**Національний авіаційний університет**

Кафедра комп’ютеризованих систем захисту інформації

**ЗВІТ**

**Про виконану лабораторну роботу №3**

**З дисципліни «Прикладна криптологія»**

Криптосистеми, засновані на використанні еліптичних кривих

Роботу виконала студентка:

Безносюк Ірина

Група: БІ – 445

Викладач:

Єгоров С.В.

Роботу захищено:

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019р.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис викладача)

КИЇВ 2019

**Мета:** Ознайомитися з принципом побудови криптосистем, за використанням еліптичних кривих.

**Теоретичні відомості**

***Еліптичні криві***

Нехай  - поле Галуа – кінцеве поле з елементів, де  ( - просте число, яке є характеристикою поля). Якщо , то  - множині цілих чисел за модулем . В загальному випадку афінне рівняння Вейерштрасса має вигляд:

,

де коефіцієнти  є елементами поля .

Якщо  та , то рівняння можливо спростити та переписати у вигляді:

.

Еліптичною кривою , що задана над полем , називають множину точок , що задовольняють рівнянню Вейерштрасса разом з елементом  - точкою в нескінченності.

Елемент  також називають невласним або нульовим елементом.

Особливий інтерес для криптографії представляє еліптична група за модулем .Така група визначається наступним чином. Виберемо два невід'ємні цілі числа,  і , які менше і задовольняють умові

**

Тоді  означає еліптичну групу по модулю , елементами якої  є пари невід'ємних чисел, які менше  і задовольняють умові:

**

разом з точкою в нескінченності .

Для еліптичної групи розглядаються тільки цілі значення від  до  у квадранті невід'ємних чисел, що задовольняють рівнянню за модулем . У загальному випадку список точок створюється за такими правилами:

1. Для кожного значення , що , обчислюється **.

2. Для кожного з отриманих на попередньому кроці значень з'ясовується, чи має це значення квадратний корінь за модулем , Якщо ні, то в немає точок з цим значенням . Якщо ж корінь існує, є два значення у, відповідних операції добування квадратного кореня (винятком є випадок, коли єдиним таким значенням виявляється ). ці значення  і будуть точками.

Алгебраїчно операція додавання ввизначається наступним чином:

1. .

2. Якщо *,* то . Точка  є від'ємним значенням точки  позначається . Зауважимо, що  лежить на еліптичній кривій і належить *.*

3. Якщо і *,* то визначається відповідно до правил:

* *

де *,* якщо *;*

та*,* якщо*.*

Операція множення на ціле число  визначається як багаторазове додавання:



***Шифрування/дешифрування з використанням еліптичних кривих***

Завданням є шифрування відкритого тексту повідомлення , яке повинне буде пересилатися в вигляді координат точки **.

Припустимо, абонент А хоче відправити абоненту В зашифроване повідомлення. Для цього йому знадобиться відкритий ключ абонента В. Генерація відкритого та закритого ключів абонента В проводиться за наступним алгоритмом:

1. Абонент В вибирає еліптичну групу .*.*

2. Абонент В вибирає генеруючу точку на кривій*.*

3. Абонент В вибирає ціле число ** – його особистий ключ.

4. Абонент В обчислює свій відкритий ключ: *.*

Таємний і відкритий ключ абонента А обчислюються аналогічним чином.

Для того, щоб відправити абоненту В повідомлення **, користувач А вибирає випадкове позитивне ціле число  і обчислює шифрований текст **, що буде складатися з пари точок

**

Зауважимо, що сторона А використовує відкритий ключ сторони В: **. Щоб дешифрувати цей шифрований текст, В помножує першу точку в парі на таємний ключ В і віднімає результат від другої точки:

**

Користувач А замаскував повідомлення ** за допомогою додавання до нього **. Ніхто, крім цього користувача, не знає значення , тому, хоча ** і є відкритим ключем, ніхто не зможе прибрати маску *.* Зловмисникові для відновлення повідомлення доведеться обчислити  за даними  і , що представляється складним завданням.

Таким чином, перехід до криптографії за використання еліптичних кривих дозволяє зберегти прийнятну довжину ключа при різкому (на декілька порядків) зрості стійкості криптосистем.

**Завдання:**

1. Розглянути принцип організації процедури шифрування з використанням еліптичних кривих.

2. Розгляньте еліптичну криву *.* Визначте всі точки *.* Значення параметрів  вибрати відповідно до варіанту, вказаною викладачем.

3. Реалізувати програмно алгоритм шифрування/ дешифрування з використанням еліптичних кривих.

**Хід роботи**

**Висновок:** в даній лабораторній роботі ми ознайомились з процедурою знаходження найбільшого спільного дільника, який використовує розширений алгоритм Евкліда. Вивчили принцип перевірки цілих чисел на простоту з використанням тестів Ферма и Міллера-Рабина.