Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Факультет компьютерных систем и сетей

Кафедра информатики

Отчет по лабораторной работе №7

**Криптография с использованием эллиптических кривых**

|  |  |
| --- | --- |
| Выполнил:  студент группы 653501  Ковалевская Алина | Проверил:  Артемьев В.С. |

Минск, 2019

**Задача**

Реализовать схему шифрования (дешифрования) для аналога алгоритма Диффи-Хеллмана на основе эллиптических кривых.

**Введение**

Эллиптическая кривая над полем K — неособая кубическая кривая на проективной плоскости над K^ (алгебраическим замыканием поля K), задаваемая уравнением 3-й степени с коэффициентами из поля K и «точкой на бесконечности». В подходящих аффинных координатах её уравнение приводится к виду:



В канонической форме если характеристика поля K не равна 2 или 3, то уравнение с помощью замены координат приводится к канонической форме (форме Вейерштрасса):



Если характеристика К = 3, то каноническим видом уравнения является вид:



Если характеристика K=2, то уравнение приводится к одному из видов:

 - суперсингулярные кривые

или

 - несуперсингулярные кривые

Особое удобство суперсингулярных эллиптических кривых в том, что для них легко вычислить порядок, в то время как вычисление порядка несуперсингулярных кривых вызывает трудности. Суперсингулярные кривые особенно удобны для создания самодельной ЕСС-криптосистемы. Для их использования можно обойтись без трудоёмкой процедуры вычисления порядка.

Точки эллиптической кривой над конечным полем представляют собой группу. И для этой группы определена операция сложения. Соответственно, можно представить умножение числа k на точку G как G+G+..+G с k слагаемыми.

Теперь можно представить, что имеется сообщение M представленное в виде целого числа. Мы можем зашифровать его используя выражение  
C=M\*G. Вопрос в том, насколько сложно восстановить M зная параметры кривой E(a,b), шифротекст С и точку G.

Данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

**Алгоритм Диффи-Хэллмана**

В данном описании криптографического протокола, аналогичный известному протоколу Диффи-Хэллмана для установления защищенной связи два пользователя А и В совместно выбирают эллиптическую кривую Е и точку Р на ней.

1 этап. Пользователь А выбирает свое секретное целое число a (b — большое число) и вычисляет произведение. Далее А пересылает вычисленное значение получателю В. Пользователь В генерирует свое секретное большое число b (b — целое число) и вычисляет произведение. В пересылает его получателю А. При этом параметры самой кривой, координаты точки на ней и значения произведений являются открытыми и могут передаваться по незащищенным каналам связи. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их.

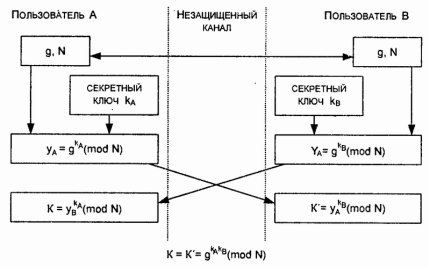
2 этап. А на основе имеющегося у пользователя числа и полученного по сети вычисляет значение В на основе имеющегося у пользователя числа и полученного по сети вычисляет значение В силу свойств операции умножения на число. Таким образом, оба пользователя получат общее секретное значение (координаты точки), которое они могут использовать для получения ключа шифрования.

Злоумышленнику для восстановления ключа потребуется решить сложную с вычислительной точки зрения задачу определения и  по известным  данным. Если эта проблема имеет эффективное решение, то и проблема Диффи-Хеллмана для эллиптических также легко решаема и рассмотренный протокол не имеет смысла. В то же время гипотеза об эквивалентности проблем дискретного логарифма и проблемы Диффи-Хеллмана для эллиптических кривых не доказана. Протокол Диффи-Хеллмана отлично противостоит пассивному нападению, но в случае реализации атаки «человек посередине» он не устоит. В самом деле, Атакующий заменяет сообщения переговоров о ключе на свои собственные и таким образом получает два ключа — свой для каждого из законных участников протокола. Далее он может перешифровывать переписку между участниками, своим ключом для каждого, и таким образом ознакомиться с их сообщениями, оставаясь незамеченным.

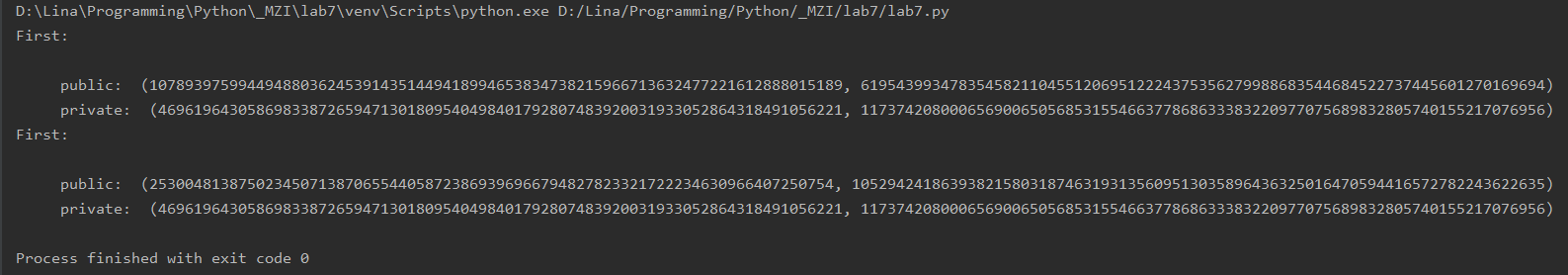
## 2.3 Безопасность алгоритма на основе эллиптических кривых

