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 Орлов Михаил Дмитриевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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**

Введение

Глава 1. Выбор подходящего задания

Глава 2. Решение задания

Заключение

Список литературы

Приложения

**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: решение одной из сложных задач, представленных в разделе CTF Archive сайта CryptoHack

Задачи учебной практики:

1. Выбор подходящего задания
2. Постановка задачи
3. Подготовка необходимых ресурсов
4. Решение задачи
5. Подготовка презентации

**ГЛАВА 1. ВЫБОР ПОДХОДЯЩЕГО ЗАДАНИЯ**

Для прохождения практики нашей группе было необходимо выбрать одну из сложных задач, представленных в разделе CTF Archive сайта CryptoHack, а также решить проблемы, возникающие на пути её решения.

Поскольку представленные в этом разделе задачи обладали достаточно высокой сложность, уже на этом этапе возникли сложности и решить получилось лишь задачу выбранную третьей, в частности – задачу под названием Unimplemented (TETCTF) от автора NDH.

Сама задача представляла собой программу на языке Python, реализующая алгоритм шифрования RSA при помощи гауссовых целых, а также набор, состоящий из публичного и приватного ключа, а также шифротекста, содержащего флаг, необходимый для выполнения задачи. Для его получения необходимо было дополнить полученную программу функцией дешифровки, что и стало основным препятствием на нашем пути.

**ГЛАВА 2. РЕШЕНИЕ ЗАДАНИЯ**

В ходе решения этой задачи основной сложностью было определение различий между обычным алгоритмом RSA и тем, что нам необходимо было реализовать. В частности, в контексте гауссовых целых чисел несколько иначе определялась phi (функция Эйлера) от модуля N.

В привычном нам RSA выбирались простые числа P и Q, определялся модуль N = P \* Q, функция phi(N) определялась как (P – 1) \* (Q – 1), после чего уже выбирался публичный ключ e и находился приватный ключ d. В нашем же алгоритме N = и, соответственно , однако функция Эйлера для гауссовых целых имеет следующий вид - , где –нормальная функция (a,b – коэффициенты действительной и мнимой части соответственно). Отсюда получаем - . Таким образом, , остальное же, в свою очередь осталось неизменным. После модифицирования этой части, оставалось лишь запрограммировать алгоритм дешифровки по аналогии с RSA.

Также во время решения задачи возникало множество мелких проблем с программной реализацией алгоритма, вроде некорректной работы библиотеки Crypto.Util.number в используемой изначально среде разработке Pycharm, не стоящих однако отдельного упоминания.

**ЗАКЛЮЧЕНИЕ**

В течение практики все задачи были выполнены, а цели достигнуты. Кроме того, были улучшены наши навыки решения криптографических задач, программирования и работы с интернет-ресурсами

**СПИСОК ЛИТЕРАТУРЫ**

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

1. Сайт Wikipedia Гауссовы целые числа – режим доступа: https://ru.wikipedia.org/wiki/Гауссовы\_целые\_числа
2. Сайт CTF Archive – режим доступа: https://cryptohack.org/challenges/ctf-archive/
3. Сайт CryptoHack RSA – режим доступа: https://cryptohack.org/challenges/rsa/
4. Сайт «Структуры и алгоритмы». – режим доступа: http://www.structur.h1.ru/
5. Структуры и алгоритмы обработки данных: Учебное пособие. – режим доступа: <http://window.edu.ru/resource/820/44820>
6. RSA: от простых чисел до электронной подписи. – режим доступа: <https://habr.com/ru/articles/534014/>
7. Основы программирования – режим доступа: http://www.intuit.ru/studies/courses/648/504/info
8. Видеолекции по курсу “Основы программирования”. – режим доступа: <http://www.youtube.com/watch?v=pxR3UoO9c9w>
9. Документация PyCryptodome. – режим доступа: <https://www.pycryptodome.org/src/util/util>
10. Learn Python Full course – режим доступа: https://www.youtube.com/watch?v=rfscVS0vtbw

