Одеський національний університет імені І. І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра комп'ютерної алгебри та дискретної математики

Дипломна робота

бакалавр

на тему: **«Застосування еліптичних кривих у криптографії»**

«Algorithmic Applications of Elliptic Curves in cryptography»

Виконала: студентка денної форми навчання
спеціальності 111 Математика
Вербецька Катерина Ігорівна

Керівник: канд. фіз.-мат. наук, доц. Савастру О. В.
Рецензент: канд. техн. наук, доц. Якімова Н. А.

Рекомендовано до захисту:

Протокол засідання кафедри

№ ___ від _____ 2022 р.

Завідувач кафедри

_____ _____

Захищено на засіданні ЕК № _____

Протокол № ___ від _____ 2022 р.

Оцінка _____ / _____ / _____

Голова ЕК

_____ _____

Одеса — 2022 р.

ЗМІСТ

ВСТУП

Актуальність теми: На сьогоднішній день галузь шифрування та захисту інформації відіграє важливу роль в царині інформатики. Це зумовлено масштабним використанням автоматизованих методів обробки та передачі даних та широким розповсюдженням методів та засобів несанкціонованого доступу до інформації, що пересилається незахищеними каналами зв'язку.

Проблему передачі деякої конфіденційної інформації адресату можна вирішити багатьма способами, проте найбільш часто використовуваними в наш час є так звані асиметричні криптосистеми. Низка провідних досліджень показує, що серед асиметричних криптосистем, або криптосистем з відкритим ключем найбільш стабільною є криптосистема з використанням еліптичних кривих. Дані криптосистеми для забезпечення достатньої криптографічної стійкості потребують довжини ключа в кілька разів меншу за ту, що необхідна для криптосистем на основі математичних операцій в скінченних полях.

Використання еліптичних кривих для створення криптосистем було незалежно запропоновано Нілом Коблицем та Віктором Міллером у 1985 році. Ключова перевага даної методології ґрунтується на двох основних особливостях точок еліптичної кривої: розподіл результату додавання точок еліптичної кривої є у великій мірі рівномірним, тобто покриває всю область значень даної кривої; наслідком цієї особливості є проблема дискретного логарифмування для еліптичних кривих. Одним з яскравих представників сімейства криптографічних алгоритмів з використанням еліптичних кривих є алгоритм електронно-цифрового підпису ECDSA.

Ці особливості і обумовлюють високу криптографічну стійкість систем з використанням еліптичних кривих. З іншого боку, слід зазначити, що криптостійкість забезпечена відсутністю субекспоненційних алгоритмів вирішення проблеми дискретного логарифмування. Таким чином, знаходження субекспоненційного підходу унеможливить використання еліптичних кривих в криптографії, хоча це і стосується в однаковій мірі і інших схем шифрування. В межах даної роботи розглядаються еліптичні криві, параметри яких визначені над скінченними полями.

Перевагою криптографічних схем з використанням еліптичних кривих над іншими (зокрема RSA) є значно вища швидкодія обчислення та більша криптостійкість схем з аналогічною довжиною ключів. Таким чином, ключі схеми шифрування з використанням еліптичних кривих, що забезпечують аналогічну криптостійкість що і, для прикладу, RSA матимуть значно меншу довжину, що робить їх більш портативними.

При застосуванні криптографічних алгоритмів з використанням еліптичних кривих дуже важливим чинником є час їхньої роботи. Експериментальні дослідження показують, що найбільш ресурсо- та часовитратними є операції, що виконуються безпосередньо з точками еліптичної кривої, зокрема для алгоритму ECDSA найбільш ресурсовитратною є операція багатократного скалярного множення точок еліптичної кривої на число. Таким чином, актуальними є дослідження способів та методів оптимізації даного обчислення.

Криптосистеми з відкритим ключем не використовуються для шифрування великих об'ємів даних так як дана процедура є обчислювально складною.

Мета дипломної роботи: ознайомлення з теорією еліптичних кривих на скінченому полі. Огляд протоколу електронного цифрового підпису (далі ЕЦП) та криптосистем на еліптичних кривих.

Предмет дослідження: еліптичні криві на скінченому полі.

Об'єкт дослідження: процеси обміну ключами, шифрування/дешифрування та створення/перевірка електронно-цифрового підпису у еліптичних криптосистемах.

Структура дипломної роботи: У розділі 1 розглядається загальний контекст досліджень, а саме – математичні основи та принципи еліптичних кривих над скінченим полем.

У розділі 2 розглянений один з яскравих представників сімейства криптографічних алгоритмів з використанням еліптичних кривих – алгоритм електронно-цифрового підпису ECDSA.

У розділі 3 розглядаються принципи реалізації операцій над точками еліптичної кривої, аналізуються алгоритми системи Ель-Гамаля та вибір

кривої та точки, а також редукція глобальної пари за модулем.

У розділі 4 розглядається метод Полларда і редукція за модулем n.

У розділі 5 представлен скріпт інтерпрітації теореми Гассе на мові програмування. а саме – Python3.

РОЗДІЛ 1

ОСНОВНІ ФАКТИ ЕЛІПТИЧНИХ КРИВИХ

Останнім часом одна з областей алгебраїчної геометрії та теорії чисел – еліптичні криві, точніше, теорія еліптичних кривих над скінченними полями, – знайшла застосування в криптографії. Основна причина цього в тім, що еліптичні криві над скінченними полями складають невичерпане джерело скінчених абелевих груп, які мають багату структуру і зручні для обчислення. В багатьох відношеннях еліптичні криві – це аналог мультиплекативних груп, але більш зручний, так як існує більша свобода у виборі еліптичної кривої, ніж під час вибору скінченого поля.

1.1. Еліптичні криві. Група точок кривої.

