**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Національний університет «Запорізька політехніка»

# МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт з дисципліни
“Протоколи цифрового підпису”
для бакалаврів спеціальності
125 «Кібербезпека та захист інформації»
усіх форм навчання

2024

Методичні вказівки до лабораторних робіт з дисципліни “Протоколи цифрового підпису” для бакалаврів спеціальності 125 «Кібербезпека та захист інформації» усіх форм навчання / Укл.: Г.Л.Козіна.–Запоріжжя: НУ «Запорізька політехніка», 2024.– 32 с.

Укладач: Г.Л.Козіна, доцент, к.ф.-м.н.

Рецензент: Л.М. Карпуков, проф., д.т.н.

Відповідальний за випуск: А.В.Коротун, доц., канд. фіз.-матем. наук

Затверджено
на засіданні кафедри
інформаційної безпеки
та наноелектроніки
Протокол № 4
від 21.12.2023 р.

Рекомендовано до видання
НМК ФРЕТ
Протокол № 5
від 24.02.2024 р.

# ЗМІСТ

# ЛАБОРАТОРНА РОБОТА № 1
# ПРОТОКОЛ МУЛЬТИПІДПИСУ

**Мета роботи:** ознайомитися з протоколом мультипідпису.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

### 1.1 Завдання на лабораторну роботу

Дано загальні параметри підпису:

основне поле – скінченне поле $GF(43)$;

еліптична крива над основним полем

$$y^2 = x^3 + 6x + 5 \mod 43.$$

Базова точка еліптичної кривої $P$ має порядок $n = 37$.

Кількість підписантів в схемі мультипідпису $t = 3$.

Допоміжне просте багаторозрядне двійкове число $\delta = 19$, $|\delta| = 5$.

1. Згенерувати відкритий та секретний ключі для кожного підписанта (див. Додаток А).

2. Обчислить мультипідпис згідно з протоколом, наведеним в Додатку А.

3. Перевірить мультипідпис, отриманий в п.2, з використанням відкритих ключів підписантів (п.1).

Значення базової точки $P$ та хеш-образу $h$ візьміть із таблиці 1.1 згідно з номером варіанта N.

### 1.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Сформовані відкриті та секретні ключі.
4. Сформований мультипідпис.
5. Результат перевірки підпису.
6. Висновки по роботі.

**Таблиця 1.1 –** Варіанти завдань

| N | *P* | *h* |
|---|---|---|
| 1 | (2,38) | 15 |
| 2 | (13,42) | 4 |
| 3 | (26,8) | 12 |
| 4 | (30,40) | 10 |
| 5 | (20,16) | 8 |
| 6 | (22,32) | 1 |
| 7 | (35,2) | 14 |
| 8 | (31,21) | 6 |
| 9 | (31,22) | 9 |
| 10 | (35,41) | 4 |

| N | *P* | *h* |
|---|---|---|
| 11 | (14,34) | 5 |
| 12 | (8,7) | 12 |
| 13 | (37,21) | 7 |
| 14 | (28,25) | 11 |
| 15 | (24,16) | 13 |
| 16 | (22,11) | 13 |
| 17 | (42,16) | 7 |
| 18 | (5,26) | 10 |
| 19 | (9,33) | 3 |
| 20 | (29,12) | 7 |

| N | *P* | *h* |
|---|---|---|
| 21 | (18,21) | 3 |
| 22 | (29,31) | 1 |
| 23 | (9,10) | 9 |
| 24 | (5,17) | 7 |
| 25 | (42,37) | 14 |
| 26 | (18,22) | 9 |
| 27 | (24,27) | 11 |
| 28 | (28,18) | 3 |
| 29 | (37,22) | 5 |
| 30 | (8,36) | 8 |

### 1.3 Контрольні питання

1. Дайте визначення поняття мультипідпису.
2. Як формується колективний відкритий ключ в наведеному протоколі?
3. Опишіть процедуру формування мультипідпису.
4. Опишіть процедуру перевірки мультипідпису.
5. Чи є обмеження по кількості підписантів у схемі мультипідпису?
6. Чи обов'язкова перевірка коректності формування відкритих ключів в схемах мультипідпису при реєстрації цих ключів в центрі сертифікації?
7. У чому полягає перевірка коректності роботи протоколу цифрового підпису?

# ЛАБОРАТОРНА РОБОТА № 2
# ПРОТОКОЛ АГРЕГОВАНОГО ПІДПИСУ

**Мета роботи:** ознайомитися з протоколом агрегованого підпису.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

### 2.1 Завдання на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(43)$;
еліптична крива над основним полем

$$y^2 = x^3 + 6x + 5 \mod 43.$$

Базова точка еліптичної кривої $P = (8,36)$ має порядок $n = 37$.
Кількість підписантів в схемі агрегованого підпису $t = 3$.
Допоміжне просте багаторозрядне двійкове число $\delta = 13$.

1. Згенерувати відкритий та секретний ключі для кожного підписанта (див. Додаток Б).
2. Обчислить агрегований підпис згідно з протоколом, наведеним в Додатку Б.
3. Перевірить агрегований підпис, отриманий в п.2, з використанням відкритих ключів підписантів (п.1).

Значення хеш-образів $h_1, h_2, h_3$ візьміть із таблиці 2.1 згідно з номером варіанта N.

### 2.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Сформовані відкриті та секретні ключі.
4. Сформований агрегований підпис.
5. Результат перевірки підпису.
6. Висновки по роботі.

**Таблиця 2.1 –** Варіанти завдань

| N | $h_1, h_2, h_3$ | N | $h_1, h_2, h_3$ | N | $h_1, h_2, h_3$ | N | $h_1, h_2, h_3$ |
|---|---|---|---|---|---|---|---|
| 1 | 2, 8,15 | 9 | 20,16,3 | 17 | 28,25,22 | 25 | 9,10,29 |
| 2 | 13,5,4 | 10 | 14,34,25 | 18 | 24,16,12 | 26 | 5,17,27 |
| 3 | 26,8,21 | 11 | 8,7,12 | 19 | 18,21,3 | 27 | 42,37,30 |
| 4 | 30,18,10 | 12 | 33,21,7 | 20 | 29,31,16 | 28 | 22,32,31 |
| 5 | 35,2,14 | 13 | 22,11,13 | 21 | 29,12,7 | 29 | 11,22,35 |
| 6 | 31,21,6 | 14 | 32,16,15 | 22 | 18,22,9 | 30 | 8,36,18 |
| 7 | 31,22,9 | 15 | 5,26,17 | 23 | 24,27,11 | 31 | 15,2,30 |
| 8 | 35,15,31 | 16 | 9,33,3 | 24 | 28,18,33 | 32 | 22,6,34 |

### 2.3 Контрольні питання

1. Дайте визначення поняття агрегованого підпису.
2. Назвіть властивості агрегованого підпису.
3. Чи є обмеження по кількості підписантів у схемах агрегованого підпису?
4. Чим відрізняється агрегований підпис від мультипідпису?
5. Які параметри схеми є загальносистемними ?
6. Опишіть процедуру генерації ключів у протоколі агрегованого підпису.
7. Опишіть процедуру формування агрегованого підпису.
8. Опишіть процедуру перевірки агрегованого підпису.
9. Які параметри впливають на криптостійкість підпису?

