# ЛАБОРАТОРНА РОБОТА № 8 КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ЕЛІПТИЧНИХ КРИВИХ (тільки пункт 4.2.2)

**Мета роботи:** ознайомитися з алгоритмами криптографічних перетворень на еліптичних кривих.

**Використовуване програмне забезпечення:** середа розробки GNU Octave.

## Теоретичні відомості

На даний час на території України діють:

а) закон України ”Про електронний цифровий підпис” – 2003, що визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису;

б) закон України ”Про електронні документи та електронний документообіг” – 2003, що встановлює основні організаційно-правові положення електронного документообігу та використання електронних документів.

Сучасні світові стандарти цифрового підпису ґрунтуються на арифметиці еліптичних кривих. Наприклад:

ДСТУ 4145-2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. Київ:- Держстандарт України, 2003.

ГОСТ Р 34.10-2001. Государственный стандарт российской федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи. М.: Госстандарт России, 2001.

ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

Еліптична крива - це математичний об'єкт, що може бути визначений над будь-яким полем, зокрема над полем дійсних чисел або над скінченним полем Галуа.

У загальному випадку еліптична крива над полем *К* має вигляд

*E*: *y*2 + *axy* + *by* = *x*3 +*cx*2 + *dx* + *e* ,

де *a*, *b*, *c*, *d*, *e K* .

На рис.4.1 поданий приклад еліптичної кривої, визначеної рівнянням

над полем дійсних чисел *R*.

*y*2 = *x*3 + *x* + 1 ,



Рисунок 4.1 - Приклад еліптичної кривої *y*2 = *x*3 + *x* + 1 над *R.*

* + 1. **Еліптичні криві над простим полем Галуа GF (p)**

У криптографії застосовуються еліптичні криві, визначені над скінченнимим полями Галуа *GF* (*q*). У цьому випадку вони являють собою множину точок *E*(*GF*(*q*)), координати яких задовольняють рівнянню кривої.

Приклад. Дано еліптичну криву *y2* = *x3* + *x* + 1(mod 5) над полем *GF*(5). Цьому рівнянню задовольняють 8 скінченних точок із координатами з *GF*(5). На рис.4.2 подано приклад цієї кривої.



Рисунок 4.2 - Приклад еліптичної кривої *y*2 = *x*3 + *x* + 1 mod 5 над полем *GF*(5)

Розглянемо еліптичні криві над простим полем *GF* (*p*):

*y*2 = *x*3 + *ax* + *b* (mod p), (4.1) де *р* - просте число - модуль перетворень; параметри кривої

*a*, *b GF* (*p*) - невід ємні і задовольняють умові гладкості кривої

4*a*3

27*b*2

0(mod *p*) , змінні *x*, *y GF* (p).

Крім точок (*x*, *y*), що задовольняють рівнянню (4.1), у множину точок еліптичної кривої також включається нескінченно віддалена точка **O** .

Наприклад, при *p* = 2 точками еліптичної кривої

*y2* = *x3* +*x* +1 (mod 2) є три точки - (0,1), (1,1) і **O** .

Позначимо через *Ep*(*a*,*b*) множину точок еліптичної кривої виду (4.1).

На множині *E*p(*a*,*b*) введемо операцію додавання + за правилом: нехай *P*1=(*x*1, *y*1) і *P*2=(*x*2, *y*2) – точки еліптичної кривої, тоді

координати суми точок *P*3 = *P*1+*P*2= (*x*3, *y*3) визначаються за формулами

*x*3 = ( 2 – *x*1 – *x*2) mod *p*

*y*3 = ( (*x*1 – *x*3) – *y*1) mod *p*

*y*2 *y*1

*x*2 *x*1

Якщо *P*1 2, то

*P*

(mod *p*) .

3*x*2 *a*

Якщо *P*1=*P*2, то Вважаємо, що P + **O** = **O** + P .

 1

2 *y*1

mod *p* .

Твердження. Множина точок еліптичної кривої *Ep*(*a*,*b*) з операцією додавання + утворює адитивну абелеву групу з нейтральним (нульовим) елементом **O**, тобто виконуються умови групи:

а) якщо *P* і *Q E*p(*a*,*b*) , то *P* + *Q E*p(*a*,*b*);

б) для будь-яких трьох точок кривої *P*, *Q*, *S E*p(*a*,*b*) *P* + (*Q* + *S*) = (*P* + *Q*) + *S* ;

в) для будь-якої точки *P* = (*x*, *y*) *E*p(*a*,*b*) існує обернена точка –*P*, така, що *P* + (–*P*) = **O** ; точка (–*P)* має координати (*x*, –*y*) .

