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 Воробьёв Денис Кириллович \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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](#_Toc139572109)

[ВВЕДЕНИЕ 3](#_Toc139572110)

[ОСНОВНАЯ ЧАСТЬ 4](#_Toc139572111)

[ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ 4](#_Toc139572112)

[ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ 4](#_Toc139572113)

[2.1. Решение задачи 4](#_Toc139572114)

[2.2 Верстка презентации 6](#_Toc139572115)

[2.3 Загрузка на github 7](#_Toc139572116)

[ЗАКЛЮЧЕНИЕ 8](#_Toc139572117)

[СПИСОК ЛИТЕРАТУРЫ 9](#_Toc139572118)

[Приложения 10](#_Toc139572119)

# 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 1n\_jection (Zh3r0 CTF V2) на сайте cryptohack.org, используя язык программирования python

**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

Дана программа, шифрующая исходное сообщение с помощью оригинального рекурсивного алгоритма. Также дан файл с выводом представленной программы. Конкретно: зашифрованное сообщение *c*. Необходимо расшифровать исходное сообщение.

Исходный код условия задачи в приложении 1.

Анализ кода зашифровывающей функции позволяет нам понять, как формируется выходное сообщение на непоследних слоях рекурсии и какой вид имеет вывод последнего слоя. На основании этих соображений выводится ряд элементарных соотношений, с помощью которых создаётся алгоритм обращения зашифровывающей функции. Вообще говоря, задача “главного” цикла нашей дешифрующей функции – аппроксимация суммы выходных данный следующих слоёв рекурсии в зашифровывающей функции для подъёма к более верхним слоям и, в конечном итоге, возвращения к входным данным зашифровывающей функции.

Для решения задачи был выбран язык программирования python, как самый простой и удобный в использовании, также, установка и подключение нестандартных библиотек осуществляется быстро и просто, при решении задачи использовалась библиотеки ***gmpy2*** для извлечения квадратного корня. Условно программа делится на две части: основной цикл, вычисляющий выводы двух предшествующих слоев рекурсии шифрующей функции, и отрезок кода, отвечающий за переход к следующим слоям рекурсии дешифрующей функции. Исходный код решения представлен в приложении 2.