# ЛАБОРАТОРНА РОБОТА № 3
# ПРОТОКОЛ КІЛЬЦЕВОГО ПІДПИСУ

**Мета роботи:** ознайомитися з протоколом кільцевого підпису з використанням спарювання Вейля.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

### 3.1 Завдання на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(2383)$;
еліптична крива над основним полем

$$y^2 = x^3 - 3x \mod 2383.$$

Базова точка еліптичної кривої $P = (81, 787)$ простого порядку $n = 149$.

Для обчислення спарювання Вейля обрана точка $S$, яка має вигляд $(xS, yS) = (0, 0)$, використовується функція спотворення $\phi(x, y) = (-x, y \cdot i)$: `phi:=proc(x,y) options operator, arrow;`mod`(-x, p), I*y end proc;`

Кількість підписантів в схемі кільцевого підпису $t = 3$.

1. Згенеруйте секретні та відкриті ключі для кожного підписанта (див. Додаток Г).

2. Оберіть підписанта від групи та обчисліть кільцевий цифровий підпис згідно з протоколом, наведеним в Додатку Г.

Значення хеш-образу $h$ електронного документу візьміть із таблиці 3.1 згідно з номером варіанта N.

3. Перевірте кільцевий цифровий підпис, отриманий в п.2, з використанням відкритих ключів підписантів (п.1).

Інформацію щодо обчислення спарювання Вейля візьміть із Додатку В.

4. Отримано кільцевий цифровий підпис $\langle r, S_1, S_2, S_3 \rangle$ електронного документу згідно з протоколом, наведеним в Додатку Г.

Перевірте справжність цифрового підпису, використовуючи відкриті ключі підписантів. Значення цифрового підпису $\langle r, S_1, S_2, S_3 \rangle$, числа $H$, яке відповідає хеш-образу повідомлення, та відкриті ключі підписантів $(U_1, Q_1)$, $(U_2, Q_2)$, $(U_3, Q_3)$ візьміть із таблиць 3.2-3.3 згідно з номером варіанту N.

**Таблиця 3.1 –** Варіанти для завдань 1-3

| N | *h* | N | *h* | N | *h* | N | *h* | N | *h* | N | *h* | N | *h* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 15 | 5 | 86 | 9 | 95 | 13 | 78 | 17 | 73 | 21 | 38 | 25 | 74 |
| 2 | 64 | 6 | 111 | 10 | 42 | 14 | 11 | 18 | 130 | 22 | 16 | 26 | 91 |
| 3 | 125 | 7 | 14 | 11 | 59 | 15 | 136 | 19 | 37 | 23 | 92 | 27 | 121 |
| 4 | 10 | 8 | 68 | 12 | 12 | 16 | 93 | 20 | 72 | 24 | 79 | 28 | 32 |

**Таблиця 3.2 –** Варіанти для завдання 4. Кільцевий підпис

| N, *H, r, S1, S2, S3* | N, *H, r, S1, S2, S3* |
|---|---|
| 1, 38, 123, 740, 521, 1943, 297, 1600, 2150 | 15, 45, 27, 1800, 293, 1800, 293, 379, 1315 |
| 2, 101, 77, 969, 1049, 1138, 2125, 1338, 978 | 16, 85, 70, 364, 997, 364, 1386, 1084, 1170 |
| 3, 101, 133, 767, 62, 929, 1510, 469, 1543 | 17, 103, 77, 1368, 815, 870, 2197, 191, 502 |
| 4, 138, 116, 787, 810, 134, 2080, 1444, 1936 | 18, 136, 18, 1084, 1213, 1129, 923, 1444, 447 |
| 5, 10, 12, 1165, 1938, 2247, 354, 1165, 1938 | 19, 115, 74, 787, 1573, 1979, 2155, 1368, 1568 |
| 6, 122, 53, 1506, 977, 1338, 1405, 1890, 1038 | 20, 22, 79, 1078, 2053, 1506, 977, 2182, 1690 |
| 7, 22, 51, 929, 873, 870, 186, 2157, 2234 | 21, 91, 8, 1444, 447, 870, 2197, 1460, 985 |
| 8, 20, 33, 930, 2349, 870, 186, 1078, 2053 | 22, 52, 28, 2037, 1195, 512, 57, 469, 840 |
| 9, 83, 84, 1086, 389, 763, 1942, 740, 521 | 23, 48, 81, 1751, 818, 1460, 985, 2037, 1188 |
| 10, 88, 26, 536, 1993, 1601, 227, 2247, 354 | 24, 130, 51, 2247, 2029, 1084, 1170, 740, 1862 |
| 11, 109, 59, 1602, 1246, 617, 2361, 969, 1334 | 25, 122, 99, 1506, 977, 1863, 213, 1940, 2215 |
| 12, 21, 60, 1940, 2215, 2088, 1652, 617, 22 | 26, 10, 56, 1533, 2252, 767, 62, 61, 1771 |
| 13, 131, 75, 469, 1543, 1273, 338, 2088, 1652 | 27, 107, 50, 1533, 2252, 1533, 131, 787, 810 |
| 14, 47, 38, 349, 862, 1084, 1170, 1273, 2045 | 28, 136, 94, 1084, 1213, 2002, 2340, 498, 1277 |

### 3.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Сформовані секретні та відкриті ключі.
4. Сформований кільцевий підпис.
5. Результат перевірки сформованого кільцевого підпису.
6. Результат перевірки отриманого кільцевого підпису