Приклад. Знайдемо точки еліптичної кривої *y*2 = *x*3 + *x* + 1(mod 5). Можливі значення змінної *x* {0, 1, 2, 3, 4}. Задаючи значення *x*, знайдемо *y* :

*x* = 0 *y*2 = 1 *y* = 1, *y* = – 1 або *y* = 4

*x* = 1 *y*2 = 3 розв'язків немає

*x* = 2 *y*2 = 11 = 1 *y* = 1, *y* = 4

*x* = 3 *y*2 = 31 = 1 *y* = 1, *y* = 4

*x* = 4 *y*2 = 69 = 4 *y* = 2, *y* = – 2 або *y* = 3

Таким чином, одержимо точки (0,1), (0,4), (2,1), (2,4), (3, 1), (3,4), (4,2), (4,3) і добавляємо точку **O**. Еліптична крива *E5*(1,1) містить 9 точок.

Визначення. Порядком групи точок еліптичної кривої *Ep*(*a*,*b*) називається число елементів цієї групи. Позначення - # *Ep*(*a*,*b*) .

Група точок еліптичної кривої *E5*(1,1) має порядок рівний 9.

* + 1. **Алгоритм обчислення точок еліптичної кривої**

Нехай задана еліптична крива *y*2 = *x*3 + *ax* + *b* (mod p). Для кожного значення *x*, 0 *x* p – 1:

а) обчислюємо A = *x*3 + *ax* + *b* (mod p);

б) вирішуємо порівняння *y*2=A (mod p). Якщо порівняння має розв'язок, то є два значення *y* (крім випадку *y* = 0) – *y*1, *y*2: *y* 2 =A (mod p). У цьому випадку точки (*x*, *y* ) і (*x*, *y* ) належать

i 1 2

еліптичній кривій.

* + 1. **Приклад додавання точок еліптичної кривої y2 = x3 + x + 1(mod 5).**

Нехай *P*1 = (0,1), *P*2 = (4,2), *x*1 = 0, *y*1 = 1, *x*2 = 4, *y*2 = 2 . а) *P*1 + *P*2 = ( *x*3, *y*3 ) .

*y*2 *y*1

*x*2 *x*1

Так як *P*1

*P*2 , то

(mod *p*) ,

= (2-1)/(4-0) = ¼ mod 5 = 4.

*x*3 = ( 2 – *x*1 – *x*2 ) mod *p* = 16 – 0 – 4 = 12 mod 5 = 2.

*y*3 = ( ( *x*1 – *x*3 ) – *y*1 ) mod *p* = 4 (0 – 2) – 1 = – 9 mod 5 = 1.

Таким чином, (0,1) + (4,2) = (2,1).

b) 2 *P*1 = ( *x*3, *y*3 )

3*x*2 *a*

Так як *P*1 = *P*2 , то

 1

2 *y*1

mod *p* ,

= (3 0 + 1)/(2 1) = 1/2 mod 5 = 3.

*x*3 = ( 2 – *x*1 – *x*2 ) mod *p* = 9 – 0 – 0 = 9 mod 5 = 4.

*y*3 = ( ( *x*1 – *x*3 ) – *y*1 ) mod *p* = 3 (0 – 4) – 1 = – 13 mod 5 = 2.

Таким чином, 2 (0,1) = (4,2).

1. Аналогічно можна обчислити

3 *P*1 = 2 *P*1 + *P*1 = (4,2) + (0,1) = (2,1)

4 *P*1 = 3 *P*1 + *P*1 = (2,1) + (0,1) = (3,4)

5 *P*1 = 4 *P*1 + *P*1 = (3,4) + (0,1) = (3,1)

6 *P*1 = 5 *P*1 + *P*1 = (3,1) + (0,1) = (2,4)

7 *P*1 = 6 *P*1 + *P*1 = (2,4) + (0,1) = (4,3)

8 *P*1 = 7 *P*1 + *P*1 = (4,3) + (0,1) = (0,4)

9 *P*1 = 8 *P*1 + *P*1 = (0,4) + (0,1) = **O**

Визначення. Точка *P Ep*(*a*,*b*) називається базовою точкою підгрупи точок еліптичної кривої *Ep*(*a*,*b*), якщо будь-яка точка *Q* цієї підгрупи може бути подана у вигляді *Q* = k *P*, де k=1,2,…,n, де n - порядок підгрупи.

Для базової точки *P* має місце рівність n∙*P* = **O** .

Приклад. Точка *P* = (0,1) є базовою для групи точок еліптичної кривої *y*2 = *x*3 + *x* + 1 (mod 5) .

