

УО «Белорусский государственный университет информатики и  
радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3  
по предмету «Теория информации»

Выполнил:

Руденя Д. А.

гр. 351001

Проверила:

Болтак С.В.

Минск 2025

## Работа алгоритма при корректных данных:

ECDSA на эллиптических кривых

Введите  $p$  (простое число  $> 3$ ):

1951

Сгенерировать группу  $EM(a,b)$

$p = 1951$   
Автоматически подобраны параметры:  
 $a = 1219$   
 $b = 834$   
Всего точек: 1969  
None  
(0, 360)  
(0, 1591)  
(4, 356)  
(4, 1595)  
(5, 582)  
(5, 1369)  
(6, 967)  
(6, 984)  
(9, 580)

Выполнить обмен ключами

Введите сообщение для подписи:

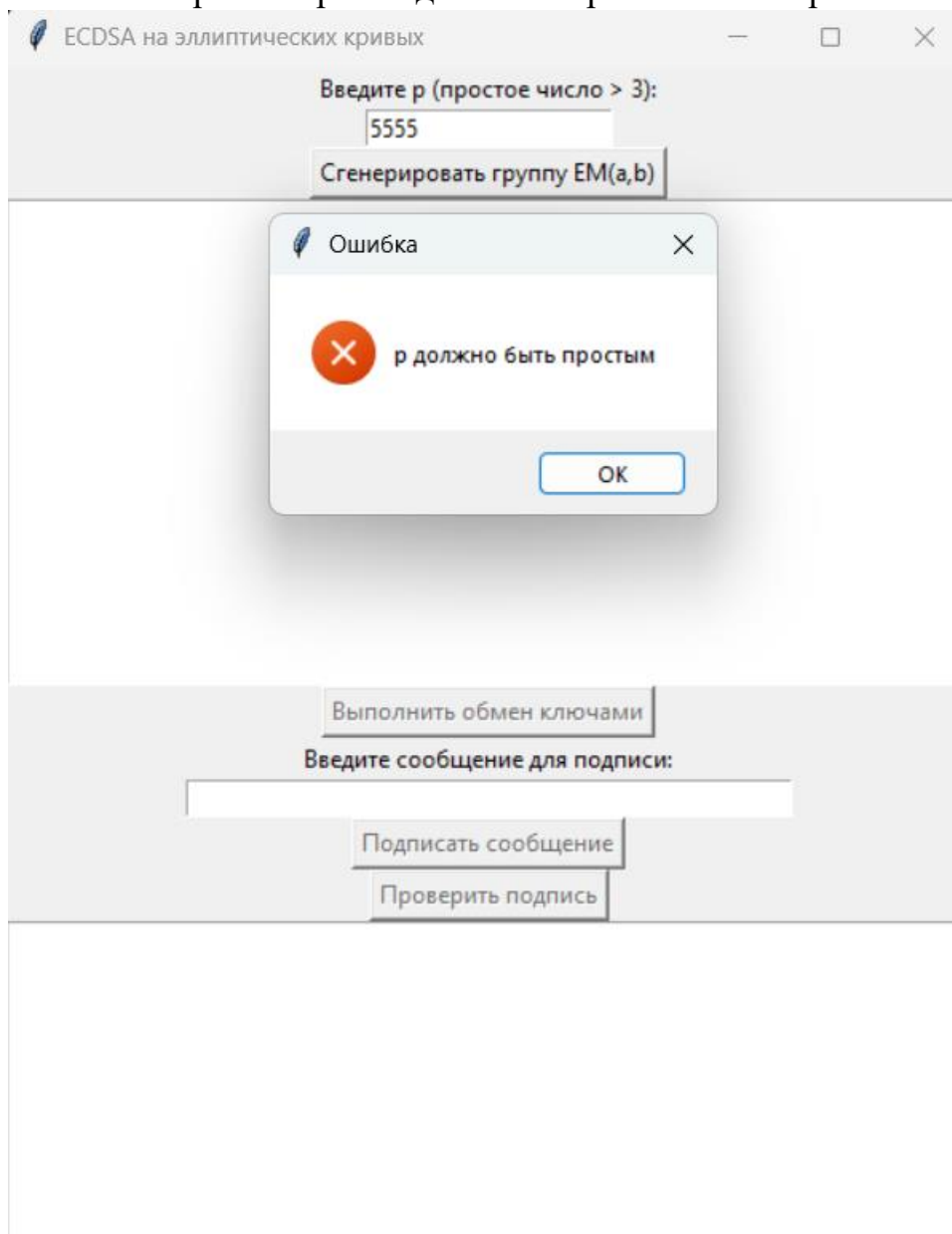
sos

Подписать сообщение

Проверить подпись

Закрытый ключ ( $d$ ): 413  
Открытый ключ ( $Q$ ): (1072, 1290)  
  
Подпись ( $r, s$ ): (1811, 620)  
Подпись верна

Работа алгоритма при введёном не простом числе  $p$ :



Работа алгоритма при  $p$  меньше 3:


ECDSA на эллиптических кривых

Введите  $p$  (простое число  $> 3$ ):

0

Сгенерировать группу  $EM(a,b)$

Ошибка

  $p$  должно быть больше 3

OK

Выполнить обмен ключами

Введите сообщение для подписи:

Подписать сообщение

Проверить подпись

## Работа алгоритма при подделке цифровой подписи:

ECDSA на эллиптических кривых

Введите  $p$  (простое число  $> 3$ ):

1951

Сгенерировать группу  $EM(a,b)$

$p = 1951$   
Автоматически подобраны параметры:  
 $a = 1579$   
 $b = 1072$   
Всего точек: 2028  
None  
(0, 252)  
(0, 1699)  
(4, 211)  
(4, 1740)  
(5, 366)  
(5, 1585)  
(6, 458)  
(6, 1493)  
(10, 693)

Выполнить обмен ключами

Введите сообщение для подписи:

sos

Подписать сообщение

Проверить подпись

Закрытый ключ ( $d$ ): 1030  
Открытый ключ ( $Q$ ): (638, 860)  
Подпись ( $r, s$ ): (10, 1853)  
Подпись неверна

## Работа алгоритма на больших сообщениях:

ECDSA на эллиптических кривых

Введите  $p$  (простое число  $> 3$ ):

2003

Сгенерировать группу  $EM(a,b)$

$p = 2003$   
Автоматически подобраны параметры:  
 $a = 1776$   
 $b = 807$   
Всего точек: 2028  
None  
(0, 984)  
(0, 1019)  
(1, 545)  
(1, 1458)  
(2, 19)  
(2, 1984)  
(4, 63)  
(4, 1940)  
(7, 160)

Выполнить обмен ключами

Введите сообщение для подписи:

With all our loveliness Deriv team

Подписать сообщение

Проверить подпись

Закрытый ключ ( $d$ ): 277  
Открытый ключ ( $Q$ ): (1256, 510)

Подпись ( $r, s$ ): (866, 1043)  
Подпись верна