**Таблиця 3.3 –** Варіанти для завдання 4. Відкриті ключі

| N, $(U_1,Q_1)$, $(U_2,Q_2)$, $(U_3,Q_3)$ |
|---|
| 1, 1138, 258, 1506, 1406, 740, 1862, 1475, 64, 764, 395, 474, 1028 |
| 2, 1890, 1345, 498, 1106, 191, 1881, 498, 1106, 1890, 1038, 1890, 1038 |
| 3, 1940, 2215, 1148, 437, 349, 1521, 1258, 370, 536, 390, 349, 1521 |
| 4, 1475, 2319, 2247, 2029, 2037, 1188, 936, 636, 1129, 1460, 61, 612 |
| 5, 536, 1993, 1639, 1538, 2017, 867, 474, 1028, 1138, 2125, 787, 1573 |
| 6, 767, 62, 1639, 845, 2088, 731, 1943, 297, 1943, 2086, 763, 1942 |
| 7, 969, 1334, 929, 1510, 195, 957, 818, 1908, 1258, 370, 1396, 795 |
| 8, 936, 636, 763, 441, 1273, 2045, 818, 475, 818, 475, 1751, 818 |
| 9, 1038, 2096, 549, 2178, 1273, 2045, 2182, 1690, 936, 1747, 1600, 2150 |
| 10, 1078, 2053, 818, 475, 818, 1908, 1475, 64, 1273, 2045, 1506, 977 |
| 11, 1038, 287, 387, 289, 1078, 2053, 757, 1716, 617, 2361, 1800, 2090 |
| 12, 213, 1462, 1943, 297, 61, 1771, 1943, 297, 1902, 2169, 1863, 213 |
| 13, 1943, 297, 1600, 2150, 1086, 1994, 195, 957, 1902, 2169, 969, 1049 |
| 14, 936, 636, 14, 1046, 1906, 2100, 1148, 437, 1086, 1994, 2088, 731 |
| 15, 549, 2178, 818, 475, 61, 1771, 387, 289, 134, 303, 1126, 1547 |
| 16, 1460, 985, 191, 502, 2002, 43, 1396, 1588, 379, 1315, 1126, 1547 |
| 17, 1940, 2215, 14, 1046, 349, 862, 1129, 923, 870, 186, 1890, 1345 |
| 18, 870, 186, 349, 862, 213, 1462, 61, 612, 2247, 2029, 740, 1862 |
| 19, 1396, 795, 936, 636, 1086, 1994, 2157, 149, 757, 1716, 870, 186 |
| 20, 536, 1993, 757, 667, 931, 1400, 1475, 2319, 1800, 293, 1038, 287 |
| 21, 2247, 354, 787, 810, 936, 1747, 1460, 1398, 763, 441, 1396, 795 |
| 22, 1943, 297, 474, 1028, 1863, 213, 387, 2094, 1460, 1398, 1890, 1345 |
| 23, 1906, 2100, 536, 1993, 474, 1028, 870, 186, 213, 1462, 1086, 389 |
| 24, 1940, 168, 2157, 2234, 787, 1573, 1751, 1565, 870, 2197, 549, 205 |
| 25, 1533, 131, 2102, 373, 2247, 354, 134, 2080, 767, 2321, 498, 1106 |
| 26, 2157, 149, 818, 1908, 1129, 923, 1751, 1565, 512, 2326, 134, 303 |
| 27, 134, 303, 1165, 445, 349, 1521, 1863, 213, 549, 205, 2182, 693 |
| 28, 1600, 233, 1129, 923, 474, 1028, 1368, 1568, 763, 1942, 763, 441 |

### 3.3 Контрольні питання

1. Дайте визначення поняття кільцевого цифрового підпису.
2. Як формуються секретні та відкриті ключі в наведеному протоколі?
3. Опишіть процедуру формування кільцевого цифрового підпису.
4. Опишіть процедуру перевірки кільцевого цифрового підпису.

## ЛІТЕРАТУРА

1. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с. – http://eir.zntu.edu.ua/handle/123456789/6528.
2. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. / Горбенко Ю.І. Горбенко І.Д. – Харків : Видавництво «Форт», 2010. – 608 с.
3. Michael Braun and Anton Kargl. A Note on Signature Standards, 2007 // http://eprint.iacr.org/2007/357
4. Кузнецов Г.В. Математичні основи криптографії / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. – Дніпропетровськ: НГУ, 2006. – 391 с.
5. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.
6. ISO/IEC 15946-2. Information Technology — Security Techniques – Cryptographic Techniques Based on Elliptic Curves – Part 2: Digital — Signatures, 2002.
7. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 552-565. Springer-Verlag, 2001.
8. Jing Xu, Zhenfeng Zhang, Dengguo Feng R. A Ring Signature Scheme Using Bilinear Pairings. Conference Paper in Lecture Notes in Computer Science. – 2004:
https://www.researchgate.net/publication/221239543.
9. Василенко, О. Н. О вычислении спариваний Вейля и Тейта. Тр. по дискр. матем., 10. – М.: Физматлит, 2007.
10. Schnorr C.P. Efficient Signature Generation by Smart Cards. J. Cryptology, 4(3): 161–174, 1991.
11. Zhao Y. Aggregation of gamma-signatures and applications to bitcoin. 2018. URL:
https://eprint.iacr.org/2018/414/20180510:203542.

# Додаток А

# Мультипідпис

При формуванні електронних документів у ряді випадків виникає необхідність підписування документів декількома учасниками. Підпис, сформований колективом рівноправних учасників підписання під спільним документом, називається *мультипідписом*.

Схеми мультипідпису призначені для розв'язання задачі одночасного підписання контрактів і скорочення розміру підписів до документів, що підписуються двома й більше суб'єктами. Особливо актуальним є питання про скорочення розміру підпису у випадках, коли електронний цифровий підпис вноситься в штрих-код або іншу машиночитаєму мітку, що наноситься на матеріальний об'єкт.

В протоколі мультипідпису здійснюється обмін відкритими параметрами по мережах зв'язку, причому кожен учасник створює свою частину підпису, після чого формується єдиний підпис. Для перевірки мультипідпису формується колективний відкритий ключ, який залежить від відкритих ключів учасників підписання електронного документа.

В розглянутому протоколі використовується в якості математичної структури група точок еліптичної кривої над скінченним полем. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій. Для хешування електронного документу може бути запропоновано використання стандартів.

## Протокол мультипідпису електронного документу на еліптичній кривій над простим полем

### Загальносистемні параметри

Еліптична крива над скінченним полем $GF(p)$

$$y^2 = x^3 + ax + b \mod p,$$

де $a, b \in GF(p), b \neq 0,$ разом із приєднаною нескінченно віддаленою точкою $\mathrm{O}$; базова точка еліптичної кривої $P \neq \mathrm{O}$ простого

порядку $n$, така що $nP = \mathrm{O}$ і $kP \neq \mathrm{O}, 0 < k < n$, $|n|$ – число двійкових розрядів в $n$; $H$ – функція хешування; $\delta$ – допоміжне просте багаторозрядне двійкове число (введення допоміжного числа $\delta$ дозволяє скоротити першу частину цифрового підпису).

**Генерація ключів**

Кожний $i$-ий ($i = 1,2,...,t$) користувач має асиметричну пару ключів: особистий $d_i$ $-1 < d_i < n$ – та відкритий $Q_i = d_i P$.