Твердження (теорема Хасе). Значення порядку групи точок еліптичної кривої над полем Галуа GF(*q*) має верхню і нижню межі:

*q* # *Eq(a,b) q*

1 2 *q*

1 2 *q*

Приклад. Нехай *Q* = (2,4) - точка еліптичної кривої

*y2 = x3 + x + 1 (mod 5).*

Тоді 2∙*Q* = (2,1), 3∙*Q* = **O**.

Точка *Q* = (2,4) породжує циклічну підгрупу порядку 3: (2,4), (2,1), **O**.

Визначення. Порядком точки *Q* еліптичної кривої називається найменше число k, таке що k *Q* = **O** .

Точка *Q* = (2,4), що належить групі точок еліптичної кривої

*y*2=*x*3 + *x* + 1 mod 5, має порядок, рівний 3.

* + 1. **Алгоритм обчислення порядку точки еліптичної кривої**

Нехай задана еліптична крива *y*2 = *x*3 + *ax* + *b* (mod p) над полем GF(p), і точка *P* належить заданій кривій. Знайдемо порядок точки *P* .

Для цього необхідно вирішити порівняння

*x P* = **O**

(адитивний аналог задачі дискретного логарифмування).

Застосуємо алгоритм великих-малих кроків.

Нехай *n* - максимальна оцінка порядку групи точок еліптичної кривої, отримана по теоремі Хасе, *P* - точка еліптичної кривої.

Обчислимо *m* := , де *a* - округлення з надлишком.

*n*

* 1. Будуємо таблицю пар ( j , j *P* ) для j = 1, 2 , *m*.
	2. Обчисляємо := - *m P* . 3. := **O** .
1. Цикл по *i* від 0 до *m* - 1
	1. перевіряємо, чи є другою компонентою у таблиці п.1

* 1. якщо = j *P* , то вважаємо *x* = *m i* + j 4.3 := + .

Приклад. Візьмемо еліптичну криву *y*2 = *x*3 + *x* + 1 над простим полем GF(*p*), *p* = 5. По теоремі Хасе максимальна оцінка порядку

1 2 *p*

5

групи точок кривої дорівнює *n*= *p*

*m*= 4.

= 5+1+2

10. Звідси

За допомогою алгоритму великих-малих кроків знайдемо порядок точки *P* = (0,1).

Побудуємо таблицю

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| j | 1 | 2 | 3 | 4 |
| j *P* | (0,1) | (4,2) | (2,1) | (3,4) |

Знайдемо t := – *m P* = – 4 (0,1) = – (3,4) = (3, – 4) = (3,1).

:= **O**.

*i* = 0 := + t = **O** + (3,1) = (3,1).

*i* = 1 = + t = (3,1) + (3,1) = (0,1).

*i* = 2 j = 1 *x* = *m i* + j = 4 2 + 1 = 9. Порядок точки *P* = (0,1) дорівнює 9.

На рис. 4.3 показаний приклад еліптичної кривої над полем *GF*(23)

*y* 2 *x*3

*x* 1(mod23) *,*

з параметрами *a* = 1, *b* = 1, *p* = 23, 4*a*3+27*b*2=8 0 (mod 23). Точки

кривої визначені як усі рішення рівняння *y* 2

*x*3 *x*

1(mod23) ,

включаючи нескінченну точку. Отже, порядок групи точок дорівнює 27+1=28.

Наведемо протокол цифрового підпису на еліптичних кривих

ГОСТ Р 34.10-2001.

Таблиця 4.1 – Протокол цифрового підпису ГОСТ Р 34.10-2001



|  |  |
| --- | --- |
| **Формування цифрового підпису** | **Перевірка цифрового підпису** |
| **Вхід**: секретний ключ *d* , відкритий ключ *Q d P* , загальносистемні параметри.**Вихід**: ЦП *r*, *s* дляповідомлення *M* . | **Вхід**: відкритий ключ *Q* , загальносистемні параметры, ЦП *r* ', *s* ' , для повідомлення *M* ' .**Вихід:** Підпис дійсний чи ні. |
| 1. *e h*(*M* ) mod*n* ;
2. Обираємо

*k* 1,...,*n* 1 **;**1. *k P* (*x*, *y*) ;
2. *r* (*x*, *y*) mod*n* ;
3. *s* (*rd ke*) mod*n* .
 | 1. *e h*(*M* ) mod*n* ;
2. *w e* 1 mod*n* ;
3. *z*1 *sw*mod *n* ;
4. *z*2 *rw*mod *n* ;
5. (*x*, *y*) *z*1 *P z*2 *Q* ;

**6.** *v* (*x*, *y*);?**7.** *r* ' *v* |

* + 1. **Алгоритм скалярного множення на еліптичній кривій**

Для множення точки еліптичної кривої на велике ціле число застосовується наступний алгоритм:

Вихідні дані: число *d* 0, точка *P*, еліптична крива E = <*a*,*b*,*p*>. Результат: точка *Q* = *d P*.