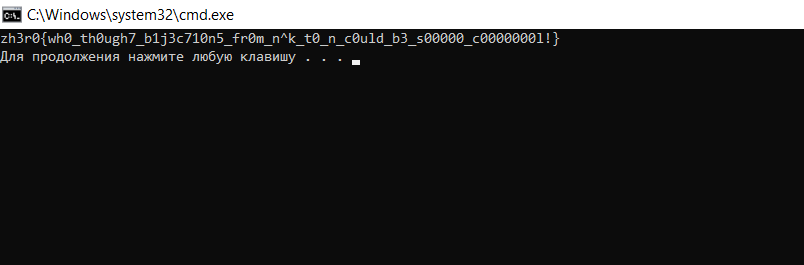


Рисунок 1. Вывод программы после выполнения

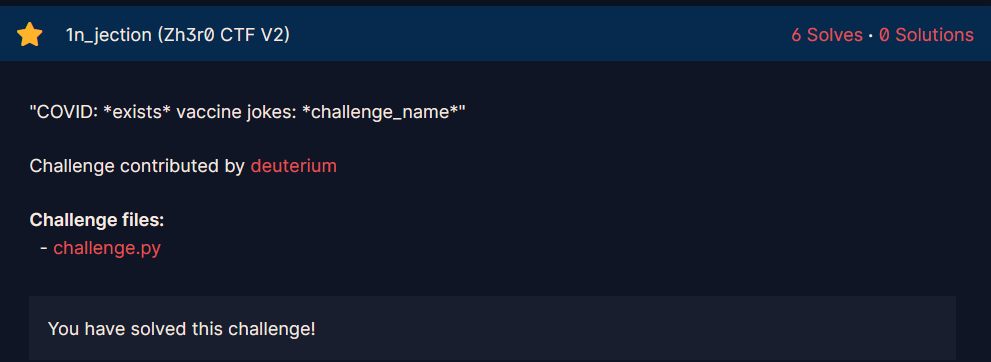


Рисунок 2. Решение принято системой cryptohack.org

# 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.

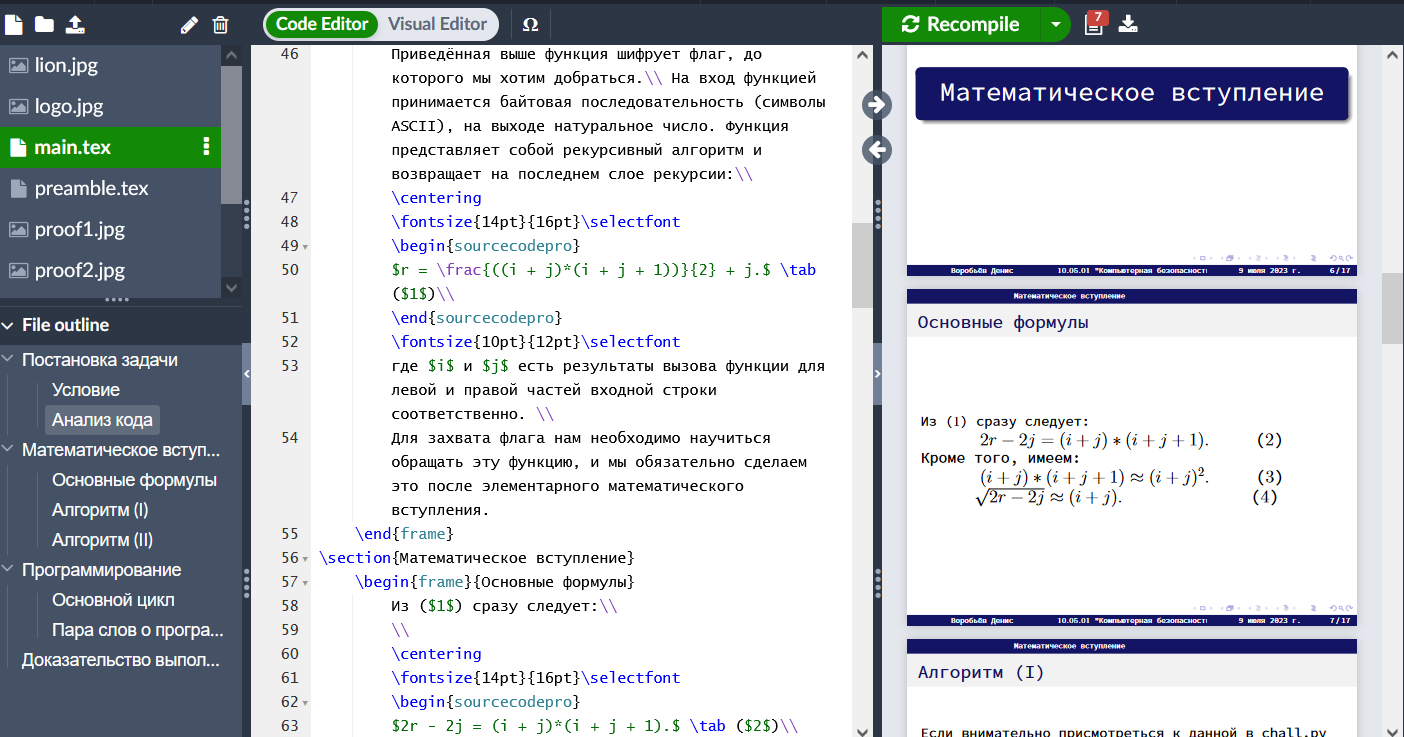


Рисунок 3. Интерфейс Overleaf

