ЛАБОРАТОРНА РОБОТА № 8. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Мета роботи: ознайомитися з алгоритмами криптографічних перетворень на еліптичних кривих, здійснивши формування спільного ключа між двома абонентами за алгоритмом Діффі-Хеллмана на еліптичних кривих.

Матеріально-технічне забезпечення: ПК зі встановленим програмним забезпеченням MS Excel та доступом до мережі Інтернет.

Теоретичні відомості

КРИПТОГРАФІЯ НА ЕЛІПТИЧНИХ КРИВИХ

Криптографія на еліптичних кривих (elliptic curve cryptography, ECC) вивчає асиметричні криптосистеми, засновані на еліптичних кривих над скінченими полями. Їх безпека, як правило, базується на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої над скінченним полем. Використання еліптичних кривих у криптографії було незалежно запропоновано Нілом Кобліцом (Neal Koblitz) та Віктором Міллером (Victor Miller) у 1985 році. З 1998 року використання еліптичних кривих для вирішення криптографічних завдань було закріплено в стандартах США ANSI X9.62 і FIPS 186-2 (FIPS 186-3 з 2009 року). В Україні на рівні національного стандарту (ДСТУ 4145-2002) прийнято алгоритм цифрового підпису, що ґрунтується на еліптичних кривих.

Основною перевагою криптосистем на еліптичних кривих у порівнянні із звичайними асиметричними алгоритмами є те, шо вони забезпечують еквівалентний захист за меншої довжини ключа (табл. 8.1).

Таблиця. 8.1. Порівняння звичайних асиметричних алгоритмів та криптосистем на еліптичних кривих

Ступінь захисту (на кожен біт ключа)	*Мінімальна довжина ключа (в бітах)*	
	RSA/DSA/DH	**ECC**
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

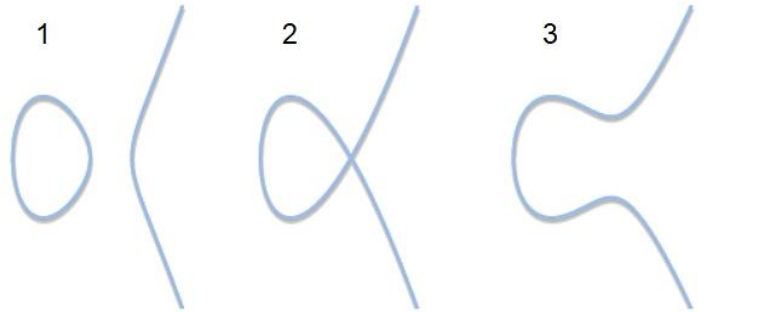
Розглянемо рівняння еліптичної кривої у спрощеному вигляді (рівняння Вейєрштрасса):

$$y^2 = x^3 + ax + b \tag{8.1}$$

Залежно від значень параметрів a і b еліптичні криві можуть приймати на площині різні форми. Так як $y = \pm\sqrt{x^3 + ax + b}$, то графік кривої симетричний відносно *Ox*.

Дискримінант рівняння: $D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$.

- $D < 0$ – три різних дійсних корені (рис. 8.1, графік 1);
- $D = 0$ – три дійсних корені, два з яких однакові (рис. 8.1, графік 2 – сингулярна крива, такі криві виключають з розгляду);
- $D > 0$ – один дійсний корінь та два комплексних (рис. 8.1, графік 3).



$y^2 = x^3 - x$ $y^2 = x^3 - 3x + 2$ $y^2 = x^3 - x + 1$

Рис. 8.1. Варіанти еліптичних кривих при $D < 0$, $D = 0$ та $D > 0$

У реальних криптосистемах використовуються еліптичні криві над скінченним полем p, що описуються рівнянням:

$$y^2 \equiv x^3 + ax + b \ (mod\ p), \tag{8.2}$$

де $(x,\ y)$ – точки еліптичної кривої,

$a,\ b$ – параметри кривої,

p – просте число ($p \neq 2, p \neq 3$).