**ПРИЛОЖЕНИЯ**

**Листинг Программы**

from collections import namedtuple

from Crypto.Util.number import getPrime

import random

Complex = namedtuple("Complex", ["re", "im"])

# Умножение комплексных чисел по модулю

def complex\_mult(c1, c2, modulus):

return Complex(

(c1.re \* c2.re - c1.im \* c2.im) % modulus, # real part

(c1.re \* c2.im + c1.im \* c2.re) % modulus, # image part

)

# Возведение комплексных чисел в степень по модулю

def complex\_pow(c, exp, modulus):

result = Complex(1, 0)

while exp > 0:

if exp & 1:

result = complex\_mult(result, c, modulus)

c = complex\_mult(c, c, modulus)

exp >>= 1

return result

# Генерация приватного (p,q) и публичного (n) ключа длиной nbits

def generate\_key\_pair(nbits):

while True:

p = getPrime((nbits + 3) // 4)

q = getPrime((nbits + 3) // 4)

n = (p \*\* 2) \* (q \*\* 2)

if n.bit\_length() == nbits:

return (p, q), n

# Заполнение текста

def pad(data, length):

assert len(data) < length

pad\_length = length - len(data) - 1

pad\_data = bytes(random.choices(range(1, 256), k=pad\_length))

sep = b'\x00'

return pad\_data + sep + data

# Разделение текста

def unpad(data):

assert b"\x00" in data, "incorrect padding"

return data.split(b"\x00", 1)[1]

# Шифровка текста

def encrypt(public\_key, plaintext):

n = public\_key

plaintext = pad(plaintext, 2 \* ((n.bit\_length() - 1) // 8))

m = Complex(

int.from\_bytes(plaintext[:len(plaintext) // 2], "big"),

int.from\_bytes(plaintext[len(plaintext) // 2:], "big")

)

c = complex\_pow(m, 65537, n)

return (c.re.to\_bytes((n.bit\_length() + 7) // 8, "big")

+ c.im.to\_bytes((n.bit\_length() + 7) // 8, "big"))

# Дешифровка шифротекста

def decrypt(private\_key, ciphertext):

(p, q) = private\_key

n = (p \*\* 2) \* (q \*\* 2)

c = Complex(

int.from\_bytes(ciphertext[:len(ciphertext) // 2], "big"),

int.from\_bytes(ciphertext[len(ciphertext) // 2:], "big")

)

e = 65537

phi = (p \*\* 4 - p \*\* 2) \* (q \*\* 4 - q \*\* 2)

d = pow(e, -1, phi)

m = complex\_pow(c, d, n)

return unpad(m.re.to\_bytes((n.bit\_length() + 7) // 8, "big")

+ m.im.to\_bytes((n.bit\_length() + 7) // 8, "big"))

def main():

private\_key = (

128329415694646850105527417663220454989310213490980740842294900866469518550360977403743209328130516433033852724185671092403884337579882897537139175073013,

119773890850600188123646882522766760423725010264224559311769920026142724028924588464361802945459257237815241227422748585976629359167921441645714382651911)

