МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

ОНК «Институт высоких технологий»

ОТЧЁТ

о прохождении учебной практики по получению первичных

профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности

на базе Высшей школы компьютерных наук и прикладной математики образовательно-научного кластера "Институт высоких технологий"

Выполнил Гервятович Олег Игоревич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

студент очной формы обучения 3 курса

специальности 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Руководитель практики от университета

доцент ОНК «ИВТ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Киршанова Е.А.

г. Калининград 2023 г.

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc139826562)

[ВВЕДЕНИЕ 3](#_Toc139826563)

[ОСНОВНАЯ ЧАСТЬ 4](#_Toc139826564)

[ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ 4](#_Toc139826565)

[ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ 4](#_Toc139826566)

[2.1. Решение задачи 4](#_Toc139826567)

[2.2 Верстка презентации 6](#_Toc139826568)

[2.3 Загрузка на github 7](#_Toc139826569)

[ЗАКЛЮЧЕНИЕ 8](#_Toc139826570)

[СПИСОК ЛИТЕРАТУРЫ 9](#_Toc139826571)

[Приложения 10](#_Toc139826572)

# ВВЕДЕНИЕ

Вид практики – учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности, далее Учебная практика.

Цель учебной практики: Сформировать и укрепить навыки владения системой верстки документов LaTeX, системой управления версиями git. Также укрепить навыки владения языком программирования python при решении поставленной задачи.

Помимо целей, представленных выше, важной задачей является сформировать умение применять полученные теоретические знания для решения практических задач.

Для того, чтобы достичь поставленных целей, были поставлены задачи:

1. Решить любую из задач в разделе CTF Archive на сайте cryptohack.org, используя любой удобный язык программирования, а также, основываясь на теоретических знаниях, полученных за период обучения.
2. Сформировать презентацию в системе верстки документов LaTeX с подробным описанием сути задачи и методах ее решения.
3. Создать открытый git-репозиторий с исходными кодами презентации и самого решения.

# ОСНОВНАЯ ЧАСТЬ

# ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

**Задание 1.** Решить задачу kaitenzushi (HackTM CTF) на сайте cryptohack.org, используя язык программирования sage.

**Задание 2.** Сформировать презентацию, описывающую решение, с помощью системы LaTeX.

**Задание 3.** Создать открытый git-репозиторий и загрузить в него исходные коды решения и презентации. Ссылку на репозиторий предоставить руководителю.

# ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ

# 2.1. Решение задачи

Даны 2 файла: chall.sage (исходный код алгоритма kaitenzushi) и output.txt (полученные данные в ходе выполнения алгоритма). Найти значение флага, использующееся в алгоритме.

Исходный код условия задачи в приложении 1.

В файле chall.sage даны простые числа p и q, длиной 768 бит; экспонента шифрования e, являющаяся простым числом, длиной 256 бит; , - первый и второй элемент вектора x; , - первый и второй элемент вектора y. Также указаны следующие условия:

В данном алгоритме выполняются следующие действия. Сначала находят переменную n (выводим её в output.txt) произведением чисел p и q. Далее идёт шифрование флага с помощью RSA. Результат шифрования присваиваем переменной c (выводим её в output.txt). После этого выбираем случайное значение в поле вещественных чисел по модулю 1337 в диапазоне. Следом создаётся матрица R (размером 2x2) со следующими значениями:

В конце находим новые векторы x (произведение старого вектора x на матрицу R) и y (произведение старого вектора y на матрицу R) и выводим их в output.txt.

Для решения задачи был выбран язык программирования sage, как наиболее удобный для решения задачи, при решении задачи использовалась библиотека ***Crypto.Util.number*** для преобразования числа в байты. Условно программу можно разделить на две части: ротация и факторизация. Исходный код решения представлен в приложении 2.

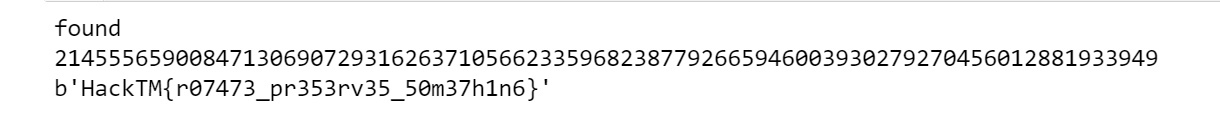


Рисунок 2. Вывод программы после выполнения



Рисунок 3. Решение принято системой cryptohack.org

# 2.2 Верстка презентации

Для верстки презентации можно было бы установить программное обеспечение, поддерживающее LaTeX, однако, было принято решение использовать отрытую платформу Overleaf. Ее главным преимуществом является бесплатность, удобность, поскольку не нужно устанавливать никакого дополнительного программного обеспечения, работа проходит в онлайн режиме. Исходный код презентации в приложении 3.