При цьому параметри кривої a та b мають задовольняти умову:

$$4a^3 + 27b^2 \neq 0 \ (\mathrm{mod}\ p).$$

Позначимо через $E_p(a,\ b)$ множину точок еліптичної кривої. У множину точок еліптичної кривої також включається нескінченно віддалена точка O.

Точка належить еліптичній кривій, якщо пара чисел $(x,\ y)$ задовольняє рівнянню (8.2).

Кількість точок кривої називається *порядком кривої.*

Приклад 8.1:

Множина точок $E_5(2,\ 1)$ еліптичної кривої $y^2 \equiv x^3 + 2x + 1\ (mod\ 5)$, складається з 6 точок, а також точки O. Порядок кривої – 7. На рис.8.2 зображено усі точки, що задовольняють рівнянню кривої.

solve	$y^2 \equiv x^3 + 2x + 1 \pmod 5$
Solutions in the least residue system:	
$x \equiv 0, y \equiv 1 \pmod 5$	
$x \equiv 0, y \equiv 4 \pmod 5$	
$x \equiv 1, y \equiv 2 \pmod 5$	
$x \equiv 1, y \equiv 3 \pmod 5$	
$x \equiv 3, y \equiv 2 \pmod 5$	
$x \equiv 3, y \equiv 3 \pmod 5$	

Рис. 8.2. Точки, що належать еліптичній кривій $y^2 \equiv x^3 + 2x + 1\ (mod\ 5)$

ОПЕРАЦІЇ НАД ТОЧКАМИ ЕЛІПТИЧНИХ КРИВИХ

Оберненою точкою до $P(x,\ y)$ називають точку еліптичної кривої, що симетрична відносно осі Ox та позначають $-P(x,\ -y)$. Варто зауважити, що $-P$ має належати $E_p(a,\ b)$.

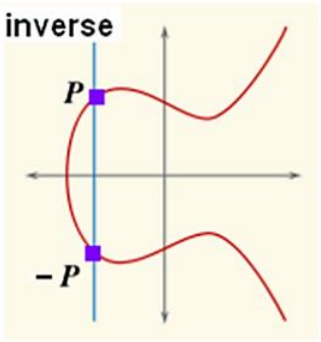


Рис. 8.3. Обернена точка еліптичної кривої

Приклад 8.2:

Якщо $P(3,\ 2)$ – точка еліптичної кривої $y^2 \equiv x^3 + 2x + 1\ (mod\ 5)$, то точка $-P\ (3,\ -2)$. Проте $-2\ mod\ 5 = 3$, тому $-P\ (3,\ 3)$.

Додавання точок. Візьмемо дві різні точки $P(x_1,\ y_1)$ та $Q(x_2,\ y_2)$, які належать E_p і проведемо через них пряму. Ця пряма обов'язково перетне криву в третій точці R. Проведемо через точку R вертикальну пряму до перетину з

кривою у точці $-R = P + Q$. Отже, сумою двох точок P та Q буде точка, обернена до третьої точки перетину еліптичної кривої і прямої, що проходить через задані точки.

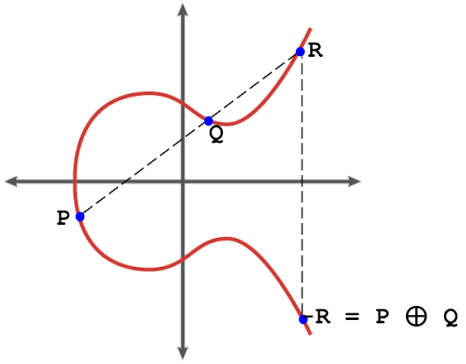


Рис. 8.4. Додавання точок еліптичної кривої

Подвоєння точки. Якщо дві точки $P(x_1, y_1)$ та $Q(x_2, y_2)$ співпадають, то $P + Q = P + P$, що рівнозначно подвоєнню точки $2P = -R$. При $P = Q$ січна перетворюється на дотичну, тому точка $2P$ є оберненою до точки R.