**Формування цифрового підпису**

Нехай колектив користувачів, $i = 1,2,...,t$, має підписати електронний документ $M$ з хеш-образом $H(M)$. Молодші $|\delta| - 1$ розряди хеш-образу $H(M)$ формують десяткове число $h$, яке використовується при обчисленні цифрового підпису.

Кожний підписант обирає одноразовий випадковий секретний ключ $k_i$, $1 < k_i < n$, обчислює координати точки

$$R_i = k_i P$$

та надає їх для колективного використання.

Далі обчислюється сума всіх точок $R_i$, $i = 1,2,...,t$:

$$R = \sum_{i=1}^{t} R_i = (xR, yR),$$

після чого формується число

$$r = h \cdot xR \bmod \delta.$$

При $r = 0$ обираються нові випадкові секретні ключі $k_i$.

Потім кожен користувач $i$ за допомогою свого особистого ключа $d_i$ та значення $k_i$ обчислює свою частину підпису

$$s_i = k_i - d_i \cdot r \bmod n,$$

після чого генерується підпис $s$:

$$s = \sum_{i=1}^{t} s_i \bmod n.$$

Число $s$ не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Мультипідписом є пара чисел $\langle r, s \rangle$.

**Перевірка цифрового підпису**

Перевірка підпису $\langle r, s \rangle$ під електронним документом $M$ здійснюється за допомогою колективного відкритого ключа

$$Q = \sum_{i=1}^{t} Q_i ,$$

який залежить від відкритих ключів $Q_i$ учасників підписання.

Обчислюється точка $\tilde{R}$ еліптичної кривої

$$\tilde{R} = sP + rQ = (x\tilde{R}, y\tilde{R})$$

після чого обчислюються хеш-образ документу $H(M)$, відповідне десяткове число $h$ та формується число $\tilde{r} = h \cdot x\tilde{R} \bmod \delta$.

Якщо $\tilde{r} = r$, мультипідпис електронного документу $M$ признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки мультипідпису:

$$\tilde{R} = sP + rQ = \left( \sum_{i=1}^{t} s_i \right) P + r \left( \sum_{i=1}^{t} Q_i \right) = \left( \sum_{i=1}^{t} k_i - d_i r \right) P + r \left( \sum_{i=1}^{t} d_i P \right) =$$

$$= \left( \sum_{i=1}^{t} k_i \right) P = \sum_{i=1}^{t} R_i = R.$$

Оскільки $\tilde{R} = R$, то і $\tilde{r} = r$.

Приклад.

Оберемо загальні параметри: основне поле – скінченне поле $GF(17)$; еліптична крива над основним полем $y^2 = x^3 + 2x + 6 \mod 17$.

Базова точка еліптичної кривої $P = (2,1)$ має порядок $n = 11$.

Допоміжне просте багаторозрядне двійкове число $\delta = 7$, $|\delta| = 3$

.

Нехай число користувачів $t = 2$.

Відповідні особисті ключі є $d_1 = 8$, $d_2 = 5$.

Тоді відкриті ключі $Q_1 = (6,8)$, $Q_2 = (1,3)$.

Нехай хеш-образ електронного документу $M$ дорівнює $h = 2$.

Кожний підписант обирає одноразовий випадковий секретний ключ $k_i$: $k_1 = 3$, $k_2 = 4$, та обчислює координати точки $R_i$: $R_1 = (6,9)$, $R_2 = (13,11)$.

Далі обчислюється $R$ – сума всіх точок $R_i$: $R = (13,6)$, після чого формується число $r$: $r = 2 \cdot 13 \bmod 7 = 5$, $r = 5$.

Потім кожний користувач $i$ за допомогою свого особистого ключа $d_i$ та значення $k_i$ обчислює свою частину підпису: $s_1 = 3 - 8 \cdot 5 \bmod 11 = 7$, $s_2 = 4 - 5 \cdot 5 \bmod 11 = 1$, $s_1 = 7$, $s_2 = 1$, після чого генерується єдиний підпис $s$: $s = 8$.

Мультипідписом є пара чисел $\langle r, s \rangle = \langle 5,8 \rangle$.

Перевірка підпису $\langle r, s \rangle = \langle 5,8 \rangle$ під електронним документом $M$ здійснюється за допомогою колективного відкритого ключа $Q$, який залежить від відкритих ключів $Q_i$ учасників підписання: $Q = (11,4)$.

Обчислюється точка $\tilde{R}$ еліптичної кривої: $sP = (6,8)$, $rQ = (2,16)$, $\tilde{R} = (13,6)$. Далі обчислюються хеш-образ документу $H(M)$, відповідне десяткове число $h = 2$ та формується число $\tilde{r} = 2 \cdot 13 \bmod 7 = 5$, $\tilde{r} = 5$.

Оскільки $\tilde{r} = r$, мультипідпис електронного документу $M$ признається справжнім.

# Додаток Б
# Агрегований підпис

Якщо учасники підписання не є рівноправними, може виникнути необхідність підписання різних документів групою осіб, кожна із котрих має право підписувати тільки свій документ. Наприклад, директор, бухгалтер, завідувач відділу кадрів, технолог підписують кожний свій електронний документ з використанням свого особистого ключа. С метою зменшення довжини підпису пропонується формування єдиного, *агрегованого*, підпису різних документів на базі елементів особистих підписів. Перевірка такого агрегованого підпису потребує знання відкритих ключів кожного із учасників підписання і відповідних кожному електронних документів.

Схеми агрегованого підпису мають призначення, аналогічне призначенню мультипідписів, але надають розширені можливості: одночасне підписання пакета контрактів і підписання різних документів різними підмножинами користувачів, що брали участь у формуванні єдиного пакета документів.

В розглянутому протоколі використовується в якості математичної структури група точок еліптичної кривої над скінченним полем. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій. Для хешування електронного документу може бути запропоновано використання стандартів.

## Протокол агрегованого цифрового підпису різних документів на еліптичній кривій над простим полем

### Загальносистемні параметри

Еліптична крива над скінченним полем $GF(p)$

$$y^2 = x^3 + ax + b \mod p,$$

де $a, b \in GF(p), b \neq 0,$ разом із приєднаною нескінченно віддаленою точкою $\mathrm{O}$; базова точка еліптичної кривої $P \neq \mathrm{O}$ простого порядку $n,$ така що $nP = \mathrm{O}$ і $kP \neq \mathrm{O}, 0 < k < n$, $|n|$ – число двійкових розрядів в $n$; $H$ – функція хешування; $\delta$ – допоміжне просте багаторозрядне

двійкове число (введення допоміжного числа $\delta$ дозволяє скоротити першу частину цифрового підпису).

**Генерація ключів**

Кожний $i$-ий ($i = 1,2,...,t$) користувач має асиметричну пару ключів: особистий $d_i$ $-1 < d_i < n$ – та відкритий $Q_i = d_i P$.

