Кафедра **Телекомунікації**

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

до бакалаврської кваліфікаційної роботи на тему:

**Дослідження способів безпечного передавання інформації через незахищений канал зв'язку**

Студент групи ТК-43 Малець Д.І.

(шифр, прізвище та ініціали)

**Керівник роботи (Чернихівський Є.М.)**

**Консультанти ( Корж Г.І. )**

**Завідувач кафедри *Климаш М.М.***

**“** **”**  **2019 р.**

***Національний Університет "Львівська Політехніка"***

(назва ВЗО)

Інститут  **ІТРЕ**  Кафедра  **ТК**

Напрямок підготовки  **6.050903 "Телекомунікації"**

|  |  |
| --- | --- |
|  | ЗАТВЕРДЖУЮ:  Зав. кафедри "Телекомунікації"  ***д.т.н., проф. Климаш М.М.***  ""  2019 p. |

З А В Д А Н Н Я

**на бакалаврську кваліфікаційну роботу студенту**

***Малецю Дмитру Івановичу***

(прізвище, ім’я, по батькові)

1. Тема роботи

**«Дослідження способів безпечного передавання інформації через незахищений канал зв’язку»**

затверджена наказом по інституту від **"31" березня 2019р**.  № ***\_\_\_\_\_***

2. Термін здачі студентом закінченої роботи **4 червня 2019р. \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

3. Вихідні дані до роботи***Дослідити способи безпечної передачі даних через незахищенні канали зв’язку.   \_\_***

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

***Вступ,Захист інформації при передачі через публічні мережі, Використання криптографії для шифрування даних, Передача даних через публічну мережу, Охорона праці, Висновок\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

***1) Блок схема алгоритму ініціалізації KDF***

***2)Блок схема алгоритму шифрування AES***

***3)Блок схема алгоритму розшифрування AES***

***4) Результат основної програми.***

6. Консультанти по роботі, із зазначенням розділів проекту, що стосуються їх

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Консультант | Підпис, дата | |
| Завдання  видав | Завдання  прийняв |
| ***технічний*** | ***Чернихівський Є.М.*** |  |  |
| ***охор. праці*** | ***Корж Г.І.*** |  |  |
|  |  |  |  |

7. Дата видачі завдання

Керівник

(підпис)

Завдання прийняв до виконання

(підпис)

КАЛЕНДАРНИЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| Пор.  № | Назва етапів роботи | Термін виконання етапів  роботи | Примітка |
| ***1*** | ***Дослідження способів безпечної передачі інформації через незахищенний канал зв’язку*** | ***01.04.2019-***  ***10.04.2019*** |  |
| ***2*** | ***Вивчення криптографічних алгоритмів, при передачі ключів через канал зв’язку*** | ***11.04.2019-***  ***23.04.2019*** |  |
| ***3*** | ***Програмна реалізація передачі даних через незахищенний канал зв’язку.*** | ***26.04.2019-***  ***23.05. 2019*** |  |
| ***4*** | ***Охорона праці*** | ***24.05.2019-***  ***31.05.2019*** |  |
| ***5*** | ***Оформлення пояснювальної записки*** | ***01.06.2019-***  ***04.06.2019*** |  |

Студент-дипломник 

(підпис)

Керівник роботи

(підпис)

Реферат

Бакалаврська кваліфікаційна робота на тему «Дослідження способів безпечного передавання інформації через незахищений канал зв’язку» містить 83 сторінок, з них: 22 рисунки.

*Ключові слова*: ECC, алгоритм Діффі-Хелманна, еліптичні криві, еліптична криптографія, KDF скрипт, AES скрипт, Python.

*Мета роботи*:дослідження безпечної передачі даних через публічні мережі, створення еліптичних ключів, генерація сесійних ключів а також шифрування та розшифрування файлу за допомогою цих ключів і скриптів на основі програмного середовища Python.

Розгянуто тему захисту інформації за допомогою криптографіного шифрування, а також освоєння навичків генерації ключів, і передавання їх від абонента А до абонента Б, програмно реалізовано метод ECDHKDF, а також за допомогою алгоритму AES зашифровано/розшифровано файл.

Зміст

[ВСТУП 5](#_Toc10801410)

[РОЗДІЛ 1. ЗАХИСТ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ЧЕРЕЗ ПУБЛІЧНІ МЕРЕЖІ 7](#_Toc10801411)

[1.1 Організація захисту інформації при передачі по каналах зв’язку 7](#_Toc10801412)

[1.2 Загальна модель системи передачі ключових даних 14](#_Toc10801413)

[1.3 Криптографія з відкритим ключем 22](#_Toc10801414)

[РОЗДІЛ 2. ВИКОРИСТАННЯ КРИПТОГРАФІЇ ДЛЯ ШИФРУВАННЯ ДАНИХ 29](#_Toc10801415)

[2.1 Криптографія на основі еліптичних кривих 29](#_Toc10801416)

[2.2 Застосування еліптичних кривих для задач захисту інформації 35](#_Toc10801417)

[2.3 Розширений стандарт шифрування 41](#_Toc10801418)

[РОЗДІЛ 3. ПЕРЕДАЧА ДАНИХ ЧЕРЕЗ ПУБЛІЧНУ МЕРЕЖУ. 46](#_Toc10801419)

[3.1 Опис середовища розробки. 46](#_Toc10801420)

[3.2 Генерація пари ключів ECC. 49](#_Toc10801421)

[3.3 Шифрування і розшифрування даних 51](#_Toc10801422)

[РОЗДІЛ4. ОХОРОНА ПРАЦІ 59](#_Toc10801423)

[4.1 Аналіз шкідливих та небезпечних чинників при роботі зПК 59](#_Toc10801424)

[4.2 Умови праці на робочому місці з ПК 60](#_Toc10801425)

[4.3 Мікроклімат та ступінь іонізації повітря в приміщенні з ПК 62](#_Toc10801426)

[4.3 Випромінювання в приміщенні з ПК 64](#_Toc10801427)

[4.4 Шум та вібрація в приміщенні з ПК 66](#_Toc10801428)

[4.5 Виробниче освітлення в приміщенні з ПК 67](#_Toc10801429)

[4.6 Електробезпека в приміщенні з ПК 71](#_Toc10801430)

[4.7 Пожежна безпека в приміщенні з ПК 73](#_Toc10801431)

[ВИСНОВКИ 75](#_Toc10801432)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 76](#_Toc10801433)

[ДОДАТОК 1. ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ 78](#_Toc10801434)

**ВСТУП**

Забезпечення інформаційної безпеки є одним з найголовніших напрямів розвитку інформаційних технологій. Набір завдань, які розглядаються в цій галузі, постійно збільшується. Одним з основних засобів, що використовуються для захисту інформації в комп’ютерних системах, є криптографічні перетворення. Проблеми криптографії виходять за рамки задач забезпечення секретності. Сучасна криптографія включає в себе чотири основних розділи: криптосистеми з відкритим ключем, симетричні криптосистеми, системи електронного підпису, управління ключами. Сучасні криптосистеми побудовані на користуванні ключами і, як правило, управління ключами є слабким місцем у криптографічних додатках. Користування криптографічними технологіями не є складним, однак складним є безпечно користуватися ключами, зберігати та обмінюватися ними. Часто неякісне управління ключами підриває навіть виключно якісні системи, так як безпека алгоритму зосереджена в ключі. Управління ключами включає генерацію, накопичення і розподіл ключів. У сучасному світі управління ключами є найважчим розділом криптографії. Проектувати безпечні криптографічні алгоритми и протоколи непросто, але наявний значний обсяг академічних досліджень. Зберегти секрет ключів набагато важче. В загалом, усі методи генерації ключів можна розділити на апаратні та програмні. Основною вимогою при цьому є рівномірність розподілу по всьому простору можливих ключів. При генерації ключів апаратним способом використовуються генератори шуму – електронні пристрої, в яких протікає випадковий фізичний процес; при програмній генерації – генератори псевдовипадкових послідовностей. Накопичення ключів пов’язане з їхнім зберіганням, обліком та видаленням. У складних інформаційних системах один користувач може працювати з великим обсягом ключової інформації, внаслідок чого виникає необхідність організації мінібаз даних з ключовою інформацією. Такі бази даних відповідають за прийняття, зберігання, облік та видалення ключів, які використовуються. Інформація про ключі повинна зберігатися зашифрованою. Ключі, які шифрують ключову інформацію називаються майстер-ключами і, як правило, не зберігаються в комп’ютерній системі, або для їхнього перетворення використовують криптографічні алгоритми. Кількість ключів, що використовується, залежить від кількості абонентів, обсягів інформації і особливостей алгоритму шифрування. Сеансові ключі повинні знищуватися. Питання оновлення ключів пов’язане з третім аспектом управління ключами – розподілом ключів. Розподіл ключів – одна з фундаментальних задач криптографії.

**РОЗДІЛ 1. ЗАХИСТ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ЧЕРЕЗ ПУБЛІЧНІ МЕРЕЖІ**

**1.1 Організація захисту інформації при передачі по каналах зв’язку**

Захист ліній зв'язку - одна з найважливіших завдань при організації безперебійної передачі інформації по каналу зв'язку, адже при відсутності стабільного з'єднання між відправником і отримувачем втрачається надійність і оперативність передачі будь-яких даних.

Також вкрай важливо переконатися в захисті ліній зв'язку від прослуховування ззовні. Розрізняють два методи боротьби з перехопленням інформації з лінії зв'язку. Це методи фізичного захисту за допомогою різних фільтрів і загороджують екранів, а також методи криптографічного захисту даних, що передається по лінії зв'язку.

Фільтри - електронні пристрої, які пропускають сигнали одного діапазону (діапазонів) частот і не пропускають іншого (інших) діапазонів. Якщо фільтр пропускає сигнали низьких частот і не пропускає сигнали високих частот, то такі фільтри називаються фільтри низьких частот (ФНЧ). Якщо навпаки, то фільтри високих частот (ВФЧ). ФНЧ використовують для виключення (ослаблення) просочування інформаційних сигналів ТЗПІ (технічні засоби прийому, обробки, зберігання та передачі інформації), що мають більш високі частоти, в колі електроживлення, заземлення, в лінії, що виходять за межі контрольованої зони.

Дані, що передаються по простим лініях зв'язку, дротових або радіоканалах, можуть бути перехоплені зловмисником. Без всяких труднощів будь-хто може вбудуватися в передавальну лінію і переглядати проходить інформацію. Один зі способів уникнути цього - шифрування даних так, щоб їх могли дешифрувати тільки ті, кому вони призначені.

Криптографічні методи забезпечують дію найбільш потужних механізмів захисту, таких, як:

* шифрування, що забезпечує конфіденційність, захист процедур аутентифікації, контроль доступу;
* імітозащіти, що підтримує забезпечення цілісності та автентичності переданих документів;
* електронний підпис, що забезпечує виконання вимог щодо аутентифікації, цілісності та автентичності, захист від відмов.

Найпоширенішим пристроєм для захисту мереж зв'язку є скремблер, який здійснює шифрування інформації перед її передачею по лінії зв'язку. У радіоканалах скремблери перетворять сигнал за часом, амплітуді і частоті. Розвиток отримали тимчасові і частотні перетворення, а також комбіновані методи.

Скремблер - це пристрій, що здійснює шифрування переданої по каналах зв'язку мови.

Скремблер приєднується прямо до телефону і в вимкненому стані ніяк себе не проявляє. Але варто власникові апарата включити його, як він тут же починає приймати всі сигнали, що йдуть з мікрофона, шифрувати їх і тільки після цього відсилати на вихід. Декодування мови відбувається в зворотному порядку. Сигнали з антени подаються в скремблер, а вже звідти - на динамік.

Основною перевагою скремблеров є висока надійність захисту. У сучасних пристроях реалізовані криптоалгоритми, що відповідають всім вимогам. Крім того, скремблери дозволяють захиститися від будь-якого способу прослуховування телефонів, в тому числі і від спеціального обладнання, встановленого у оператора. На жаль, є у цієї технології і недоліки. І найголовніше з них - необхідність обом абонентам мати сумісні пристрої для проведення приватної бесіди.

Для захисту розмов і передачі мовного сигналу через мережі зв'язку використовують кріптофони - спеціальний пристрій або програмне забезпечення, яке необхідно встановити на смартфон для захисту телефонної розмови. По суті, кріптофон представляє пристрій шифрування з певним ключем. Даний спосіб зручний для захисту внутрішніх корпоративних мереж від прослушки.

Активним способом захисту є лінійне зашумлення. Для виключення перехоплення побічних електромагнітних випромінювань по електромагнітному каналу використовується просторове зашумлення, а для виключення знімання наведень інформаційних сигналів з сторонніх провідників і сполучних ліній ВТСС- лінійне зашумлення. У найпростішому випадку система лінійного зашумлення є генератор шумового сигналу, що формує шумове маскує напруга із заданими спектральними, часовими і енергетичними характеристиками, який гальванічно підключається в зашумлять лінію (сторонній провідник). Системи лінійного зашумлення (СЛЗ) застосовуються у випадках:

• недостатніх рівнів перехідних затуханий між впливають і схильними до впливу кабелями і сполучними лініями;

• впливу на ланцюгу, дроти та пристрої допоміжної апаратури низькочастотних електромагнітних полів основної апаратури;

• наявності електроакустичних перетворень в допоміжній апаратурі.

До заходів захисту інформації від витоку по електромагнітному каналу з використанням пасивних засобів відносяться локалізація випромінювань шляхом екранування і заземлення технічних засобів, а також екранування цілих приміщень.

Обмеження небезпечних сигналів полягає в тому, що електронний пристрій - обмежувач, пропускає сигнали високого рівня і не пропускає слабкі сигнали, які можуть виникнути в результаті наведень або на виході елементів, що володіють «мікрофонний ефект».

Захист лінії зв'язку, що виходять за межі приміщень, що охороняються або за межі всього об'єкта, являє собою дуже серйозну проблему, так як ці лінії найчастіше виявляються безконтрольними, і до них можуть підключатися різні засоби знімання інформації.

Екранування інформаційних ліній зв'язку між пристроями технічних засобів передачі інформації (ТЗПІ) має на меті, головним чином, захисту ліній від наведень, створюваних лініями зв'язку в навколишньому просторі. Найбільш економічним способом екранування є групове розміщення інформаційних кабелів в екранувальній ізольованому коробі. Коли такий короб відсутня, доводиться екранувати окремі лінії зв'язку.

Для контролю стану лінії зв'язку використовуються різні індикатори як пасивні, так і активні. Вони дозволяють визначити як паралельне підключення до лінії, так і послідовне

До засобів пасивного захисту відносяться фільтри і інші пристосування, призначені для зриву деяких видів прослуховування приміщень за допомогою телефонних ліній, що знаходяться в режимі відбою. Ці кошти можуть встановлюватися в розрив телефонної лінії або вбудовуватися безпосередньо в ланцюзі телефонного апарату.

Позитивні властивості:

* запобігання перехоплення мовної інформації методом ВЧ-нав'язування;
* запобігання перехоплення мовної інформації через витік мікро-ЕРС ланцюга дзвінка;
* запобігання перехоплення за допомогою мікрофонів, що передають мовну інформацію по телефонній лінії в довгохвильовому діапазоні, за умови правильного розміщення фільтра телефонної лінії.

Недоліком засобів пасивного захисту є те, що вони не захищають від інших систем перехоплення.

**1.1.1 Проблеми передачі інформації по відкритим (публічним) каналам зв'язку**

В даний час спостерігається постійне зростання обсягів інформації. Причому ця інформація не тільки накопичується, але і потребує передачі і обміні. Тому, кількістьпереданої інформації по різних каналах зв'язку також щодня зростає. Одним з найбільш доступних каналів стала мережа Інтернет. Перевагою мережі є її відкритість і публічність. При цьому в наше життя міцно увійшли IT-технології, зокрема обмін електронною інформацією. Ця інформація дуже часто передається з використанням відкритих каналів зв'язку. Під відкритим каналом зв'язку розуміється незахищений канал, доступ до якого може отримати будь-яка людина. У зв'язку з цим все більш актуальною стає проблема захисту інформації, що передається. Сучасні системи захисту повинні забезпечувати збереження наступних властивостей інформації:

* Конфіденційність - доступність інформації тільки для певного кола осіб;
* Цілісність - достовірність, точність і захищеність від спотворення;
* Готовність інформації до обробки в потрібний момент часу.

Зараз існує величезна кількість безпечних способів і технологій передачі інформації по відкритих каналах зв'язку. Наприклад, програми, які здійснюють захист даних з

допомогою шифрування, або забезпечують парольний захист. Але при цьому існує проблема передачі самого пароля. Його передача по відкритих каналах небезпечна, томупотрібно шукати альтернативні варіанти передачі (наприклад, по телефону).

Основною проблемою передачі інформації по відкритих каналах зв'язку є збереження її конфіденційності. Інформація зберігається на веб-серверах і інших носіях ввідкритому вигляді, а також передається з публічних каналах зв'язку знову ж у відкритому стані, існує небезпека перехоплення даних, а в подальшому і підробки або спотворенняінформації зловмисником. Так як електронна пошта та інші мережеві зв'язку мають слабкі механізми захисту, то практично будь-яке повідомлення може бути прочитано безліччюлюдей, які не мають відношення ні до відправника, ні до одержувача листа.

При перехопленні інформації зловмисник може підмінити будь-які дані, наприклад дані ключа. В такому випадку, він може розшифрувати його і, підмінивши відправити людині, якій спочатку призначався цей ключ. Якщо зловмисник має можливість перехоплювати всі повідомлення, що надсилаються між користувачами, то він довгий час можеконтролювати хід листування. Тому додатковим завданням для безпечної передачі інформації є не тільки шифрування повідомлень, а й при собі посвідчення особивідправника.

Електронний цифровий підпис може гарантувати те, що документ був відправлений саме цією людиною і не зазнавав змін в процесі передачі. адресату

досить лише звірити підпис відправника, таким чином, підтвердивши достовірність.

**1.1.2 Концепція безпеки мережі**

Безпека мережі починається з аутентифікації , як правило, з іменем користувача та паролем . Оскільки це вимагає лише однієї деталі аутентифікації імені користувача, тобто пароля, це іноді називають однофакторною аутентифікацією. З двофакторною аутентифікацією також використовується щось, що має користувач (наприклад, маркер безпеки або « ключ », картка банкоматів або мобільний телефон ); і з трьохфакторною аутентифікацією, що також використовується користувачем (наприклад, сканування відбитків пальців або сітківки ).