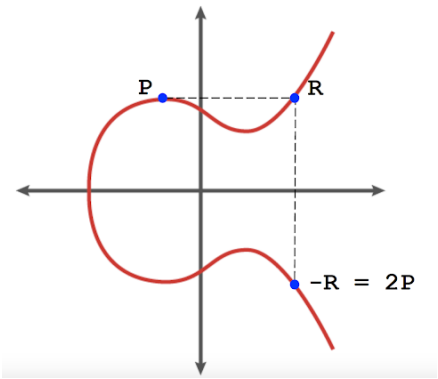


Рис. 8.5. Подвоєння точки еліптичної кривої

Координати $-R(x_3, y_3)$ визначаються за формулами, де λ – кутовий коефіцієнт січної, що проведена через точки $P(x_1, y_1)$ та $Q(x_2, y_2)$.

Додавання точок (якщо $P \neq Q$)	***Подвоєння точки (якщо $P = Q$)***
$x_3 = \lambda^2 - x_1 - x_2 (mod\ p);$	$x_3 = \lambda^2 - 2x_1\ (mod\ p);$
$y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p);$	$y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p);$
$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p).$	$\lambda = \frac{3x_1^2 + a}{2y_1} (mod\ p).$

Приклад 8.3:

Рівняння еліптичної кривої має вигляд:

$$y^2 \equiv x^3 + x + 1\ (mod\ 23), \tag{8.3}$$

Потрібно перевірити чи точки $P(3,\ 10)$ та $Q(9,\ 7)$ належать кривій та знайти $P + Q$.

Підставимо значення $P(3,\ 10)$ та $Q(9,\ 7)$ у рівняння еліптичної кривої (8.3) та переконаємося, що точки належать кривій:

$$10^2 \equiv 3^3 + 3 + 1\ (mod\ 23) \rightarrow 100\ mod\ 23 \equiv 31(mod\ 23);$$

$$7^2 \equiv 9^3 + 9 + 1\ (mod\ 23) \rightarrow 49\ mod\ 23 \equiv 739(mod\ 23).$$

Виконаємо додавання точок $P(3,\ 10)$ та $Q(9,\ 7)$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mod\ p) = \frac{7-10}{9-3}(mod\ 23) = -\frac{3}{6}(mod\ 23) = -\frac{1}{2}(mod\ 23) =$$

$$= \frac{22}{2}(mod\ 23) = 11.$$

Знаходимо:

$$x_3 = \lambda^2 - x_1 - x_2(mod\ p) = 121 - 3 - 9(mod\ 23) = 109(mod\ 23) = 17$$

$$y_3 = \lambda(x_1 - x_3) - y_1(mod\ p) = 11(3 - 17) - 10(mod\ 23) = -164(mod\ 23) =$$

$$= 20.$$

Отже $P + Q = (3,\ 10) + (9,\ 7) = (17,\ 20)$.

Приклад 8.4:

Додати точки $P(12,\ 19)$ та $Q(5,\ 4)$ еліптичної кривої 2.1.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mod\ p) = \frac{4-19}{5-12}(mod\ 23) = \frac{-15}{-7}(mod\ 23) = \frac{15}{7}(mod\ 23).$$

Якщо записати $15 \cdot \frac{1}{7}(mod\ 23) \rightarrow 5 \cdot 7^{-1}(mod\ 23)$, то потрібно знайти обернений елемент, розв'язавши рівняння:

$7 \cdot Z \equiv 1\ (mod\ 23) \rightarrow Z = 10$ (*за розширеним алгоритмом Евкліда*).

$$\lambda = 15 \cdot 10\ (mod\ 23) = 12.$$

$$x_3 = \lambda^2 - x_1 - x_2(mod\ p) = 144 - 12 - 5(mod\ 23) = 127(mod\ 23) = 12.$$

$$y_3 = \lambda(x_1 - x_3) - y_1(mod\ p) = 12(12 - 12) - 19(mod\ 23) = 4(mod\ 23) = 4.$$

Отже $P + Q = (12,\ 19) + (5,\ 4) = (12,\ 4)$.