**Формування цифрового підпису**

Нехай колектив із $t$ користувачів має створити агрегований підпис під набором електронних документів $\{M_1, M_2, ..., M_t\}$, причому кожен користувач $i$, $i = 1,2,...,t$, має підписати свій електронний документ $M_i$ з хеш-образом $H(M_i)$. Молодші $|n|-1$ розряди хеш-образу $H(M_i)$ формують десяткове число $h_i$, яке використовується при обчисленні цифрового підпису.

Кожний підписант обирає одноразовий випадковий секретний ключ $k_i$, $1 < k_i < n$, обчислює координати точки

$$R_i = k_i P$$

та надає їх для подальшого використання.

Далі обчислюється сума всіх точок $R_i$, $i = 1,2,...,t$:

$$R = \sum_{i=1}^{t} R_i = (xR, yR),$$

після чого формується число $r = xR \bmod \delta$.

При $r = 0$ обираються нові випадкові секретні ключі $k_i$.

Потім кожний користувач $i$ за допомогою свого особистого ключа $d_i$, значення $k_i$, хеш-образу $h_i$ та числа $r$ обчислює свою частину підпису

$$s_i = k_i - d_i \cdot h_i \cdot r \bmod n,$$

після чого генерується єдиний підпис $s$:

$$s = \sum_{i=1}^{t} s_i \bmod n.$$

Параметр підпису $s$ не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Агрегованим підписом є пара чисел $\langle r, s \rangle$.

**Перевірка цифрового підпису**

Перевірка підпису $\langle r, s \rangle$ під електронними документами $\{M_1, M_2, ..., M_t\}$ з відповідними хеш-образами $\{h_1, h_2, ..., h_t\}$ здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = \sum_{i=1}^{t} h_i \cdot Q_i,$$

яка залежить від відкритих ключів $Q_i$ учасників підписання та хеш-образів електронних документів $h_i$.

Обчислюється точка $\tilde{R}$ еліптичної кривої

$$\tilde{R} = sP + rQ = (x\tilde{R}, y\tilde{R})$$

після чого формується число

$$\tilde{r} = x\tilde{R} \bmod \delta.$$

Якщо $\tilde{r} = r$, агрегований цифровий підпис під набором електронних документів $\{M_1, M_2, ..., M_t\}$ признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки агрегованого підпису:

$$\tilde{R} = sP + rQ = \left(\sum_{i=1}^{t} s_i\right)P + r\left(\sum_{i=1}^{t} h_i \cdot Q_i\right) =$$

$$= \left(\sum_{i=1}^{t} k_i - d_i h_i r\right)P + r\left(\sum_{i=1}^{t} h_i d_i P\right) = \left(\sum_{i=1}^{t} k_i\right)P = \sum_{i=1}^{t} R_i = R.$$

Оскільки $\tilde{R} = R$, то і $\tilde{r} = r$.

Приклад.

Оберемо загальні параметри:
основне поле – скінченне поле $GF(13)$;
еліптична крива над основним полем

$$y^2 = x^3 + 2x + 4 \mod 13.$$

Базова точка еліптичної кривої $P = (7,6)$ має порядок $n = 17$.

Допоміжне просте багаторозрядне двійкове число $\delta = 7$.

Нехай число користувачів $t = 3$.

Відповідні особисті ключі є $d_1 = 8$, $d_2 = 5$, $d_3 = 15$.

Тоді відкриті ключі $Q_1 = (5,10)$, $Q_2 = (8,8)$, $Q_3 = (9,7)$.

Нехай хеш-образи електронних документів $M_1$, $M_2$, $M_3$ дорівнюють відповідно $h_1 = 9$, $h_2 = 10$, $h_3 = 13$.

Кожний підписант обирає одноразовий випадковий секретний ключ $k_i$: $k_1 = 5$, $k_2 = 10$, $k_3 = 9$ та обчислює координати точки $R_i$: $R_1 = (8,8)$, $R_2 = (0,11)$, $R_3 = (5,3)$.

Далі обчислюється $R$ – сума всіх точок $R_i$: $R = (0,2)$, після чого формується число $r$:

$$r = 0 \bmod 7 = 0.$$

Оскільки $r = 0$, необхідно обрати нові випадкові секретні ключі $k_i$: $k_1 = 3$, $k_2 = 4$, $k_3 = 12$. Відповідно $R_1 = (10,7)$, $R_2 = (12,1)$, $R_3 = (8,5)$. Тоді $R = (9,6)$, і число $r = 9 \bmod 7 = 2$, $r = 2$.

Далі кожний користувач $i$ за допомогою свого особистого ключа $d_i$, значення $k_i$, хеш-образу $h_i$ та числа $r$ обчислює свою частину підпису:

$$s_1 = 3 - 8 \cdot 9 \cdot 2 \bmod 17 = 12,\ s_1 = 12,$$

$$s_2 = 4 - 5 \cdot 10 \cdot 2 \bmod 17 = 6,\ s_2 = 6,$$

$$s_3 = 12 - 15 \cdot 13 \cdot 2 \bmod 17 = 13,\ s_3 = 13,$$

після чого генерується єдиний підпис $s$: $s = 14$.

Агрегованим підписом є пара чисел $\langle r, s \rangle = \langle 2,14 \rangle$.

Перевірка підпису $\langle r, s \rangle = \langle 2,14 \rangle$ під набором електронних документів $\{M_1, M_2, M_3\}$ з відповідними хеш-образами $h_1 = 9$, $h_2 = 10$, $h_3 = 13$ здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = 9Q_1 + 10Q_2 + 13Q_3 = (2,9),\ Q = (2,9).$$

Обчислюється точка $\tilde{R} = sP + rQ$ еліптичної кривої:

$$sP = (10,6),\ rQ = (8,8),$$

$$\tilde{R} = (9,6).$$

Звідси $\tilde{r} = 9 \bmod 7 = 2$, $\tilde{r} = 2$.

Оскільки $\tilde{r} = r$, агрегований цифровий підпис під набором електронних документів $\{M_1, M_2, M_3\}$ признається справжнім.

# Додаток В
# Спарювання Вейля точок еліптичної кривої

Розглянемо еліптичну криву над скінченним полем $GF(p)$

$$y^2 = x^3 + ax \mod p,$$

де $p = 3 \pmod 4$, $a \in GF(p)$; $G$ – адитивна група точок еліптичної кривої простого порядку $n$ з базовою точкою $P$, $nP = \mathrm{O}$, O – нескінченно віддалена точка; $V$ – мультиплікативна група простого порядку $n$ з нейтральним елементом **1**.