* + - 1. Якщо *d*=1, то *Q*:=*P*; закінчити роботу алгоритму.
			2. *k*:=*ld*–2; *Q*:=*P,* де *ld* – довжина множника *d* в бітах;
			3. Для *i*, що приймає значення від *k* до 0, виконати шаги 4-5. 4. *Q* := *Q*+*Q*.
1. Якщо *i*-й біт *d* дорівнює 1, то *Q* := *Q+P*.
2. Закінчити роботу алгоритму.

## Завдання на лабораторну роботу



* + 1. Дано еліптичну криву

*y* 2 *x*3

*ax b* (mod13) .

Параметри *a*, *b* відповідають номеру варіанта (табл. 4.2). Необхідно:

* знайти всі точки, що належать заданій кривій і порядок кривої. Використовувати середу розробки GNU Octave;
* знайти базову точку;
* представити кожну точку як кратну базовій (знайти показник кратності).

Таблиця 4.2 – Варіанти завдань

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. a=1,b=1 | 11. a=2,b=1 | 21. a=2,b=11 | 31. a=3,b=11 | 41. a=4,b=10 |
| 2. a=1,b=2 | 12. a=2,b=2 | 22. a=2,b=12 | 32. a=3,b=12 | 42. a=4,b=12 |
| 3. a=1,b=4 | 13. a=2,b=3 | 23. a=3,b=1 | 33. a=4,b=1 | 43. a=5,b=1 |
| 4. a=1,b=5 | 14. a=2,b=4 | 24. a=3,b=2 | 34. a=4,b=3 | 44. a=5,b=2 |
| 5. a=1,b=6 | 15. a=2,b=5 | 25. a=3,b=4 | 35. a=4,b=4 | 45. a=5,b=3 |
| 6. a=1,b=7 | 16. a=2,b=6 | 26. a=3,b=5 | 36. a=4,b=5 | 46. a=5,b=4 |
| 7. a=1,b=8 | 17. a=2,b=7 | 27. a=3,b=6 | 37. a=4,b=6 | 47. a=5,b=5 |
| 8. a=1,b=9 | 18. a=2,b=8 | 28. a=3,b=7 | 38. a=4,b=7 | 48. a=5,b=6 |
| 9. a=1,b=11 | 19. a=2,b=9 | 29. a=3,b=8 | 39. a=4,b=8 | 49. a=5,b=7 |
| 10. a=1,b=12 | 20. a=2,b=11 | 30. a=3,b=9 | 40. a=4,b=9 | 50. a=5,b=8 |

* + 1. Реалізувати в середы розробки GNU Octave алгоритм цифрового підпису ГОСТ Р 34.10. Для тестування використати наступні параметри (в шестнадцатерічній формі):

Модуль перетворень

m=8000000000000000000000000000000000000000000000000000000000000431;

Еліптична крива

a=7;

*y* 2 *x*3

*ax b* ( mod *m*)

b=5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514COCE9DAE23B7E;

Базова точка P(x,y);

Px=2; Py=8E2A8A0E65147D4BD6316030E16D19C85C97F0A9CA267122B96ABBCEA7E8FC8;

Порядок базової точки:

n= 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3;

Секретний ключ

d=7A929ADE789BB9BE10ED359DD39A72C11B60961F49397EEE1D19CE9891EC3B28;

Результат множення (відкритий ключ) точка Q(Qx,Qy)

Qx=7F2B49E270DB6D90D8595BEC458B50C58585BA1D4E9B788F6689DBD8E56FD80B; Qy=26F1B489D6701DD185C8413A977B3СВВAF64D1C593D26627DFFB101A87FF77DA.

## Зміст звіту

* + 1. Титульний лист, тема і мета роботи.
		2. Відповіді на контрольні питання.
		3. Тексти програм (тільки пункту 4.2.2).
		4. Результати обчислень (тільки пункту 4.2.2).
		5. Висновки.

## Контрольні питання

* + 1. Дати визначення еліптичної кривої.
		2. Як визначити точку, обернену даній?
		3. Які параметри еліптичної кривої необхідно знати для її застосування?
		4. Дати визначення порядку групи точок еліптичної кривої?
		5. Дати визначення порядку точки еліптичної кривої?
		6. Як визначити базову точку?
		7. У яких криптографічних алгоритмах застосовуються еліптичні криві?