Приклад 8.5:

Дано точку $P(5,\ 4)$ еліптичної кривої 2.1. Знайти $2P$ та $3P$.

$$\lambda = \frac{3x_1^2 + a}{2y_1}(mod\ p) = \frac{3 \cdot 25 + 1}{2 \cdot 4}(mod\ 23) = \frac{76}{2 \cdot 4}(mod\ 23) = \frac{19}{2}(mod\ 23).$$

Знайдемо обернений елемент $2^{-1}(mod\ 23)$, розв'язавши рівняння:

$$2 \cdot Z \equiv 1\ (mod\ 23) \rightarrow Z = 12.$$

$$\lambda = 19 \cdot 12\ (mod\ 23) = 21.$$

$$x_3 = \lambda^2 - 2x_1 (mod\ p) = 441 - 10 (mod\ 23) = 431 (mod\ 23) = 17.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p) = 21(5 - 17) - 4 (mod\ 23) = -256 (mod\ 23) =$$

$$= 20.$$

Отже $2P = (17,\ 20)$.

Далі знайдемо суму точок $P + 2P = (5,\ 4) + (17,\ 20)$.

$$\lambda = \frac{20-4}{17-5} (mod\ 23) = \frac{16}{12} (mod\ 23) = \frac{4}{3} (mod\ 23).$$

Знайдемо обернений елемент, розв'язавши рівняння:

$$3 \cdot Z \equiv 1\ (mod\ 23) \rightarrow Z = 8.$$

$$\lambda = 4 \cdot 8\ (mod\ 23) = 9.$$

$$x_3 = 9^2 - 5 - 17 (mod\ 23) = 81 - 22 (mod\ 23) = 13.$$

$$y_3 = 9(5 - 13) - 4 (mod\ 23) = 9 \cdot (-8) - 4 (mod\ 23) = -76 (mod\ 23) = 16.$$

Отже $3P = (13,\ 16)$.

Множина точок еліптичної кривої $E_p(a,\ b)$ разом із введеною точкою на нескінченності O утворює комутативну групу щодо операції додавання точок. Для цього виконуються усі необхідні властивості:

1) Якщо P і $Q \in E_p(a,\ b)$, то $P + Q \in\ E_p(a,\ b)$ – замкнутість;

2) $P + Q = Q + P$ – комутативність;

3) $(P + Q) + R = P + (Q + R)$ – асоціативність;

4) $P + (-P) = O$ – обернений елемент;

5) $P + O = O + P = P$ – нейтральний елемент.

Скалярне множення точки на число. Із попередніх операцій додавання точок та подвоєння точки випливає операція скалярного множення точки на число:

$$2P = P + P$$
$$3P = P + P + P$$
$$\dots$$
$$mP = \underbrace{P + P + P + \cdots + P}_{m \text{ разів}}$$

Скалярне множення є аналогом піднесення до степеню в звичайних асиметричних шифрах. Прямою задачею є обчислення $mP\ = Q$. Зворотна задача

полягає у тому, що знаючи точки P та Q, знайти m важко (дискретне логарифмування у групі точок еліптичної кривої).

Точка $G \in E_p(a,b)$ називається **базовою точкою** підгрупи точок еліптичної кривої $E_p(a,b)$, якщо будь-яка точка P цієї підгрупи може бути подана у вигляді $P = mG$, де $m = 1,\ 2, \ldots n$, де n – порядок підгрупи.

Для базової точки G має місце рівність $nG = O$.