Після перевірки автентичності брандмауер застосовує політику доступу, наприклад, до яких послуг дозволено користуватися мережеві користувачі. Хоча цей компонент є ефективним для запобігання несанкціонованому доступу, він може не перевіряти потенційно шкідливий вміст, наприклад, комп'ютерні черв'яки або трояни, які передаються через мережу. Антивірусне програмне забезпечення або система запобігання вторгненню (IPS) допомагають виявляти та перешкоджати дії таких шкідливих програм . Система виявлення вторгнень на основі аномалій може також контролювати мережу, подібно до трафіку мережевого сигналу і може реєструватися для цілей аудиту та для подальшого високорівневого аналізу. Більш нові системи, що поєднують без нагляду машинне навчання з повним аналізом мережевого трафіку, можуть виявити активних зловмисників мережі зловмисних інсайдерів або цільових зовнішніх зловмисників, які скомпрометували машину або обліковий запис користувача.

Зв'язок між двома хостами за допомогою мережі може бути зашифрована для підтримки конфіденційності.

Honeypots , по суті, примушують доступні до мережі ресурси, можуть бути розгорнуті в мережі як засоби спостереження та раннього попередження, оскільки медіа-бари зазвичай не доступні для законних цілей. Методи, які використовуються зловмисниками, які намагаються скомпрометувати ці ресурси підмани, вивчаються під час та після нападу, щоб стежити за новими методами експлуатації . Такий аналіз може бути використаний для подальшого посилення безпеки фактичної мережі, що захищається приставкою. Медпот може також спрямовувати увагу атакуючого від легітимних серверів. Медник спонукає зловмисників витрачати свій час і енергію на сервер приманки, відволікаючи їх увагу від даних на реальному сервері. Подібно до притулку, мережа - це мережа, створена з навмисними вразливостями. Його мета також полягає у запровадженні атак, щоб можна було вивчити методи атакуючого, і цю інформацію можна використовувати для підвищення безпеки мережі. Медсетка, як правило, містить один або більше мультипотів.

***Управління безпекою***

Управління безпекою для мереж відрізняється для всіх видів ситуацій. Домашній або невеликий офіс може вимагати лише базової безпеки, тоді як великим підприємствам може знадобитися високотехнологічне та сучасне програмне та апаратне забезпечення для запобігання зловмисним атакам від злому та спаму .

***Типи атак***

Мережі підлягають атакам зловмисних джерел. Атаки можуть бути з двох категорій: "Пасивний", коли мережевий зловмисник перехоплює дані, що переміщуються по мережі, і "Активні", в яких зловмисник ініціює команди для порушення нормальної роботи мережі або для проведення розвідки і бічного руху, щоб знайти і отримати доступ до активів, доступних через мережу.

Типи атак включають:

Пасивний:

* Мережа;
* Прослуховування;
* Сканер портів;
* Сканування в режимі очікування;
* Шифрування;
* Аналіз трафіку.

Активний:

* Вірус;
* Підслуховування;
* Модифікація даних;
* Атака відмови в обслуговуванні;
* Спуфінг DNS;
* Людина в середині;
* ARP отруєння;
* Перемикання VLAN;
* Атака Смурфа;
* Переповнення буфера;
* Переповнення купою;
* Формування атаки рядка;
* Ін'єкція SQL;
* Фішинг;
* Міжсайтовий сценарій;
* CSRF;
* Кібер-атака.

**1.2 Загальна модель системи передачі ключових даних**

У криптографічних додатках найбільш складною організаційно-технічною проблемою є управління ключами. Під управлінням ключами розуміється їхня генерація, тестування, розподіл, введення в дію, зміна, облік, зберігання і знищення. У статті розглядається один з аспектів управління ключами - безпечна передача ключових даних незащищеними каналами зв’язку. Далі під каналом зв'язку розуміється канал доставки. Під ключовими даними (КД) розуміються власне криптографічні ключі або дані, що служать для їхнього виготовлення.

Розглянемо модель системи передачі КД, що включає трьох учасників - двох законних користувачів, що можуть виступати в ролі відправника або одержувача КД, і супротивника. Між відправником і одержувачем є незахищений канал зв'язку (будемо його також називати основним каналом). Супротивник веде перехоплення повідомлень, переданих по основному каналу, через канал перехоплення. Задача законних користувачів - установити загальний секретний ключ, скориставшись незахищеним основним каналом, і створити в каналі перехоплення перешкоди, що запобігають одержанню ключа супротивником. Перешкоди в каналі перехоплення розуміються в широкому розумінні, наприклад, необхідність розв’язання ворогом обчислювально складної задачі, у тому числі, необхідність перебору всіх можливих значень ключа, перешкода в теоретико-інформаційному змісті, створення невизначених ситуацій у процесі передачі КД, перекручене або неповне знання даних перехоплення та ін.

Законні користувачі можуть виконувати два основних сценарії: у першому випадку відправник генерує ключ і безпечним способом передає його одержувачу; у другому випадку користувачі реалізують безпечний протокол обміну даними, що служать для виготовлення загального секретного ключа за заданим алгоритмам.

Поведінка супротивника також може створювати різні ситуації в розглянутій моделі. Зокрема, дії супротивника можуть бути пасивними або активними.

При пасивному нападі ведеться перегляд усіх переданих повідомлень і їх наступний криптоаналіз. При активному нападі супротивник виступає в ролі активного ретранслятора, або здійснює маскарад чи іншим способом порушує протокол. Слід зазначити, що в статті не розглядаються проблеми автентифікації користувачів і повідомлень.

Важливими в даній моделі є характеристики основного каналу і каналу перехоплення. На практиці в ролі основного каналу можуть виступати фізичні лінії, канали зв’язку різного типу (радіо-, проводні і т.п), канал читання з пристроїв зберігання КД, квантові канали, кур’єрський зв’язок і ін. Канал перехоплення теж може бути організований по різному: безпосереднє підключення до основного каналу, втручання в квантовий канал, копіювання з пристроїв зберігання КД, перехоплення по побічним електромагнітним випромінюванням і наведенням.

Розглянемо існуючі підходи до розв’язання проблеми передачі КД незахищеним каналах зв’язку.

Традиційно передача КД здійснювалася за сценарієм, коли відправник (наприклад, центр розподілу ключів) генерував ключ і безпечним способом передавав його одержувачу (одержувачам) для організації захищеного каналу. З погляду класичної криптографії, в основі якої лежать симетричні шифри, дана проблема є парадоксальною. КД передаються для організації захищеного каналу, але для їхньої передачі потрібно, у свою чергу, організувати захищений канал, тому що одним з основних допущень є можливість супротивника переглядати всі повідомлення в каналі. За даною логікою, найбільш простим методом захисту КД при передачі є їхнє шифрування, що вимагає попереднього розподілу ключів шифрування КД захищеними каналами. Даний метод широко використовується на практиці. Зокрема, починаючи з американського стандарту ANSIX9.17, пропонується використовувати дво- або трирівневі схеми розподілу ключів . Ключі різних рівнів утворюють ієрархію. Вищий в ієрархії ключ доставляється вручну, інші ключі передаються каналом зв’язку, зашифрованим на ключах більш високого рівня ієрархії.

Очевидно, що даний метод є не рішенням, а відходом від проблеми: незахищений канал заміняється захищеним у традиційному сенсі, тобто реалізується засекречування переданих повідомлень. Крім того, фаза ручної доставки ключа не завжди припустима і для неї потрібно організовувати захищений канал.

Поява несиметричних криптосистем дещо знизила гостроту проблеми, але відразу слід зазначити як недолік, що їхня теоретична стійкість дотепер не доведена. У найбільше простому сценарії відправник зашифровує повідомлення на відкритому ключі одержувача, отриманому з загальнодоступного довідника, і передає результат одержувачу, що розшифровує повідомлення на своєму несиметричному секретному ключі. Даний метод лежить в основі гібридних криптосистем, у яких подібним способом передається ключ симетричного шифрування. Основні проблеми перебувають в автентичній доставці відкритих ключів користувачів у загальнодоступний довідник і забезпеченні довіри до довідника, тому що фальсифікація відкритих ключів дозволяє ворогу здійснити маскарад. Розв’язання цих проблем вимагає окремих, найчастіше складних організаційних і технічних рішень, наприклад, створення органів сертифікації відкритих ключів .

Окремо існує проблема забезпечення безпеки КД при рішенні задач їх автоматизованого децентралізованого виготовлення, обліку, збереження і дистанційного введення в апаратуру. У даний час для забезпечення безпеки КД у цьому випадку застосовують комплекс організаційно-технічних заходів . У цілому це дозволяє забезпечити необхідний рівень безпеки КД, однак часто вимоги виявляються настільки жорсткими, що їхнє виконання приводить або до надзвичайно великих розмірів контрольованих зон, або до ускладнення конструкцій, збільшення ваги і вартості устаткування.

**1.2.1 Кодовий захист ключових даних для моделі джерела “унікальних повідомлень”**

Одним із способів захисту КД є кодовий захист (КЗ). Спосіб КЗ базується на теорії завадостійкого кодування і концепції каналу з витоком А.В. Вайнера і відноситься до класу ймовірносно-криптографічних систем захисту.

Його сутність полягає в наступному. Фізичний датчик випадкових чисел формує послідовність рівноймовірних і взаємонезалежних двійкових символів *γ*R*k'*R. Цю послідовність розбивають на блоки довжини *k*=*n- k¢,* де *n*– загальна довжина блоку коду *V*. Блоки *k*вважають інформаційними символами коду *V*і для них у кодері по правилам цього коду знаходитися k¢ перевірочних символів *f*(*γ*R*k'*R). Перевірочні символи складають послідовно по *mod*2 з інформаційними символами *S*R*k*R і суми *S*R*k*R + *f*(*γ*R*k*R) відправляють у основний канал безпосереднього запису *k*-блоку випадкових символів *γ*R*k'*R*.* Таким чином, *A*по каналу передає *n*-блоки наступного вигляду:

*X*R*n*R=(*γ*R*k'* R*, S*R*k*R*+ f*(*γ*R*k'*R)), (1.1)

де *f*(*γ*R*k*R) - правило формування перевірочних символів коду *V*,

*γ*R*k'*R – блоки випадкових символів,

*S*R*k*R – блоки інформаційних символів R

На прийомному боці спочатку за отриманими *γ*R*k'*R випадковими символами формують *k*перевірочних символів (за однаковим з кодуванням правилом *f*(*γ*R*k*R)), а після цього результат складають побітно з інформаційними *k*-блоками:

*Y*R*n*R=*S*R*k*R+ *f*(*γ*R*k*R)+ *f*(*γ*R*k*R)= *S*R*k*R , (1.2)

де *Y*R*n*R – отримана *B*інформація

З (1.2) слідує, що *B*отримує *S*R*k*R без помилок.

В каналі перехоплення супротивник отримує *Z*R*n*R з ймовірністю помилки *p*, що дорівнює накладанню вектора помилки *E*R*n*R: *Z*R*n*R*=Y*R*n*R*+ E*R*n*

*Z*R*n*R=(*γ*R*k'*R +*E*R*n*R, *S*R*k*R+ *f*(*γ*R*k*R)+*E*R*n*R), (1.3)

де *E*R*n*R - вектор помилки довжиною *n*, *p*(*E*=1)=*p*, *p*(*E*=0)=1-*p*.

Це приводить до значного розмноження помилок, тому при *n®¥* кількість інформації в каналі перехоплення відносно переданої інформації *I*(*S*R*k*R*/Z*R*n*R) прямує до нуля, що виключає можливість правильного декодування перехопленної інформації. Ефект досягається ціною ускладнення кодування і створення лише деякого погіршення якості каналу перехоплення в порівнянні з каналом одержувача. При такому підході передбачається, що супротивник має у своєму розпорядженні такою ж самою апріорну сукупність відомостей, що і законнийкористувач, тобто ніякі секретні дані (ключові дані) для реалізації способу кодового захисту не використовуються.

Внаслідок особливостей моделі беззбиткових джерел (КД, як повідомлення, відносяться до такого класу джерел), повідомленнями якого є КД, можливості й оцінки ефективності кодового захисту КД також мають специфіку.

КД, як повідомлення джерела, мають властивість унікальності. У було введене поняття “унікального повідомлення” (УП). УП має ту властивість, що до моменту початку його передачі в точці прийому вже є інформація, що дозволяє, у принципі, єдиним способом визначити це повідомлення. Це може бути зроблено, наприклад, повним перебором усіх можливих повідомлень і перевіркою їх на допустимість. Необхідність передачі УП по каналах зв'язку пояснюється трудомісткістю цієї процедури.

Варто розрізняти УП зі штучною або природною надмірністю, де також можна перевірити допустимість прийнятих повідомлень, але повний перебір принципово не дозволяє виділити єдине повідомлення.

Нехай E = f (S) - обчислювально необоротна функція (ОНФ) , тобто така, що зворотна функція S = φ(E) існує, однак, обчислення S за відомим E вимагає невиконанно великого числа операцій або ємності устаткування. Тоді, якщо E відомо в точці прийому, то S при передачі по каналу зв’язку буде являти собою УП. Найбільше важливим випадком УП, що і аналізується в даній статті, є КД для спеціальної апаратури, що можуть зберігатися, оброблятися і передаватися сполучними лініями або навіть спеціальними каналами зв’язку.

Можна також вважати, що УП у вигляді КД “передаються” каналом зв’язку з перешкодами й у тому випадку, коли робиться спроба несанкціонованого зчитування КД із запам’ятовувальних пристроїв шифраторів після виконання процедури аварійного стирання їхнього вмісту. Характерною рисою УП у вигляді КД є їх відносно малий об’єм і рівноймовірність, тобто відсутність збитковості.

Залежність РRеR від p для різних параметрів кодів приведена на рисунку

З отриманих результатів слідує, що чим довше коди, тим ефективніше кодовий захист, тим ближче канал перехоплення до “обриву” (ймовірність помилки в ньому наближається до 0,5).

Також в залежності від умов застосування КЗ УП, можна визначити найбільш оптимальний код для визначеної області значень p.

Крітерій PRе Rпростий та зручнийR Rдля розрахунків, але ж він не може одностайно визначити ефективність КЗ УП. Наприклад, при використанні тривіального коду з *r* однаковими перевірочними символами, отриманими як поелементна сума за mod2 усіх інформаційних, дає максимальне значення PRеR. Тому велике значення PRеR є необхідною, але недостатньою умовою ефективності застосування КЗ УП, що вимагає проведення розрахунків за іншими критеріями. Наступними шляхами досліджень застосування КЗ при передачі УП незащищеними каналами зв’язку є оцінка ефективності за критерієм оптимальної обробки при декодуванні списком об’єму N з мінімальною ймовірністю помилкового декодування PRпдR. Графік залежності (рис. 1.1)

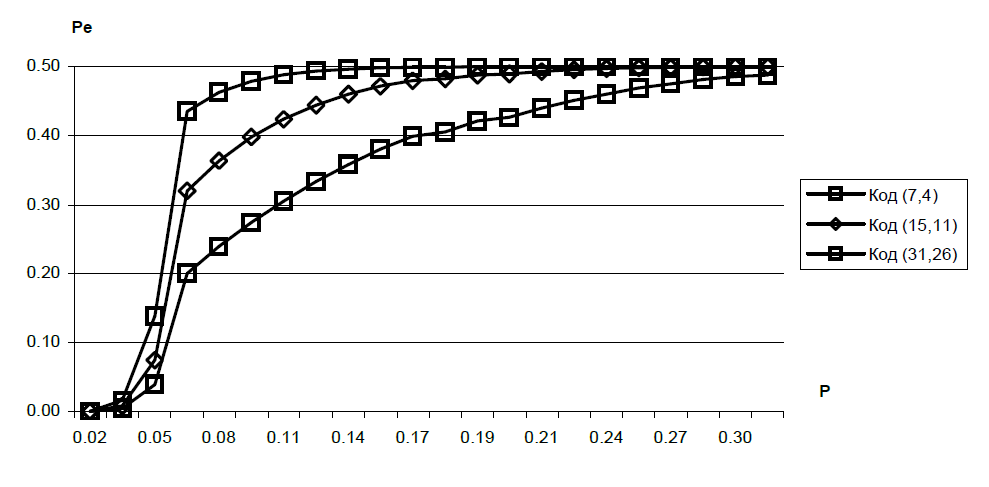


Рис.1.1.Залежність РRеR від p

**1.2.2 Обмін ключами через канали зв’язку**

Обмін ключами - це будь-який метод криптографії, за допомогою якого криптографічні ключі обмінюються між двома сторонами, що дозволяє використовувати криптографічний алгоритм.

Якщо відправник і одержувач бажають обмінюватися зашифрованими повідомленнями, кожен повинен бути обладнаний для шифрування повідомлень, що надсилаються, і розшифровувати отримані повідомлення. Характер необхідного обладнання залежить від техніки шифрування , яку вони можуть використовувати. Якщо вони використовують код , то обом буде потрібно копія тієї ж кодової книги . Якщо вони використовують шифр , їм потрібні відповідні ключі. Якщо шифр є симетричним шифром ключа , то обом буде потрібна копія одного ключа. Якщо шифр асиметричного ключа з властивістю відкритого / приватного ключа, обом потрібен відкритий ключ іншого.

***Канал обміну***

Обмін ключами здійснюється або в діапазоні, або поза діапазоном. При обміні ключами в діапазоні ключі ключі обмінюються через той самий канал зв'язку, який буде зашифрований. У ключі поза діапазоном ключі обмінюються каналом, відмінним від того, який буде зашифрований.

***Проблема обміну ключами***

Проблема обміну ключами описує способи обміну будь-яких ключів або іншої інформації, необхідної для створення безпечного каналу зв'язку, щоб ніхто не міг отримати копію. Історично, перед винаходом криптографії з відкритим ключем (асиметрична криптографія), криптографія симетричних ключів використовувала єдиний ключ для шифрування і дешифрування повідомлень. Для конфіденційної комунікації між двома сторонами вони повинні спочатку обміняти секретний ключ, щоб кожна сторона могла шифрувати повідомлення перед відправкою і розшифровувати отримані. Цей процес відомий як обмін ключами.

Загальною проблемою з симетричною криптографією або криптографією з одним ключем є те, що вона вимагає передачі секретного ключа через довірених кур'єрів, дипломатичних мішків або будь-якого іншого безпечного каналу зв'язку. Якщо дві сторони не можуть встановити безпечний початковий обмін ключами, вони не зможуть безпечно спілкуватися без ризику перехоплення та розшифрування повідомлень третьою стороною, яка придбала ключ під час обміну первинним ключем.

Криптографія з відкритим ключем використовує систему з двома ключами, що складається з загальнодоступних і приватних ключів, де повідомлення шифруються одним ключем і розшифровуються іншим. Це залежить від обраного криптографічного алгоритму, який використовується для шифрування повідомлень, а також для розшифровки. Наприклад, в RSA закритий ключ використовується для розшифрування повідомлень, тоді як в алгоритмі цифрового підпису (DSA) закритий ключ використовується для їх шифрування. Відкритий ключ може бути відправлений через незахищені канали або загальнодоступний; приватний ключ доступний лише його власнику.