ciphertext = b'\x00h\xbe\x94\x8c\xcd\xdd\x04\x80\xf4\x9d\t\xd8\x8dO\x08\xf1\xd1\xc4\xb9\xa06\xe7\xe3\xb6\xc3\x01+\xa9\xf2\xb9\xe8\x8d\xe6\xc9\x0c\_#\x93\x11\xad\x0f\x90\xd3\x0b6\xb0n\x13\xea~"V6\xdbA&\x87\xfe\xa3C\xcb\x16\xae\xd9\x83\xdbU\xc6\x06\xcd\x9a\x94\xa9\xce\x15{d\x95s\xc2\xfb\x90q\xe7\x02\xa2\x081:\_C\xc68\x00y\x7fj4@\xd2\xcdE\x06\x943\xbe\xbcC3\xca\x91\xb4\x0e}C\xab\xff?X\xc30u\x069:Dc\xb5\xdc\x9b0%\x98\xbd\xd9\x13\xc0\x02w\xc5\xe5:\xca\xcf\x0c\xab\xc2\x9b}\xab\xd0\xcc\xbc\x0f\x9e9\t\xf7M\xb3\xed\x86\xb5E\x8b\xbc4\xfaH\x9b4\x1c\xc4\xab\xc0\xaf\x8a5XcX\x19K\xed\x19\xe1\x1c\xd0\x1e\x97c\x9fF:L\x9d\x90p\x99\xb8\xde\xcblM\xb3\x80sSL\xe1\xa4\xd6,\x81\xd6\x9c\xf1\xbb\x9c)\xf03\x155\xc0\xd5v\x13\xd6#\xb7\x19\xdea%\xce<\x1c\xf7\xf2!;\xc1\xd7w\xd1\xc8\x8d/\xaew\xa1\x1d\xc5(\xc8\x9d\x82v\xf6j\x90A,e\xbd\xa7]\x10\x8f\xe5\xe7\x93}:\xdf1~\xec\xd0-o`\r\x96\xe4\x03\xb9E\x9fdF\xc3\xf8L\xa0\xda\xf0E[\xf7\x02\xef|\*\x08\x8a5pI&\xa9i\x0fZ\xa8\xb3H\xed\xe8v\xc4H\xff\xdb\xcb\x00\xf1\xae\x9bO\x18\xd5\xd8&p\xf5\xf6\xe9\xf1\x1brs\xc2\r\xceZ\xd0\xb24\x97+\x98b\x0e\xbb\xb8.\x8dT\xe4"\xad\xe4\xa3f\xd0M\xbf\xafX\xbb"[\x99\xdap\xa5\xcfT2Wx\x87M\x7f\x99!>B[Q\x04\xf6\x03\xbc\x84\xf4\xdfj\xdd1^I\x1a\x05\x81\x91\xde9Mf\*\x8e\x8d\xe64\xf8\x93\x99&yP\xcd\x00!\x82\xab\xbcy\xed\xf1\x13\xd3\x81\xeaz\xbbP>\x9a2\x8c\x08\x0es\xbc\xa9\xf6\xa3\x8c\xb0\xb9t\xd9?\x06@\xc9\x90\xb7\xa7<\x85\xeb\x1a\x88#\x1c\xc3 \xec\xc7\x94d\x99\xd6\x8e>\x06\xf8Y\xf4\x19\xcaI/hy\x18\x8e\x0e8\xf8\r\xbb\xf6\x11\xb9\x8dCWB6 '

print(decrypt(private\_key, ciphertext))

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

main()

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**

Орлов Михаил Дмитриевич, 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.

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)** |
|  |  |  |
|  |  |  |
|  |  |  |

**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 | Получение индивидуального задания |  |
| 2 | 27.06.2023 | Выбор подходящей задачи |  |
| 3 | 28.06.2023 | Распределение обязанностей в группе |  |
| 4 | 29.06.2023 | Решение задачи |  |
| 5 | 30.06.2023 | Решение задачи |  |
| 6 | 1.07.2023 | Выходной |  |
| 7 | 2.07.2023 | Решение задачи |  |
| 8 | 3.07.2023 | Решение задачи |  |
| 9 | 4.07.2023 | Подготовка презентации |  |
| 10 | 5.07.2023 | Подготовка презентации |  |
| 11 | 6.07.2023 | Оформление отчёта по практике |  |
| 12 | 7.07.2023 | Оформление отчёта по практике |  |
| 13 | 8.07.2023 | Выходной |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**4. Отзыв руководителя практики**

Орлов Михаил Дмитриевич, 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 (не) выполнены. Отчёт по практике (не) сдан и (не) защищён на отчётной конференции.

Студент Орлов Михаил Дмитриевич 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.