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

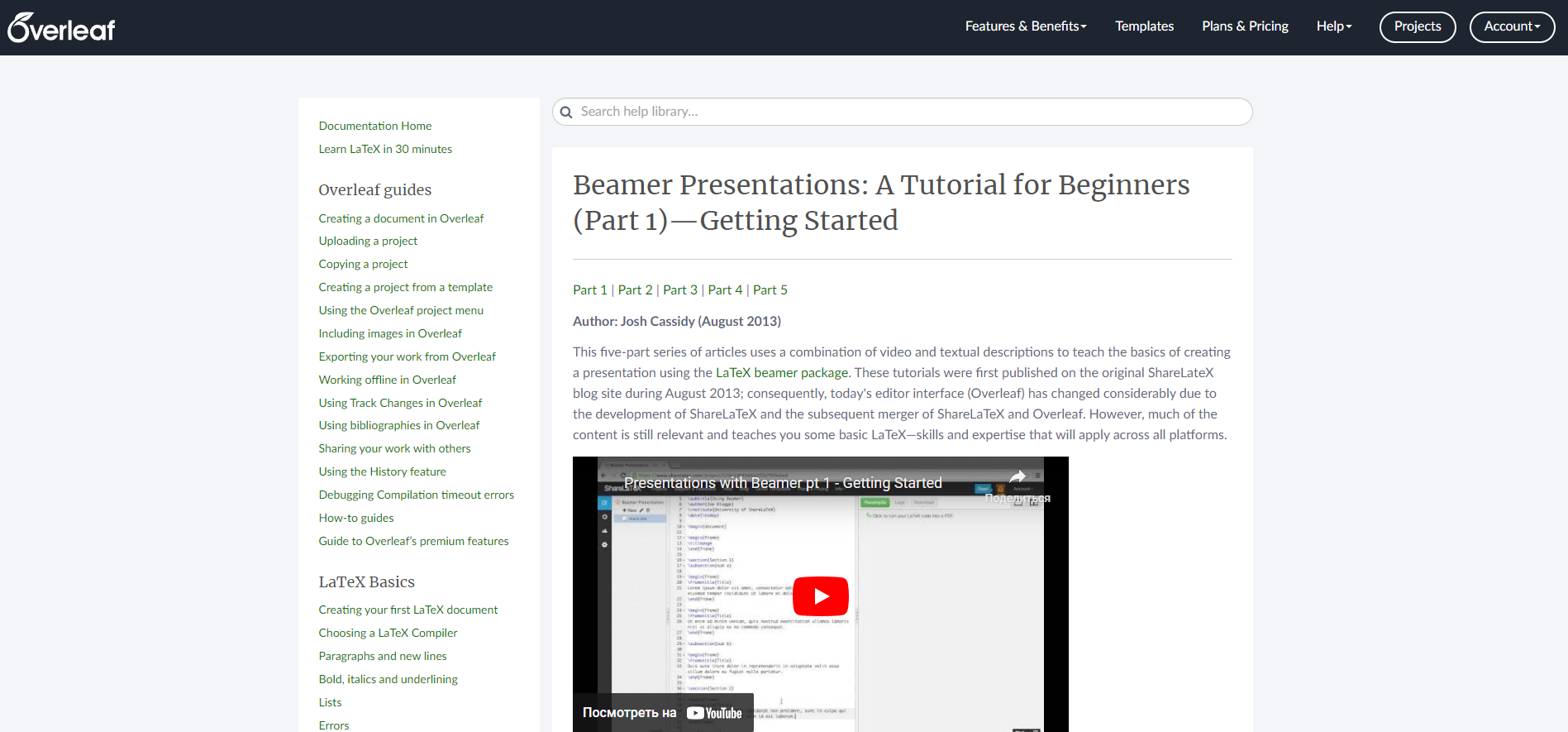


Рисунок 4. Руководство Overleaf

# 2.3 Загрузка на github

На сайте github.com создаю открытый репозиторий, после чего с помощью опций графического интерфейса github добавляю все необходимые файлы.