Криптографічні додатки теорії еліптичних кривих - дуже молодий розділ в криптографії. Його поява диктується необхідністю пошуку завдань такої обчислювальної складності, яка б гарантовано забезпечувала стійкість криптографічних об'єктів. N. Koblitz був одним з авторів ідеї застосування еліптичних кривих в даній області. Головним тут стало використання групи точок кривої в тій же якості, в якому теоретико-групові об'єкти присутні в двохключового криптографії. Ця група, взагалі кажучи, не є циклічною. Відсюди виникають надії на ускладнення обчислювальних задач, пов'язаних з такою групою.

Означення 1.1. Еліптична криптографія – це розділ криптографії, що використовує еліптичні криві з параметрами, визначеними над скінченними полями для реалізації схем шифрування.

Головним напрямком застосування еліптичних кривих в криптографічних схемах є системи з відкритим ключем. Ключовим математичним об'єктом еліптичної криптографії є еліптична крива.

Позначимо через K деякие поле. Нас будуть цікавити перш за все поля: $\mathbb{R}$ дійсних чисел, $\mathbb{Q}$ - раціональних чисел і $\mathbb{F}_{\text{||}}$, що має $q = p^r$ елементів.

Нехай **K** - це поле: або поле **R** дійсних чисел, або поле **Q** раціональних чисел, або поле **C** комплексних чисел, або поле F_q з $q = p^r$ елементів.

Означення 1.2. Нехай **K** - поле характеристики, відмінної від 2,3 і $x^3 + ax + d$ (де a,$b \in$ K) - кубічний многочлен без кратних коренів. *Еліптична крива над* ***K*** - це безліч точок (x, y), де x,$y \in$ K, задовольняють рівнянню

$$y^3 = x^3 + ax + b \tag{1.1}$$

разом з елементом, позначається через і званим *«нескінченно віддаленою точкою»*.

Якщо K – поле характеристики 2, то еліптична крива над K – це множина точок, задовольняющих рівнянню або типу

$$y^2 + cy = x^3 + ax + b \tag{1.2}$$

або типу

$$y^2 + xy = x^3 + ax^2 + b \tag{1.3}$$

Якщо K – поле хпрпкьеристики 3, тоді еліптична кривая над K – це множина точок, яка задовольняє рівнянню

$$y^2 = x^3 + ax^2 + bx + c \tag{1.4}$$

Зауваження 1.1. Маємо загальну форму елуптичної кривої, яку можемо приминіма при будь-якому полі: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$; у вападку коли char $K \neq 2$, її можливо привести до виду $y^2 = x^3 + ax^2 + bx + c$ (або до виду $y^2 = x^3 + bx + c$, якщо $K > 3$). У випадку, коли поле K має характеристику 2, це рівняння переходить до виду (1.2), або до виду (1.3).

Зауваження 1.2. Якщо $F(x,y) = 0$ – неявне рівняння, яке виражає y як функцію x в 1.2, тобто $F(x,y) = y^2 - x^3 - ax - b($ або $F(x,y) = y^2 + cy + x^3 + ax + b, y^2 + xy + x^3 + ax + b, y^2 - x^2 - x^3 - ax^2 - bx - c)$, то точка (x,y) цієї криво називається *неособливою* (або *гладкою*) точкою, якщо, хоча б одна з часткових похідних $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ в цій точці дорівнює нулю.

1.2. Еліптичні криві над скінченним полем.

До кінця цього розділу буде кінцевим полем F_q, що має $q = p^r$ елементів. Нехай буде еліптичною кривою, визначеною над полем F_q. Легко помітити, що еліптична крива може мати щонайбільше $2q + 1$ F_q-точок: точка в нескінченності і $2q$ пар (x,y), причому $x,y \in F_q$, задовольняють рівняння (1.1). Бачимо, що для кожного з q можливих значень існує не більше двох значень , які задовольняють рівняння (1.1).

Однак, оскільки тільки половина ненульових елементів поля F_q мають квадратні корені, можна було очікувати, що (враховуючи $x^3 + ax + b$ випадковим елементом цього поля) кількість F_q - точок на кривій в два рази менше. Детальніше, нехай χ буде квадратичним характером поля F_q. Це відображення, яке кожному елементу $\chi \in F_q^*$ зіставляє ± 1, в залежності від того, чи має χ квадратний корінь в F_q (і, крім того, $\chi(0) = 0$).

$$1 + \sum_{x \in F_q} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in F_q} \chi(x^3 + ax + b) \qquad (1.5)$$

Можна очікувати, що значення $\chi(x^3 + ax + b)$ буде однаково часто дорівнювати +1 і -1.

Ця сума нагадує підсумовування в «випадковому кроці»: кидається q раз монета, при випаданні орла робимо крок вперед, при випаданні решки - крок назад. Використовуючи метод теорії ймовірностей, можна обчислити, що при q кидках монети середнє значення, на яке відійдемо, таким чином, від вихідного положення, має порядок q.

Сума

$$\sum \chi(x^3 + ax + b) \qquad (1.6)$$

подібна сумі в «випадковому кроці», і виявляється, що для неї відповідну оцінку є $2q$.

Теорема 1.1. *Теорема Гассе.*

Нехай $\boldsymbol{N}$ *– число* F_q*-точек на еліптичній кривій, визначеной над* F_q*. Тоді*

$$|N - (q+1)| \leq 2\sqrt{q}.$$

Доповнення до числа N елементів на еліптичній кривій над F_q потрібно знати будову абелевої групи. Вона – не обов'язково циклічна. Це значить, що група ізоморфна добутку p-примарних груп виду $\frac{\boldsymbol{Z}}{p^\alpha \boldsymbol{Z}} \times \frac{\boldsymbol{Z}}{p^\beta \boldsymbol{Z}}$, де добуток береться по всім простим дільникам N(тут $\alpha \geqslant 1, \beta \geqslant 0$). Під типом абелевої групи F_q-точек на E ми розуміємо список $(\dots, p^\alpha, p^\beta, \dots)_{(p|N)}$ порядків циклічних $p-$примарних співмножників у вигляді добутку (якщо $\beta = 0, p^\beta$ опускаємо).

