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	(Потенційні) товари/концепції конкурентів				W	N	S
		Boxcryptor	AppLock	SuperBeam	Portal			
1	Передача	Wifi	Wifi	QR-коди або NFC-модуль	WiFi			+
2	Об’єкти прийому	телефон	телефон	телефон	Тільки з ПК на телефон		+	
3	Наявність інтернету	Не треба	Треба	Не треба	Не треба	+		
4	Собівартість	Середня	Висока	Середня	Висока			+
5	Контактцентр	+	-	-	+			+
6	Час доступу	+	+	+	-			+
7	Шифрування файлів	+	-	+	-		+	

4.2. Технологічний аудит ідеї проекту

Проводиться аудит технологій, за допомогою якої може бути реалізована ідея проекту, тобто технології створення товару. Технологічна здійсненість ідеї проекту показано в таблиці 4.3.

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Шифрування даних	Anroid/IOS	наявна	доступна
2	Доступ через мережу	SIM карта	наявна	доступна
3	Персональний онлайн сервіс	Програмне забезпечення для ОС: Windows, Android, Mac	необхідно розробити	доступна
4	Режими шифрування	AES, DES, CAMELLIA	наявна	доступна

У таблиці 4.3 надано результати огляду основних видів технологій, які можуть бути використані з метою реалізації мобільного додатку стартаппроекту.

4.3. Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які визначаються під час ринкового впровадження проекту, ринкових загроз, які також можуть перешкоджати реалізації проекту, дозволяє спланувати основні напрями розвитку проекту із урахуванням стану ринкового середовища, а також потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Було проведено аналіз попиту: обсяг, динаміка розвитку ринку, наявність попиту. Результати аналізу представлені у таблиці 4.4.

Таблиця 4.4 – Попередня характеристика потенційного ринку

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	4

2	Динаміка ринку (якісна оцінка)	Зростає
3	Наявність обмежень для входу (вказати характер обмежень)	Відсутні
4	Специфічні вимоги до стандартизації та сертифікації	Конфіденційність оброблювання даних
5	Середня норма рентабельності в галузі (або по ринку), %	47%

Дії, необхідні для виходу на такий ринок, залежать в тому числі і від потенційних споживачів. Аналіз цільових аудиторій споживачів даного продукту наведено у таблиці 4.5.

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Додатки, що забезпечують захист даних. Збереження цілісності інформації.	Компанії, які працюють з конфіденційною інформацією	Залежно від цільової групи послуга комплектується різного роду додатками для зручності користування. Залежно від вподобань цільових сегментів, пристрій синхронізовано з різними ОС.	- надійність - зручність - доступність - простота - швидкість

Відповідно до результатів аналізу цільових аудиторій, слід спрямовувати зусилля на активне просування проекту в приватних та державних підприємствах. Важливим процесом для виходу на ринок є аналіз можливих загроз стартап-проекту, що можуть спричинити значні проблеми для розвитку. Результати відповідного аналізу факторів загроз наведено в таблиці 4.6.

Таблиця 4.6 – Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу клієнт може не зацікавитись послугами	Внесення сервісних послуг та зниження цін
2	Конкуренція	Поява іноземних конкурентів з товарами низької вартості	Акцентування уваги на якості результату, що надає продукт

Конкуренція на ринку може стати як стимулом, так і причиною занепаду завдяки якому стартап-проект значно покращить якість послуг та отримає корисний для майбутнього розвитку досвід. На основі аналізу конкуренції із урахуванням основних характеристик ідеї проекту, вимог споживачів до товару та факторів маркетингового середовища визначається та обґрунтовується перелік факторів конкурентоспроможності що наведено у таблиці 4.7.

Таблиця 4.7 – Обґрунтування факторів конкурентноспроможності

№	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)

1	Раціональніший ціновий показник	Можливість більш раціонально використати ресурсів
2	Надання персональних сервісних послуг 24/7	Сервісна підтримка апаратної та програмної частини
3	Синхронізованість	Синхронізація з усіма ОС.
4	Спектр застосувань	Використання для ряду потреб користувачів.