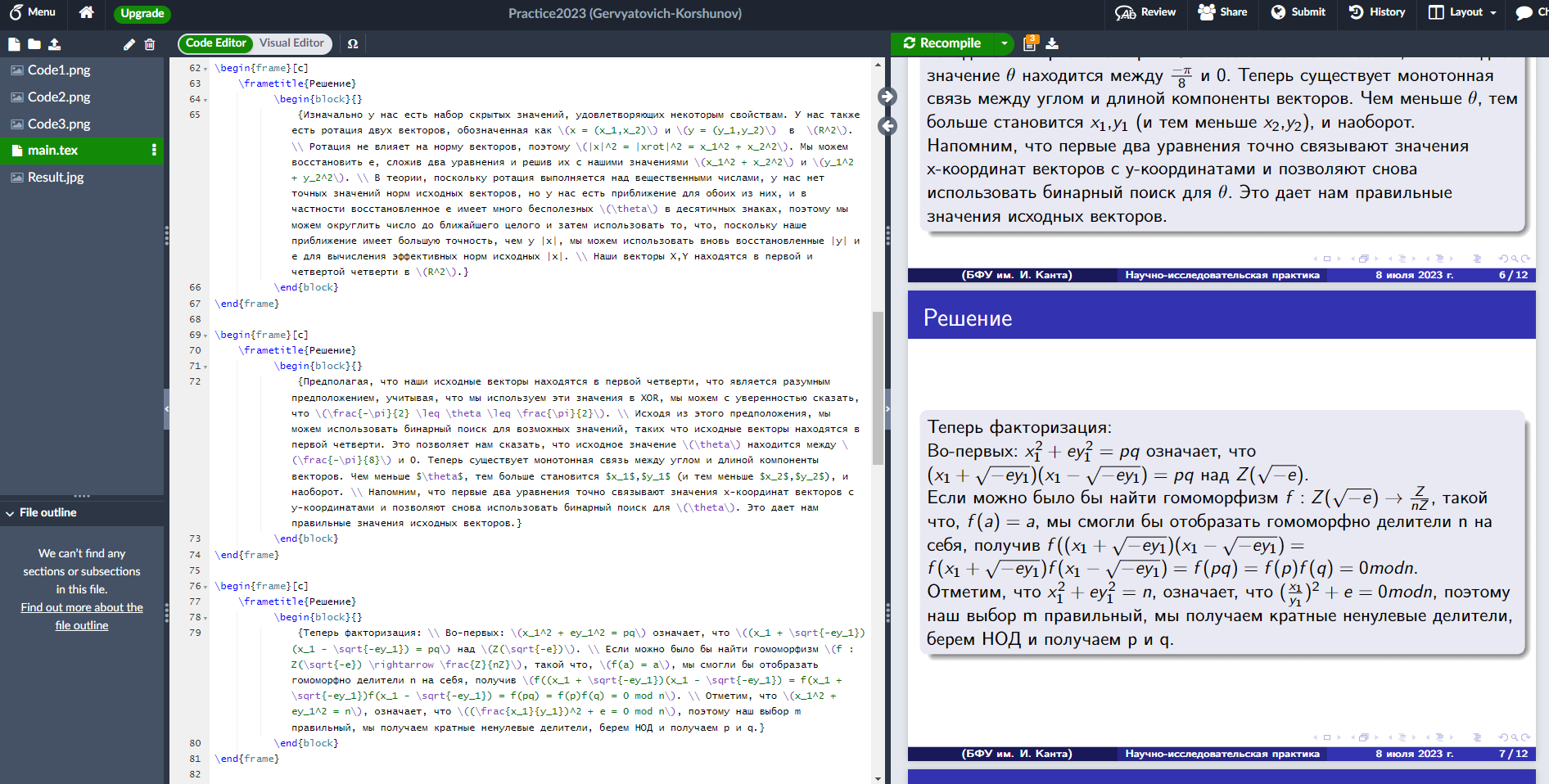


Рисунок 4. Интерфейс Overleaf

Также у Overleaf есть собственное руководство с видео-уроками, из-за чего обучение протекало быстро и понятно.