Відомий як обмін ключами Діффі-Хеллмана, ключ шифрування можна відкрито повідомляти, оскільки він не становить ризику для конфіденційності зашифрованих повідомлень. Одна сторона обмінюється ключами з іншою стороною, де вони потім можуть шифрувати повідомлення за допомогою ключа і відправляти назад текст шифру. Лише ключ дешифрування - в даному випадку це закритий ключ - може розшифрувати це повідомлення. Ні в якому разі під час обміну ключами Діффі-Хеллмана не було жодної конфіденційної інформації, яка піддається ризику компромісу, на відміну від симетричного обміну ключами.

**1.3 Криптографія з відкритим ключем**

Криптографія з відкритим ключем , або асиметрична криптографія , являє собою криптографічну систему, яка використовує пари ключів : відкриті ключі, які можуть широко розповсюджуватися, і приватні ключі, які відомі тільки власникові. Генерування таких ключів залежить від криптографічних алгоритмів, що базуються на математичних задачах для створення односторонніх функцій . Ефективна безпека вимагає лише збереження приватного ключа; відкритий ключ може бути відкрито розповсюджений без шкоди для безпеки.

У такій системі будь-яка людина може зашифрувати повідомлення, використовуючи відкритий ключ одержувача, але це зашифроване повідомлення може бути розшифровано лише за допомогою закритого ключа отримувача.

Міцна аутентифікація також можлива. Відправник може об'єднати повідомлення з закритим ключем, щоб створити короткий цифровий підпис у повідомленні. Будь-який користувач з відповідним відкритим ключем може комбінувати повідомлення, передбачуваний цифровий підпис на ньому, і відомий відкритий ключ, щоб перевірити, чи підпис був дійсний, тобто зроблений власником відповідного закритого ключа.

Алгоритми відкритих ключів є фундаментальними інгредієнтами безпеки в сучасних криптосистемах, додатках і протоколах, що забезпечують конфіденційність, автентичність і неможливість відмови від електронних комунікацій і зберігання даних. Вони підтримують різні стандарти Інтернет, такі як безпека транспортного шару (TLS) , S / MIME , PGP і GPG . Деякі алгоритми відкритих ключів забезпечують розподіл ключів і секретність (наприклад, обмін ключами Діффі-Хеллмана), деякі надають цифрові підписи (наприклад, алгоритм цифрового підпису), а деякі надають обидва (наприклад, RSA).Приклад зображений на рис.1.2.

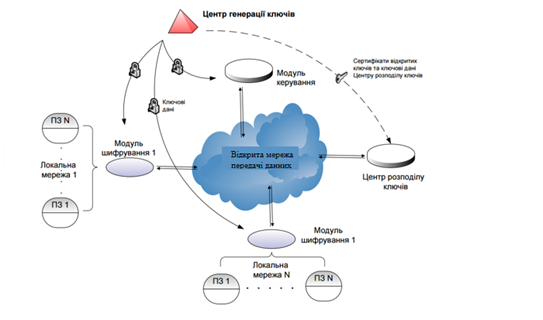


Рис 1.2 Криптографічний захист

Двома з найбільш відомих способів використання криптографії відкритого ключа:

* Шифрування відкритого ключа , в якому повідомлення шифрується за допомогою відкритого ключа одержувача. Повідомлення не може бути розшифровано будь-ким, хто не має відповідного закритого ключа, який, таким чином, вважається власником цього ключа і особою, пов'язаною з відкритим ключем. Це використовується для спроб забезпечення конфіденційності .
* Цифрові підписи , у яких підписується повідомлення з приватним ключем відправника і може бути перевірено будь-ким, хто має доступ до відкритого ключа відправника. Ця перевірка доводить, що відправник мав доступ до закритого ключа, і тому, ймовірно, буде особою, пов'язаною з відкритим ключем. Це також гарантує, що повідомлення не було підроблено, оскільки підпис математично пов'язаний з повідомленням, з якого він спочатку був зроблений, і перевірка не пройде практично для будь-якого іншого повідомлення, незалежно від того, наскільки схоже на початкове повідомлення.

Одним з важливих питань є довіра / доказ того, що певний відкритий ключ є автентичним, тобто, що він є правильним і належить особі або юридичній особі, що претендує, а також не підроблений або замінений злочинною третьою стороною. Є кілька можливих підходів, включаючи:

Інфраструктура відкритого ключа (PKI), в якій одна або більше третіх сторін - відомі як сертифікаційні органи - засвідчують право власності на пари ключів. TLS покладається на це.

"Мережа довіри", яка децентралізує аутентифікацію, використовуючи індивідуальні підтвердження зв'язку між користувачем і відкритим ключем. PGP використовує цей підхід, а також пошук у системі доменних імен (DNS). Система DKIM для цифрового підпису електронних листів також використовує цей підхід.

**1.3.1 Слабкі сторони відкритого ключа**

* Алгоритми

Всі схеми відкритих ключів теоретично сприйнятливі до "грубої атаки". Такі атаки, однак, непрактичні, якщо обсяг обчислення, необхідний для досягнення успіху, - називається "фактор роботи" Клода Шеннона - недоступний для всіх потенційних нападників. У багатьох випадках фактор роботи можна збільшити, просто вибравши більш довгий ключ. Але інші алгоритми можуть мати набагато нижчі робочі фактори, що робить опір атаці грубої сили нерелевантним. Деякі спеціальні і специфічні алгоритми були розроблені, щоб допомогти в нападі на деякі алгоритми шифрування відкритих ключів - як RSA, так і ElGamal шифрування мають відомі атаки, які набагато швидше, ніж підхід грубої сили.

Були виявлені основні недоліки для декількох раніше перспективних алгоритмів асиметричних ключів. Алгоритм "упаковки ранцевих" виявився небезпечним після розробки нової атаки. Нещодавно деякі спроби, засновані на ретельному вимірюванні точної кількості часу, необхідного для зашифрування звичайного тексту, використовувалися для спрощення пошуку ймовірних ключів дешифрування (див. розділ " Атака бічного каналу "). Зараз активно проводиться багато активних досліджень з метою виявлення і захисту від нових алгоритмів атаки.

* Зміна відкритих ключів

Іншою потенційною вразливістю безпеки при використанні асиметричних ключів є можливість атаки "людина-в-середині" , в якій комунікація відкритих ключів перехоплюється третьою стороною ("людина в середині"), а потім змінюється на надавати різні відкриті ключі. Зашифровані повідомлення та відповіді також повинні бути перехоплені, розшифровані та повторно зашифровані зловмисником, використовуючи правильні відкриті ключі для різних сегментів зв'язку, у всіх випадках, щоб уникнути підозр.

Ця атака може здатися важкою для реалізації на практиці, але це неможливо при використанні небезпечних носіїв (наприклад, публічних мереж, таких як Інтернет або бездротові форми зв'язку) - наприклад, зловмисний співробітник мережі Alice або Internet Постачальник послуг (ISP) може виявити його досить простим у здійсненні.

* Інфраструктура відкритого ключа

Один з підходів до запобігання подібним атакам полягає у використанні інфраструктури відкритого ключа (PKI); набір ролей, політик і процедур, необхідних для створення, управління, розповсюдження, використання, зберігання та скасування цифрових сертифікатів, а також керування шифруванням із публічним ключем. Однак це, у свою чергу, має потенційні слабкі сторони.

Наприклад, центр сертифікації, який видає сертифікат, повинен довіряти, що він правильно перевірив особистість ключа, повинен гарантувати правильність відкритого ключа, коли він видає сертифікат, повинен бути захищений від комп'ютерного піратства і повинен мати домовленості всім учасникам перевіряти всі свої сертифікати перед тим, як захистити зв'язок. Веб-браузери , наприклад, постачаються з довгим списком "самозаписуваних сертифікатів ідентичності" від провайдерів PKI - вони використовуються для перевірки достовірності сертифікату, а потім, на другому етапі, сертифікатів потенційних комунікаторів. Зловмисник, який може знищити будь-який один з цих сертифікатів у видачі сертифікату для фіктивного відкритого ключа, може тоді підняти атаку "людина-в-середині" так само легко, як якщо б схема сертифікатів взагалі не використовувалася. У альтернативному сценарії, що обговорюється рідко, зловмисник, який проник на сервери авторитету і отримав свій магазин сертифікатів і ключів (публічних і приватних), міг би підміняти, маскувати, розшифровувати і підробляти транзакції без обмежень.

Незважаючи на свої теоретичні та потенційні проблеми, цей підхід широко використовується. Приклади включають TLS і його попередник SSL , які зазвичай використовуються для забезпечення безпеки для транзакцій веб-браузера (наприклад, для надійної передачі даних кредитної картки в інтернет-магазин).

Окрім опору атаці конкретної пари ключів, при розгортанні систем відкритих ключів необхідно враховувати безпеку ієрархії сертифікації. Деякі центри сертифікації - зазвичай це спеціально побудована програма, що працює на серверному комп'ютері - гарантує ідентичності, призначені для певних приватних ключів, виробляючи цифровий сертифікат. Цифрові сертифікати відкритого ключа , як правило, діють протягом декількох років одночасно, тому пов'язані закриті ключі повинні бути надійно збережені протягом цього часу. Коли приватний ключ, який використовується для створення сертифіката вище в ієрархії серверів PKI, скомпрометований або випадково розкритий, то можливо "атака на людину в середині", що робить будь-який підлеглий сертифікат повністю небезпечним.

**1.3.2 Криптографія симетричного ключа**

Криптографія з симетричним ключем, де використовується один ключ для шифрування і дешифрування

Криптографія за допомогою симетричного ключа відноситься до методів шифрування, в яких і відправник, і одержувач мають один і той же ключ (або, рідше, у яких їхні ключі різні, але пов'язані легко обчислювальним способом). Це був єдиний вид шифрування, який був загальновідомий до червня 1976 року. Симетричні шифри ключів реалізовані як блокові шифри, так і потокові шифри . Блоковий шифр шифрує введення в блоки відкритого тексту, на відміну від окремих символів, форму введення, використовувану потоковим шифром.(рис.1.3)

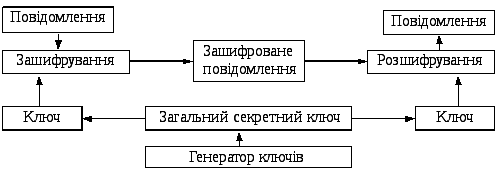


Рис. 1.3 Схема з симетричним шифруванням

Стандарт шифрування даних (DES) і стандарт Advanced Encryption Standard (AES) - це конструкції блокових шифрів, які уряд США призначив криптографічними стандартами (хоча призначення DES остаточно було скасовано після прийняття AES). Незважаючи на його зневажливість як офіційний стандарт, DES (особливо його все ще схвалений і набагато більш безпечний варіант Triple-DES ) залишається досить популярним; він використовується в широкому діапазоні додатків, від шифрування ATM до конфіденційності електронної пошти і безпечного віддаленого доступу . Багато інших блокових шифрів були розроблені і випущені, зі значними відмінностями у якості. Багато, навіть розроблені здатними практиками, були ретельно зруйновані, такі як FEAL .

Поточні шифри, на відміну від типу блоку, створюють довільно довгий потік матеріалу ключа, який поєднується з відкритим текстом біт-за-бітом або символом за символом, подібно до одноразової панелі . У потоковому шифрі вихідний потік створюється на основі прихованого внутрішнього стану, що змінюється, коли шифр працює. Цей внутрішній стан спочатку встановлюється з використанням матеріалу секретного ключа. RC4 є широко використовуваним потоковим шифром. Блокові шифри можуть використовуватися як потокові шифри.

Криптографічні хеш-функції є третім типом криптографічного алгоритму. Вони беруть повідомлення будь-якої довжини як вхідні дані, і виводять короткий хеш фіксованої довжини, який може бути використаний в (наприклад) цифровому підписі. Для хороших хеш-функцій зловмисник не може знайти двох повідомлень, які створюють один і той же хеш. MD4 - це давно використовувана хеш-функція, яка тепер порушена; MD5 , посилений варіант MD4, також широко використовується, але порушується на практиці. Агентство національної безпеки США розробило серію Secure Hash Algorithm з MD5-подібних хеш-функцій: SHA-0 був недосконалим алгоритмом, який агентство вилучило; SHA-1 широко розгортається і більш безпечний, ніж MD5, але криптоаналітики визначили напади на нього; родина SHA-2 покращує SHA-1, але стає вразливою до зіткнень станом на 2011 рік; і американський орган з питань стандартів вважав, що з точки зору безпеки «розважливо» розробити новий стандарт для «значного поліпшення надійності загального алгоритму хеш-алгоритму NIST ». Таким чином, конкурс дизайну хеш-функцій мав на меті вибрати до 2012 року новий національний стандарт США, який буде називатися SHA-3 . Конкурс завершився 2 жовтня 2012 року, коли NIST оголосила, що Keccak буде новим SHA- 3 хеш-алгоритму. На відміну від блокових і потокових шифрів, які є оберненими, криптографічні хеш-функції виробляють хешований вихід, який не може бути використаний для отримання вихідних вхідних даних. Криптографічні хеш-функції використовуються для перевірки достовірності даних, отриманих з ненадійного джерела, або для додавання шару безпеки.

Коди аутентифікації повідомлень (MAC) дуже схожі на криптографічні хеш-функції, за винятком того, що секретний ключ може використовуватися для аутентифікації хеш-значення при отриманні; Це додаткове ускладнення блокує схему атаки на алгоритми голого дайджесту , і тому вважається вартим зусиль.

**РОЗДІЛ 2. ВИКОРИСТАННЯ КРИПТОГРАФІЇ ДЛЯ ШИФРУВАННЯ ДАНИХ**

**2.1 Криптографія на основі еліптичних кривих**

Криптографія еліптичної кривої (ECCcryprography) є підходом до криптографії публічних ключів на основі алгебраїчної структури еліптичних кривих над кінцевими полями . Для забезпечення еквівалентної безпеки ECC вимагає менших ключів у порівнянні з криптографією, яка не є EС (на основі звичайних полів Галуа ).

Еліптичні криві застосовні для узгодження ключів , цифрових підписів , псевдовипадкових генераторів та інших завдань. Непрямо вони можуть бути використані для шифрування шляхом комбінування ключової угоди з симетричною схемою шифрування . Вони також використовуються в декількох алгоритмах цілочисельної факторизації , заснованих на еліптичних кривих, які мають застосування в криптографії, такі як елліптична крива Ленстра .

***Обгрунтування***

Криптографія з відкритим ключем базується на непорушності деяких математичних задач . Ранні системи публічних ключів є надійними, вважаючи, що важко оцінити велике ціле число, яке складається з двох або більше великих простих факторів. Для протоколів на основі еліптичних кривих передбачається, що знаходження дискретного логарифма елемента випадкової еліптичної кривої щодо загальновідомої базової точки неможливе: це "проблема дискретного логарифма еліптичної кривої" (ECDLP). Безпека криптографії еліптичної кривої залежить від здатності обчислювати множення точок і неможливості обчислювати мультиплікату з урахуванням початкових і товарних точок. Розмір еліптичної кривої визначає складність задачі.

Основною перевагою, яку обіцяє криптографія еліптичної кривої, є менший розмір ключа , що знижує вимоги до зберігання та передачі, тобто група еліптичних кривих може забезпечити той же рівень безпеки, який забезпечується системою на основі RSA з великим модулем і відповідно більшим ключем: Наприклад, відкритий ключ 256-бітової еліптичної кривої повинен забезпечувати порівнянну безпеку відкритого ключа 3072-бітного RSA.

Для поточних криптографічних цілей еліптична крива - це плоска крива над кінцевим полем (а не дійсними числами), яка складається з точок, що задовольняють рівняння

, (2.1)

поряд з визначною точкою на нескінченності , позначеної ∞. (Координати тут вибираються з фіксованого кінцевого поля характеристики, що не дорівнює 2 або 3, або рівняння кривої буде дещо складніше.)

Це безліч разом з груповою операцією еліптичних кривих є абелевою групою , з точкою на нескінченності як елемент ідентичності. Структура групи успадковується від групи дільників основного алгебраїчного різноманіття .

, (2.2)

**2.1.1 Криптографічні схеми**

Кілька дискретних логарифмічних протоколів були адаптовані до еліптичних кривих, замінюючи групуз еліптичною кривою:

* Схема еліптичної кривої Діффі – Хеллмана (ECDH) заснована на схемі Діффі-Хеллмана ,
* Схема інтегрованого шифрування еліптичної кривої (ECIES), також відома як схема розширеної шифрування еліптичної кривої або просто схема еліптичної кривої,
* Алгоритм цифрового підпису еліптичної кривої (ECDSA) базується на алгоритмі цифрового підпису ,
* Схема деформації з використанням п-адичної метрики Манхеттена Харрісона,
* Алгоритм цифрового підпису Edwards (EdDSA) заснований на підписі Schnorr і використовує криві Edwards ,
* Схема ключової угоди ECMQV базується на схемі ключових угод MQV ,
* Схема неявних сертифікатів ECQV .

Останнім часом було запроваджено велику кількість криптографічних примітивів на основі білінійних відображень на різних групах еліптичних кривих, таких як парі Вейля і Тейта . Схеми, засновані на цих примітивах, забезпечують ефективне шифрування на основі ідентичності , а також підписи на основі парних з'єднань , шифрування підписів, угоду про ключ і повторне шифрування проксі-серверів .

**2.1.2 Реалізація ECC**

**Параметри домену**

Для використання ECC всі сторони повинні узгодити всі елементи, що визначають еліптичну криву, тобто параметри домену схеми. Поле визначається p у простому випадку, а пара m та f - у двійковому випадку. Еліптична крива визначається константами a та b, що використовуються в її визначальному рівнянні. Нарешті, циклічна підгрупа визначається її генератором (aka базовою точкою ) G. Для криптографічного застосування порядок G , тобто найменший позитивний номер n такий, що ( точка на нескінченності кривої і елемент ідентичності ), як правило, проста. Оскільки n - розмір підгрупи з теореми Лагранжа випливає, що число є цілим числом. У криптографічних додатках це число h , зване кофактором , має бути малим () і, переважно,. Підсумовуючи: у простому випадку параметри домену є (p,a,b,G,n,h) ; у двійковому випадку вони є (m,f,a,b,G,n,h) .

Якщо не існує гарантії того, що параметри домену генеруються стороною, довіреною щодо їх використання, параметри домену повинні бути перевірені перед використанням.