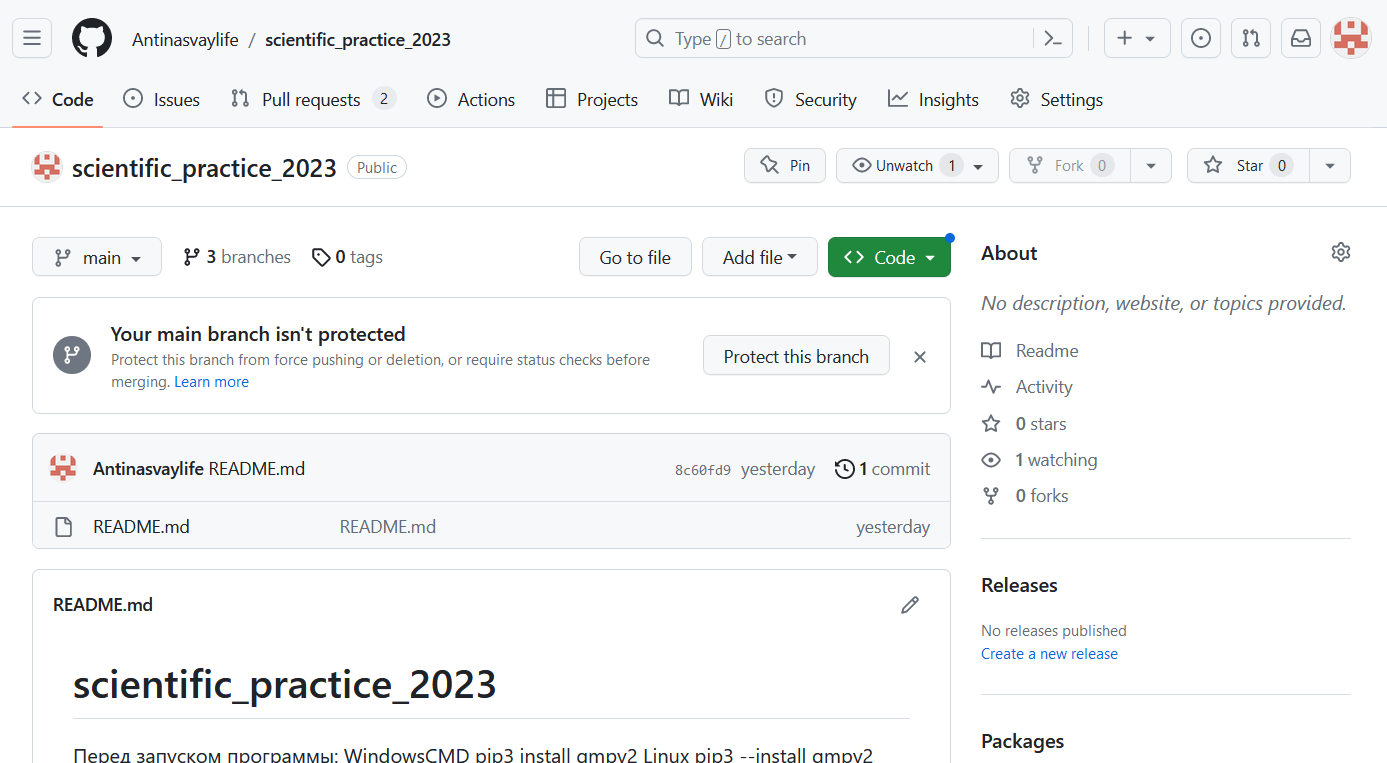
******

Рисунок 5. Интерфейс GitHub

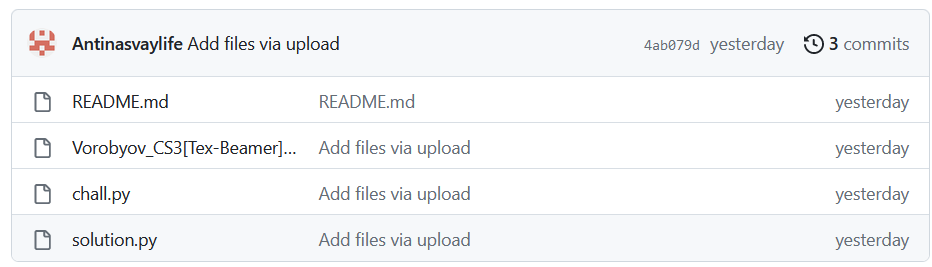


Рисунок 6. Онлайн репозиторий

Репозиторий доступен по ссылке: <https://github.com/Antinasvaylife/scientific_practice_2023>

# 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/
3. Официальный сайт git - [https://git-scm.com/](https://git-scm.com/%20)
4. Официальная документация git - <https://git-scm.com/docs>

# Приложения

Приложение 1

from secret import flag

def nk2n(nk):

l = len(nk)

if l==1:

return nk[0]

elif l==2:

i,j = nk

return ((i+j)\*(i+j+1))//2 +j

return nk2n([nk2n(nk[:l-l//2]), nk2n(nk[l-l//2:])])

print(nk2n(flag)) #2597749519984520018193538914972744028780767067373210633843441892910830749749277631182596420937027368405416666234869030284255514216592219508067528406889067888675964979055810441575553504341722797908073355991646423732420612775191216409926513346494355434293682149298585