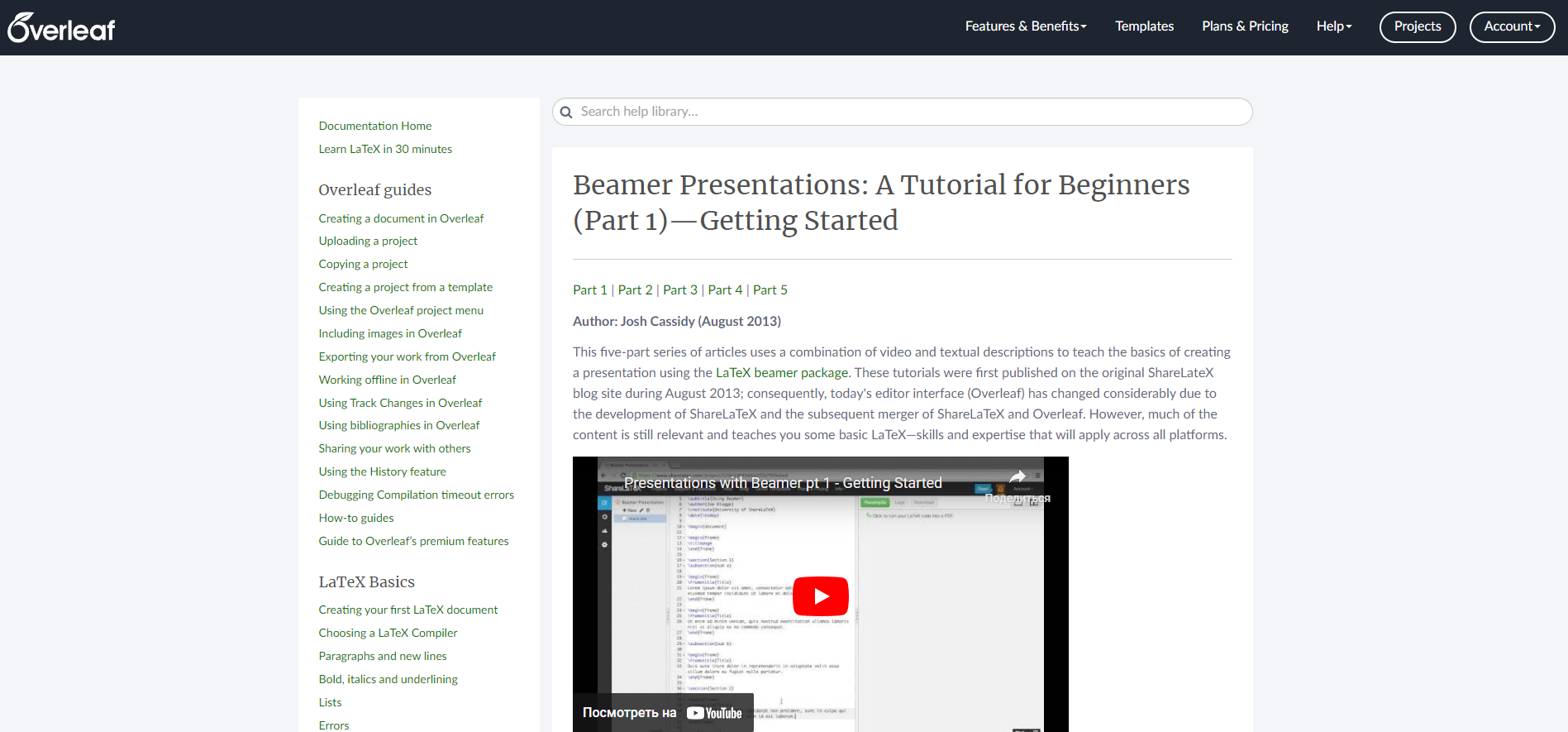
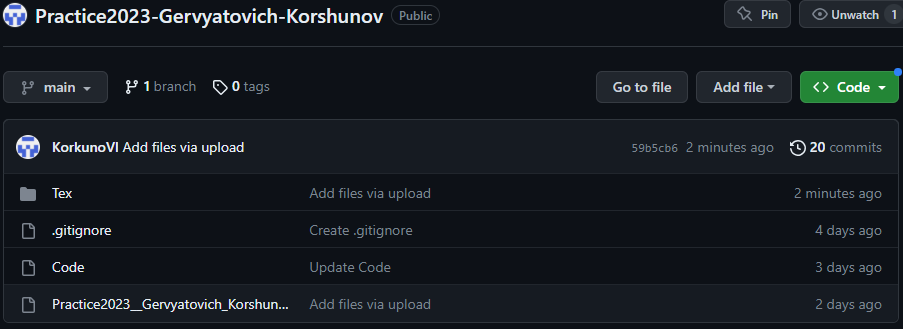