Приклад 1.1. *Знайти тип для кривої $y^2 = x^3 - x$ над $F_{(71)}$.*

Розв'язок. Знаходимо на початку число точек N. Помітимо, що в сумі 1.5 для x та для $-x$ скорочуються один з одним:

$$\chi((-x)^3 - (-x)) = \chi(-1)\chi(x^3 - x), \text{ так як } 71 \equiv 3 \ (mod\ 4),$$

і тоді $\chi(-1) = -1$. Як наслідок, $N = q + 1 = 72$. Далі, маємо у точності чотири точки порядку 2 (включаючи "нескінченну"точку O): вони відповідають кореням полінома $x^3 - x = x(x+1)(x-1)$. Це означає, що 2-примарна частина групи має тип (4,2) і, таким чином, тип групи – це (4,2,3,3) або (4,2,9), все залежить від того, дорівнює 9 чи 3 число точек порядка 3. Отже, залишається дізнатись, чи існує 9 точок порядка 3. Зауважимо, що умова $3P = O$ при $P \neq O$ еквівалентно умові $2P \neq \pm P$, тобто тому, що x-координати точок $2P$ і P однакові.

Згідно з формули для координат подвійної точки P:

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1,$$

$$y_3 = -y_1 + \frac{3x_1^2+a}{2y_1}\big(x_1 - x_3\big).$$

– це означає, що $(\frac{(3x^2-1)^2}{2y})^2 - 2x = x$, тобто $(3x^2-1)^2 = 12xy^2 = 12x^4 - 12x^2$. Спрощуючи, отримаємо $3x^4 - 6x^2 - 1 = 0$. Це рівняння має, саме велике, 4 корені в $F_{(71)}$. Кожен корень може давати не більше двох точок (при $y = \pm\sqrt{x^3 - x}$, якщо $x^3 - x$ є квадрат по модулю 17), і якщо

було б 4 корені, то отримали 9 точок порядка 3 (і стало б, у точності 3 таких точки). Однак, якщо корень x біквадратного рівняння такий, що $x^3 - x$ є квадрат за модулем 71, тоді для іншого кореня $-x$ отримуємо, що $(-x)^3 - (-x) = -(-x^3 - x)$ не є квадратом. Значить, що число точек порядка 3 не може бути равно 9 і тому тип групи – (4,2,9).

РОЗДІЛ 2

ПРОТОКОЛ ЕЦП НА ЕЛІПТИЧНІЙ КРИВІЙ. АЛГОРИТМ ECDSA

Найбільш популярними напрямками еліптичної криптографії, тобто сферами, в яких криптостійкість базується на задачі дискретного логарифмування для еліптичних кривих або ECDLP, є шифрування з відкритим ключем та алгоритм електронно-цифрового підпису.

В даному підрозділі буде розглянуто різноманітні схеми обміну ключами. Як зазначалось раніше, існують два види використання шифрування з ключами – симетричний (існує єдиний секретний ключ, що має бути переданий між відправником та отримувачем захищеним каналом) та асиметричний (існує пара ключів – приватний та публічний, що може бути переданий незахищеним каналом). В межах даної роботи детально розглядається другий варіант, а саме асиметричне шифрування.

ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм з відкритим ключем для створення цифрового підпису, аналогічний, за своєю будовою, DSA, але визначений, на відміну від нього, не над полем цілих чисел, а у групі точок ЕК.

Розглянемо використання алгоритму ECDSA з використанням еліптичної кривої з параметрами, визначеними над скінченим полем.

2.1. Алгоритм генерації ключів

1) Вибирають еліптичну криву E, що визначається над Z_ρ. Число точок кривої $E(Z_\rho)$ має ділитися на велике просте число n.
2) Обирають точку $P \in E(Z_\rho)$ порядка n.
3) Вибирають випадкове число $d \in (1, n)$.
4) Обчислюють $Q = dP$.
5) Секретним ключем оголошують d, відкритим – (E, P, n, Q).

2.2. Алгоритм формування підпису під повідомлення M

1) Вибирають випадкове число $k \in (1, n)$.
2) Обчислюють $kP = (x_1, y_1)$ і вважають $r = x_1 \ (mod\ n)$. Якщо $r \neq 0 \ (mod\ n)$, то переходять до кроку 3, інакше - до кроку 1.
3) Обчислюють $k^{-1} \ (mod\ n)$.
4) Обчислюють $s = k^{-1} \ (h(M) + dr)(mod\ n)$. Якщо $s \neq 0 \ (mod\ n)$, то переходять до кроку 5, інакше - до кроку 1.
5) Підписом під повідомленням M вважають пару цілих чисел (r,s).

Зауваження 2.1. $h(x)$ – хеш-функція (у вказаному стандарті – $SHA-1$).

Зауваження 2.2. При $r = 0$ результат обчислення залежить від d.

Зауваження 2.3. При $s = 0$ не існує $s^{-1} \ (mod\ n)$, що необхідно для перевірки підпису.

2.3. Алгоритм перевірки підпису (r, s) під повідомленням M за допомогою відкритого ключа (E, P, n, Q)

1) Якщо r і s – цілі числа із $(1, n)$, то переходять до кроку 2, інакше підпис відкидається.
2) Обчислюють $w = s^{-1} \ (mod\ n)$ і $h(M)$.
3) Обчислюють $u_1 = h(M)w \ (mod\ n)$ і $u_2 = r \ (mod\ n)$.
4) Обчислюють $u_1P + u_2Q = (x_0, y_0)$ і $v = x_0 \ (mod\ n)$
5) Підпис вважають вірним у тому й лише тому випадку, коли $v = r$.