Генерація параметрів домену зазвичай не робиться кожним учасником, оскільки це передбачає обчислення кількості точок на кривій, що вимагає багато часу і важко реалізувати. Як результат, кілька стандартних органів опублікували параметри домену еліптичних кривих для кількох загальних розмірів полів. Такі параметри домену зазвичай відомі як "стандартні криві" або "названі криві"; названа крива може посилатися або на ім'я, або на унікальний ідентифікатор об'єкта, визначений у стандартних документах:

* NIST , рекомендовані еліптичні криві для державного використання
* SECG , SEC 2: Рекомендовані параметри домену еліптичної кривої
* ECC Brainpool ( RFC 5639 ), стандартні криві ECC Brainpool і генерація кривих

Тест-вектори SECG також доступні. NIST схвалив багато кривих SECG, тому існує значне перекриття між специфікаціями, опублікованими NIST і SECG. Параметри домену EC можуть бути вказані за значенням або за назвою.

Якщо один (незважаючи на вищенаведене) хоче побудувати власні параметри домену, слід вибрати основне поле, а потім скористатися однією з наступних стратегій, щоб знайти криву з відповідним (тобто, майже простим) числом точок, використовуючи один з наступних методів. :

* Виберіть випадкову криву і використовуйте загальний алгоритм підрахунку точок, наприклад, алгоритм Шуофа або алгоритм Шуофа – Елкіса – Аткина
* Виберіть випадкову криву від сім'ї, яка дозволяє легко обчислити кількість точок (наприклад, криві Кобліца ), або
* Вибираємо кількість точок і генеруємо криву з цією кількістю точок, використовуючи складну техніку множення .

Кілька класів кривих слабкі і їх слід уникати:

* Криві надз неприйнятними m є вразливими до Вейля .
* Криві такі, що n ділить (де p - характеристика поля: q для простого поля, або 2 для двійкового поля) для досить малих B уразливі до атаки Менеза – Окамото – Ванстона (MOV), яка застосовує звичайну задачу дискретного логарифму (DLP) в області розширення малого ступеня вирішувати ECDLP. Зв'язане B слід вибирати таким чином, щоб дискретні логарифми у полі щонайменше так само важко обчислити як дискретні журнали на еліптичній кривій.
* Криві такі, що є вразливими до атаки, яка відображає точки на кривій на адитивну групу .

**Розміри ключів**

Тому що всі найшвидші відомі алгоритми, які дозволяють вирішувати ECDLP ( дитячий крок гіганта, рол Полларда тощо), потребують З кроків, випливає, що розмір базового поля повинен бути приблизно вдвічі більшим за параметр безпеки. Наприклад, для 128-бітової безпеки потрібна крива , де . Це можна протиставити криптографії кінцевого поля (наприклад, DSA ), яка вимагає 3072-бітних відкритих ключів і 256-бітових закритих ключів і криптографії цілочисельної факторизації (наприклад, RSA ), яка вимагає 3072-бітове значення n , де приватний ключ має бути настільки ж великим. Проте відкритий ключ може бути меншим, щоб пристосувати ефективне шифрування, особливо коли обчислювальна потужність обмежена.

Найбільш складна схема ECC (публічно) порушена на сьогоднішній день мала 112-бітний ключ для простого випадку поля і 109-бітний ключ для бінарного поля. У першому випадку це було порушено в липні 2009 року за допомогою кластера з більш ніж 200 ігрових консолей PlayStation 3 і може бути завершено через 3,5 місяці за допомогою цього кластера під час безперервної роботи. Двійковий полевий випадок був розбитий у квітні 2004 року за допомогою 2600 комп'ютерів протягом 17 місяців.

Нинішній проект спрямований на подолання виклику ECC2K-130 від Certicom, використовуючи широкий спектр різних апаратних засобів: CPU, GPU, FPGA.

**Проективні координати**

Ретельне вивчення правил додавання показує, що для того, щоб додати дві точки, потрібно не тільки кілька доповнень і множень але також операція інверсії. Інверсія (для заданого знайти такий, що на один-два порядки повільніше, ніж множення. Однак точки на кривій можуть бути представлені в різних системах координат, які не вимагають операції інверсії для додавання двох точок. Було запропоновано декілька таких систем: у проективній системі кожна точка представлена ​​трьома координатами (X,Y,Z) використовуючи наступне співвідношення: ; в системі Якобіан точка також представлена ​​трьома координатами(X,Y,Z), але використовується інше співвідношення:; у системі Лопес-Дахаб це співвідношення ; в модифікованій системі Якобіан використовуються однакові відносини, але зберігаються і використовуються для розрахунку чотири координати; а в системі Якова Чудновського використовуються п'ять координат. Зауважимо, що можуть існувати різні правила іменування, наприклад, стандарт IEEE P1363 -2000 використовує "проективні координати" для позначення того, що зазвичай називають координатами Якобіан. Додаткове прискорення можливе при використанні змішаних координат.

**Швидке зменшення (криві NIST)**

Скорочення по модулю p (яке необхідно для складання і множення) може бути виконано набагато швидше, якщо простое p - псевдо- Мерсеннове просте , тобто ; наприклад, або . У порівнянні зі скороченням Барретта , може бути прискорене на порядок. Прискорення тут є скоріше практичним, ніж теоретичним, і випливає з того, що модулі чисел проти чисел близько двох потужностей можуть бути ефективними за допомогою комп'ютерів, що працюють на двійкових числах з побітовими операціями .

Криві над з псевдо-Мерсенне p рекомендовано NIST. Ще однією перевагою кривих NIST є те, що вони використовують a = −3, що покращує додавання до координат Якобіан.

На думку Бернштейна і Ланге, багато рішень, пов'язаних з ефективністю в NIST FIPS 186-2, є не оптимальними. Інші криві більш безпечні і працюють так само швидко.

**2.2 Застосування еліптичних кривих для задач захисту інформації**

Захист інформації відіграє одну з ключових ролей в забезпеченні інформаційної безпеки держави. В останні роки в зв’язку з швидким розвитком інформаційних технологій, що залучають все більше і більше користувачів, які в процесі роботи обмінюються інформацією за допомогою систем електронного зв’язку, виникає необхідність розвитку засобів захисту інформації. Вирішити задачу захисту інформації можна шляхом використання криптографічних алгоритмів

Розрізняють два типи криптографічних алгоритмів: симетричні і асиметричні. В першому випадку обидва абоненти, що беруть участь в процесі передачі інформації, використовують однаковий ключ, а в другому — різні, “секретний” і “відкритий”.

В останні роки інтенсивно розвивається криптографія еліптичних кривих (ЕК), де основною криптографічною операцією є пошук кратних точок еліптичної кривої, тобто множення точки еліптичної кривої на скаляр на основі операції додавання цих точок. Особливий інтерес до криптографії еліптичних кривих обумовлений такими перевагами – швидкодія та невелика довжина ключа.

У сучасних криптосистемах на основі еліптичних кривих бінарної розмірності в діапазоні від 150 до 350 забезпечується рівень криптографічної стійкості, який потрібно використовувати у відомих криптографічних системах бінарної розмірності від 600 до 1400 і більше.

У приведеній нижче табл. 2.1 порівнюються наближені розміри параметрів еліптичних систем і криптосистеми RSA, що забезпечують однакову стійкість шифру. Ці дані отримані на основі сучасних методів розв’язання задачі дискретного логарифмування еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) та факторизації (пошуку дільників) для великих цілих чисел.

Як показує аналіз таблиці, використання еліптичних кривих дозволяє будувати стійкі системи з ключами значно менших розмірів у порівнянні з традиційними асиметричними криптоалгоритмами. Такі системи потребують меншого обсягу обчислювальних ресурсів, тому зручні для використання у смарт-картках та портативних телефонах.

Таблиця 2.1

|  |  |
| --- | --- |
| Система на основі еліптичної кривої (точка P) | RSA (довжина модуля n) |
| 1024 біт | 3084 біт |
| 3250 біт | 9750 біт |
| 15500 біт | 46500 біт |

На сьогодні еліптичні криві застосовують для реалізації різноманітних класів криптосистем, зокрема їх можна використовувати для побудови симетричних, асиметричних систем та систем електронного цифрового підпису (ЕЦП) (рис. 2.1). Класифікуються так:

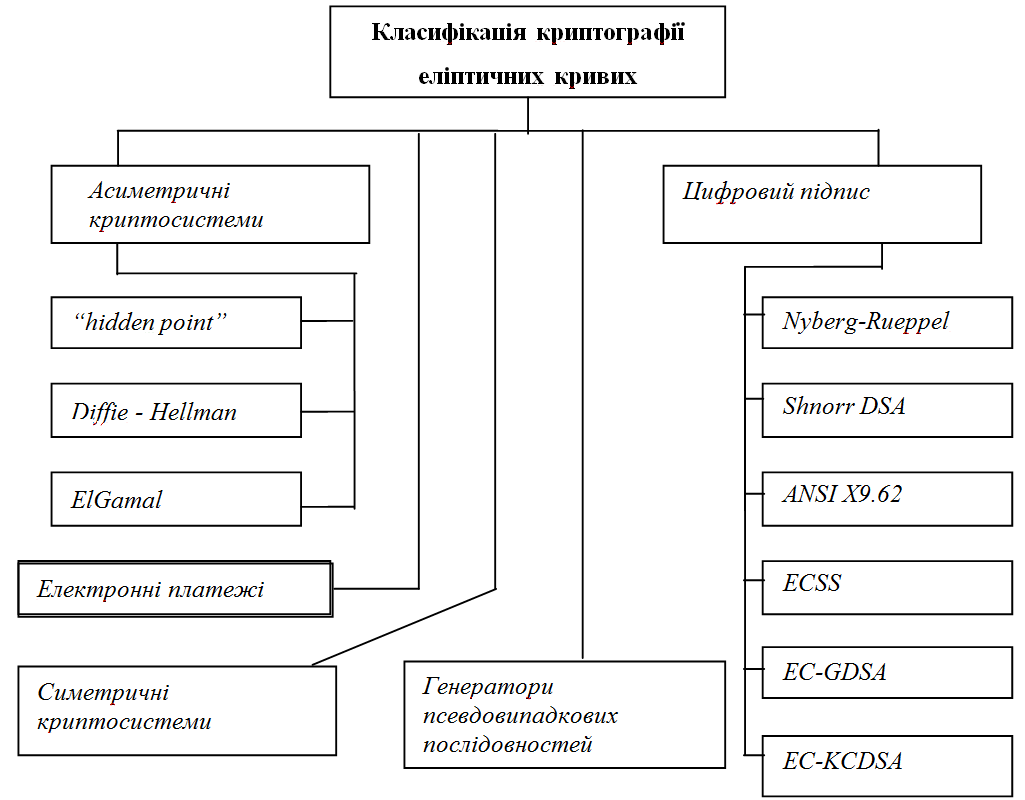


Рис. 2.1 Класифікація застосування еліптичних кривих для задач захисту інформації

На рис. 2.1 зображено класифікацію сучасних методів криптографії, що базуються на застосуванні еліптичних кривих. Аналіз показує, що математичний апарат еліптичних кривих можна застосовувати

1) в асиметричних криптосистемах;

2) в симетричних криптосистемах;

3) для реалізації електронного цифрового підпису;

4) для електронних платежів;

5) як генератори псевдовипадкових послідовностей.

**2.2.1 Проблеми застосування еліптичних кривих**

Незважаючи на вагомі переваги існують і певні проблеми та труднощі застосування ЕК. Зокрема, виділяють такі класи задач:

1)генерування параметрів еліптичної кривої;

2)обчислення точок еліптичної кривої;

3)проблема дискретного логарифма.

Задачею генерування параметрів еліптичної кривої виду

(2.1)

, над простим полем GF(p) є знаходження таких параметрів:

a) просте число p – модуль перетворення груп точок еліптичної кривої;

b) просте число q, яке визначає порядок циклічної підгрупи групи точок еліптичної кривої EК;

c) коефіцієнти, що задають еліптичну криву EК.

Просте число p має задовольняти нерівність . Верхня границя значення числа визначаєтьсяконкретною реалізацією криптосистеми. Для створення цифрового підпису довжиною 512 біт, як це було длястандарту ГОСТ 34.310-95, число р має задовольняти нерівність. В подальшому вважаємо, що числоp лежить у межах.

Для генерації простого числа можна використовувати:

* процедуру генерації числа q в стандарті ГОСТ 34.310-95;
* генерацію випадкового простого числа довжиною 256 біт;
* генерацію сильного простого числа.

В стандарті Х9.62-1998 пропонується 3 способи отримання параметрів еліптичної кривої. Перший спосіб полягає у використанні кривих, заданих у стандарті Х9.62-1998. Серед них тільки одна еліптична крива задовольняє потрібному простому числу. Другий спосіб полягає у випадковому виборі еліптичної кривої і перевірці її параметрів. Третій спосіб полягає в виборі потрібних параметрів і побудові кривої за цими параметрами.

Незважаючи на існуючі підходи до вирішення задачі генерування параметрів ЕК існують певні проблеми стосовно продуктивності генерування потрібного числа кривих за певний період часу. Тому актуальною залишається розробка нових методів, що дозволяют ефективно вирішити цю задачу.

**2.2.2 Використання еволютивного підходу до задач генерування параметрів ЕК**

Якщо на деякій множині задана складна (цільова) функція від кількох змінних, то еволютивний алгоритм – це алгоритм, який дозволяє за оптимальний час знаходити максимально наближене значення . Таким чином еволютивний підхід може бути ефективно застосований для знаходження оптимальних (або квазі-оптимальних) рішень в задачах з обмеженням на часовий ресурс.

Для реалізації еволютивного підходу до вирішення задачі генерування параметрів еліптичної кривої авторами взято за основу алгоритм А.12.4. стандарту IEEE P1363. На основі цього алгоритму авторами розроблено алгоритм генерування параметрів еліптичної кривої з використанням еволютивного підходу. Схему запропонованого алгоритму зображено на рис. 1.

Ключовим моментом при розробці еволютивних алгоритмів є визначення критерію (цільової функції), на основі якого здійснюється відбір нових об’єктів. Авторами розроблено такий критерій на основі наведеного в стандарті співвідношення оцінки гладкості кривої :

(2.2)

де

Робота розробленого алгоритму схожа з роботою типових генетичних алгоритмів і полягає в наступному. Спочатку в “Ініціалізації популяції” генеруються випадковим чином об’єкти з параметрами еліптичної кривої a,b. На наступному етапі здійснюється їх сортування в порядку зростання значення f. З першого етапу вибираються 1024 найкращі, тобто абсолютне значення критерію f є найменшим, і заносяться в породжувальний масив. Далі здійснюється ітеративна процедура модифікації об’єктів Pi з породжувального масиву шляхом застосування операції мутації, причому в операторі мутації враховано напрям зміни коефіцієнтів a, b. Це дозволило суттєво підвищити ефективність роботи алгоритму. Далі обчислюється критерій f для отриманого шляхом мутації нового об’єкта. Якщо отримане абсолютне значення менше за попереднє, то новий об’єкт записується на місце попереднього (предка). В кінці алгоритму здійснюється перевірка на невиродженість отриманої еліптичної кривої.

На основі запропонованого алгоритму розроблено програмний засіб, який дозволяє отримати пари коефіцієнтів a, b, придатні для побудови стійких криптосистем на основі еліптичних кривих. Результати роботи програми наведено у табл. 2.2 і 2.3. Загалом було отримано більше 600 пар, проте після додаткової перевірки на невиродженість залишилось 208. В таб. 2.2 наведено коефіцієнти сі, для яких згідно з алгоритмом розраховувалися коефіцієнти a, b.

Таблиця 2.2

|  |  |
| --- | --- |
| Коефіцієнт | Значення коефіцієнта |
|  | 51799996682396758944004974568555459888197891979211637345686009034147319967190 |
|  | 1418654552780437532991559434618384197125875637142781736228970970729409852026 |
|  | 34002950479911914546202967720669257702764443651718841281013484396596574419760 |
|  | 36717165088815776642377839043303773285890560685433992542928258356134033756828 |
|  | 2635944249223345268139692779222765471465111458745629045410922635067996930132 |
|  | 3845057412174940409062799905218778690139552101034540626848544521540032909299 |

У таб. 2.3 наведено кількість згенерованих пар коефіцієнтів ЕК при певних коефіцієнтах сі. Також в таблиці показано кількість пар коефіцієнтів a, b однакової та різної розмірності.

Для підвищення ефективності розробленого програмного засобу проводяться роботи щодо реалізації розподілених обчислень на кластері з 5–10 машин, об’єднаних в мережу. Це дасть змогу зменшити часовий ресурс та збільшити загальну кількість пар коефіцієнтів, що генеруються. Схема для генерації (рис.2.2).

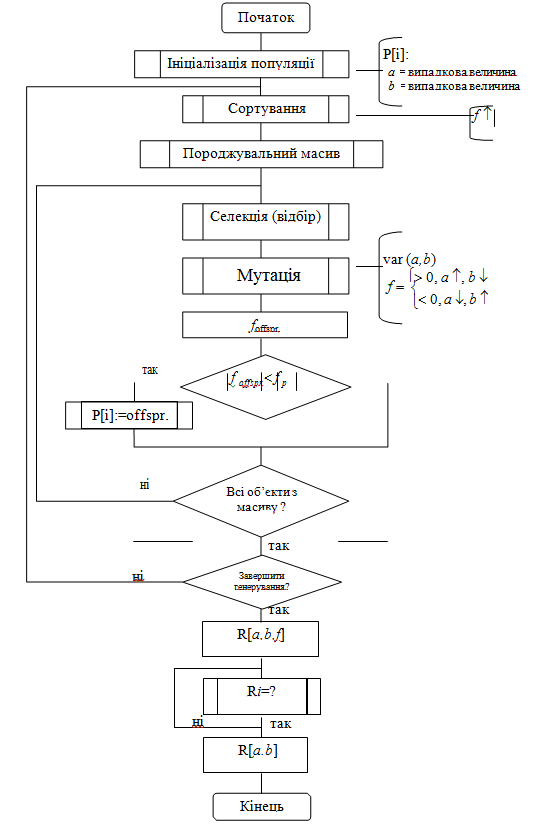


Рис.2.2 Схема алгоритму генерування параметрів еліптичної кривої

Для підвищення ефективності розробленого програмного засобу проводяться роботи щодо реалізації розподілених обчислень на кластері з 5–10 машин, об’єднаних в мережу. Це дасть змогу зменшити часовий ресурс та збільшити загальну кількість пар коефіцієнтів, що генеруються.

Запропонованоалгоритмгенеруванняпараметрівеліптичноїкривоїдляцифровогопідпису,щодозволяєефективновизначатикоефіцієнтиеліптичноїкривої. Розроблений метод базується на еволютивному підході, що значно спрощує застосування запропонованого алгоритму на практиці. Наведено результати роботи програми, розробленої на основі даного методу, які підтверджують ефективність методу. Отже, доцільно використовувати розроблений метод в криптосистемах, що базуються на еліптичних кривих для захисту інформації на практиці.

