**Министерство образования и науки Российской Федерации**

**федеральное государственное автономное образовательное  
учреждение высшего образования  
«Санкт-Петербургский национальный исследовательский  
университет информационных технологий, механики и оптики»**

**Факультет:** Безопасности информационных технологий

**Направление:** 10.03.01 «Информационная безопасность»

**Дисциплина**

Криптографические методы защиты информации

**ЛАБОРАТОРНАЯ РАБОТА**

Криптография на эллиптических кривых

**Выполнил:**

студент группы N3464

Перфильев В.Е.

**Преподаватель:**

Михайличенко О.В.

Санкт-Петербург

2019 г.

Содержание

[Шифрование ОТ на элл. Крив 3](#_30j0zll)

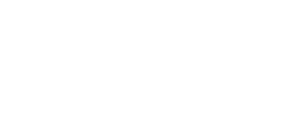
[Расшифрование ШТ на элл. Крив 9](#_1fob9te)

[Расчет точки 2P+3Q 12](#_3znysh7)

[Расчет точки nP 14](#_2et92p0)

[Получение ЭЦП на эл кривых 17](#_tyjcwt)

[Проверка ЭЦП на эл кривых 19](#_3dy6vkm)



Лабораторная работа по эллиптическим кривым.

Вариант 5.

**Первая часть лабораторной**

# Шифрование ОТ на элл. Крив

Шифрование открытого текста на основе эллиптических кривых

Цель работы: зашифровать открытый текст, используя алфавит, приведенный в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография» в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая E751( -1,1) − и генерирующая точка G = (0, 1))».

Открытый ключ B (425, 663)

Пользователь А решил отправить пользователю B сообщение: «ренессанс». В нашем алфавите эти буквы кодируется следующим образом:

Pm(у) = (247, 485)

Pm(в) = (229, 151)

Pm(е) = (234, 587)

Pm(р) = (243, 87)

Pm(о) = (240, 309)

Pm(в) = (229, 151)

Pm(а) = (228, 271)

Pm(т) = (247, 266)

Pm(ь) = (256, 121)

Значения случайных чисел k для букв открытого текста соответствующие буквам:

K= 6, 14, 5, 7, 12, 11, 4, 9, 19

Пользователь А имеет значения k для каждой буквы, а открытым ключом B является точка Pb = (425, 663)

Шифрованный текст имеет вид .

Находим

Для нахождения kG используем правила сложения точек эллиптической кривой:

λ=

Вычисляем 2G:

Расширенный алгоритм Евклида:

)

**2G = (188,93)**

Вычисляем 3G = 2G + G:

Расширенный алгоритм Евклида:

)

**3G = (56,419)**

Вычисляем 4G = 2G + 2G:

Расширенный алгоритм Евклида:

)

**4G = (16,416)**

Вычисляем 5G = 4G + 1G:

Расширенный алгоритм Евклида:

)

**5G = (425,663)**

Вычисляем 6G = 4G + 2G:

Расширенный алгоритм Евклида:

)

**6G = (725,195)**

Вычисляем 7G = 6G + 1G:

Расширенный алгоритм Евклида:

)

**7G = (135,82)**

Вычисляем 8G = 4G + 4G:

Расширенный алгоритм Евклида:

)

**8G = (346,242)**

Вычисляем 9G = 8G + 1G:

Расширенный алгоритм Евклида:

)

**9G = (489,468)**

Вычисляем 10G = 8G + 2G:

Расширенный алгоритм Евклида:

)

**10G = (377,456)**

Вычисляем 11G = 10G + G:

Расширенный алгоритм Евклида:

)

**11G = (179,275)**

Вычисляем 12G = 11G + G:

Расширенный алгоритм Евклида:

)

**12G = (286,136)**

Вычисляем 14G = 12G + 2G:

Расширенный алгоритм Евклида:

)

**14G = (596,433)**

Вычисляем 16G = 8G + 8G:

Расширенный алгоритм Евклида:

)

**16G = (72,254)**

Вычисляем 19G = 16G + 3G:

Расширенный алгоритм Евклида:

)

**19G = (568,355)**

**Вычисляем для каждой буквы в слове:**

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

**Итог шифрования:**

Cm(у) = {(725, 195), (620, 680)};

Cm(в) = {(596, 433), (39, 171)};

Cm(е) = {(425, 663), (654, 102)};

Cm(р) = {(135, 82), (85, 716)};

Cm(о) = {(286, 136), (99, 295)};

Cm(в) = {(179, 275), (526, 412)};

Cm(а) = {(16, 416), (458, 490)};

Cm(т) = {(489, 468), (140, 115)};

Cm(ь) = {(568, 355), (400, 56)};

**Вторая часть лабораторной**

# Расшифрование ШТ на элл. Крив

Секретный ключ nb = 41.

Пользователь B для расшифрования сообщения должен провести следующие вычисления:

1 буква: {(283, 493), (314, 127)};

2 буква: {(425, 663), (561, 140)};

3 буква: {(568, 355), (75, 433)};

4 буква: {(440, 539), (602, 627)};

5 буква: {(188, 93), (395, 414)};

6 буква: {(179, 275), (25, 604)};

7 буква: {(72, 254), (47, 349)};

8 буква: {(72, 254), (417, 137)};

9 буква: {(188, 93), (298, 225)};

10 буква: {(56, 419), (79, 111)}

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

Расшифровываем слово по полученным точкам используя таблицу алфавита, представленную в лабораторной работе.