Приклад 2.1. Христина вирішує написати тарасу повідомлення із підписом на основі еліптичної кривої. Вона використовує алгоритм ECDSA (у разі з деяким спрощенням). Її повідомлення M = "BEST"$\rightarrow$ 0104189 $\rightarrow$ 1041819. Вона вибирає криву $y^2 = x^3 + 145x + 217$ над полем F_{4001}. Число точок кривої $N = 3992$. Це число ділиться на просте $n = 499$. На кривій Христина

вибирає точку $P = (20, 927)$, порядок якої дорівнює 499. Далі Христина вибирає випадкове число $d = 399$ та обчислює точку $Q = dP = (200, 1986)$. І оголошує відкритим ключем елементи (E, P, n, Q). Секретним ключем у неї залишається $d = 399$. Під час підписування повідомлення Христина робить наступні кроки:

1) Вибирають випадкове число $k = 98$.
2) Обчислюють $kP = (1384, 37)$ і вважають $r = 1384(mod\ 499) = 386$.
3) Обчислюють $k^{-1}\ (mod\ 499) = 433$.
4) Обчислюють $s = 443((1041819) + 399 * 1984)(mod\ 499) = 443 * 229(mod\ 499) = 150$, тут $H(x) = x\ (mod\ n)$ для простоти демонстрації.
5) Видає підпис $(386, 150)$.

Тарас починає перевірку підпису та виконує наступні кроки:

1) Виявляє, що елементи пари є натуральними числами з проміжку $(1, n)$.
2) Обчислюють $w = 336\ (mod\ 499)$ і $H(M) = 406(mod\ 499)$.
3) Обчислюють $u_1 = 409 * 339\ (mod\ 499)189$ і $u_2 = 386 * 336\ (mod\ 499) = 455$.
4) Обчислюють точку $u_1P + u_2Q = 189(20, 927) + 455(20, 1986 = (793, 1110) + (3653, 2072) = (1384, 37))$ і $v = 1384\ (mod\ 499) = 386$.
5) Переконується, що $v = r = 386$. Таким чином, підпис було згенеровано власником секретного ключа.

РОЗДІЛ 3

КРИПТОСИСТЕМА НА ЕЛІПТИЧНИХ КРИВИХ

3.1. Кратні точки.

Для еліптичних кривих аналог добутку двох елементів групи F_q^* є сума двох точок еліптичної кривої E, визначеної над F_q.

Таким чином, аналог возведення в степінь k елемента з F_q^* – це добуток точки $P \in E$ на ціле число k. Піднесення до $k-$ї степені у F_q^* методом повторного піднесення до квадрату можна здійснити за $O(log\ k\ log^3\ q)$ двійкових операцій методом повторного подвоєння.

Приклад 3.1. Для того, щоб знайти $100P$, записуємо $100P = 2(2(P + 2(2(2(P + 2P)))))$ і доходимо до цілі, відтворюючи шість подвоєнь та дві суми точек на кривій.

Припущення 3.1. *Нехай еліптична крива E визначена рівнянням Вейєрштраса (рівнянням (1.2), (1.3) або (1.4)) на скінченим полем F_q. Якщо задана точка P на E, то координати kP можно знайти за $O(log\ k\ log^3\ q)$ двійкових операцій.*

Доведення. Помітимо, що обчислення координат суми двох точек за рівняннями :

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, \tag{3.1}$$

$$y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) \tag{3.2}$$

та

$$x_3 = (\ \frac{3x_1^2 + a}{2y_1})\ ^2 - 2x_1, \tag{3.3}$$

$$y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) \tag{3.4}$$

потребує не більше 20 дій у F_q (добутків, діленнь, сум та різниць). Тому, сума двох точок (або подвоєння точки) займає час $O(log^3\ q)$. Так як при методі повторного подвоєння виконується $O(log\ k)$ однакових шагів, ми отримуємо, що координати точки kP рахуються за допомогою $O(log\ k\ log^3\ q)$ двійкових операцій.

Зауваження 3.1. Оцінки часу роботи у припущенні[3.1] не є найкращим, особливо для скінчених полів характеристики $p = 2$. Достатньо оцинок, що сілдує з найбільш очевидних алгоритмів арифметики у скінченних полях.

Зауваження 3.2. Якщо відомо число N точек на нашій еліптичній кривій E та якщо $k > N$, тоді в силу рівняння $NP = O$ ми можемо замінити k його найменшим невід'ємним лишком за модулем N; в цьому випадку тимчасова оцінка замінюється на $O(log^4\ q)$.

3.2. Алгоритм системи Ель-Гамаля

Це криптосистема з відкритим ключем для передання повідомлень P_m. Ми відштовхуємось від данних несекретних:

- скінченого поля F_q;
- визначеної над ним еліптичною кривою E;
- точки-"засновника"B на кривій.

Кожен користувач обирає випадкове ціле число a, яке тримає у секреті, потім знаходить і робить доступною точкою для всіх aB.

для того, щоб надіслати Тарас повідомлення P_m, Христина обирає випадково ціле число k і надсилає напу точок $(kB, P_m + k(a_BB))$ (де a_BB

- відкритий ключ Тараса). Для того, щоб прочитати повідомлення, Тарас помножує свою точку з отриманої пари на своє секретне число a_B і віднімає результат добутку з другої точки:

$$P_m + k(a_B B) - a_B(kB) = P_m.$$

Таким чином, Христинка посилає замасковане P_m разом з підказкою kB за допомогою якої можна зняти "маски"$ka_B B$, якщо знати таємне число a_B. Злодій, який вміє розв'язувати задачі дискретного логарифмування на E, може, звісно, знайти a_B, знаючи $a_B B$ і B.