Таблиця 2.3

|  |  |  |  |
| --- | --- | --- | --- |
| Коефіцієнт с | Загальна к-сть пар | К-сть пар приблизно рівної розмірності | К-сть пар при різної розмірності |
|  | 4 | 1 | 3 |
|  | 18 | 9 | 9 |
|  | 16 | 5 | 11 |
|  | 20 | 7 | 13 |
|  | 125 | 63 | 62 |
|  | 25 | 16 | 9 |
| Всього | 208 | 101 | 107 |

**2.3 Розширений стандарт шифрування**

Розширений стандарт шифрування ( AES ), також відомий під назвою Rijndael - симетричний алгоритм блочного шифрування (розмір блоку 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийняття як американський стандарт шифрування урядом США . Вибір на AES з розширення на широке використання та активний аналіз алгоритму, як це було з його попереднього, DES . Державний інститут стандартів і технологій ( англ. National Institute of Standardsand Technology, NIST) США опублікували попередню специфікацію AES 26 жовтня 2001 року, після п'ятилітної підготовки. 26 травня 2002 року АЕС оголосила стандартні стандарти шифрування. Станом на 2009 рік AES є одним із найпоширеніших алгоритмів симетричного шифрування.

В принципі, алгоритм, пропонований Рейменом і Дейцменом, і AES не одне і те ж. Алгоритм Рейндол підтримує широкий діапазон розміру блоку та ключа. AES має фіксовану довжину в 128 біт, а розмір ключа може бути значення 128, 192 або 256 біт.У той час, коли Рейндол підтримує блоку та ключ із кроком, 32 біт у діапазоні від 128 до 256. Через фіксований розмір блоку AES оперує з масивом 4 × 4 байт , що накладає старий ( версію алгоритму із більшим розміром блоку додаткових колонок).

Для ключа 128 біт алгоритм має 10 раундів у яких послідовно виконуються операції

1. subBytes ()
2. shiftRows ()
3. mixcolumns () (у 10-му раунді пропускається)
4. xorRoundKey ()

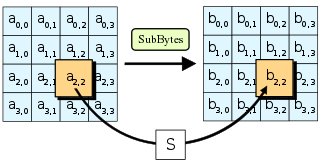


Рис. 2.3 ПроцедураSubBytes

A) Процедура SubBytes (рис. 2.3) обробляє кожен байт стану незалежно, проводячи нелінійну заміну байтів, використовуючи таблицю заміну (S-box). Така операція передбачає нелінійність алгоритму шифрування. Побудова S-box складається з двох кроків. По-перше, проводити отримання зворотного числа в полі Галуа . По-друге, до кожного байту b з, який складається S-boxreces така операція:

(2.3)

де, , Iде є і-ий біт b, a – і-ий біт константи

(2.4)

Таким чином, забезпечується захист від атак, закладених на простих алгебраїчних властивостях.

S-box можна відобразити таблицю простої підстановки (рис.2.3).

Наприклад, на вході 19 на виходять отримані d4.

Фактично це звичайний шифр простої підстановки.



Рис. 2.4 Таблиця простої підстановки S-box

B) ShiftRows (рис. 2.5)

У процедурах ShiftRows , байти в кожному ряду стан циклічно змушують вліво. Розмір зміщення байтів кожного рядка відсутній

ShiftRows працює з рядками таблиці. При цій трансформації рядів стан циклічно збігається на байтах по горизонталі, залежно від номера рядка. Для нульового рядка r = 0, для першого рядка r = 1 і т. д. Таким чином, кожна колонка вихідного стану після застосування ShiftRows складається з байтів з кожної колонки початкового стану. Для алгоритму Rijndael патерн зсуві рядки для 128 - і 192-бітних рядків єдиний. Однак для блочного розміру 256 збігається від попереднього тим, що 2, 3, і 4-й рядки змінюються на 1, 3, і 4 байта, відповідно, фактично це проста перестановка байтів таблиць 4х4.

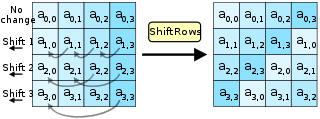


Рис 2.5 Процедура ShiftRows

С) MixColumns (рис.2.6)

У процедурі MixColumns , кожна колонка стану змінюється з фіксованим багаточленом c (x) .

У процедурах MixColumns , чотири байки кожної колонки змінюються, використовуючи для цього зворотний лінійну трансформацію. MixColumns опрацьовує стан за колонками, трактуючи кожний з них як поліном четвертого ступеня . Над цими поліномами виконується множення в по модулю на фіксований многочлен. Разом з ShiftRows , MixColumns вносить дифузію в шифр .

Під час цієї операції, кожен стовпчик множиться на матрицю, яка для 128-бітного ключа має вигляд

(2.5)

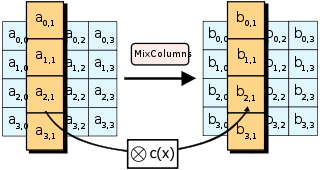


Рис 2.6 ПроцедураMixColumns

D) AddRoundKey (рис.2.7)

У процедурі AddRoundKey , яка базується на об'єкті RoundKey, використовуючи операцію XOR .

У процедурах AddRoundKey , RoundKey кожен раунд об'єднаний зі статусом. Для кожного раунду, що виходить з CipherKey, використовуючи процедуру KeyExpansion ; кожен RoundKey такого ж розміру, що і держава.

Процедура виробляє побітний XOR кожного байта держави з кожним байтом RoundKey .Фактично це звичайний побайтовий XOR байт ключа з байтами таблиць.

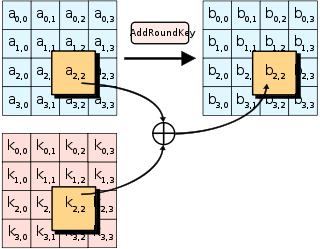


Рис 2.7 Процедура AddRoundKey

**РОЗДІЛ 3. ПЕРЕДАЧА ДАНИХ ЧЕРЕЗ ПУБЛІЧНУ МЕРЕЖУ**

**3.1 Опис середовища розробки**

Для генерації, шифрування/розщифрування було обране середовище Python 3.7.3

Python - це мова програмування з декількома парадигмами . Об'єктно-орієнтоване програмування та структуроване програмування повністю підтримуються, і багато з його функцій підтримують функціональне програмування та аспектно-орієнтоване програмування (у тому числі метапрограмуванням та метаоб'єктами (магічними методами)). Багато інших парадигм підтримуються за допомогою розширень, включаючи розробку за контрактом і логічне програмування .

Python використовує динамічну типізацію, атакож комбінацію підрахунку опорних даних і колектор авиявлення сміття для керування пам'яттю. Вона також має динамічну роздільну здатність імен (пізнєзв'язування), яка пов'язує метод і імена змінних підчас виконання програми.

Дизайн Python пропонує певну підтримку функціонального програмування в традиції Lisp . Він має функції filter , map та reduce ; список розуміння , словники , множини та генераторні вирази. Стандартна бібліотека має два модулі (itertools і functools), які реалізують функціональні інструменти, запозичені з Haskell і Standard ML.

Вона підтримує декілька парадигм програмування, включаючи об'єктно-орієнтовану, важливу, функціональну та процедурну, і має велику і всеосяжну стандартну бібліотеку. Інтерпретатори Python доступні для багатьох операційних систем. CPython, еталонна реалізація Python, є програмним забезпеченням із відкритим кодом і має спільну модель розвитку, як і майже всі його варіанти реалізації. CPython керує неприбутковий Python Software Foundation.

Серед основних її переваг можна назвати такі:

• чистийсинтаксис (для виділення блоків слід використовувати відступи);

• переносність програм (що властиве більшості інтерпретованих мов);

• стандартний дистрибутив має велику кількість корисних модулів (включно з модулем для розробки графічного інтерфейсу);

• можливість використання Python в діалоговому режимі (дуже корисне для експериментування та розв'язання простих задач);

• стандартний дистрибутив має просте, але разом із тим досить потужне середовище розробки, яке зветься IDLE і яке написане на мові Python;

• зручний для розв'язання математичних проблем (має засоби роботи з комплексними числами, може оперувати з цілими числами довільної величини, у діалоговому режимі може використовуватися як потужний калькулятор);

• відкритий код (можливість редагувати його іншими користувачами).

Python має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис Python, динамічна обробка типів, а також те, що це інтерпретована мова, роблять її ідеальною для написання скриптів та швидкої розробки прикладних програм у багатьох галузях на більшості платформ.

Інтерпретатор мови Python і багата Стандартна бібліотека (як вихідні тексти, так і бінарні дистрибутиви для всіх основних операційних систем) можуть бути отримані з сайту Python www.python.org, і можуть вільно розповсюджуватися. Цей самий сайт має дистрибутиви та посилання на численні модулі, програми, утиліти та додаткову документацію.

Інтерпретатор мови Python може бути розширений функціями та типами даних, розробленими на C чи C++ або на іншій мові, яку можна викликати із C). Python також зручна як мова розширення для прикладних програм, що потребують подальшого налагодження.

***Переваги мови***

Безсумнівною перевагою є те, що інтерпретатор Python реалізований практично на всіх платформах і операційних системах. Першою такою мовою була C, проте його типи на різних машинах могли займати різну кількість пам'яті і це служило деяким перешкодою при написанні дійсно яку переносять програми. Python ж таким недоліком не володіє.

Наступна важлива риса - розширюваність мови, цього надається велике значення і мова була задумана саме як розширювана. Це означає, що є можливість вдосконалення мови усіма бажаючими. Інтерпретатор написаний на С і вихідний код доступний для будь-яких маніпуляцій. У разі необхідності, можна вставити його в свою програму і використовувати як вбудовану оболонку. Або ж, написавши на C свої доповнення до Python і скомпілювавши програму, отримати «розширений» інтерпретатор з новими можливостями.

Наступне гідність - наявність великого числа підключаються до програми модулів, що забезпечують різні додаткові можливості. Такі модулі пишуться на С і на самому Python і можуть бути розроблені усіма досить кваліфікованими програмістами. Як приклад можна навести такі модулі:

Numerical Python - розширені математичні можливості, такі як маніпуляції з цілими векторами і матрицями;

Tkinter - побудова додатків з використанням графічного інтерфейсу користувача (GUI) на основі широко розповсюдженого на X-Windows Tk-інтерфейсу;

OpenGL - використання великої бібліотеки графічного моделювання дво- і тривимірних об'єктів Open Graphics Library фірми Silicon Graphics Inc. Даний стандарт підтримується, в тому числі, в таких поширених операційних системах як Microsoft Windows 95 OSR 2, 98 і Windows NT 4.0.

***Недоліки мови***

Єдиним недоліком, поміченим автором, є порівняно невисока швидкість виконання Python-програми, що обумовлено її інтерпретованих. Однак на наш погляд, це з лишком окупається перевагами мови при написанні програм не дуже критичних до швидкості виконання.

Завдяки простоті і гнучкості мови Python, його можна рекомендувати користувачам (математикам, фізикам, економістам і т.д.) які не є програмістами, але використовують обчислювальну техніку та програмування в своїй роботі.

Програми на Python розробляються в середньому в півтора-два (а часом і в два-три) рази швидше, ніж на компільованих мовах (С, С ++, Pascal). Тому, мова може представляти не малий інтерес і для професійних програмістів, що розробляють додатки, не критичні до швидкості виконання, а також програми, що використовують складні структури даних. Зокрема, Python добре зарекомендував себе при розробці програм роботи з графами, генерації дерев.

**3.2 Генерація пари ключів ECC**

Для початку потрібно згенерувати 4 ECC ключа (2 на стороні А приватний «PrivateKey\_A.pem» та публічний «PublicKey\_A.pem» і 2 на стороні Б приватний«PrivateKey\_B.pem» та публічний «PublicKey\_B.pem»)

Для цього запускаємо програму GenerateKeys.pyна основі середовища Python.

На рис. 3.1 зображено запущену програму, яка згенерувала ключі.

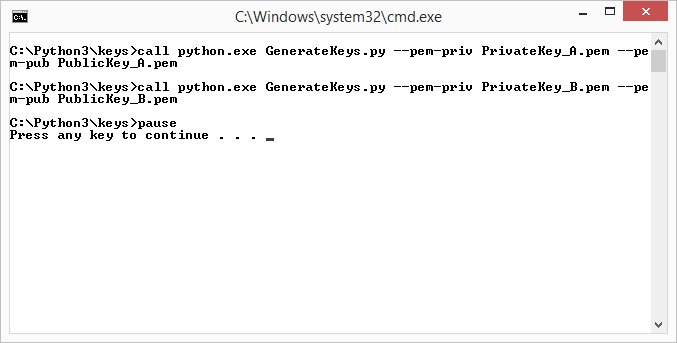


Рис. 3.1 Програма для генерування ЕСС ключів

***Код програми для генерації ключів з коментарями.***

# Підключаемо необхідні бібліотеки

importclick

fromjwcryptoimportjwk

# Задаємо команди та аргументи запуску програми

@click.command()

@click.option('--pem-priv', 'pemPriv',

type=click.File('wb'),

default=None,

help='Name of the private key in PEM format to create. If it is not given PEM file will not be created.')

@click.option('--pem-pub', 'pemPub',

type=click.File('wb'),

default=None,

help='Name of the public key in PEM format to create. If it is not given PEM file will not be created.')

def main(pemPriv, pemPub):

# Генераціяключа

key = jwk.JWK.generate(kty='EC', crv='P-256', use='sig')

if pemPriv != None:

# Запис згенерованого приватного ключа у файл

pemPriv.write(key.export\_to\_pem(private\_key=True, password=None))

if pemPub != None:

# Запис згенерованого публічного ключа у файл

pemPub.write(key.export\_to\_pem(private\_key=False, password=None))

if \_\_name\_\_ == "\_\_main\_\_":

main()

Після цього у нас появляються 4 ключа. Таб. 3.1.

Таблиця 3.1.

Згенеровані пари ключів приватний A/Б та публічний А/Б

|  |  |
| --- | --- |
| «PrivateKey\_A.pem» | MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgWLoU4f99zeLauQCa  fZu8PQ4BtQJ8CGXdHzEGVFQvLcyhRANCAAQ2AIThYnmuRYwV5H69Ljhx+JqSxbG/  Z9Kgf1SDMKjeIN3g3RBOOTCrIhT64OIn4KJnA7zgZ9CwOL81euaRTzDS |
| «PrivateKey\_B.pem» | MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQg5zbRwJJj0lJvd6HD  wLypynob89FhJCId3SB5NMNGA1qhRANCAATawccKQRkm0168PiGOjRUOdJ2c0O2P  ES8MJYZXspY97Oprqkd9bqqtyzLVnPUB4sz49Nox/UmQU5xocGAhHdNp |
| «PublicKey\_A.pem» | MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEWumMZfQLTbsK0wjtJLAMaBOsmZOM  PrwDlw8YCeJ7UvR35Jr5Yjr42thDhhowivyabqsL+Tm344tWfv0pdZ7L6w== |
| «PublicKey\_B.pem» | MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2sHHCkEZJtNevD4hjo0VDnSdnNDt  jxEvDCWGV7KWPezqa6pHfW6qrcsy1Zz1AeLM+PTaMf1JkFOcaHBgIR3TaQ== |

**3.3 Шифрування і розшифрування даних**

Для початку треба підключити скрипта. А самеecc\_kdfіaes\_cipher, вони потрібні для того щоб проїніціалізувати і зашифрувати/розшифрувати файл.

Для реалізації механізму Діффі-Хеллмана кожна зі сторін генерує ключову пару протоколу узгодження ключів Діффі-Хеллмана, яка стає їх поточної ключовою парою.

Кожне повідомлення починається з заголовка, що містить поточний відкритий ключ відправника. При отриманні повідомлення відкритий ключ відправника використовується для здійснення кроку механізму Діффі-Хеллмана, в рамках якого виробляється загальний ключовийДля реалізації механізму Діффі-Хеллмана кожна зі сторін генерує ключову пару протоколу узгодження ключів Діффі-Хеллмана, яка стає їх поточної ключовою парою. Кожне повідомлення починається з заголовка, що містить поточний відкритий ключ відправника. При отриманні повідомлення відкритий ключ відправника використовується для здійснення кроку механізму Діффі-Хеллмана, в рамках якого виробляється загальний ключовий матеріал і генерується нова ключова пара.

Таким чином сторони зв'язку безперервно обмінюються відкритими ключами і оновлюють їх ключові пари. матеріал і генерується нова ключова пара. Таким чином сторони зв'язку безперервно обмінюються відкритими ключами і оновлюють їх ключові пари (додаток 1).

fromcryptography.hazmat.backendsimportdefault\_backend

fromcryptography.hazmat.primitives import hashes

from cryptography.hazmat.primitives.asymmetric import ec

from cryptography.hazmat.primitives.kdf.hkdf import HKDF

from cryptography.hazmat.primitives import serialization

import codecs

import os

class ECDH\_KDF(object):

def \_\_init\_\_(self, private\_key, public\_key, key\_length, salt, info):

salt\_length = 16

self.backend = default\_backend()

self.host\_key\_pair serialization.load\_pem\_private\_key(self.read\_key\_bytes(private\_key), password=None, backend=self.backend)

#Deserialize public key: extract from private or directly from pem file

try:

self.device\_public\_key serialization.load\_pem\_private\_key(self.read\_key\_bytes(public\_key), password=None, backend=self.backend).public\_key()

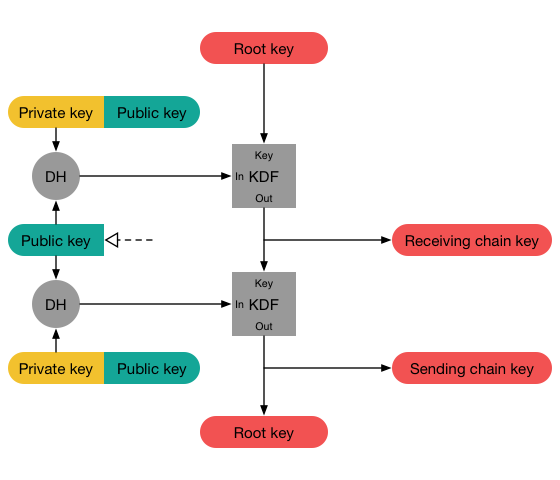


Рис 3.2 Блок схема алгоритму ініціалізації KDF

Для шифрування в алгоритмі AES застосовуються такі процедури перетворення даних:

1. ExpandKey - Обчислення раундова ключів для всіх раундів.

2. SubBytes - Підстановка байтів за допомогою таблиці підстановок;

3. ShiftRows - Циклічний зсув рядків у формі на різні величини;

4. MixColumns - Змішування даних всередині кожного стовпця форми;

5. AddRoundKey - Додавання ключа раунду з формою.

Порядок виконання процедур 2 і 3 можна поміняти місцями в силу визначення цих операцій.