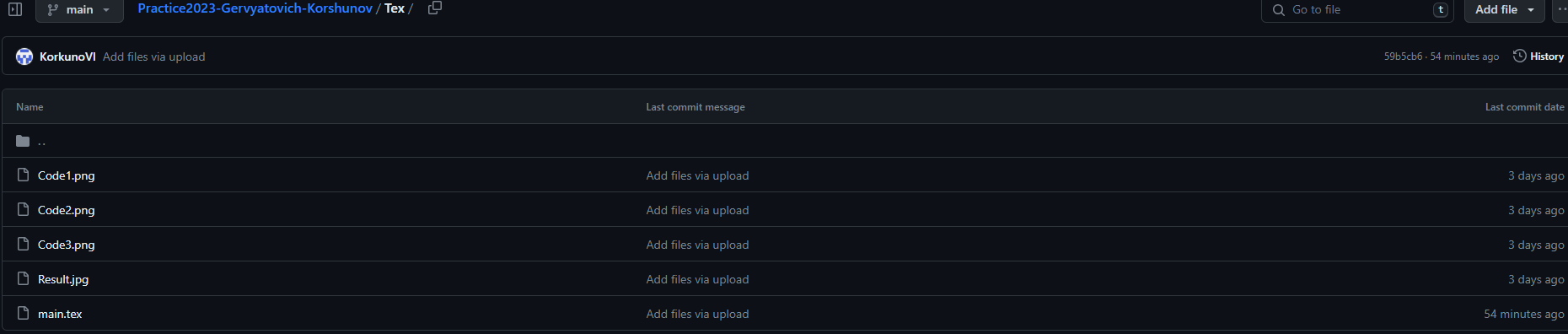
Рисунок 5. Руководство Overleaf

# 2.3 Загрузка на github

На сайте github.com создаю открытый репозиторий, в который добавляю презентацию, решение задачи и папку с исходными файлами презентации.



Рисунки 6. Онлайн репозиторий



Рисунки 7. Папка с исходными материалами

Репозиторий доступен по ссылке: <https://github.com/KorkunoVl/Practice2023-Gervyatovich-Korshunov>

# ЗАКЛЮЧЕНИЕ

В течение учебной практики все поставленные задачи были выполнены, цели достигнуты.

Я укрепил свои навыки программирования на python. Также улучшил навыки работы с LaTeX, git и github.

Помимо этого, навыки исследовательской и научной деятельности были укреплены, удалось применить теоретические знания на практике.

# СПИСОК ЛИТЕРАТУРЫ

**Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

1. Официальный сайт Overleaf с видео-уроками - <https://www.overleaf.com/learn/latex/Beamer_Presentations%3A_A_Tutorial_for_Beginners_(Part_1)%E2%80%94Getting_Started>
2. Условие решаемой задачи - https://cryptohack.org/challenges/ctf-archive/

# Приложения

Приложение 1

import os

from math import gcd

from Crypto.Util.number import bytes\_to\_long, isPrime

from secret import p, q, x1, y1, x2, y2, e

flag = os.environ.get("FLAG", "FAKEFLAG{THIS\_IS\_FAKE}").encode()

# properties of secret variables

assert isPrime(p) and p.bit\_length() == 768

assert isPrime(q) and q.bit\_length() == 768

assert isPrime(e) and e.bit\_length() == 256

assert gcd((p - 1) \* (q - 1), e) == 1

assert x1.bit\_length() <= 768 and x2.bit\_length() <= 768

assert y1.bit\_length() <= 640 and y2.bit\_length() <= 640

assert x1 \*\* 2 + e \* y1 \*\* 2 == p \* q

assert x2 \*\* 2 + e \* y2 \*\* 2 == p \* q

# encrypt flag by RSA, with xor

n = p \* q

c = pow(bytes\_to\_long(flag) ^^ x1 ^^ y1 ^^ x2 ^^ y2, e, n)

print(f"{n = }")

print(f"{c = }")