3.3. Випадковий вибір (E,B)

Взяв будь-яке велике скінчене поле F_q, можна наступним чином здійснити одночасний вибір E та $B = (x, y) \in E$. Обираємо спочатку випадковістю три елементи з F_q^* у якості x,y,a. Далі полагаємо $b = y^2 - (x^3 + ax)$. Бачимо, що кубічний поліном $x^3 + ax + b$ не має кратних коренів, що рівнозначно перевірці умови $4a^3 + 27b^2 \neq 0$. (Якщо ця умова не виконується, то можемо взяти іншу трійку x,y,a.)

Покладемо $B = (x,y)$. Тоді B - точка на еліптичній кривій $y^2 = x^3 + ax + b$.

Число N точок кривої можно знайти кількома способами. перший поліноміальний алгоритм для обчислення E, побудований Рене Шуфом, є навіть детерміністичним. Він засновується на знаходженні значення E за модулем l для всіх простих чисел l, меньших деякої границі. Для цього аналізується дія автоморфізму Фробеніуса (відображення ρ-ю степінь) на точках порядку l.

У статті Шуфа оцінка часу роботи була фактично $O(log^8 q)$, тобто хоч і поліноміальною, однак швидко виростаючей. Спочатку здається, що алгоритм не має практичного значення. Однак з тих пір багато хто намагався підвищити швидкістьалгоритма Шуфа (Міллер, Елкіс, Бухман та ін.). Крім того, Еткін розробив інший метод, який, хоча і не гарантує поліноміального часу роботи, на практиці дає задовільні результати. У висновку всіз зусиль

стало можливим знаходити порядок довільної еліптичної кривої над f_q, якщо q - степінь простого числа, яка записується 50 або навіть 100 знаками.

Але треба відмітити, що для реальзіції системи Ель-Гамаля знати N не потрібно. Однак, на практиці необхідно бути впевненим в їх надійності, яка залежить від того, чи має N великий простий дільник.

3.4. Редукція глобальної пари (E,B) за модулем ρ

Другий спосіб знаходження пари, яка складає елептичну криву і точки на ній. Обераємо спочатку один раз "глобальну"еліптичну криву і точку нескінченного порядку на ній. Отже, нехай E - еліптична крива, яка визначена над полем раціональних чисел та B - точку нескінченного порядку E.

Приклад 3.2. Точка $B = (0,0)$ є точкою нескінченного порядку на еліптичній кривій $E : y^2+y = x^3-x$ і фактично породжує всю групу раціональних точок на E.

Приклад 3.3. Точка $B = (0,0)$ є точкою нескінченного порядку на еліптичній кривій $E : y^2+y = x^3+x^2$ і фактично породжує всю групу раціональних точок на E.

Далі ми обираємо велике просте число ρ і розглядаємо редукцію E і B за модулем ρ. Точніше, для всіх ρ, за виключенням декількох малих простих чисел, коефіцієнти в рівнянні для E мають взаємно прості з ρ знаменники і можуть розглядатися як коефіцієнти в рівнянні над F_q до виду $y^2 = x^3 + ax + b$, то кубічний поліном у правій частині не буде мати кратних коренів і дає тому еліптичну криву над F_q (яку будемо позначати $E(mod\ \rho)$). Координати точки B, будучи зведенними по модулю ρ, дають точку на еліптичній кривій $E(mod\ \rho)$, яку будемо зазначати, як $B(mod\ \rho)$.

При використовування цього другого методу ми один раз фіксуємо E і B та за їх рахунок отримаємо багато різних можливостей для зміни простого ρ.

3.5. Порядок точки B

З якою ймовірністю випадкова точка B на випадковій еліптичній кривій буде породжувальним елементом? Або, у випадку другого метода вибіру (E,B), яка ймовірність того, що (для випадкового ρ) точка B при редукції за модулем ρ дає утворюючий елемент кривої E $(mod\ \rho)$?

Криптосистеми можуть бути надійними, навіть якщо точка B не є породжуючим елементом. Фактично необхідно, щоб у циклічній групі, породжуємий елемент B, задача логорифмування не була ефективно розв'язуємой. Це буде так, якщо порядок B поділяється на дуже велике просте число, скажімо, маюче порядок величини, близькій до N.

Один із способів це гарантувати, що вибір B є правильним – це взяти таку еліптичну криву і таке скінчене поле, щоб число точек N було простим числом. Тоді будь-яка точка $B \neq O$ буде породжуючим елементом. Якщо використовувати перший з методів вище, то при фіксованому F_ρ можна продовжувати вибір пар (E, B), поки не знайдеться така, для якої число точок на E є просте число.

Зауваження 3.3. Для того щоб E $(mod\ \rho)$ мала простий порядок N при великому ρ, треба обирати E так, щоб на неї не було точок скінченого порядку, окрім O. У іншому випадку N буде поділятись на порядок періодичної підгрупи.

РОЗДІЛ 4

РОЗКЛАД НА МНОЖНИКИ ЗА ДОПОМОГОЮ ЕЛІПТИЧНИХ КРИВИХ

Основною причиною великого інтересу частини криптографів до еліптичних кривих є знайдене Ленстрою застосування еліптичних кривих у новому методі факторизації, якій у багатьох відношеннях ліпше існуючого раніше. З точки зору практики, це просунення не настільки значне, щоб погрожувати надійності криптосистем, заснованих на труднощах задач розкладання на множники. Тим не меньш, відкриття більш досконалого методу, використовувавший несподіваний новий інструментарій, застерігає від благодушності з приводу неможливості існування просування у задачі розкладання на множники.