Процедури 4 і 5 теж можна виконувати в різному порядку, але при цьому змінюється кількість їх викликів, оскільки MixColumns (AddRoundKey (A, B)) =

AddRoundKey (MixColumns (A), MixColumns (B)).

Детальніше описано в п.2.3та в додатку 1

Шифрування показано на схемі (рис.3.3).

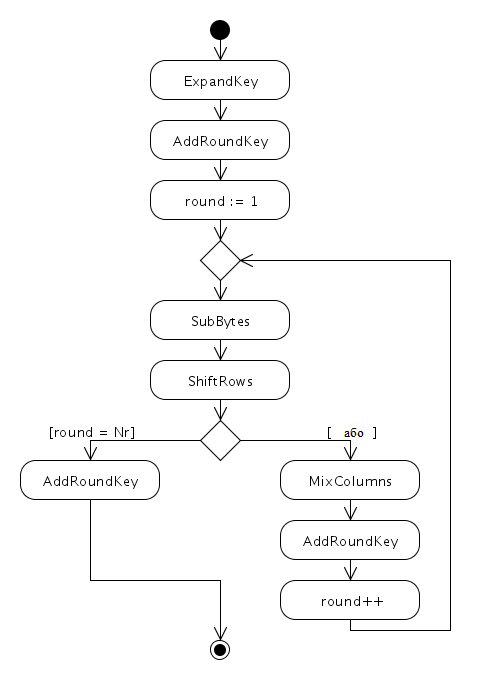


Рис. 3.3 Блок схема алгоритму шифрування AES

При розшифруванні всі перетворення відбуваються в зворотному порядку. Використовуються такі зворотні перетворення натомість відповідних шифруючих:

• InvSubBytes - Підстановка байтів за допомогою зворотного таблиці підстановок;

• InvShiftRows - Циклічний зсув рядків у формі на різні величини;

• InvMixColumns - Змішування даних всередині кожного стовпця форми;

Розшифування показано на схемі (рис. 3.4.)

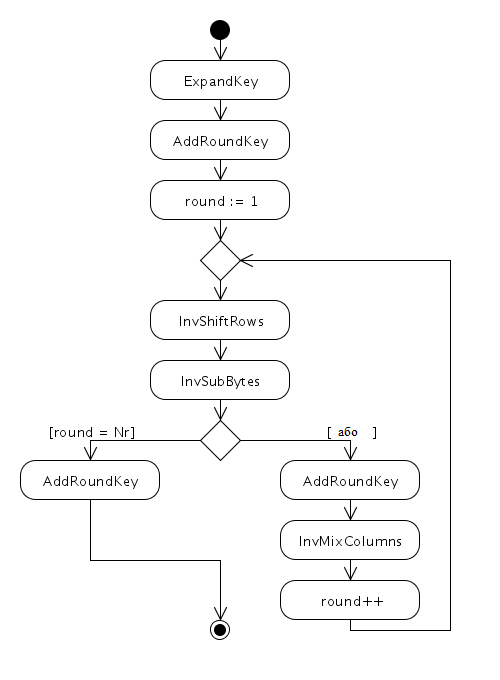


Рис 3.4. Блок схема алгоритму розшифрування AES

Після цих встановлених скриптів підключається основнапрограма.

Код основної програми має такий вигляд:

# Підключаємо необхідні бібліотеки

from aes\_cipher import \*

from ecc\_kdf import ECDH\_KDF

# Параметри роботи з ключами

key\_length = 16 #bytes

salt = b'\_salt\_can\_be\_rnd'

info = b'\_handshake\_data\_'

def side\_A\_part(not\_encrypted, encrypted):

# Задаємо шляхи для ключів

private\_key = 'keys/PrivateKey\_A.pem'

public\_key = 'keys/PublicKey\_B.pem'

print('Викликаємо функцію шифрування / розшифрування ключів')

# Викликаємо функцію шифрування / розшифрування ключів

kdf\_object = ECDH\_KDF(private\_key, public\_key, key\_length, salt, info)

# Виводимо ключ на екран

print('Ключ на стороні A: ' + kdf\_object.derived\_key.hex())

aes = AESCipherCBC(kdf\_object.aes\_key, kdf\_object.iv)

print('Відкриваємо файл для читання розшифрованого ключа (' + not\_encrypted + ')')

# Відкриваємо файл для читання розшифрованого ключа

ne\_file = open(not\_encrypted, "rb")

# Відкриваємо файл для запису зашифрованого ключа

print('Відкриваємо файл для запису зашифрованого ключа (' + encrypted + ')')

enc\_file = open(encrypted, "wb")

# Записуємо ключ у файл

print('Записуємо ключ у файл...\n')

enc\_file.write(aes.encrypt(ne\_file.read()))

# Закриваємо файли

ne\_file.close()

enc\_file.close()

def side\_B\_part(encrypted, decrypted):

# Задаємо шляхи для ключів

private\_key = 'keys/PrivateKey\_B.pem'

public\_key = 'keys/PublicKey\_A.pem'

print('Викликаємо функцію шифрування / розшифрування ключів')

# Викликаємо функцію шифрування / розшифрування ключів

kdf\_object = ECDH\_KDF(private\_key, public\_key, key\_length, salt, info)

# Виводимо ключ на екран

print('Ключ на стороні В: ' + kdf\_object.derived\_key.hex())

aes = AESCipherCBC(kdf\_object.aes\_key, kdf\_object.iv)

# Відкриваємо файл для читання розшифрованого ключа

print('Відкриваємо файл для читання розшифрованого ключа (' + encrypted + ')')

enc\_file = open(encrypted, "rb")

print('Відкриваємо файл для запису зашифрованого ключа (' + decrypted + ')')

# Відкриваємо файл для запису зашифрованого ключа

#print('')

dec\_file = open(decrypted, "wb")

# Записуємо ключ у файл

print('Записуємо ключ у файл...\n')

dec\_file.write(aes.decrypt(enc\_file.read()))

# Закриваємо файли

enc\_file.close()

dec\_file.close()

def main():

# Задаємо шляхи до файлів

not\_encrypted = 'files/not\_encrypted.txt'

encrypted = 'files/encrypted.txt'

decrypted = 'files/decrypted.txt'

side\_A\_part(not\_encrypted, encrypted)

side\_B\_part(encrypted, decrypted)

if \_\_name\_\_ == "\_\_main\_\_":

main()

Файли: not\_encrypted encrypted і decrypted мають такий зміст (було вибрано число Пі) (рис. 3.5):

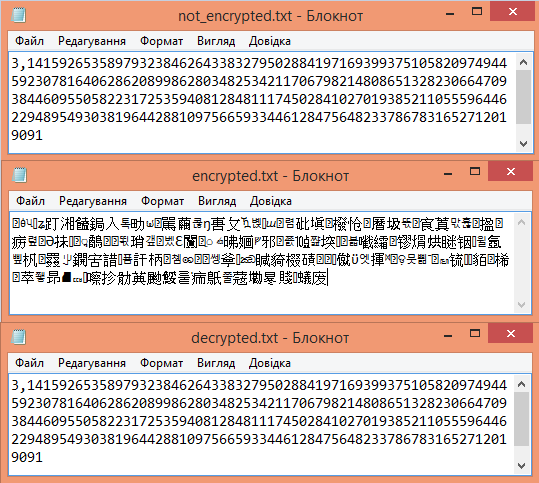


Рис 3.5. Файли шифрування, до/під час/після

Запускаємо за допомогою командної строки (cmd), іполучаєморезультат (рис.3.6). Якщоключінадвохсторонахзбігаються, тодіпрограма працює правильно.

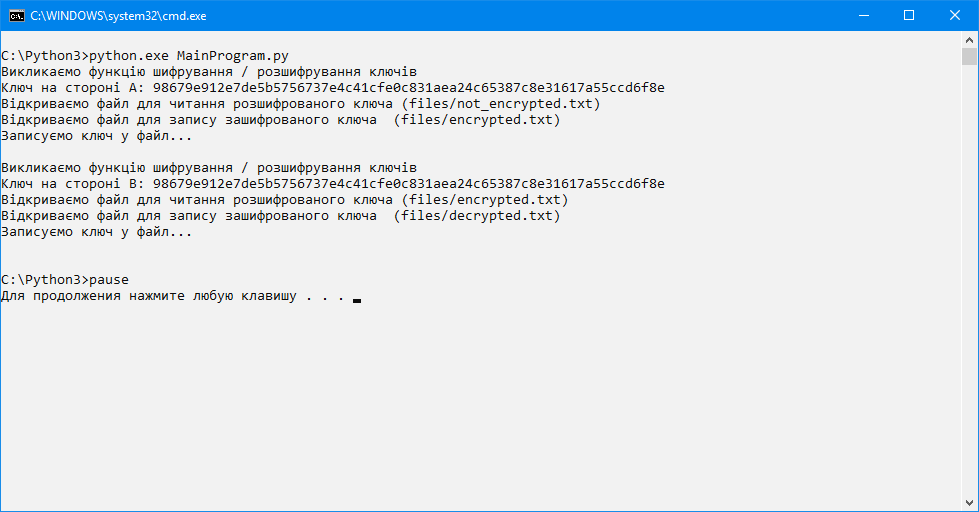


Рис 3.6. Результат основної програми.

Отже, за допомогою генератора ECCключів,згенерувались приватні/публічні ключі на двох сторонах, на стороні А пронініціалізувати його приватним ключем А і публічним ключем Б, так і на стороні Б приватним ключем В і публічним ключем А. Також получилось згенерувати на стороні А сесійні ключі, використовуючи дві рандомні стрічки. Використати сесійні ключі і скрипт AES, для того щоб зашифрувати файл після чого взяти на стороні Б і згенерувати сесійні ключі. Вже після цих всіх дій потрібно розшифрувати сесійними ключами і цим самим AES скриптом зашифрований файл.Такий метод є безпечним, тому що можна двом і більше сторонам получити загальний секретний ключ використовуючи незахищенний канал зв’язку.

**РОЗДІЛ 4. ОХОРОНА ПРАЦІ**

Однією із характерних особливостей сучасного розвитку суспільства є зростання сфер діяльності людини, в яких використовуються інформаційні технології. Широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає вдосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'якористувачів.

**4.1 Аналіз шкідливих та небезпечних чинників при роботі зПК**

До основних шкідливих факторів при роботі з комп'ютером відносять: тривале сидяче положення, електромагнітне випромінювання, навантаження на зір, перевантаження кистьових суглобів, можливість захворювань органів дихання, алергії, порушення нормального перебігу вагітності та ін. Тривале сидяче положення приводить до напруги м'язів шиї, голови, рук і плечей, остеохондрозу, у дітей - ще й до сколіозу. Тривале сидяче положення ще приводить до застою крові в тазових органах і, як наслідок, до простатиту й геморою. Не секрет, що малорухливий спосіб життя призводить до ожиріння. Остеохондроз виникає при порушенні міжхребцевих дисків, яке призводить до випинання в яку або сторону (грижі міжхребцевого диска). Грижа може зашкодить спинний мозок і нервові відростки. Наслідки можуть бути найрізноманітнішими, від болів в спині і кінцівках, до паралічу кінцівок і смерті. Одна з поширених причин остеохондрозу - дистрофія м'язів спини. Людина, провідний в основному сидячий спосіб життя, цілком може захворіти остеохондрозом. Ознаки початку захворювання: дискомфорт у спині та больові відчуття, головні болі, порушення роботи внутрішніх органів. До факторів ризику захворювання гемороєм відносять: сидячий спосіб життя, ожиріння, надмірне вживання копчених, гострих, солоних і пряних продуктів, запальні захворювання малого таза та ін Ожиріння виникає через нераціональне харчування, малорухомого і в тому числі сидячого способу життя, неадекватної реакції на стресові ситуації, надмірно довгий сон, застосування гормональних препаратів, перевантаження організму харчовими жирами і ін Ожиріння призводить до збільшення навантаження на серце, зміни конфігурації та положення серця в грудній порожнині, підвищення вмісту холестерину в крові, в результаті він відкладається на стінках судин ( атеросклероз). Підвищений скупчення жиру всередині грудної порожнини впливає на роботу органів дихання, що призводить до появи задишки та гіпоксії органів і тканин. ^ Навантаження на зір. Людське око реагує на найдрібнішу вібрацію тексту і на мерехтіння екрану. М'язи ока, керуючі кришталиком, перебувають у постійній напрузі, що обов'язково призводить до втрати гостроти зору. Немаловажне значення для профілактики зорових дисфункцій надають: правильний чи рекомендований підбір кольору, шрифтів, компоновки вікон у використовуваних додатках, орієнтація дисплея монітора. Тривала робота за комп'ютером - це величезне навантаження на очі, оскільки зображення на моніторі складається не з безперервних ліній, як на папері, а з окремих точок, які світяться і мерехтять. У користувача неминуче погіршується зір, очі починають сльозитися, з'являється головний біль, втома, зображення двоїться і спотворюється. ^ Перевантаження суглобів кистей рук приводить головним чином до такого явища, як синдром зап'ястного каналу

**4.2 Умови праці на робочому місці з ПК**

Навчальний процес з використанням комп’ютера, відбувається в середовищі, яке в певній мірі впливає на функціональний стан студентів, які перебувають у комп’ютерній аудиторії. Найважливішими несприятливими факторами середовища при роботі за комп'ютером є :

* фізичні параметри мікроклімату; освітлення; електромагнітні
* випромінювання різних частотних діапазонів; виробничий шум та
* вібрація; іонізація повітря; статична електрика;

психофізіологічні - перенапруження зорового аналізатора; недостатня рухома діяльність; нервово-емоційне напруження.

Аналіз умов праці виконується для приміщення аудиторії №419 яка знаходиться, на 4 поверсі п’ятиповерхової будівлі.

Відповідно до НПАОП 0.00-7.15- 18 є неприпустимим розташування приміщень, призначених для роботи з ВДТ у підвалах та цокольних поверхах. Також забороняється розташування вибухонебезпечних приміщень категорії А і Б (ДСТУ Б.В. 1.1-36:2016) та виробництв з мокрими технологічними процесами поряд з приміщенням, де розташовуються ЕОМ (ПЕОМ), а також над такими приміщеннями, або під ними. Окрім того, виробничі приміщення для роботи з ВДТ не повинні межувати з приміщеннями, у яких рівень шуму та вібрації перевищує допустимі значення.

У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці і відпочинку. У противному випадку в працюючого за ПК відзначаються значна напруга зорового апарата з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, утома і хворобливі відчуття в очах, у попереку, в області шиї і руках.

Розташування робочого місця особи, що працює з ПК, в даному випадку студента, повинне відповідати вимогам ГОСТ 22.269-79

Облаштування робочого місці повинно забезпечувати:

* правильне розміщення робочого місця у виробничому приміщенні;
* належні умови освітлення приміщення і робочого місця, відсутність відблисків;
* належні ергономічні характеристики основних елементів робочого місця;
* характер та особливості трудової діяльності.

Для зменшення втоми, місця користувачів ЕОМ мають бути зручними.

Конструкція робочого місця користувача ПК, (при роботі сидячи) має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками:

- ступні ніг - на підлозі або на підставці для ніг;

- стегна — в горизонтальній площині;

- передпліччя - вертикально;

- лікті - під кутом 70-90° до вертикальної площини;

- зап'ястя зігнуті під кутом не більше 20° відносно горизонтальноїплощини;

- нахил голови - 15-20° відносно вертикальної площини.

Робоче місце користувача ПК , обладнується робочим столом, стільцем і підставкою для ніг. Висота робочого стола має бути в межах від 0,65 до 0,8 м, а ширина повинна забезпечувати можливість виконання операцій в зоні досяжності моторного поля.

Клавіатуру слід розташовувати на поверхні столу на відстані 200 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачатися опорний пристрій (виготовлений із матеріалу з високим коефіцієнтом тертя, що перешкоджає його переміщенню), який дає змогу змінювати кут нахилу поверхні клавіатури у межах 5...15°.

**4.3 Мікроклімат та ступінь іонізації повітря в приміщенні з ПК**

Як фактор виробничого середовища, мікроклімат впливає на теплообмін організму людини з цим середовищем. Необхідною умовою життєдіяльності людини є терморегуляція, тобто здатність організму регулювати віддачу тепла в оточуюче середовище. Цей процес визначається параметрами мікроклімату. Метеорологічні умови визначаються такими параметрами:

* + температурою повітря в приміщенні, С;
  + відносною вологістю повітря, %;
  + рухливістю повітря, м/с;
  + тепловим випромінюванням, Вт/м3.

Принцип нормування мікроклімату – створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Параметри мікроклімату, вміст шкідливих речовин на робочих місцях, оснащених моніторами, відповідають вимогам ДСН 3.3.6.042-99 «Державні санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 «ССБТ. Воздух рабочей зоны. Общие санитарно-гигиенические требования к воздуху рабочей зоны».

Обчислювальна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості в приміщенні.

В приміщеннях, де встановлені комп'ютери, повинні дотримуватися оптимальні параметри мікроклімату, які визначають комфортні умови. Ці параметри залежать від періоду року, категорії робіт за важкістю, і від теплових характеристик виробничого приміщення (табл. 4.1).

Робота за комп’ютером характеризується малими фізичним навантаженнями, цей вид діяльності належить до категорії легких робіт-lа за критерієм загальних енерговитрат організму (ДСН 3.3.6.042-99)

Під час роботи комп’ютерної техніки в повітряному середовищі відбувається суттєва трансформація іонного складу, істотно знижується концентрація легких, середніх та важких негативно зарядних частинок. Така зміна балансу іонного складу призводить до негативного впливу на здоров’я працюючих

Таблиця 4.1

Параметри мікроклімату

|  |  |  |  |
| --- | --- | --- | --- |
| Період року | Категорія робіт | Параметр мікроклімату | Величина |
| Холодний | Роботи легкі  l а | Температура повітря в приміщенні  Відносна вологість  Швидкість руху повітря | 22÷24°С  40÷60%  до 0,1м/с |
| Теплий | Температура повітря в приміщенні  Відносна вологість  Швидкість руху повітря | 23÷25°С  40÷60%  0,1.0,2м/с |

**4.3 Випромінювання в приміщенні з ПК**

Дисплеї на основі ЕПТ є потенційним джерелом випромінювання кількох діапазонів електромагнітного спектра: рентгенівського, оптичного, радіочастотного. Кожний вид випромінювання відрізняється своїми особливими характеристиками впливу на організм людини.