Білінійним спарюванням точок називається функція

$$e : G \times G \to V,$$

для якої виконуються властивості:

1. $e(P+Q,R) = e(P,R) \cdot e(Q,R)$, $e(P,Q+R) = e(P,Q) \cdot e(P,R)$
2. $e(k \cdot P, Q) = e(P,Q)^k$, $e(P, k \cdot Q) = e(P,Q)^k$,
3. $e(k \cdot P, Q) = e(P, k \cdot Q)$
4. $e(k \cdot P, m \cdot Q) = e(P,Q)^{k \cdot m}$,
5. $e(P,P) \neq 1$

### Спарювання Вейля точок еліптичної кривої

Спарювання Вейля $e(P,Q)$ точок $P$, $Q$ еліптичної кривої задається формулою:

$$e(P,Q) = \frac{F(P,Q+S) \cdot F(Q,-S)}{F(P,S) \cdot F(Q,P-S)} \qquad \forall S \in G, \qquad \text{(Б.1)}$$

де $F(T,Q)$ – функція Вейля для точок $T$, $Q$.

Функцію Вейля для точок $T$, $Q$, які мають порядок $n$, можна обчислить за допомогою рекурсивного алгоритму Міллера:

$$f_{1,T}(Q)=1 \qquad \forall Q\in G$$

$$f_{i+j,T}(Q)=f_{i,T}(Q)\cdot f_{j,T}(Q)\cdot\left.\frac{l_{i,j}}{v_{i+j}}\right|_{Q}, \qquad i+j<n, \qquad \text{(Б.2)}$$

$$F(T,Q)=f_{n,T}(Q),$$

де $l_{i,j}=\alpha x+\beta y+\gamma$ – рівняння прямої, яка проходить через точки $i\cdot T$, $j\cdot T$, $v_{i+j}=x-x_R$, $R=(i+j)\cdot T=(x_R,y_R)$.

В криптографії для обчислення спарювання Вейля використовується функція спотворення $\phi(x,y)=(-x,y\cdot i)$, яка забезпечує виконання властивостей 1-5:

```
phi:=proc(x,y) options operator,arrow;`mod`(-x, p), I*y
end proc;
```

Спарювання Вейля точок еліптичної кривої обчислюється за правилом: $e(P,Q)\to e(P,\phi(Q))$.

**Допоміжні функції пакету MAPLE**

Процедура *fWP(xP,yP,xQ,yQ)* обчислення спарювання Вейля точок $P=(xP,yP)$, $Q=(xQ,yQ)$ еліптичної кривої $y^2=x^3+ax \mod p$ з базовою точкою порядку $n$ та довільною точкою $S=(xS,yS)$ згідно з формулою (Б.1) має вигляд:

```
fWP:=proc(xP,yP,xQ,yQ) local fQ,PQS,QS,PS,QPS;
global a,p,n,xS,yS;
fQ:=phi(xQ,yQ);
PQS:=fv(xP,yP,smp(fQ,xS,yS));
QS:=fv(fQ,xS,-yS mod p);
PS:=fv(xP,yP,xS,yS);
QPS:=fv(fQ,smp(xP,yP,xS,-yS mod p));
return((PQS*QS)/(PS*QPS)) mod p;
end proc;
```

Процедура *fWP* включає процедуру *fv(xT,yT,xQ,yQ)* обчислення функції Вейля за алгоритмом Міллера для точок еліптичної кривої $T=(xT,yT)$, $Q=(xQ,yQ)$, які мають порядок $n$.

Процедура *fv* згідно з формулами (Б.2) має вигляд:

```
fv:=proc(xT,yT,xQ,yQ) local A,f,mlist,i,t,ff;
global a,p,n;
mlist:=convert(n,base,2);f:=1;A:=(xT,yT);
t:=length(convert(n,binary))-1;
for i from t by -1 to 1 do
f:=((f^2)*lv(A,A)) mod p;
ff:=unapply(f,x,y);f:=(ff(xQ,yQ)) mod p; A:=smp(A,A);
if (mlist[i]=1) then f:=f*lv(A,xT,yT) mod p;
A:=smp(A,xT,yT);ff:=unapply(f,x,y);f:=ff(xQ,yQ) mod p;
fi; od;
return f;
end proc;
```

Процедура *fv* включає процедуру *lv(x1,y1,x2,y2)* обчислення множника $\frac{l_{i,j}}{v_{i+j}}$ в формулі (Б.2), де $(x1,y1)=i\cdot T$, $(x2,y2)=j\cdot T$.

Процедура *lv* згідно з формулами (Б.2) має вигляд:

```
lv := proc(x1,y1,x2,y2) local lm; global a,p;
if x1 = x2 and y1 = `mod`(-y2, p) or y2 = "0" then
return `mod`(x-x1, p) end if;
if x1 = x2 and y1 = y2 then lm :=
`mod`((1/2)*(3*x1^2+a)/y1, p) end if;
if x1<>x2 then lm := `mod`((y1-y2)/(x1-x2), p) end if;
return `mod`((y-y1-lm*(x-x1))/(x+x1+x2-lm^2), p);
end proc;
```

В процедурі *fv* використовується процедура *smp(x1,y1,x2,y2)* суми точок $(x1,y1)$, $(x2,y2)$ еліптичної кривої $y^2=x^3+ax \mod p$:

```
smp:= proc(x1,y1,x2,y2) local lm,x3,y3; global a,p;
if x1 = "0" and y1 = "0" and x2 = "0" and y2 = "0" then
return "0", "0" end if;
```

```
if x1 = "0" and y1 = "0" then return x2, y2 end if;
if x2 = "0" and y2 = "0" then return x1, y1 end if;
if x1 = x2 and y2 = `mod`(-y1, p) then return "0", "0"
end if;
if x1 = x2 then lm := `mod`((1/2)*(3*x1^2+a)/y1, p)
else lm := `mod`((y1-y2)/(x1-x2), p) end if;
x3:=`mod`(lm^2-x1-x2,p); y3 := `mod`(lm*(x1-x3)-y1,p);
return x3,y3;
end proc;
```

Для реалізації криптографічних алгоритмів також використовується процедура *kxP(xP,yP,k)* множення точки $(xP, yP)$ на число $k$:

```
kxP:=proc(xP,yP,k) local N,A,V,i;
N:=k;A:=(xP,yP);V:=("0","0");
for i while (N>0) do
if ((N mod 2) = 1) then V:=smp(V,A); fi;
A:=smp(A,A); N:=floor(N/2); od;
return V; end proc;
```

**Приклад обчислення спарювання Вейля точок еліптичної кривої**

Оберемо загальні параметри:
основне поле – скінченне поле $GF(2383)$;
еліптична крива над основним полем

$$y^2 = x^3 - 3x \mod 2383.$$

Базова точка еліптичної кривої $P = (81, 787)$ має простий порядок $n = 149$.