Зашифрованное слово: «допустимый».

**Третья часть лабораторной**

# Расчет точки 2P+3Q

Найти точку 2P + 3Q – R.

P = (59, 386)

Q = (70, 195)

R = (72, 254)

Для нахождения точки 2P + 3Q – R используем правила сложения точек эллиптической кривой:

λ=

Вычисляем 2P:

Расширенный алгоритм Евклида:

)

**2P = (93, 267)**

Вычисляем 2Q:

Расширенный алгоритм Евклида:

)

**2Q = (234, 587)**

Вычисляем 3Q:

Расширенный алгоритм Евклида:

)

**3Q = (551, 487)**

Вычисляем 2P + 3Q:

Расширенный алгоритм Евклида:

)

**2P + 3Q = (281, 233)**

Вычисляем 2P + 3Q – R:

2P + 3Q – R = (93, 267) + (551, 487) - (72, 254) = (281, 233) *+* (72, -254)

Расширенный алгоритм Евклида:

)

**Результат: 2P + 3Q – R = (177, 189)**

**Четвёртая часть лабораторной**

# Расчет точки nP

Расчет точки nP на эллиптической кривой.

P = (36, 87)

n = 111

Для упрощения счёта используем алгоритм удвоения-сложения:

Переводим 111 в двоичную систему исчисления: n2=01101111

Для нахождения точки 110 \* P используем правила сложения точек эллиптической кривой:

λ=

Вычисляем 2P = P+P:

Расширенный алгоритм Евклида:

)

**2P = (651, 560)**

Вычисляем 4P = 2P+2P:

Расширенный алгоритм Евклида:

)

**4P = (302, 486)**

Вычисляем 8P = 4P+4P:

Расширенный алгоритм Евклида:

)

**8P = (616, 400)**

Вычисляем 32P = (8P+8P) \*2 = 16P + 16P

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

**32P = (125, 459)**

Вычисляем 64P = 32P+32P:

Расширенный алгоритм Евклида:

)

**64P = (616, 400)**

С использованием алгоритма удвоения-сложения получаем - 111P = 64P + 32P + 8P + 4P + 2P + P:

Вычисляем 64P + 32P = (616, 400) + (125, 459) = (283, 493)

Расширенный алгоритм Евклида:

)

Вычисляем 64P + 32P + 8P = (283, 493) + (616, 400) = (616, 351)

Расширенный алгоритм Евклида:

)

Вычисляем 64P + 32P + 8P + 4P = (616, 351) + (302, 486) **=** (302, 265)

Расширенный алгоритм Евклида:

)

Вычисляем 64P + 32P + 8P + 4P +2P = (302, 265) + (651, 560) = (651, 191)

Расширенный алгоритм Евклида:

)

Вычисляем 64P + 32P + 8P + 4P +2P+P = (651, 191) + (36, 87) = (36, 664)

Расширенный алгоритм Евклида:

)

**Результат 111P = (36, 664)**

**Пятая часть лабораторной**

# Получение ЭЦП на эл кривых

Получение ЭЦП на основе эллиптических кривых.

Цель работы: сгенерировать ЭЦП для сообщения с известным значением хэш-свертки e, зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k. Используется эллиптическая кривая E751(−1,1) и генерирующая точка G = (416, 55) порядка n =13.

Вариант 5: E = 5; d = 12; k = 6.

Пусть абонент, подписывающий сообщение, выбрал k = 6.

Тогда:

Для нахождения точки используем правила сложения точек эллиптической кривой:

λ=

Промежуточные вычисления:

Вычисляем

Расширенный алгоритм Евклида:

)

Вычисляем

Расширенный алгоритм Евклида:

)

Вычисляем

Расширенный алгоритм Евклида:

)

Вычисляем

Расширенный алгоритм Евклида:

)

1. Вычисляем
2. Используем расширенный алгоритм Евклида:
3. Вычисляем
4. Таким образом, – цифровая подпись данного абонента для сообщения.

**Шестая часть лабораторной**

# Проверка ЭЦП на эл кривых

Цель работы: проверить подлинность ЭЦП (r,s) для сообщения с известным значением хэш-свертки e, зная открытый ключ проверки подписи Q. Используется эллиптическая кривая E751(−1,1) и генерирующая точка G = (562, 89) порядка n = 13.

Пусть теперь необходимо проверить подлинность подписи. Открытый ключ абонента, подписавшего сообщение, равен

Вариант 5: E = 2, ,

1. Проверка подлинности подписи начинается с проверки условий:

Общая формула

Вычисляем:

1. Последовательно вычисляем:

Расширенный алгоритм Евклида:

1. Находим точку X:

(455, 383)

Промежуточные вычисления:

Вычисляем

Расширенный алгоритм Евклида:

)

Расширенный алгоритм Евклида:

)

**3G = (384, 276)**

Расширенный алгоритм Евклида:

)

**6G = (455, 368)**

Расширенный алгоритм Евклида:

)

**9G = (596, 433)**

Вычисляем :

Расширенный алгоритм Евклида:

)

**2Q = (596, 318)**

Расширенный алгоритм Евклида:

)

**4Q = (416, 696)**

Расширенный алгоритм Евклида:

)

**8Q = (384, 276)**

Расширенный алгоритм Евклида:

)

**12Q = (135, 82)**

Сумма:

Расширенный алгоритм Евклида:

)

1. Наконец, сравниваем значения r и x mod n, если они совпадают, следовательно, подпись действительная.

**Результат: Подпись фальшивая.**