Рентгенівське випромінювання. Дослідження показують ,що відеотермінал не несе небезпеки для користувача ПЕОМ, оскільки інтенсивність такого випромінювання нижча за гранично допустимі норми (ГДН). Відповідно до «Норм радіаційної безпеки України» (НРБУ-97) гранично допустимапотужність експозиційної дози рентгенівського випромінювання на відстані 5см від поверхні екрана відеотермінала становить 7,74∙10-12 Кл/кг, що відповідає еквівалентній дозі 0,1 мбер/год. (100 мкР/год.)

Оптичне випромінювання.Оптичні види випромінювання виникають завдяки взаємодії електронів з шаром люмінофору, нанесеного на екран ВДТ. Область оптичного випромінювання включає ультрафіолетове (УФ), світлове та інфрачервоне (ІЧ) випромінювання.

УФ-випромінювання впливає на шкіру та очі людини. Такий вплив на шкірі проявляється досить швидко, а для очей характерним є період прихованої дії. Рівень УФ- випромінювання, який був виявлений, досить низький і становить 1 середньому 0,001Вт/м².

Світлове випромінювання впливає в основному на око і призводить до втоми очей, запалення райдужної оболонки. Однак ці симптоми швидко минають і не викликають патологічних змін.

ІЧ-випромінювання - довжина хвиль обмежена від 0,76мм до 1мм. Для більшості біологічних матеріалів випромінювання цього діапазону вважаються непрозорими. Інтенсивність інфрачервоних випромінювань нижча за значення, передбачені ДсанПіН 3.3.2.-007-98.

Електромагнітні випромінювання (ЕМВ) радіочастотного діапазону. Джерелом ЕМВ є відеотермінал. Тому, обираючи робоче місце для комп'ютера, необхідно пам'ятати, що його задня і бокові стінки можуть бути джерелом значно більшого ЕМВ, ніж екран.

З метою профілактики несприятливого впливу електромагнітного випромінювання від ВДТ на користувача необхідно:

- встановити на робочому місці відеотермінал, що відповідає сучасним вимогам стосовно захисту від. випромінювань;

- не переобтяжувати приміщення значною кількістю робочих місць з ВДТ;

- не концентрувати на робочому місці великої кількості радіоелектрон-них пристроїв.

Гранично допустимі рівні випромінювань на робочих місцях з ПК наведено в таблиці 4.3

Таблиця 4.3

Допустимірівні випромінювань

|  |  |  |
| --- | --- | --- |
| Вид випромінювання | Діапазон хвиль (частот) | Гранично допустимий рівень |
| Іонізуюче випромінювання | | |
| М’яке рентгенівське випромінювання  ( на відстані 0,05 м від екрана та корпуса ВДТ) | 0,01 – 1 нм | 100мкР/год |
| Оптичні випромінювання | | |
| Ультрафіолетове випромінювання | 315 – 400 нм | 10 Вт/м |
| Видиме випромінювання (яскравість) | 400 – 700 нм | 1000 кд/м |
| Інфрачервоне випромінювання | 700 нм – 1мм | 100 Вт/м |
| Електромагнітні випромінювання ( поля радіочастотного та низькочастотного діапазонів) | | |
| Вид випромінювання | Діапазон хвиль (частот) | Гранично допустимий рівень |
| Напруженість електромагнітного поля на відстані 0,5 м навколо монітору за електричною складовою | 2 кГц – 400 кГц  5 Гц – 2 кГц | 2,5 В/м  25 В/м |
| Щільність магнітного потоку | 2 кГц – 400 кГц  5 Гц – 2 кГц | 25 нТл  250 нТл |
| Електростатичні поля | | |
| Поверхневий  електростатичний потенціал | – | 500 В |

**4.4 Шум та вібрація в приміщенні з ПК**

Відомо, що шум несприятливо діє на слуховий аналізатор та інші органи та системи організму людини. Визначальне значення щодо такої дії має інтенсивність шуму, його частотний склад, тривалість щоденного впливу, індивідуальні особливості людини, а також специфіка виробничої діяльності. Ті види діяльності, у яких поєднується напружена розумова робота та інтенсивне використання комп’ютера (редагування тексту, верстка оригіналу, "запуск" та відлагодження програм тощо) характеризується відчутним впливом навіть незначних рівнів шуму. Цей вплив виражається у зниженні розумової працездатності, швидкій втомлюваності, послабленні уваги, появі головного болю та ін.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ВДТ і ПК визначені ДСанПіН 3.3.2-007-98 не повинні перевищувати 65 дБА . Для приміщення аудиторії , рівень шуму не перевищує 60 дБА.

Для забезпечення нормованих рівнів шуму у виробничих приміщеннях та на робочих місцях застосовуються шумопоглинальні засоби, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками.

**4.5 Виробниче освітлення в приміщенні з ПК**

Близько 90% всiєї iнформацiї, що отримується людиною, приходиться на органи зору. Органiзацiя освiтленостi робочих мiсць грає велику роль у житті людини. Недостатнє та нерацiональне освiтлення веде до втомлення очей, розладу центральної нервової системи, зниженню розумової та фiзичної працездатностi, а у рядi випадкiв може бути причиною травматизму (близько 5% травм приходиться на частку нерацiонального та недостатнього освiтлення).

Щоб уникнути перевтоми, а також для профілактики професійних захворювань та виробничого травматизму потрібно дотримуватись наступних вимог:

* створювати на робочій поверхні освітленість, що відповідає характеру зоро­вої роботи і не є нижчою за встановлені норми;
* забезпечити достатню рівномірність та постійність рівня освітленості у вироб­ничих приміщеннях, щоб уникнути частої переадаптації органів зору;
* не створювати засліплювальної дії як від самих джерел освітлення, так і від інших предметів, що знаходяться в полі зору;
* не створювати на робочій поверхні різких та глибоких тіней (особливо рухомих);
* повинен бути достатній для розрізнення деталей контраст поверхонь, що освітлюються;
* не створювати небезпечних та шкідливих виробничих чинників (шум, теплові випромінювання, небезпека ураження струмом, пожежо- та вибухонебезпека світильників);
* повинно бути надійним і простим в експлуатації, економічним та естетичним.

Приміщення аудиторії №419 має природну та штучну системи освітлення, які повинні відповідати вимогам ДБН В.2.5-28-2996 «Інженерне обладнання будинків та споруд. Природне та штучне освітлення».

Штучне освітлення в приміщенні з комп'ютеризованим робочим місцем здійснюється системою загального освітлення.

Як джерела світла в разі штучного освітлення застосовуються світильники серії ЛПО353. Світильники укомплектовані високочастотними пускорегулювальними апаратами (ВЧ ПРА). Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 град. з вертикаллю в повздовжній та поперечній площинах становить не більше

200 кд/м, захисний кут світильників – не менше ніж 40 град.

Рівень освітленості у аудиторії, Е= 300лк.

**4.5.1 Розрахунок природного освітлення для роботи з ПК**

Природне освітлення - освітлення приміщень денним світлом, що потрапляє через світлові отвори (вікна) в зовнішніх захищаючих конструкціях приміщення. Природне освітлення характеризується тим, що змінюється в широких межах залежно від часу дня, пори року і ряду інших чинників.

Перевірочний розрахунок виконується в такій послідовності:

1 . Нормативне значення коефіцієнта природного освітлення для IV поясу світлового клімату ,%.

Визначається відповідно до ДБНВ.2.5-28:2018. Для зорових робіт середньої точності при найменшому розмірі об'єкта розпізнавання 0,5-1,0 мм при боковому освітленні (так званий IV розряд зорової роботи) = 1,5% ;

2. Коефіцієнт світлового клімату m.

Для Львівської області, що належить до IV поясу світлового клімату відповідно до рекомендацій:

m = 0,9.

3. Коефіцієнт сонячності клімату с.

Для світлових отворів (вікон) в зовнішніх стінах будівель, розташованих у IV поясі світлового клімату та зорієнтованих по азимуту в діапазоні 46... 135 градусів відповідно до рекомендацій.

с = 0,75.

4. Нормоване значення коефіцієнта природного освітлення для розрахункових умов ен,%:

5. Коефіцієнт запасу, що використовується при розрахунку природного освітлення к3. Відповідно до рекомендацій.

к3=1,3...1,5.

Прийнято к3 -1,4.

6. Відношення довжини приміщення а до його ширини b, а/b:

а/b = 5/5 = 1,0.

7. Відношення ширини приміщення b до відстані від верхньої кромки вікна до робочої поверхні h, b/h =5/2,5 = 2.

8. Світлова характеристика вікна зв.

Визначається відповідно до рекомендації зв = f(а/b, b/h) при а/b = 1,0 і b/h= 2

=16.

9. Коефіцієнт світлопропускання матеріалу .

Визначається згідно рекомендаціям відповідно до склопакетів

=0,8.

10. Коефіцієнт, що враховує втрати світла у віконні рамі . Визначається згідно рекомендацій. Для дерев'яних одинарних рам

= 0,75.

11. Коефіцієнт, що враховує втрати світла у несучих конструкціях . При боковому освітленні згідно рекомендацій:

=1.

12. Коефіцієнт, що визначає втрату світла у сонцезахисних конструкціях . Для внутрішніх регульованих штор з рекомендації:

=1.

13. Загальний коефіцієнт світлопропускання

= \* \* \* =0,8\*0,75\*1\*1=0,6

14. Коефіцієнт відбиття внутрішніх поверхонь приміщення: сстелі, сстін, спідлоги,%

Дані показники визначаються відповідно до для:

- для свіжопобіленої стелі стелі = 80%;

- для стін обклеєних шпалерами світлого тону сстін =40%;

- Для підлоги спідлоги = 35%.

15. Площі внутрішніх поверхонь: стелі Sстелі, Sстін, Sпідлоги, м2

Sстелі = a\*b = 5\*5 = 25 м2 (4.1)

Sстін = 2\* (a+b)\* H = 2\*(5+5)\*2,5 = 50 м2 (4.2)

Sпідлоги = 25 м2.

16. Середнє значення коефіцієнта відбиття с сер.

17. Співвідношення, що характеризують геометрію приміщення а/b, b/h, l/b

а/b=1,0 b/h = 2,0 1/b = 0,2.

18. Коефіцієнт, що враховує підсилення коефіцієнта природного освітлення за рахунок світла, що відбивається від внутрішніх поверхонь приміщення r1.

Відповідно до рекомендацій:

r1 = f(с сер, а/b, b/h, 1/b) (4.3)

При с сер = 0,654, а/b =1,09, b/h = 2,5,1/b = 0,28.

r1 = 3,2.

19. Відношення відстані до протилежної будівлі D до висоти карнизу протилежної будівлі над підвіконням Н', D/Н':

D/Н'= 32/15 = 2,13.

20. Коефіцієнт, що враховує вплив протилежної будівлі на освітленість у приміщенні, кбуд.

Відповідно до стандарту кбуд = f (D/Н'). =2,13

кбуд = 1,1.

21. Площа вікон, що необхідна для забезпечення нормованого коефіцієнта освітлення у розрахунковому приміщенні SВ, м2:

(4.4)

N= Sв/S1 =4.7/1.6 = 3

В приміщенні розташовано 3 вікна розмірами d х с = 1,1 \* 1,45 = 1,6 (), їх загальна площа складає Sв= 4,8.Приплощі приміщенні 25 і при 4 робочих місцях з ПК.

Таким чином передбаченої кількості вікон (їх площі) вистачає для забезпечення вимог санітарних норм щодо природного освітлення виробничого приміщення для якого розробляються окремі питання з охорони праці.

**4.6 Електробезпека в приміщенні з ПК**

Приміщення відноситься до приміщень без підвищеної небезпеки за ПУЕ - 2017.

ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПВЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Використання нульового робочого провідника як нульового захисного провідника забороняється.

Нульовий захисний провід прокладається від склейки групового розподільчого щита до розеток живлення.

Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі повинна бути не менше площі перерізу фазового провідника. Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПВЕ.

З метою підвищення рівня електробезпеки в приміщенні аудиторії № 419 неприпустимим є:

-експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час екплуатації, ізоляцією;

-залишення під напругою неізольованих кабелів та проводів;

-застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами;

-застосування для опалення приміщення нестандартного (само-робного) електронагрівального обладнання.

ВДТ є джерелом електростатичних зарядів. Тривале перебування в електростатичному полі, створеному цими зарядами, негативно впливає на здоров'я працюючих: бронхо-легеневі захворювання, порушення серцево-судинної та нервової систем, ураження шкіри тощо.

Напруженість електростатичного поля на робочих місцях, в тому числі й з ВДТ, не повинна перевищувати 20 кВ/м відповідно до ГОСТ 12.1.045-84 "ССБТ. Электростатические поля. Допустимые уровни на рабочих местах и требования к проведенню контроля", поверхневий електростатичний потенціал відеотермінала не повинен перевищувати 500В.

Для запобігання створенню значної напруженості поля та захисту від статичної електрики необхідно:

* встановити нейтралізатори статичної електрики;
* підтримувати в приміщенні з ВДТ відносну вологість повітря не нижче 45—50% (чим сухіше повітря тим більше електростатичних зарядів); можна для цього використати навіть побутові зволожувачі;
* застелити підлогу в приміщеннях з ВДТ антистатичним лінолеумом і проводити щоденне вологе прибирання;
* складати всі полімерні покриття (чохли) ВДТ у найбільш віддаленому від користувачів місці розміщення;
* протирати екран та робоче місце спеціальною антистатичною серветкою або зволоженою тканиною.

**4.7 Пожежна безпека в приміщенні з ПК**

Пожежна безпека при роботі за комп'ютером повинна забезпечуватись у відповідності з вимогами Закону України «Про пожежну безпеку» та НПАОП 0.01-1.01-95 «Правил пожежної безпеки в Україні»та інших нормативних документів.

Відповідно до ДСТУ Б.В. 1.1.36:2016. приміщення відноситься до категоріїВ, тому що там знаходяться матеріали, які здатні вибухати і горіти або тільки горіти під час взаємодії з водою, киснем, повітрям або один з одним; а такожтверді горючі або важкогорючі речовини і матеріали (включно горючий пил або волокна).

Найбільш імовірною причиною виникнення пожеж в приміщенні є порушення вимог при експлуатації комп'ютерної техніки та займання електропроводки внаслідок коротких замикань.

Для того щоб уникнути виникнення пожежі, потрібно дотримуватися наступних заходів:

* дотримання правил пожежної безпеки при роботі з комп’ютером,

електрообладнанням та освітлювальними приладами;

* періодичний контроль цілісності і надійності електроізоляції;
* наявність інструкцій з пожежної безпеки;
* навчання, атестація і переатестація персоналу з пожежної безпеки;
* наявність системи захисту від атмосферної електрики;
* періодичне зняття зарядів статичної електрики;
* заборона куріння в приміщенні.
* застосування будівельних конструкцій із ступенем вогнестійкості не нижче II, а також використання важкогорючих або негорючих матеріалів в інтер’єрі виробничого приміщення;
* наявність схеми евакуації;
* наявність пристроїв автоматичного вимкнення ПЕОМ та іншого електроустаткування на випадок пожежі;
* наявність первинних засобів пожежогасіння ( вогнегасник ВВК-5 -3шт на 25).
* ступень вогнестійкості більший за ДБН В.1.1.7:2016

**Висновки до розділу**

Під час написання цього розділу проведено аналіз чинників, які можуть негативно повпливати на здоров’я та життя людини під час роботи над дипломним проектом. Зокрема розглянуто фактори негативного впливу на організм людини при роботі за комп’ютером. До яких відносяться: різні види випромінення, напруження зору, статичне навантаження на мязи та кістки, ймовірність виникнення трамв рук, через монотонні повторювані рухи.

Також розглянуто етапи облаштування робочого місця та вимоги до нього згідно норм. Зокрема ергономіку робочого місця, освітлення, рівень шуму і вібрація, вибухо та пожежонебезпеку, електробезпеку та мікроклімат. Приміщення в якому проводилась робота відповідає усім нормам.

До того ж у розділі наведено правила техніки безпеки з лазерними пристроями, а також фактори негативного впливу на організм людини при роботі з лазерними пристроями.

Здобуті знання та досвід пригодяться в майбутньому при працевлаштуванні та безпосередній праці.

# ВИСНОВКИ

У бакалаврській кваліфікаційній роботі було розглянуто питання захисту інформації в публічних мережах. Було створено програму для захисту файлів шляхом шифрування(розшифрування) еліптичними ключами. Досліджено алгоритм Діффі – Хелмана. Ознайомлено з криптографічним шифруванням, як його і де використовують.

У першому розділі розглянуті питання актуальності захисту мережі, розглянено проблеми, які можуть виникнути при такій передачі, визначено загрози/атаки які можуть бути на незахищенні канали зв’язку. Розглянута проблема розподілу/передавання ключів для криптографічного захисту інформації та методи захисту цієї інформації. Також перераховано основні алгоритми які використовуються, а також досліджено їх особливості, вразливості, вузькі місця.

У другому розділі була зосереджена увага на використанні криптографії на основі еліптичних кривих, так звана (ECCcryptography). А також на використанні еліптичної криптографії для процедури генерації сесійних ключів на основі пар приватний/публічний ключ (метод ECDHKDF). А також були наведені приклади методу еліптичної криптографії Діффі-Хеллмана на основі алгоритму KDF.

Втретьомурозділі програмно реалізований метод ECDHKDF, показано усі складові, такі як пари ключів, сесійні ключі, тощо… Реалізований приклад шифрування даних алгоритму AES (128/192/256) і сесійним ключем на одному кінці. Також реалізовано генерацію сесійних ключів на іншому кінці ( за допомогою ECDHKDF ) і розшифрування цього файлу. Вхідні дані порівняли з вихідними.