Приклад 8.6:

Точка $G = (0,\ 1)$ є базовою точкою для групи точок еліптичної кривої $y^2 \equiv x^3 + x + 1\ (mod\ 5)$. Вона генерує усі інші точки підгрупи:

$$\boldsymbol{G} = (0,\ 1) \rightarrow \boldsymbol{2G} = (4,\ 2) \rightarrow \boldsymbol{3G} = (2,\ 1) \rightarrow \boldsymbol{4G} = (3,\ 4) \rightarrow \boldsymbol{5G} = (3,\ 1) \rightarrow \boldsymbol{6G} = (2,\ 4) \rightarrow \boldsymbol{7G} = (4,\ 3) \rightarrow \boldsymbol{8G} = (0,\ 4) \rightarrow \boldsymbol{9G} = O.$$

АЛГОРИТМ ДІФФІ-ХЕЛМАНА НА ЕЛІПТИЧНИХ КРИВИХ

1. Абоненти А і В спільно обирають просте число p та параметри еліптичної кривої a та b.
2. У групі точок еліптичної кривої $E_p(a,\ b)$ також обирається спільна базова точка $G = (x, y)$, що має дуже великий порядок n.
3. Абонент *A* обирає $x < n$, обчислює $X_A = xG$ та відправляє його *B*.
4. Абонент *B* обирає $y < n$, обчислює $Y_B = yG$ та відправляє його *A*.
5. Абонент *A* обчислює закритий ключ за формулою $K_A = xY_B$.
6. Користувач *B* обчислює закритий ключ за формулою $K_B = yX_A$.

Приклад 8.7:

1. Нехай абоненти обрали параметри еліптичної кривої $p = 23$, $a = -2$, $b = 15$, тобто $y^2 \equiv\ x^3 - 2x + 15\ (mod\ 23)$.
2. Нехай $G = (4,\ 5)$ – базова очка.
3. Абонент *A* обирає $x = 3$ та обчислює $X_A = 3G = 2G + G = (13,\ 22)$.
4. Абонент *B* обирає $y = 7$ обчислимо $Y_B = 7G = 2G + 4G + G = (17,\ 8)$.
5. Абонент *A* обчислює закритий ключ $K_A = 3Y_B = 2Y_B + Y_B = (15,\ 5)$.
6. Абонент *B* обчислює закритий ключ $K_B = 7X_A = 2X_A + 4X_A + X_A = (15,\ 5)$.

Секретний ключ, обчислений обома сторонами – $(15,\ 5)$.

Завдання до лабораторної роботи

Знайти спільний секретний ключ K_A та K_B, *що формується обома абонентами за алгоритмом обміну ключами Діффі-Хеллмана на еліптичних кривих.*

Кроки алгоритму з усіма повними обчисленнями описати у звіті.

Значення параметрів еліптичної кривої a і b, p та базова точка G визначається згідно варіанту. Окрім спільного ключа, необхідно обчислити значення відкритих параметрів X_A та Y_B для кожного абоненту.

Варіант №	***p***	***a***	***b***	***G***	Абонент А ***x***	Абонент В ***y***
1.	29	2	1	(5, 7)	4	6
2.	19	1	5	(1, 8)	6	7
3.	23	-2	4	(3, 5)	7	4
4.	29	-3	7	(1, 11)	3	7
5.	23	2	5	(8, 2)	6	4
6.	19	3	5	(4, 10)	5	6
7.	29	-1	2	(10, 8)	7	4
8.	23	5	3	(7, 17)	4	7
9.	31	1	-4	(7, 6)	6	5
10.	23	5	-3	(3, 4)	7	4
11.	29	-2	3	(11, 6)	4	6
12.	19	4	1	(0, 18)	5	8
13.	31	2	5	(5, 4)	3	6
14.	23	-1	3	(13, 5)	4	7
15.	19	-2	5	(0, 9)	3	7

Контрольні запитання:

1. Який загальний вигляд має крива, що використовується в криптографічних системах, заснованих на еліптичних кривих?
2. Дайте визначення порядку групи точок еліптичної кривої.
3. Дайте визначення порядку точки еліптичної кривої.
4. Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих?
5. Які основні операції виконуються над точками еліптичних кривих при їх використанні в криптографічних системах?
6. Опишіть алгоритми додавання та подвоєння точки.
7. Опишіть алгоритм скалярного множення точки на число.
8. Опишіть алгоритм Діффі-Хелмана на еліптичних кривих.