**Министерство науки и высшего образования РФ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

УДК 004.8

Срок хранения 2 года

ВЛГУ.10.05.04.04.05.00 ПЗ

**ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ**

«**ЛАБОРАТОРНАЯ РАБОТА №5 Протокол Фиата-Шамира**»

Специальность 10.05.04 – «Информационно-аналитические системы безопасности»

|  |  |  |
| --- | --- | --- |
| Руководитель |  | к.т.н. доцент кафедры ИЗИ Д. В. Мишин |
|  |
| Исполнитель |  | студент группы ИСБ-119 Д. А. Журавлёв |
|  |  |  |  |

Владимир 2023 г.

**ЛАБОРАТОРНАЯ РАБОТА №5 Протокол Фиата-Шамира**

**Задание**: Изучить и реализовать протокол Фиата-Шамира (Протокол аутентификации с нулевым разглашением).

**Краткие сведения:**

Протокол Фиата — Шамира — это один из наиболее известных протоколов идентификации с нулевым разглашением (Zero-knowledge protocol). Протокол был предложен Амосом Фиатом (англ. Amos Fiat) и Ади Шамиром (англ. Adi Shamir)

Пусть А знает некоторый секрет s. Необходимо доказать знание этого секрета некоторой стороне В без разглашения какой-либо секретной информации. Стойкость протокола основывается на сложности извлечения квадратного корня по модулю достаточно большого составного числа n, факторизация которого неизвестна.

**Алгоритм работы:**

Следующие действия последовательно и независимо выполняются **t** раз. **В** считает знание доказанным, если все **t** раундов прошли успешно.

* **А** выбирает случайное **r** , такое, что �∈[1,�−1]r принадлежит [1, n-1] и отсылает �=�2(mod�)x = r2  (mod n) стороне **B** (доказательство)
* **B** случайно выбирает бит **e** (**e**=0 или **е**=1) и отсылает его **A** (вызов)
* **А** вычисляет **у** и отправляет его обратно к **B**. Если **e**=0, то �=�y=r, иначе �=�∗�(mod�)y = r \* s (ответ)
* Если **y**=0, то **B** отвергает доказательство или, другими словами, **А** не удалось доказать знание **s**.
* В противном случае, сторона **B** проверяет, действительно ли �2=�∗��(mod�)y2 = x \* ve (mod n) и, если это так, то происходит переход к следующему раунду протокола.

**Диаграмма последовательностей:**

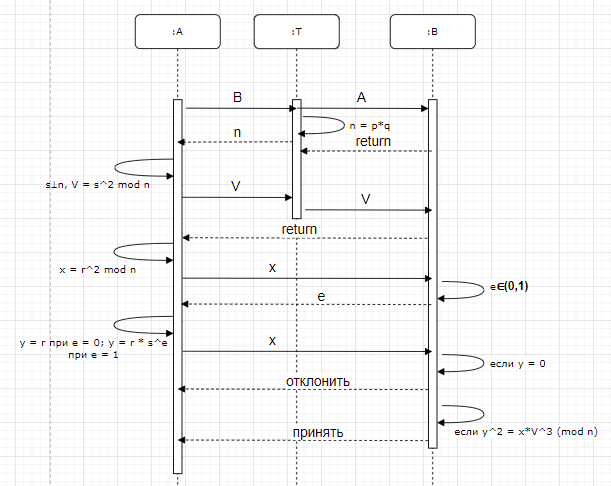
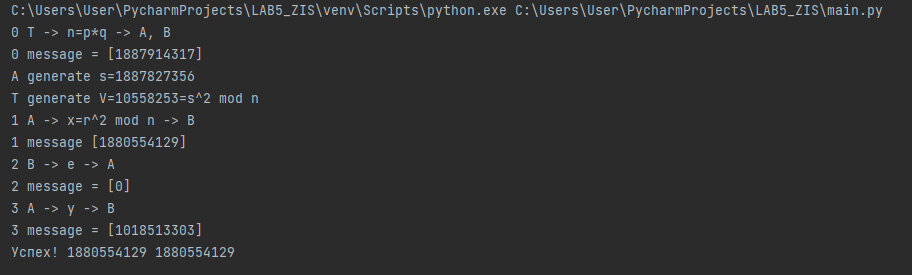


Рисунок 1 – Диаграмма последовательности

**Программа:**

Программа написана на языке python. Программа реализует протокол Фиата-Шамира по шагам. В результате работы клиент B аутентифицирует клиента A. Код программы представлен в приложении.

Вывод:



**Вывод:**

В процессе работы был изучен протокол Фиата-Шамира, была разработана программа реализующая данный протокол.

**Приложение**

import random

def is\_prime(a):

if a % 2 == 0:

return a == 2

d = 3

while d \* d <= a and a % d != 0:

d += 2

return d \* d > a

def fi(n):

f = n

if n%2 == 0:

while n%2 == 0:

n = n // 2

f = f // 2

i = 3

while i\*i <= n:

if n%i == 0:

while n%i == 0:

n = n // i

f = f // i

f = f \* (i-1)

i = i + 2

if n > 1:

f = f // n

f = f \* (n-1)

return f

prime = []

def f0():

for i in range(100000, 1000, -1):

if is\_prime(i):

prime.append(i)

p = prime.pop(random.randint(0, len(prime)))

q = prime.pop(random.randint(0, len(prime)))

n = p \* q

s = fi(n)

V = s\*\*2 % n

print('0 T -> n=p\*q -> A, B')

print(f'0 message = [{n}]')

print(f'A generate s={s}')

print(f'T generate V={V}=s^2 mod n')

return n, s, V

def f1(n, s):

r = random.randint(1, n-1)

x = r\*\*2 % n

print(f'1 A -> x=r^2 mod n -> B')

print(f'1 message [{x}]')

return x, r

def f2():

e = random.randint(0, 1)

print(f'2 B -> e -> A')

print(f'2 message = [{e}]')

return e

def f3(n, e, r, s):

if e == 0:

y = r

else:

y = (r \* s) % n

print(f'3 A -> y -> B')

print(f'3 message = [{y}]')

return y

def f4(x, y, e, n, V):

if y\*\*2 % n == (x\*V\*\*e) % n:

print("Успех!", y\*\*2 % n, (x\*V\*\*e) % n)

else:

print("НЕ успех: ",y\*\*2, (x\*(V\*\*e)) % n)

n, s, V = f0()

x, r = f1(n, s)

e = f2()

y = f3(n, e, r, s)

f4(x, y, e, n, V)