4.1. $\rho - 1$-метод Полларда

Нехай ми розкладаємо на множники складене число n і припускаємо, що ρ - це його простий дільник. Якщо ρ такий, що $\rho - 1$ не має великих простих дільників, то ρ можна знайти наступний чином.

1) Обираємо ціле число k, кратне всім або більшості цілих чисел, меньших деякої границі B. Наприклад, у якості k можна взяти $B!$ або спільне найменьше кратне всіх цілих чисел, яке не пперевищує B.
2) Обираємо ціле число a між 2 та $n-2$. Наприклад, a може дорівнювати $2, 3$ або випадково обранному цілому числу.
3) Обчислюємо a^k за модулем n повторно возведенним в квадрат.
4) Обчислюємо $d = \text{НСД}(a^k - 1, n)$, використовуючи алгоритм Евкліда та лишок $a^k \ (mod\ n)$ з кроку 3.
5) Якщо d не є нетривіальний дільник n, то повторюємо всі кроки з новим a та/або новим k.

Для того щоб зрозуміти при яких умовах алгоритм буде працювати, припустимо, що k ділиться на всі натуральні числа, не більше B. Далі,

нехай ρ - простий дільник n для якого $\rho - 1$ представляється у вигляді добутку степенів невеликих простих чисел. Звідси можемо сказати, що k кратно $\rho - 1$. Тому за малою теоремою Ферма. маємо $a^k \equiv 1\ (mod\ \rho)$. Тоді НСД $(a^k - 1,n)$ може ділитись на ρ. аким чином, едина перешкода, яке може заважаи отримати на четвертому кроці нетривіальний дільник n - це випадок, коли $a^k \equiv 1\ (mod\ n)$.

Приклад 4.1. Розкладемо вказаним методом $n = 54143$. Обираємо $B = 8$ (тоді наслідок, що $k = 840$ - спільному найменькому кратному 1,2,...,8) і $a = 2$. Знаходимо, що $2^{840}\ (mod\ n)$ - це 53047 і НСД(53046,n) = 421. Тим самим доходимо до $540143 = 421 * 1283$.

Основна слабкість метода Поллара, очевидно, проявляється при спробах його застосування в тих чи інших випадках, коли всі прості дільники ρ числа n такі, що $\rho - 1$ може поділитись на відносно велике просте число (або на велику степінь простого числа).

4.2. Еліптичні криві - редукція за модулем n

Нехай n - непарне складене число і ρ - простий дільник n. Будемо вважати, що $\rho > 3$. Нехай m - ціле число та $x_1 - x_2$ – два раціональних числа із знаменниками, взаємно простими з m; будемо писати $x_1 \equiv x_2\ (mod\ m)$, якщо чисельник різниці $x_1 - x_2$, записанний у вигляді нескоротного дробу, подляються на m. Для будь-якого раціонального числа x_1 із знаменником, взаємно простим з m, існує таке однозначно зазначене ціле число x_2 між 0і$m - 1$ (найменьший невід'ємний лишок), що $x_1 \equiv x_2\ (mod\ m)$.

Нехай дани рівняння виду $y^2 = x^3 + ax + b, a, b, \in Z$, і точка, що задовольняє $P = (x,y)$. На практиці елвптична крива E разом із точкою P будуть породжувати деяким "випадковим"способом. Наприклад, можна вибрати три випадкових простих числа a, x, y з деякої області і потім покласти $b = y^2 - x^3 - ax$. Будемо припускати, що кубічний поліном $x^3 + ax + b$ має різні корені, тобто що $4a^3 + 27b^2 \neq 0$; ця умова виконується майже завжди, якщо коефіцієнти обираються описаним визе випадковим способом. Практично. обрав a, b ми можемо перевірити це, знайшовши

НСД $(4a^3 + 27b^2, n)$. Якщо число більше 1, то або $n|(4a^3 + 27b^2)$ (тоді слід обрати інші a та b), або вже знайшли нетривіальний дільник n і тоді задача розв'язана. Тоді будемо припускати, що НСД $(4a^3 + 27b^2, n) = 1$.

Теорема 4.1. *Нехай E - еліптична крива з рівнянням $y^2 = x^3 + ax + b$, де $a, b \in Z$ і НСД $(4a^3 + 27b^2, n) = 1$. Нехай P_1 і P_2 - це дві точки на E. у яких знаменники взаємно прості з n, і $P_1 \neq -P_2$. Тоді $P_1 + P_2 \in E$ має координати, у яких знаменники взаємно прості з n, тоді і тільки тоді, коли у n немає простого дільника ρ, для котрого сума точок $P_1 \ (mod\ \rho)$ і $P_2 \ (mod\ \rho)$ на еліптичній кривій $E \ (mod\ \rho)$ дорівнювала б точці в нескінченності $O \ (mod\ \rho) \in E \ (mod\ \rho)$. Тут $E \ (mod\ \rho)$ набуває значення еліптичної кривої над F_ρ, отриманною зведенням за модулем ρ коефіцієнтів рівняння $y^2 = x^3 + ax + b$.*