Аналіз, який був показаний у всіх даних таблицях, дав можливість виявити слабкі та сильні сторони для запуску стартап-проекту. Зібрані факти показано у таблиці 4.8.

Таблиця 4.8 – Аналіз стартап-проекту

Сильні сторони: надання персональних сервісних послуг 24/7, синхронізованість.	Слабкі сторони: раціональніший ціновий показник.
Можливості: використання для ряду потреб користувачів.	Загрози: незацікавленість клієнтів, втрата монополії.

4.4. Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у таблиці 4.9 потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.9 – Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами

1	Якість	Висока якість, захист, швидкість передачі.	захист
2	Дешевизна	Раціональне використання коштів	дешевизна

Таблиця 4.10 – Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуютьс я цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Придбання місячної або річної підписки	Мережні ресурси	Синхронізов аність з будь-якими ОС, Конфіденцій ність	Показати переваги сервісу, перед конкурентами	Представити продукції відправною точкою на шляху до безпеки

4.5. Висновки

Після проведення детального аналізу комерціалізацію стартап-проекту мобільного додатку «Secure data transfer», можна вважати доцільною. В ході складання документації було розглянуто основні технології, що можуть бути використані під час реалізації системи стартап-проекту. На дану пропозицію на ринку присутній попит серед державних та приватних підприємств, наразі він не задовольняється послугами замінників. Рентабельніть на ринку послуг насамперед обумовлена широким спектром застосування та персональним сервісом, доступним клієнтам цілодобово.

Впровадження є перспективним, оскільки основними групами клієнтів є люди різних цільових аудиторій: корпоративні мережі банків, клієнти, бізнесмени та люди, які хочуть безпечно передати інформацію через незахищену мережу.

Проаналізувавши та обґрунтувавши фактори конкурентоспроможності, порівнявши сильні та слабкі сторіни проекту, результати були використані для аналізу проекту.

На основі результатів робимо висновок, що впровадження проекту є доцільною, оскільки рентабельність потенційних груп клієнтів створює досить сприятливі умови для розвитку проекту.

ВИСНОВКИ

1. Розглянуто методи шифрування даних та їх особливості.
2. Сформовано основні переваги криптографії як методу захисту конфіденційної інформація.
3. Оглянуто принцип роботи програми CyberSafe.
4. Проведено детальний аналіз передачі даних при використанні різних способів шифрування та перенаправлення даних.
5. Розроблено та проаналізовано провадження стартап-проекту «Secure mobile data transfer».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Проскурин, В.Г. Защита в операционных системах / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич. – М.: Радио и связь, 2000.
2. Вербіцький О.В. Вступ до криптології. – Львів: Видавництво науковотехнічної літератури, 1998. – 249 с.
3. Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н.. Криптографическая защита информации. – Тамбов:Из-во Тамб. Гос. Тех.. ун-та, 2006. – 140 с.
4. Остапов С.Е., Валь Л.О. Основи криптографії: Навчальний посібник. – Чернівці: Книга – XXI, 2008. – 188 с.
5. Г.Ф. Конахович «Оценка эффективности методов стеганографического встраивания информации в спектральную область изображений» // АСУ и приборы автоматики. 2014. №168. С.59-63.
6. Конахович Г.Ф. Комп’ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.
7. CyberSafe. URL: https://habr.com/ru/company/cybersafe/blog.
8. Моргун О.М. Кріптографічні методи захисту інформації. Режим доступу: http://a-morgun.narod.ru/a10-01/LK02.pdf.
9. Современная криптография алгоримы шифрования. URL: https://artismedia.by/blog/sovremennaya-kriptografiya-algoritmyshifrovaniya/.
10. Класифікація криптоалгоритмів. URL: https://wiki.tntu.edu.ua/Класифікація_криптоалгоритмів.