Нехай $Q = 3 \cdot P = (1863, 213)$, $R = 5 \cdot P = (1368, 1568)$.

Перевіримо виконання властивостей 1-5 спарювання Вейля для точок $P$, $Q$, $R$.

В початок документу Maple необхідно помістити такі процедури *smp*, *kxP*, *lv*, *fv*, *fWP*.

Далі задати криву та інші загально системні параметри.

```
p:=2383;a:=-3;
phi:=proc(x,y) options operator,arrow;`mod`(-x,p),I*y
end proc;
P:=(81,787); n:=149; (xS,yS):=(0,0);
k:=3; m:=5;
Q:=kxP(P,k);R:=kxP(P,m);
```

Q = 1863, 213

R = 1368, 1568

```
fWP(smp(P,Q),R);
fWP(P,R);
fWP(Q,R);
fWP(P,R)*fWP(Q,R) mod p;
```

1283 + 1240 I

1855 + 2008 I

1416 + 364 I

1283 + 1240 I

```
fWP(P,smp(Q,R)); fWP(P,Q)*fWP(P,R) mod p;
```

25 + 976 I

25 + 976 I

```
fWP(kxP(P,k),Q); fWP(P,kxP(Q,k)); fWP(P,Q)^k mod p;
```

203 + 1502 I

203 + 1502 I

203 + 1502 I

```
fWP(kxP(P,k),kxP(Q,m)); fWP(P,Q)^(k*m) mod p;
```

815 + 298 I

815 + 298 I

```
fWP(P,P);
```

716+1466*I

# Додаток Г
# Кільцевий підпис

Кільцевий підпис (ring signature) це варіант реалізації електронного підпису, при якому відомо, що повідомлення підписано одним з членів списку потенційних підписантів, але не розкривається, ким саме. Підписант самостійно формує список з довільного числа різних осіб, включаючи в нього і себе. Для накладення підпису підписанту не потрібні дозвіл, сприяння або допомога з боку включених до списку осіб, використовуються тільки відкриті ключі всіх членів списку і закритий ключ лише самого підписанта.

Перший алгоритм кільцевого підпису був розроблений Рональдом Рівестом, Аді Шаміром і Яелем Тауманом, і представлено в 2001 році на міжнародній конференції Asiacrypt 2001 [7]. За твердженням авторів, вони намагалися в назві підкреслити відсутність центральної або координуючої структури при формуванні такого підпису: «... кільця являють собою геометричні фігури з однорідною периферією і без центру».

В розглянутому нижче протоколі [8] використовується в якості математичної структури група точок еліптичної кривої над скінченним полем. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій. Для хешування електронного документу може бути запропоновано використання стандартів.

В протоколі кільцевого підпису обраний від групи підписант обчислює підписи для кожного учасника групи і формує кінцевий кортеж підписів. Перевірка підпису здійснюється за допомогою спарювання Вейля точок еліптичної кривої. При цьому використовуються відкриті ключі всіх учасників групи. В процедурі перевірки неможливо визначити, хто саме підписав електронний документ від імені групи.

Схеми кільцевого підпису призначені для розв’язання задачі анонімного підписання документів, наприклад, рецензій, від імені деякого колективу.

Недоліком схем кільцевого підпису є великий розмір кінцевого кортежу підписів. Тому їх недоцільно використовувати в ситуаціях, де величина розміру підписів є критичною.

## Протокол кільцевого цифрового підпису електронного документу на еліптичній кривій над простим полем

### Загальносистемні параметри

Еліптична крива над скінченним полем $GF(p)$

$$y^2 = x^3 + ax \mod p,$$

де $p = 3 \pmod 4$, $a \in GF(p)$; $G$ – адитивна група точок еліптичної кривої простого порядку $n$ з базовою точкою $P$, $nP = \mathrm{O}$, O – нескінченно віддалена точка; $H$ – функція хешування. Для обчислення спарювання Вейля використовується функція спотворення $\phi(x, y) = (-x, y \cdot i)$.

### Генерація ключів

Кожний $i$-ий $(i = 1,2,...,t)$ користувач має асиметричну пару ключів: особистий $(c_i, d_i)$ – $1 < c_i, d_i < n$ – та відкритий $(U_i, Q_i)$, $U_i = c_i P$, $Q_i = d_i P$.

### Формування цифрового підпису

Нехай одному $A_L$ з членів списку потенційних підписантів $A_i$, $i = 1,2,...,t$, необхідно підписати електронний документ $M$ з хеш-образом $H(M)$. Молодші $|n|-1$ розряди хеш-образу $H(M)$ формують десяткове число $h$, яке використовується при обчисленні та перевірці цифрового підпису.

Підписант $A_L$ обирає одноразові випадкові числа $r$, $k_i$, $1 < r, k_i < n$, $i \neq L$, та обчислює координати точок

$$S_i = k_i P,$$

$$S_L = \left( \frac{1}{h + c_L + d_L \cdot r} \mod n \right) \cdot \left( P - \sum_{i \neq L} k_i \cdot \left( h \cdot P + U_i + r \cdot Q_i \right) \right).$$

Кільцевим підписом є набір $\langle r, S_1, S_2, ..., S_t \rangle$.

**Перевірка цифрового підпису**

Перевірка підпису $\langle r, S_1, S_2, ..., S_t \rangle$ електронного документу $M$ з відповідним його хеш-образу $H(M)$ числом $h$ здійснюється за допомогою відкритих ключів $(U_i, Q_i)$ підписантів $A_i$, $i = 1, 2, ..., t$, відповідно.

Якщо виконується

$$\prod_{i=1}^{t} e(h \cdot P + U_i + r \cdot Q_i, S_i) = e(P, P) \mod p$$

кільцевий цифровий підпис електронного документу $M$ признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки кільцевого підпису:

$$e(h \cdot P + U_L + r \cdot Q_L, S_L) =$$

$$= e\left( \left( h + c_L + r \cdot d_L \right) \cdot P, \frac{1}{h + c_L + r \cdot d_L} \cdot \left( P - \sum_{i \neq L} k_i \cdot \left( h \cdot P + U_i + r \cdot Q_i \right) \right) \right) =$$

$$= e\left( P, P - \sum_{i \neq L} k_i \cdot \left( h \cdot P + U_i + r \cdot Q_i \right) \right) =$$

$$= e(P, P) \cdot \prod_{i \neq L} e\left( P, k_i \cdot \left( h \cdot P + U_i + r \cdot Q_i \right) \right)^{-1}$$

Звідси

$$\prod_{i=L} e\left( P, k_i \cdot \left( h \cdot P + U_i + r \cdot Q_i \right) \right) = e(P, P)$$

Приклад.

Оберемо загальні параметри:

основне поле – скінченне поле $GF(2383)$;

еліптична крива над основним полем $y^2 = x^3 + -3x \bmod 2383$.