В четвертому розділі з охорони праці розглянуто проблеми які можуть виникнути при роботі з ПК, а саме фактори які можуть негативно вплинути на здоров’я людини, розгялнуто ергономіку, освітлення, рівень шуму, пожежнонебезпеку, електронебезпеку та мікроклімат. Розраховано природнє освітлення в приміщенні де розташовується 4 робочих місця з ПК.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://uk.wikipedia.org.
2. Брюс Шнайер //Прикладна криптографія.
3. Кавун С.В. Інформаційна безпека. Навчальний посібник./ С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ–2008. – 352 с.
4. https://studopedia.info/ukr/.
5. Joseph H. Silverman. The Arithmetic of Elliptic Curves. / N. Y.: Springer– 2009.
6. Мао, Венбао. Сучасна криптографія: теорія і практика. // Пер. с англ.Видавничий дім «Вільямс»–2005. — 768c.
7. W. Diffie and M. Hellman // New directions in cryptography. Information Theory, IEEE Transactions on elliptic Curves, –1976. – C. 644-654.
8. http://csm.kiev.ua.
9. http://www.znanius.com.
10. D. E. Knuth. The Art of Computer Programming: Seminumerical Algorithms, volume 2. // Addison-Wesley, Reading, Mass– 1981–№ 2.
11. V.S. Miller. Use of Elliptic Curves in Cryptographypage. – 1986 – 417c.
12. Князькіна, О.С. Спосіб генерування випадкового простого числа заданої довжини / М.В. Онай, О.С. Князькіна // Праці міжнародн. конф «СНКПМІ-2012». — 2012. — С. 52-54.
13. Василенко О. Теоретико-числовые алгоритмы в криптографии/ Василенко О. Н.// М.: МЦНМО, 2003. – 178 с.
14. https://github.com.
15. Природнє і штучне освітлення / ДБН В.2.5-28:2015 – [Чинний від 2015-01-01]. – К. // Міністерство будівництва, архітектури та житловокомунального господарства України, 2015. – 171 с.
16. Гайворонський М.В. Безпека інформаційно-комунікаційних систем./Гайворонський М.В., Новіков О.М. // К.: Видавнича група BHV, 2009. –608c.
17. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. // СПб. : СПбГУ ИТМО, 2010. – 98c.
18. http://gc.ua/business-news/oxoronapraci-v-ofisi-vimogi-do-robochogo-miscya-ofisnogo-pracivnika/.
19. Типові норми належності вогнегасників (затверджено наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 2 квітня 2004 р. N 151).
20. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98 (затверджено Постановою Головного державного санітарного лікаря України від 10.12.1998 р. № 7).

ДОДАТОК 1. ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ

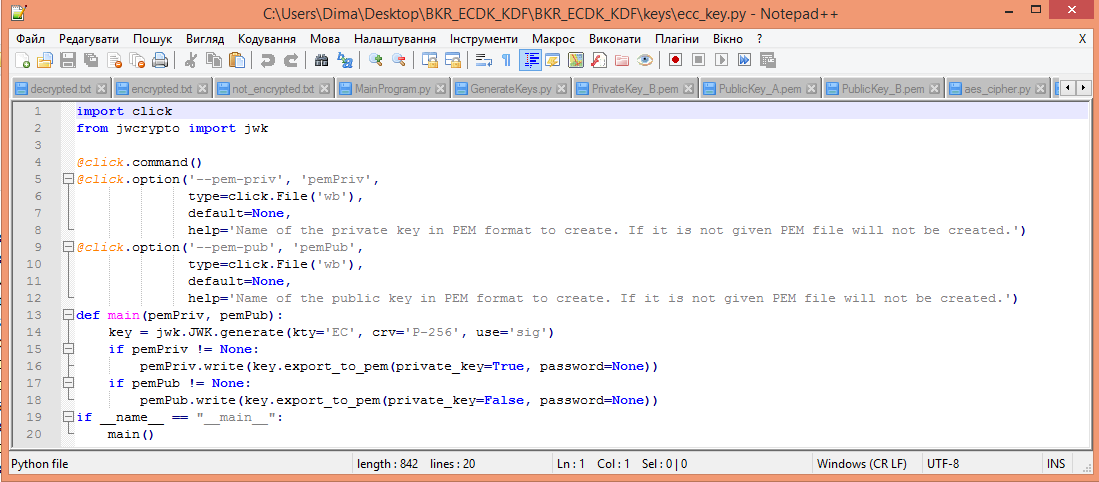


Рисунок 1 – Генерація пар ключів

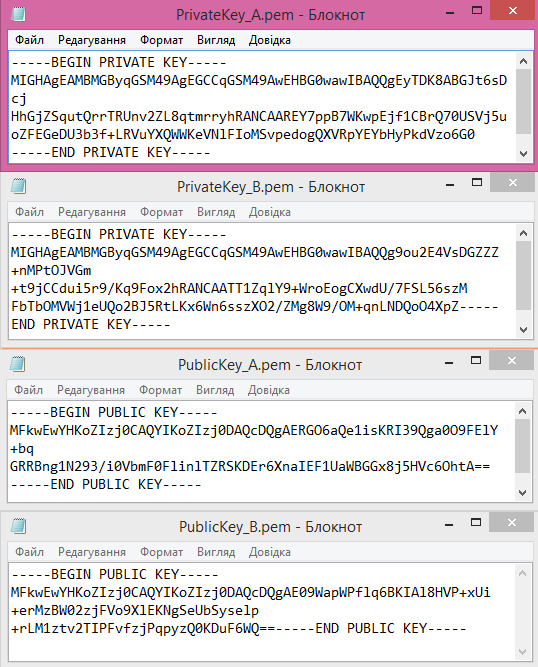


Рисунок 2 – Згенеровані пари ключів

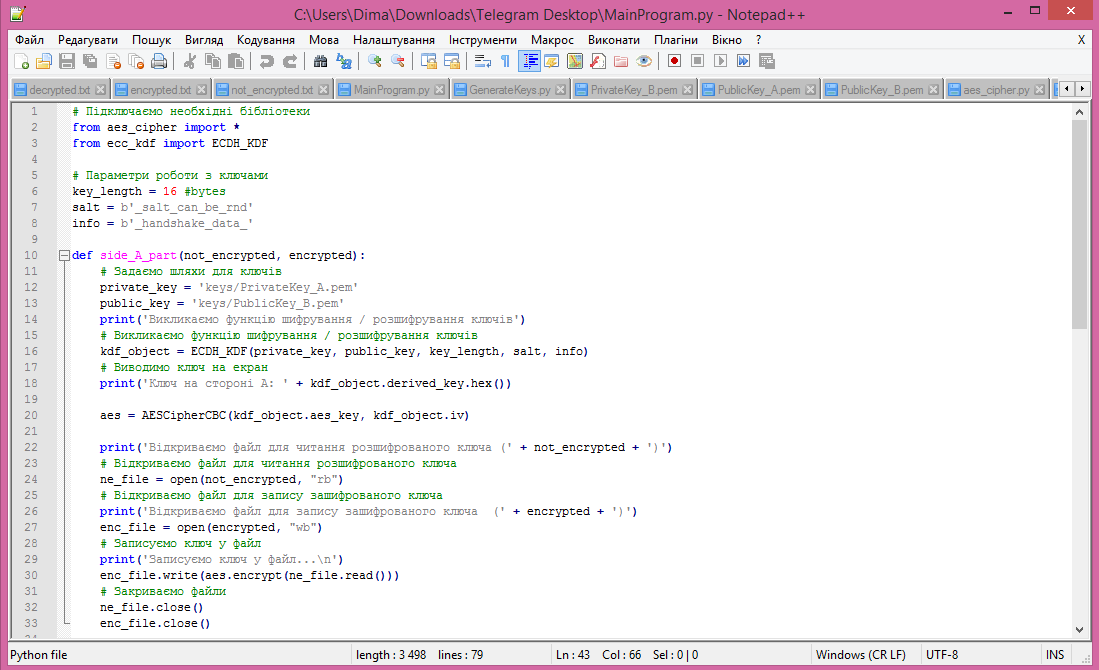
****

Рисунок 3 – Основна програма ½

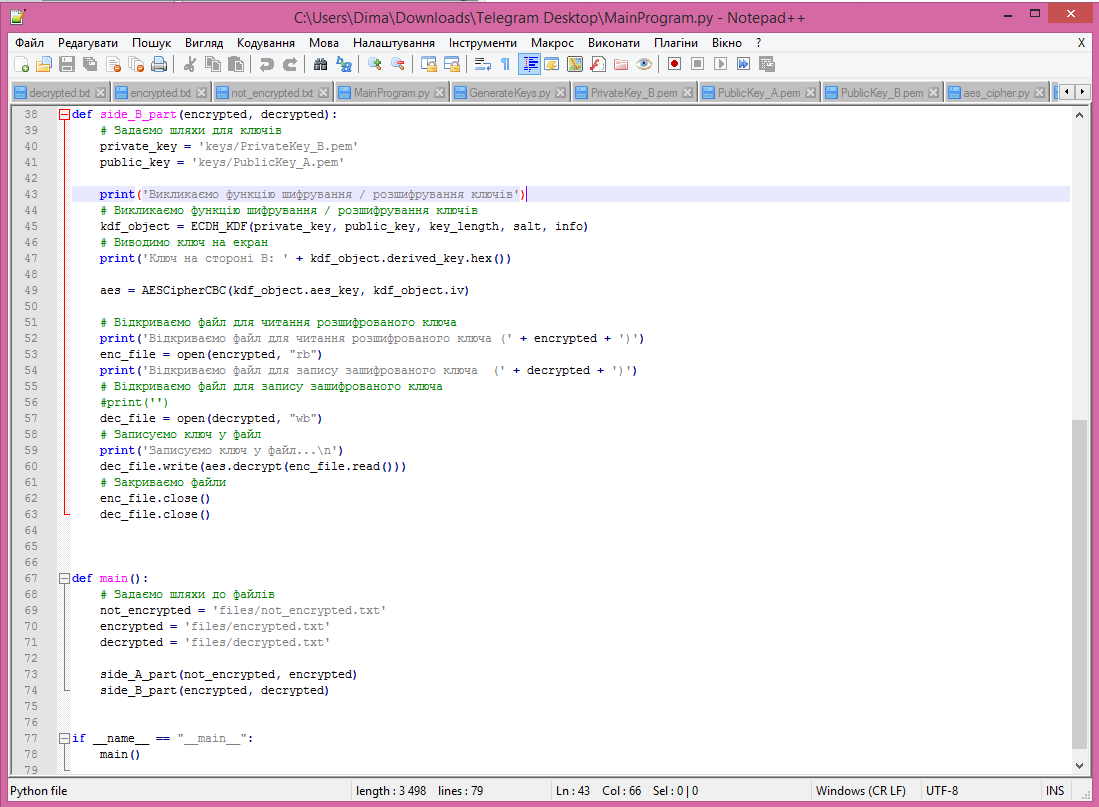


Рисунок 4 – Основна програма 2/2.

**Допоміжні скрипти**

***Скрипт для ініціалізації ключівна двох сторонах***

fromcryptography.hazmat.backendsimportdefault\_backend

fromcryptography.hazmat.primitives import hashes

from cryptography.hazmat.primitives.asymmetric import ec

from cryptography.hazmat.primitives.kdf.hkdf import HKDF

from cryptography.hazmat.primitives import serialization

import codecs

import os

class ECDH\_KDF(object):

def \_\_init\_\_(self, private\_key, public\_key, key\_length, salt, info):

salt\_length = 16

self.backend = default\_backend()

self.host\_key\_pair serialization.load\_pem\_private\_key(self.read\_key\_bytes(private\_key), password=None, backend=self.backend)

#Deserialize public key: extract from private or directly from pem file

try:

self.device\_public\_key serialization.load\_pem\_private\_key(self.read\_key\_bytes(public\_key), password=None, backend=self.backend).public\_key()

except:

self.device\_public\_key serialization.load\_pem\_public\_key(self.read\_key\_bytes(public\_key), backend=self.backend)

self.key\_length = key\_length

self.iv\_length = 16

if salt is not None:

self.salt = ECDH\_KDF.get\_bytes(salt)

else:

self.salt = os.urandom(salt\_length)

self.info = ECDH\_KDF.get\_bytes(info)

self.derived\_key = self.derive\_key()

self.aes\_key = self.derived\_key[:self.key\_length]

self.iv = self.derived\_key[self.key\_length:]

@staticmethod

def get\_bytes(inputdata):

if type(inputdata) is str:

return str.encode(inputdata,'utf-8')

elif type(inputdata) is bytes:

return inputdata

else:

raise Exception("Unknown input data type...")

def read\_key\_bytes(self, key\_file):

with open(key\_file, "rb") as key\_file:

return key\_file.read()

def derive\_key(self):

shared\_key=self.host\_key\_pair.exchange(ec.ECDH(), self.device\_public\_key)

derived\_key =HKDF(algorithm=hashes.SHA256(),

length=self.key\_length + self.iv\_length,

salt=self.salt,

info=self.info,

backend=self.backend).derive(shared\_key)

return derived\_key

def main():

pass

if \_\_name\_\_ == "\_\_main\_\_":

main()

***Скрипт для шифрування/розшифрування (AES)***

import click

from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes

from cryptography.hazmat.primitives.ciphers.aead import AESGCM

from cryptography.hazmat.backends import default\_backend

from cryptography.hazmat.primitives import padding

class AESCipher(object):

def \_\_init\_\_(self, key, IV):

self.backend = default\_backend()

self.key = AESCipher.get\_bytes(key)

self.iv = AESCipher.get\_bytes(IV)

self.block\_size = 128

@staticmethod

def get\_bytes(inputdata):

if type(inputdata) is str:

return str.encode(inputdata,'utf-8')

elif type(inputdata) is bytes:

return inputdata

else:

raise Exception("Unknown input data type...")

class AESCipherCBC(AESCipher):

def \_\_init\_\_(self, key, IV):

super().\_\_init\_\_(key, IV)

self.cipher = Cipher(algorithms.AES(self.key), modes.CBC(self.iv), backend=self.backend)

def encrypt(self, raw):

encryptor = self.cipher.encryptor()

padder = padding.PKCS7(self.block\_size).padder()

return encryptor.update(padder.update(raw) + padder.finalize()) + encryptor.finalize()

def decrypt(self, enc):

decryptor = self.cipher.decryptor()

unpadder = padding.PKCS7(self.block\_size).unpadder()

return unpadder.update(decryptor.update(enc) + decryptor.finalize()) + unpadder.finalize()

class AESCipherGCM(AESCipher):

def \_\_init\_\_(self, key, IV, auth\_data):

super().\_\_init\_\_(key, IV)

self.cipher = AESGCM(self.key)

self.auth\_data = str.encode(auth\_data,'utf-8')

def encrypt(self, raw):

return self.cipher.encrypt(self.iv, raw, self.auth\_data)

def decrypt(self, enc):

return self.cipher.decrypt(self.iv, enc, self.auth\_data)

def read\_key\_from\_file(keyfile):

with open(keyfile) as f:

content = f.read().splitlines()

if len(content) < 2:

raise Exception("Not anough AES input data: in the file should be two lines: key, iv ...")

key = content[0]

iv = content[1]

if 8\*len(key) not in set([128, 192, 256]):

raise Exception("Invalid AES Key length: should be 128, 192 or 256 bits")

check\_iv\_length(iv)

return key, iv

def check\_iv\_length(iv):

if 8\*len(iv) != 128:

raise Exception("Invalid AES IV length: should be 128 bits")

return True

@click.command()

@click.option('-k', '--keyfile')

@click.option('-a', '--auth\_data', default='default data')

@click.option('-m', '--mode', default='CBC')

@click.argument('inputfile')

@click.argument('outputfile')

def main(keyfile, auth\_data, mode, inputfile, outputfile):

key, iv = read\_key\_from\_file(keyfile)

if mode == 'CBC':

check\_iv\_length(iv)

aes = AESCipherCBC(key, iv)

elif mode == 'GCM':

aes = AESCipherGCM(key, iv, auth\_data)

else:

raise Exception("Selected mode is not supported...")

inFile = open(inputfile,"rb")

outFile = open(outputfile,"wb")

outFile.write(aes.encrypt(inFile.read()))

inFile.close()

outFile.close()

if \_\_name\_\_ == "\_\_main\_\_":

main()

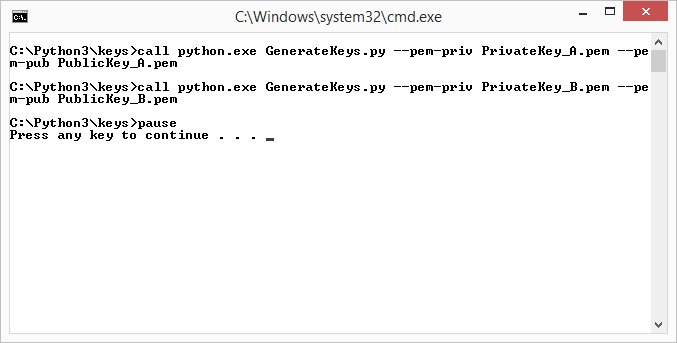


Рисунок 5 – Запущена програма яка згенерувала ключі на рис.2

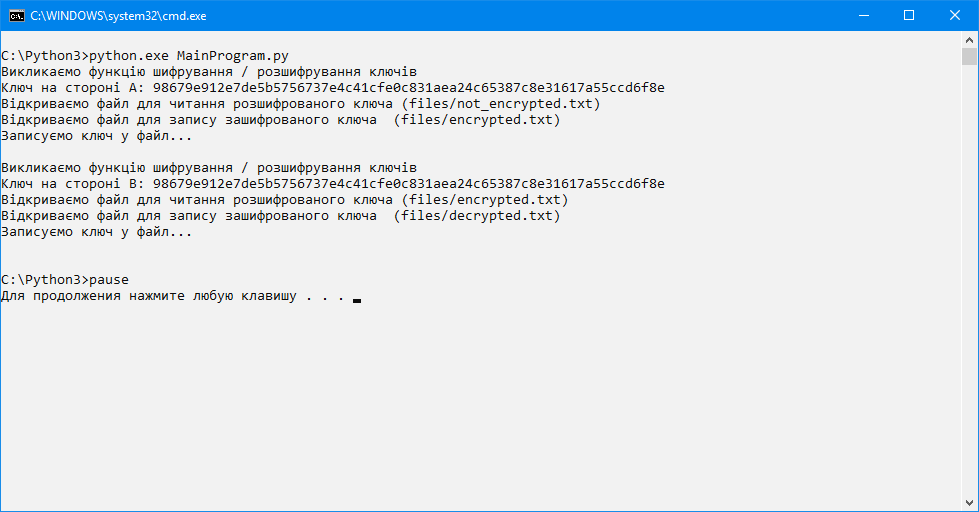


Рисунок 6 – Запущена основна програма яка зашифрувала/дешифрувала ключі

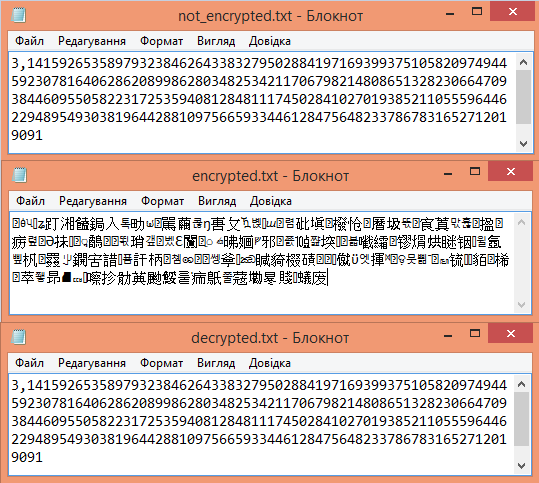


Рисунок 7 – Файли шифрування