Доведення. Нехай всі точки $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ і $P_1 + P_2 \in E$ спочатку мають координати з знаменниками, взаємно простими з n. Потрібно довести, що для будь-якого простого дільника ρ числа n сума $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) \neq O$. Якщо $x_1 \not\equiv x_2 \ (mod\ \rho)$, то відповідно з описом закона про складання на $E \ (mod\ \rho)$ одразу же заключаємо, що $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) \neq O \ (mod\ \rho)$. Тепер припустимо, що $x_1 \equiv x_2 \ (mod\ \rho)$. При $P_1 = P_2$ координати точки $P_1 + P_2 = 2P_1$ визначаються формулою 3.3, 3.4 і $2P_1(mod\ \rho)$ знаходяться за той же формулой з зміною кожного члена і його лишком за модулем ρ. Потрібно показати, що знаменник $2y_1$ дробу в правій частині 3.3, 3.4 не ділиться на ρ. Але якби він ділився на ρ, тоді $3x_1^2 + a$ ділилось би на ρ. Тоді x_1 був би коренем за модулем ρ як полінома $x^3 + ax + b$, так і його похідної $3x^2 + a$, що протиречить припущенню, про відсутність кратних коренів за модулем ρ у цього полінома. Тепер нехай $P_1 \neq P_2$. Так як $x_2 \equiv x_1 \ (mod\ \rho)$ і $x_2 \neq x_1$, можна записати $x_2 = x_1 + \rho^r x$ обрано так, що ані чисельник, ані знаменник x не поділиться на ρ. По припущенню знаменники координат точки $P_1 + P_2$ не дільться на ρ, тому має вид $y_1 + \rho^r y$. З іншого боку

$$\mathrm{y}_2^2 = (x_1 + \rho^r x)^3 + a(x_1 + \rho^r x) + b$$

$$\equiv x_1^3 + ax_1 + b + \rho^r x(3x_1^2 + a) = y_1^2 + \rho^r x(3x_1^2 + a)(mod\ p^{r+1})(4.1).$$

Так як $x_2 \equiv x_1 \ (mod\ \rho)$ і $y_2 \equiv y_1 \ (mod\ \rho)$, тоді $P_1 \ (mod\ \rho) = P_2 \ (mod\ \rho)$ тобто $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) = 2P_1 \ (mod\ \rho)$. Видно, що $2P_1 \ (mod\ \rho) = O \ (mod\ \rho)$ тоді і тільки тоді, коли $y_1 \equiv y_2 \equiv 0 \ (mod\ \rho)$. Якщо це порівнння виконано, тоді $y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1)$ повинно ділитись на ρ^{r+1}. Тому із порівняння 4.2 слід, що $3x_1^2 + a \equiv 0 \ (mod\ \rho)$. Но це неможливо т.к $x^3 + ax + b$ не має кратних коренів за модулем ρ, тобто x_1 не може бути спільним коренем цього полінома та його похідної. Значить, $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) \not\equiv O \ (mod\ \rho)$, як і стверджувалось.

Назад, нехай $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) \not\equiv O \ (mod\ \rho)$ для кожного простого дільника ρ числа n. Покажемо, що знаменники координат $P_1 + P_2$ взаємно прості з n, тобто знаменники не поділяються на будь-який простий дільник ρ числа n . Фіксуємо деякі $\rho | n$. Формули 3.1, 3.2 показують, що якщо $x_2 \equiv x_1 \ (mod\ \rho)$, то тих, що діляться на ρ знаменників немає. Тому припустимо, що $x_2 \equiv x_1 \ (mod\ \rho)$. Тоді $y_2 \equiv + - y_1 \ (mod\ \rho)$; однак $P_1 \ (mod\ \rho) + P_2 \ (mod\ \rho) \neq O \ (mod\ \rho)$, тоді $y_2 \equiv y_1 \not\equiv 0 \ (mod\ \rho)$. При $P_2 = P_1$ формула 3.1, 3.2 разом з умовою $y_1 \not\equiv 0 \ (mod\ \rho)$ показує, що знаменники координат точки $P_1 + P_2 = 2P_1$ взаємно прості з ρ. Нарешті, якщо $P_2 \neq P_1$, ми знов пишемо $x_2 = x_1 + \rho^r x$ з x, не ділившимся на ρ, і, використовуючи порівняння 4.2, отримаємо $\frac{(y_2^2 - y_1^2)}{(x_2 - x_1)} \equiv 3x - 1^2 + a \ (mod\ \rho)$. Т.к ρ не ділить $y_1 + y_2 \equiv 2y_1 \ (mod\ \rho)$, звідси і отримаємо, що знаменник числа $\frac{(y_2^2 - y_1^2)}{(y_1 - y_2)(x_2 - x_1)} = \frac{y_2 - y_1}{x_2 - x_1}$ не ділиться на ρ, і в силу формули 3.1 знаменники координат точки $P_1 + P_2$ не діляться на ρ. Теорема доведена.

РОЗДІЛ 5

ПРАКТИЧНА ІНТЕРПРИТАЦІЯ МОВОЮ PYTHON

5.1. Програма Python для ілюстрації теореми Гассе

Завдання 1

Проілюструвати модель теореми Гассе.

Лістинг 1

```
import math

INF_POINT = None


class EllipticCurve:
        def __init__(self, a, b, p):
                self.a = a
                self.b = b
                self.p = p
                self.points = []
                self.define_points()


        def define_points(self):
                self.points.append(INF_POINT)
                for x in range(self.p):
                        for y in range(self.p):
                                if self.equal_modp(y * y,
                                            x * x * x + self.a * x
                                                + self.b):
                                        self.points.append((x,y))


        def addition(self, P1, P2):
                if P1 == INF_POINT:
                        return P2
                if P2 == INF_POINT:
```

```
                        return P1

                x1 = P1[0]
                y1 = P1[1]
                x2 = P2[0]
                y2 = P2[1]

                if self.equal_modp(x1, x2) and self.equal_modp(y1, -y2):
                        return INF_POINT

                if self.equal_modp(x1, x2) and self.equal_modp(y1, y2):
                        u = self.reduce_modp((3 * x1 * x1 + self.a)
                                        * self.inverse_modp(2 * y1))
                else:
                        u = self.reduce_modp((y1 - y2)
                                    * self.inverse_modp(x1 - x2))

                v = self.reduce_modp(y1 - u * x1)
                x3 = self.reduce_modp(u * u - x1 - x2)
                y3 = self.reduce_modp(-u * x3 - v)
                return (x3, y3)


        def test_associativity(self):
                n = len(self.points)
                for i in range (n):
                        for j in range(n):
                                for k in range(n):
                                        P = self.addition(self.points[i],
                                                self.addition
                                                 (self.points[j],
                                                    self.points[k]))
                                        Q = self.addition(self.addition
                                                 (self.points[i],
                                                    self.points[j]),
                                                      self.points[k])
                                        if P != Q:
                                                return False
                return True