Базова точка еліптичної кривої $P = (81,787)$ має порядок $n = 149$

.

Нехай число користувачів в групі дорівнює $t = 3$: $A_1$, $A_2$, $A_3$.

Відповідними особистими ключами є $(c_1, d_1) = (4,5)$, $(c_2, d_2) = (2,1)$, $(c_3, d_3) = (6,3)$.

Тоді відкритими ключами є $(U_1, Q_1) = ((213,1462),(1368,1568))$, $(U_2, Q_2) = ((1602,1137),(81,787))$, $(U_3, Q_3) = ((14,1046),(1863,213))$.

Нехай підписантові $A_1$ необхідно підписати електронний документ $M$ з хеш-образом $H(M)$ і відповідним йому числом $h = 4$.

Підписант $A_1$ обирає одноразові випадкові числа $r = 5$, $k_2 = 3$, $k_3 = 5$ та обчислює координати точок $S_2$, $S_3$, та $S_1$:

$$S_2 = k_2 P = (1863,213),\ S_3 = k_3 P = (1368,1568),$$

$$S_1 = \left( \frac{1}{h + c_1 + d_1 \cdot r} \bmod n \right) \cdot \left( P - k_2 \cdot \left( h \cdot P + U_2 + r \cdot Q_2 \right) - k_3 \cdot \left( h \cdot P + U_3 + r \cdot Q_3 \right) \right) =$$

$$= \left( \frac{1}{33} \bmod 149 \right) \cdot \left( P - \left( 3 \cdot \left( 4 \cdot P + U_2 + 5 \cdot Q_2 \right) + 5 \cdot \left( 4 \cdot P + U_3 + 5 \cdot Q_3 \right) \right) \right) =$$

$$= 140\left( (81,787) - \left( (1902,214) + (516,1993) \right) \right) =$$

$$= 140\left( (81,787) - (1940,2215) \right) = 140\left( (81,787) + (1940,168) \right) = (740,521)$$

$$\frac{1}{33} \bmod 149 = 140.$$

Кільцевим підписом є набір

$$\langle r, S_1, S_2, S_3 \rangle = \langle 5, (740,521), (1863,213), (1368,1568) \rangle.$$

Перевірка підпису

$$\langle r, S_1, S_2, S_3 \rangle = \langle 5, (740,521), (1863,213), (1368,1568) \rangle$$

електронного документу $M$ з відповідним його хеш-образу $H(M)$ числом $h$ здійснюється за допомогою відкритих ключів ( $(U_1, Q_1) = ((213,1462),(1368,1568))$, $(U_2, Q_2) = ((1602,1137),(81,787))$, $(U_3, Q_3) = ((14,1046),(1863,213))$, підписантів $A_1$, $A_2$, $A_3$ відповідно.

Обчислимо

$$e(h \cdot P + U_1 + r \cdot Q_1, S_1) = 25 + 1407i$$
$$e(h \cdot P + U_2 + r \cdot Q_2, S_2) = 2312 + 2028i$$
$$e(h \cdot P + U_3 + r \cdot Q_3, S_3) = 467 + 1168i$$
$$e(h \cdot P + U_3 + r \cdot Q_3, S_3) \times e(h \cdot P + U_3 + r \cdot Q_3, S_3) \times$$
$$\times e(h \cdot P + U_3 + r \cdot Q_3, S_3) \bmod p = 716 + 1466i$$

та

$$e(P, P) = 716 + 1466i .$$

Оскільки перевірочне співвідношення виконується, кільцевий цифровий підпис електронного документу $M$ признається справжнім.

**Допоміжні функції пакету MAPLE**

В початок документу Maple необхідно помістити такі процедури *smp*, *kxP*, *lv*, *fv*, *fWP*.

Далі задати криву та інші загально системні параметри.

```
p:=2383; a:=-3; P:=(81,787); n:=149; (xS,yS):=(0,0);
phi:=proc(x,y) options operator,arrow;`mod`(-x, p), I*y
end proc;
```

Нехай $P = (81,787)$, $T = (1890,\ 1038)$ – точки еліптичної кривої над полем $GF(p)$.

Для обчислення $P-T$ можна використати $P+(-T)$, де $T=(T[1],T[2])$, $-T=(T[1],-T[2])$ :

```
smp(P,T[1],-T[2] mod p);
```

767, 2321

Множник $\dfrac{1}{h+c_L+d_L\cdot r}$ в формулі

$$S_L=\frac{1}{h+c_L+d_L\cdot r}\left(P-\sum_{i\neq L}k_i\cdot\left(h\cdot P+U_i+r\cdot Q_i\right)\right)$$

можна обчислить таким чином.
Нехай $h=136$ , $c3=50$, $d3=25$ , $r=80$ , $n=149$ . Тоді

```
u3:=d3*r+c3+h mod n;
```

100

```
k3:=1/u3 mod n;
```

76

Якщо $u3=0$, необхідно обрати інше значення $r$ .

Нехай отримано кільцевий цифровий підпис $\langle r,S_1,S_2,S_3\rangle=\langle 118,498,1106,1890,1345,1129,1460\rangle$ електронного документу згідно з протоколом, наведеним в Додатку Б. Нехай хеш-образу отриманого повідомлення відповідає число $H=116$.

Перевіримо справжність цифрового підпису, використовуючи відкриті ключі підписантів $(U_1,Q_1)=((695,2063),(1078,2053))$, $(U_2,Q_2)=((1126,836),(1368,1568))$, $(U_3,Q_3)=((870,2197),(1475,64))$ відповідно $S_1,S_2,S_3$.

```
p:=2383; a:=-3; P:=(81,787); n:=149; (xS,yS):=(0,0);
phi:=proc(x,y) options operator,arrow;`mod`(-x, p), I*y
end proc;
     H:=116;
```

```
     r:=118;
     S1:=(498,1106); S2:=(1890,1345); S3:=(1129,1460);
     U1:=(695,2063); Q1:=(1078,2053);
     U2:=(1126,836); Q2:=(1368,1568);
     U3:=(870,2197); Q3:=(1475,64);
W1:=smp(kxP(P,H),smp(U1,kxP(Q1,r)));
W2:=smp(kxP(P,H),smp(U2,kxP(Q2,r)));
W3:=smp(kxP(P,H),smp(U3,kxP(Q3,r)));
fWP(W1,S1)*fWP(W2,S2)*fWP(W3,S3) mod p;
                716 + 1466 I
fWP(P,P);
                716 + 1466 I
```

Оскільки перевірочне співвідношення

*fWP(W1,S1)*fWP(W2,S2)*fWP(W3,S3) mod p = fWP(P,P)*

виконується, кільцевий цифровий підпис електронного документу *M* признається справжнім.