Безопасность, обеспечиваемая криптографическим подходом на основе эллиптических кривых, зависит от того, насколько трудной для решения оказывается задача определения {\displaystyle k}k по данным {\displaystyle kP}kP и {\displaystyle P}P. Эту задачу обычно называют проблемой логарифмирования на эллиптической кривой. Наиболее быстрым из известных на сегодня методов логарифмирования на эллиптической кривой является так называемый {\displaystyle p}p-метод Полларда. В таблице (см. ниже) сравнивается эффективность этого метода и метод разложения на простые множители с помощью решета в поле чисел общего вида. Из нее видно, что по сравнению с RSA в случае применения методов криптографии на эллиптических кривых примерно тот же уровень защиты достигается со значительно меньшими значениями длины ключей.

**Блок-схема алгоритма**

Блок-схема алгоритма Диффи-Хеллмана

**Демонстрация работы программы**



**Вывод**

В ходе написания лабораторной работы были изучены алгоритмы шифрования и дешифрования для аналога алгоритма Диффи-Хеллмана на основе эллиптических кривых, а также написаны их программные реализации. Были получены навыки усложнения и увеличения криптостойкости алгоритма Диффи-Хеллмана на основе эллиптических кривых, а также изучены модификации и режимы работы алгоритма Диффи-Хеллмана на основе эллиптических кривых.

**Программный код**

**lab7.py**

from codecs import getdecoder

from codecs import getencoder

def strxor(a, b):

mlen = min(len(a), len(b))

a, b, xor = bytearray(a), bytearray(b), bytearray(mlen)

for i in range(mlen):

xor[i] = a[i] ^ b[i]

return bytes(xor)

\_hexdecoder = getdecoder("hex")

\_hexencoder = getencoder("hex")

def hexdec(data):

return \_hexdecoder(data)[0]

def hexenc(data):

return \_hexencoder(data)[0].decode("ascii")

def bytes2long(raw):

return int(hexenc(raw), 16)

def long2bytes(n, size=32):

res = hex(int(n))[2:].rstrip("L")

if len(res) % 2 != 0:

res = "0" + res

s = hexdec(res)

if len(s) != size:

s = (size - len(s)) \* b"\x00" + s

return s

def modinvert(a, n):

if a < 0:

# k^-1 = p - (-k)^-1 mod p

return n - modinvert(-a, n)

t, newt = 0, 1

r, newr = n, a

while newr != 0:

quotinent = r // newr

t, newt = newt, t - quotinent \* newt

r, newr = newr, r - quotinent \* newr

if r > 1:

return -1

if t < 0:

t = t + n

return t

MODE2SIZE = {

2001: 32,

2012: 64,

}

DEFAULT\_CURVE = "GostR3410\_2001\_CryptoPro\_A\_ParamSet"

# Curve parameters are the following: p, q, a, b, x, y

CURVE\_PARAMS = {

"GostR3410\_2001\_CryptoPro\_A\_ParamSet": (

"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD97",

"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD94",

"00000000000000000000000000000000000000000000000000000000000000a6",

)

}

for c, params in CURVE\_PARAMS.items():

CURVE\_PARAMS[c] = [hexdec(param) for param in params]

class Curve(object):

def \_\_init\_\_(self, p, a, b):

self.p = bytes2long(p)

self.a = bytes2long(a)

self.b = bytes2long(b)

def \_pos(self, v):

if v < 0:

return v + self.p

return v

def \_add(self, p1x, p1y, p2x, p2y):

if p1x == p2x and p1y == p2y:

# double

t = ((3 \* p1x \* p1x + self.a) \* modinvert(2 \* p1y, self.p)) % self.p

else:

tx = self.\_pos(p2x - p1x) % self.p

ty = self.\_pos(p2y - p1y) % self.p

t = (ty \* modinvert(tx, self.p)) % self.p

tx = self.\_pos(t \* t - p1x - p2x) % self.p

ty = self.\_pos(t \* (p1x - tx) - p1y) % self.p

return tx, ty

def exp(self, degree, x=None, y=None):

x = x or self.x

y = y or self.y

tx = x

ty = y

degree -= 1

if degree == 0:

raise ValueError("Bad degree value")

while degree != 0:

if degree & 1 == 1:

tx, ty = self.\_add(tx, ty, x, y)

degree = degree >> 1

x, y = self.\_add(x, y, x, y)

return tx, ty

def ellept(d\_a, d\_b, G):

curve = Curve(\*CURVE\_PARAMS["GostR3410\_2001\_CryptoPro\_A\_ParamSet"])

H\_a = curve.exp(d\_a, \*G)

H\_b = curve.exp(d\_b, \*G)

secret\_a = curve.exp(d\_a, \*H\_b)

secret\_b = curve.exp(d\_b, \*H\_a)

print('First: \n')

print('\t public: ', H\_a)

print('\t private: ', secret\_a)

print('First: \n')

print('\t public: ', H\_b)

print('\t private: ', secret\_b)

assert secret\_a == secret\_b

return secret\_a

if \_\_name\_\_ == '\_\_main\_\_':

d\_a = 123123

d\_b = 432123

G = (123123, 12312311)

key = ellept(d\_a, d\_b, G)