```

```
70          def number_points(self):
71                  return len(self.points)
72
73
74          def discriminant(self):
75                  D = -16 *(4 * self.a * self.a *
76                              self.a + 27 * self.b * self.b)
77                  return self.reduce_modp(D)
78
79
80          def print_points(self):
81                  print(self.points)
82
83
84          def verify_hasse(self):
85                  return abs(self.number_points() - (self.p + 1))
86                                  <= 2 * math.sqrt(p)
87
88
89          def lower_hasse_bound(self):
90                  return math.ceil(self.p + 1 - 2
91                                  * math.sqrt(self.p))
92
93
94          def upper_hasse_bound(self):
95                  return math.floor(self.p + 1 + 2
96                              * math.sqrt(self.p))
97
98          # helper functions
99
100         def reduce_modp(self, x):
101                 return x % self.p
102
103
104         def equal_modp(self, x, y):
105                 return self.reduce_modp(x - y) == 0
106
107
108         def inverse_modp(self, x):
109                 for y in range(self.p):
110                         if self.equal_modp(x * y, 1):
```

```
                                return y
                return None



p = 101

epsilon = 2 * math.sqrt(p)
lower_hasse_bound = math.ceil((p + 1) - epsilon)
upper_hasse_bound = math.floor((p + 1) + epsilon)

group_orders = []

for a in range(0, p):
        for b in range(0, p):
                ec = EllipticCurve(a, b, p)
                if ec.discriminant() == 0:
                        continue
                group_orders.append(ec.number_points())
                if ec.verify_hasse() == False:
                        # this case should not happen
                        print("THE HASSE THEOREM FAILED?")
                        break


print("Hasse lower bound =", lower_hasse_bound)
print("Minimum group order =", min(group_orders))

print("Hasse upper bound =", upper_hasse_bound)
print("Maximum group order =", max(group_orders))


# test to see that all numbers in the "Hasse interval" are
# equal to the order of some elliptic curve

not_group_orders = []
for i in range(lower_hasse_bound, upper_hasse_bound + 1):
        if i not in group_orders:
                not_group_orders.append(i)

if len(not_group_orders) == 0:
```

```
        print("Every integer in the possibe range is a group order.")
else:
        # this case should not happen
        print("The following are not the orders of any elliptic curve.")
        print(not_group_orders)

# average group order
print("Average group order =", sum(group_orders) / len(group_orders))
print("p + 1 =", p + 1)
```

Результати

```
"C:\Program Files\Python39\python.exe"
//bank.lan/data/homefolders/k.verbetska/Desktop
/Verbetska/venv/Gasse.py


Hasse lower bound = 82
Minimum group order = 82
Hasse upper bound = 122
Maximum group order = 122
Every integer in the possibe range is a group order.
Average group order = 102.0
p + 1 = 102
```

РОЗДІЛ 6

ВИСНОВОК

В даній роботі було виконано дослідження підходів та методів шифрування/дешифрування з використанням еліптичних кривих.

В основному, в межах даної роботи були розглянуті еліптичні криві, параметри яких визначені над скінченними полями.

Розглянуті основи математичної теорії скінченних полів, над якими визначається еліптична крива, яка використовується в підходах та методах побудови криптосистем, описаних у розділі 1. Скінченні поля представляють особливий інтерес з огляду на ефективність їх застосування в апаратних та програмних реалізаціях криптосистем заснованих на еліптичній кривій, через свою очевидну близькість до апаратного (двійкового) подання значень та виконання операцій на обчислювальних приладах.

Умовно, операції, що виконуються в рамках застосування алгоритмів шифрування з використанням еліптичної криптографії можна розділити на декілька основних класів. але саме в цій дипломній роботі розлядався тип операції нижнього та верхнього рівня, де операції нижнього рівня – це арифметичні операції над елементами скінченних полів та арифметичні операції над точками еліптичної кривої.

Розроблений програмний комплекс для перевірки технічної роботи теореми Гассе дозволяє практично подивитись на знаходження меж та груп. Приклад наведен у розділі 5 з результатами відпрацювання комплексу.

Загалом, враховуючи інформацію, наведену в даному розділі, можна стверджувати, що криптосистеми, засновані на еліптичних кривих, довели свою цінність та високий рівень захищенності. В даному розділі було розглянуто ряд існуючих протоколів розподілу ключів в асиметричних криптосистемах, а також алгоритмів електронно-цифрового підпису на еліптичних кривих.

У методах шифрування еліптичної криптографії та схемах цифрового підпису, що ґрунтуються на властивостях адитивної абелевої групи,

утвореної точками ЕК.

СПИСОК ЛІТЕРАТУРИ

1. Кобліц Н. Курс теорії чисел та криптографії / Н. кобліц. — М.: Наукове видання, 2001. — 254 с.
2. Stein W. Elementary Number Theory and Elliptic Curves / W. Stein. — Department of Mathematics Harvard University, 2003. — 238 с.
3. Ященко В. В. Введенние в криптографию / В. В. Ященко — М.: Высшая школа, 1998. — 235 с.
4. Смарт Н. Світ програмування: криптографія / Н. Смарт. — М.: ТЕХНОСФЕРА, 2005. — 528 с.
5. Вербецька К. І. Курсова робота "Цифровий підпис"/ К. І. Вербецька. — 27 с.