Приложение 2

import gmpy2

# enc - зашифрованная строка

# dep - глубина рекурсии

def inv\_nk2n(enc,dep):

if enc < 128:

# отрезок строки соответствует ascii символу

print(chr(enc))

return

# полагаем e = sqrt(2r)

e, nul = gmpy2.iroot(2 \* enc, 2) # функция iroot возвращает ненужный bool вторым аргументом

# округляем e вниз

e = int(e)

while True:

# аппроксимация j

j = (2 \* enc - (e \* (e + 1))) // 2

if j < 0:

e = e - 1

continue

# вычисление е'

e1, nul = gmpy2.iroot(2 \* enc - 2 \* j, 2)

if e == e1:

i = e - j

# проверка равенства (1)

assert ((i + j) \* (i + j + 1)) // 2 + j == enc

break

e = e - 1

# переход на следующий слой

if i < 128:

print(chr(i), end = "")

print(chr(j), end = "")

return

elif j < 128:

inv\_nk2n(i, dep + 1)

print(chr(j), end = "")

else:

inv\_nk2n(i, dep + 1)

inv\_nk2n(j, dep + 1)

# условие задачи

enc = 2597749519984520018193538914972744028780767067373210633843441892910830749749277631182596420937027368405416666234869030284255514216592219508067528406889067888675964979055810441575553504341722797908073355991646423732420612775191216409926513346494355434293682149298585

inv\_nk2n(enc,0)

print()

Приложение 3

\documentclass[11pt]{beamer} % Определяем тип документа как презентацию

% в квадратных скобках размер шрифта: 8pt, 9, 10, 11 (def), 12, 14, 17, 20.

\input{preamble}

% В преамбуле можно сделать небольшие изменения (цвет, шрифт итд.) Если есть желание изменить больше, возможно, проще выбрать другой шаблон.

\newcommand\tab[1][1cm]{\hspace\*{#1}}

% Начнем работу с презентацией

%Для начала подготовим титульный лист и оглавление

\input{title}

\begin{document} % начнем саму презентацию

\frame{\titlepage} % сделаем титульный слайд и оглавление:

\begin{frame}

\frametitle{Оглавление}

\tableofcontents

\end{frame}

% Далее начнем работу со слайдами:

\section{Постановка задачи}

\begin{frame}{Условие}

Файл chall.py содержит только одну функцию \\

и только один зашифрованный флаг\\

\begingroup

\fontsize{14pt}{16pt}\selectfont

\begin{sourcecodepro}

def nk2n(nk):\\

\tab l = len(nk)\\

\tab if l == 1:\\

\tab[2cm] return nk[0]\\

\tab elif l==2:\\

\tab[2cm] i,j = nk\\

\tab[2cm] return ((i+j)\*(i+j+1))//2 +j\\

\tab return nk2n([nk2n(nk[:l-l//2]), nk2n(nk[l-l//2:])])\\

\end{sourcecodepro}

\endgroup

\end{frame}

\begin{frame}{Анализ кода}

Приведённая выше функция шифрует флаг, до которого мы хотим добраться.\\ На вход функцией принимается байтовая последовательность (символы ASCII), на выходе натуральное число. Функция представляет собой рекурсивный алгоритм и возвращает на последнем слое рекурсии:\\

\centering

\fontsize{14pt}{16pt}\selectfont

\begin{sourcecodepro}

$r = \frac{((i + j)\*(i + j + 1))}{2} + j.$ \tab ($1$)\\

\end{sourcecodepro}

\fontsize{10pt}{12pt}\selectfont

где $i$ и $j$ есть результаты вызова функции для левой и правой частей входной строки соответственно. \\

Для захвата флага нам необходимо научиться обращать эту функцию, и мы обязательно сделаем это после элементарного математического вступления.