# hints 🍣

F = RealField(1337)

x = vector(F, [x1, x2])

y = vector(F, [y1, y2])

# rotate

theta = F.random\_element(min=-pi, max=pi)

R = matrix(F, [[cos(theta), -sin(theta)], [sin(theta), cos(theta)]])

x = R \* x

y = R \* y

print(f"{x = }")

print(f"{y = }")

Приложение 2

from Crypto.Util.number import long\_to\_bytes

n = 990853953648382437503731888872568785013804329239290721076418541795771569507440261620612308640652961121590348037236708702361580700250705591203587939980126323233833431892076634892318387020242015741789265095380967467201291693288654956012435416445991341222221539511583706970342630678909437274145759598920314784293470918464283814408418704426938549136143925649863711450268227592032494660523680280136089617838412326902639568680941504799777445608524961048789627301462833

c = 312168688094168684887530746663711142224819184527420449851136749248641895825646649162310024737395663075921549510262779965673286770730468773215063305158197748549937395602308558217528064655976647148323981103647078862713773074121667862786737690376212246588956833193632937835958166526006128435536115531865213269197137648990987207140262543956087199861542889002996727146832659889656384027201202873352819689303456895088190857667281342371263570535523695457095802010885279

rot\_x = (9.93659400123277470926327676478883140697376509010297766512845139881487348637477791719517951397052010880811619509960535668814993293095146708957649613776125686226138447162258666762024346093786649228730054881453449071976210130217897905782845690384638460560301964009359233596889465133986468021963885911072779457835979983964294586954038412718305000570678333513135467257498071686562749882446495426493483289204e230, -1.20540611958254673086539287012513674064476659427085664430224592760592531301348857885707154893714440960111029743010026152632150988429192286517249118913535366887447596463819555191858702861383725310592687577510708180057642425944345656558038998574368521689142109798891989865473206201635908814994474491537093810680632691594902962470061189337645818851446622588020765058461348047229165216450857822980873846637e230)

rot\_y = (9.02899744041999015549480362358897037217795303901085937071039171882835297563545959015336648016772002396355451308252077767567617065937943765701645833054147976124287566465577491039263554806622908070370269238064956822205986576949383035741108310668397305286076364909407660314991847716094610949669608550117248147017329449889127749721988228613503029640191269319151291514601769696635252288607881829734506023770e191, 2.82245306887391321716872765000993510002376761684498801971981175059452895101888694909625866715259620501905532121092041448909218372087306882364769769589919830746245167403566884491547911250261820661981772195356239940907493773024918284094309809964348965190219508641693641202225028173892050377939993484981988687903270349415531065381420872722271855270893103191849754016799925873189392548972340802542077635974e192)

F = RealField(1337)

rot\_x = vector(F, rot\_x)

rot\_y = vector(F, rot\_y)

nxsq\_old =rot\_x \* rot\_x

nysq\_old =rot\_y \* rot\_y

e = (2\*n - nxsq\_old) / nysq\_old

e = ZZ(QQ(e.numerical\_approx(prec = 700, digits = 400)))

nysq = ZZ(nysq\_old.round())

nxsq = ZZ(2\*n - e\*nysq)

lb = -pi/2

up = pi/2

theta = (lb+up) / 2

R = matrix(F, [[cos(theta), -sin(theta)], [sin(theta), cos(theta)]])

Rinv = R^-1

newx = Rinv \* vector(rot\_x)

newy = Rinv \* vector(rot\_y)

tmpx1 = round(newx[0])

tmpx2 = round(newx[1])

tmpy1 = round(newy[0])

tmpy2 = round(newy[1])

if (tmpx2 < 0 or tmpy2 < 0):

up = theta

elif (tmpx1 < 0 or tmpy1 < 0):

lb = theta

elif (tmpx1.nbits() >768 or tmpy1.nbits()>640):

up = theta

elif (tmpx2.nbits() >768 or tmpy2.nbits()>640):

lb = theta

for j in range(8000):

theta = (lb+up) / 2

R = matrix(F, [[cos(theta), -sin(theta)], [sin(theta), cos(theta)]])