\end{frame}

\section{Математическое вступление}

\begin{frame}{Основные формулы}

Из ($1$) сразу следует:\\

\\

\centering

\fontsize{14pt}{16pt}\selectfont

\begin{sourcecodepro}

$2r - 2j = (i + j)\*(i + j + 1).$ \tab ($2$)\\

\end{sourcecodepro}

\raggedright

\fontsize{12pt}{14pt}\selectfont

\begin{sourcecodepro}

Кроме того, имеем: \\

\end{sourcecodepro}

\centering

\fontsize{14pt}{16pt}\selectfont

\begin{sourcecodepro}

$(i + j)\*(i + j + 1) \approx (i + j)^{2}.$ \tab ($3$)\\

$\sqrt{2r - 2j} \approx (i + j).$ \tab[3.04cm] ($4$)

\end{sourcecodepro}

\end{frame}

\begin{frame}{Алгоритм (I)}

\raggedright

Если внимательно присмотреться к данной в chall.py функции, становится ясно, что до финального слоя рекурсии доходит последовательность из двух чисел. С этого мы и начнём дешифрование.\\

Положим $enc := r$.\\

Заметим $\sqrt{2enc} = \sqrt{(i + j)\*(i + j + 1) + 2j}$.\\

Сейчас мы будем аппроксимировать $i + j$ с помощью $\sqrt{2enc}$ следующим способом.\\ Из формулы ($2$): $j = \frac{2r - (i + j)^2 - (i+j)}{2} = \frac{2enc - (i + j)^2 - (i+j)}{2}.$ \\

Перейдём, положив $e = \lfloor\sqrt{2enc}\rfloor$, к $j\_{k} = \frac{2enc - (e - k)\*((e - k) + 1)}{2}.$ \\ Начиная с некоторого $k$ выполняется: $j\_{k} > 0.$

\end{frame}

\begin{frame}{Алгоритм (II)}

Теперь положим $e' = \sqrt{2\*enc - 2\*j\_{k}}.$\\

Если $e' = e\_{k}$, то из формулы ($4$) имеем $e' = \sqrt{2\*enc - 2\*j\_{k}} = e\_{k} \approx (i + j)$, полагая теперь $i = e\_{k} - j\_{k}$ проверяем формулу ($1$).\\ Если ($1$) не выполняется, возвращаемся в начало цикла, инкрементируя $k = k + 1$.

\end{frame}

\section{Программирование}

\begin{frame}{Основной цикл}

\begingroup

\fontsize{10pt}{12pt}\selectfont

\begin{sourcecodepro}

e, nul = gmpy2.iroot(2 \* enc, 2)\\

e = int(e)\\

while True:\\

\tab j = (2 \* enc - (e \* (e + 1))) // 2\\

\tab if j < 0:\\

\tab[2cm] e = e - 1\\

\tab[2cm] continue\\

\tab e1, nul = gmpy2.iroot(2 \* enc - 2 \* j, 2)\\

\tab if e == e1:\\

\tab[2cm] i = e - j\\

\tab[2cm] assert ((i + j) \* (i + j + 1)) // 2 + j == enc\\

\tab[2cm] break\\

\tab e = e - 1\\

\end{sourcecodepro}

\endgroup

\end{frame}

\begin{frame}{Пара слов о программе}

\fontsize{10pt}{12pt}\selectfont

Во-первых, нетрудно заметить, что "существующего в теории" счётчика $k$ в основном цикле нет. Дело в том, что на практике он оказался просто не нужен. Вычитать из $e$ единицу на каждом шаге можно и без него, а хранить последовательность $j\_{k}$ или даже сам счётчик счётчик $k$ - бесполезно.\\

Во-вторых, появилась странная переменная nul в двух местах. Спешу успокоить читателя: она нужна лишь потому, что функция iroot() возвращает два значения - собственно корень нужной степени и значение типа bool, истинность которого говорит о существовании вещественного корня.\\

В-третьих, в презентации не представлен полный код программы. На это мы пошли умышленно: для лаконичности, связности повествования, а ещё потому, что остальной код является сугубо служебным и не представляет большого интереса с точки зрения криптографии.

\end{frame}

\section{Доказательство выполнения работы}

\begin{frame}

\includegraphics{proof1}

\end{frame}

\begin{frame}

\includegraphics{proof2}

\end{frame}

\section\*{}

\begin{frame}

\centered

Код программы и этот документ находятся в GitHub: \\

\href{https://github.com/Antinasvaylife/scientific\_practice\_2023}{--> нажмите на меня <--}

\end{frame}

\section\*{}

\begin{frame}

\textcolor{darkblueNES}{\Huge{\centerline{Спасибо за внимание!}}}

\end{frame}

\end{document}

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**

Воробьёв Дени с Кириллович 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**

Воробьёв Денис Кириллович 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 Воробьёв Денис Кириллович 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.