Rinv = R^-1

newx = Rinv \* vector(rot\_x)

newy = Rinv \* vector(rot\_y)

tmpx1 = round(newx[0])

tmpx2 = round(newx[1])

tmpy1 = round(newy[0])

tmpy2 = round(newy[1])

lhs1 = tmpx1^2 + e\*tmpy1^2

lhs2 = tmpx2^2 + e\*tmpy2^2

if (lhs1 > n or lhs2 <n):

up = theta

else:

lb = theta

if (abs(lhs1 - n) == 0 and abs(lhs2 - n)==0):

print("found")

x1 = tmpx1

x2 = tmpx2

y1 = tmpy1

y2 = tmpy2

break

assert x1.nbits() <= 768 and x2.nbits() <= 768

assert y1.nbits() <= 640 and y2.nbits() <= 640

assert x1 \*\* 2 + e \* y1 \*\* 2 == n

assert x2 \*\* 2 + e \* y2 \*\* 2 == n

assert x1^2 + x2^2 == nxsq

assert y1^2 + y2^2 == nysq

tmp = int(x1 \* pow(y1, -1, n))

assert((tmp^2 + e) % n == 0)

pfake =(x2 + tmp\*y2) % n

qfake =(x2 - tmp\*y2) % n

p = gcd(pfake, n)

q = n//p

phi = (p-1)\*(q-1)

d = pow(e, -1, phi)

m = pow(c, d, n)

m = int(m) ^^ x1 ^^ x2 ^^ y1 ^^ y2

print(m)

print(long\_to\_bytes(m))

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

ОНК «Институт высоких технологий»

ДНЕВНИК

учебной практики по получению первичных

профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности

г. Калининград 2023 г.

**1.Информационная часть**

Гервятович Олег Игоревич студент очной формы обучения 3 курса группы 05\_КБ\_20\_О\_/ специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» в соответствии с приказом №2218-ст от 06 июня 2023 г. направляется на учебную практику по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности в Высшую школу компьютерных наук и прикладной математики образовательно-научного кластера "Институт высоких технологий".

Период практики – с 26.062023 г. по 08.07.2023 г.

Руководитель практики от университета – доцент ОНК «ИВТ» Киршанова Елена Алексеевна.

ОНК «Институт высоких технологий»

Контактный номер телефона +7 (4012) 338 217

Первый заместитель

директора ОНК «ИВТ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шпилевой А.А.

**2. Программа практики**

**2.1. План работы**

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Рабочее место практиканта, вид работы** | **Продолжительность**  **(в днях)** |
| **1.** | Компьютерный класс, ауд. 230 | **14** |
|  |  |  |
|  |  |  |

**2.2. Индивидуальное задание по профилю подготовки/специальности**

1. Пройти инструктаж по технике безопасности.
2. Ознакомиться и выполнить задачи на практику.
3. Написать отчет по практике.

Руководитель практики от университета

доцент ОНК «ИВТ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Киршанова Елена Алексеевна

**3. Ход выполнения практики**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п.п.** | **Дата** | **Описание выполненной работы** | **Отметки**  **руководителя практики от профильной организации** |
| 1 | 26.06.2023 | Пройден инструктаж по технике безопасности |  |
| 2 | 27.06.2023-30.06.2023 | Решение задачи. Написание программы на языке программирования Python |  |
| 3 | 06.07.2023 | Создание презентации на основе системы верстки LaTeX |  |
| 4 | 06.07.2023 | Создание открытой онлайн репозитории с исходным кодом презентации и решения |  |
| 5 | 07.07.2023 | Подготовка отчета по учебной практике |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**4. Отзыв руководителя практики**

Гервятович Олег Игоревич студент очной формы обучения 3 курса группы 05\_КБ\_20\_О\_/ специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» в соответствии с приказом №2218-ст от 06 июня 2023 г. направляется на учебную практику по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности в Высшую школу компьютерных наук и прикладной математики образовательно-научного кластера "Институт высоких технологий".

Период практики – с 26.06.2023 г. по 08.07.2023 г.

Программа практики и индивидуальное задание на практику выполнены. Отчёт по практике сдан и защищён на отчётной конференции.

Студент Гервятович Олег Игоревич в процессе прохождения практики справился с поставленными задачами, приобрёл первичные профессиональные навыки и компетенции, в том числе:

* способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
* способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.

Учебная практика оценена на оценку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики от университета –

доцент ОНК «ИВТ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Киршанова Елена Алексеевна

«08» июля 2023 г.