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 Борзенко Михаил Андреевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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**](#_csp4m3pzjq97) **1**

[**ВВЕДЕНИЕ**](#_qj4nmze035m2) **3**

[**ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ**](#_fzzd8s22nxm7) **4**

[**ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ**](#_u5kwbisane2l) **5**

[Анализ поставленной задачи](#_dvstke897go) 5

[Решение](#_iuawr2mwob3v) 6

[Алгоритм для решения задачи](#_59mtpnv8kjme) 8

[**ЗАКЛЮЧЕНИЕ**](#_f38tay9unjvm) **9**

[**СПИСОК ЛИТЕРАТУРЫ**](#_kr7qwj8k18cc) **10**

# ВВЕДЕНИЕ

Практика является одним из наиболее важных частей обучения для студентов в любых профессиях. Она позволяет студентам приобретать реальные навыки и знания, необходимые для профессионального роста. Она помогает студентам получить практический опыт в профессиональной среде, показывающий им, как применить знания, полученные в учебном заведении, в практической среде. Она также помогает студентам развивать аналитические навыки, закаляя их профессиональное мышление и креативность. В целом, практика предоставляет студентам много возможностей и важных знаний для их профессионального будущего.

Однако, практика также имеет свои трудности и проблемы. Студенты могут столкнуться с различными препятствиями и сложностями в процессе прохождения практики. Поэтому, студентам необходимо быть готовыми к возможным сложностям и проблемам, которые могут возникнуть в ходе практики, и иметь стратегии для их преодоления. Студентам также необходимо иметь четкое представление о своих целях и задачах, которые они хотят достичь в ходе практики, и следовать им. Кроме того, студентам необходимо активно участвовать в практике, проявлять инициативу, интерес, ответственность и коммуникабельность. Таким образом, студенты смогут получить максимальную пользу от практики и повысить свой профессиональный уровень.

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: Применить полученные в течении курса теоретические знания на практической задаче: решении “CTF таска”.

Задачи учебной практики:

* Найти интересную задачу из архива сайта https://cryptohack.org/;
* Провести анализ “таска”;
* Составить математическое описание решения “таска”, придумать программный алгоритм решения;
* Реализовать алгоритм программы.

# ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Как было сказано ранее задача практики - отработать полученные теоретические знания, поэтому нами был выбрано задание под названием “d-phi-enc (HackTM CTF)” в котором нам предстоит дешифровать секретное сообщение, так называемый “флаг”, который зашифрован посредством RSA. Данный таск мы выбрали потому что большую часть семестра изучали принцип работы RSA и различные атаки на этот тип ассиметричного шифрования.

В описании задания не так много информации, сказано только “In CTF, there are many people who mistakenly encrypt p, q in RSA. But this time…”, что переводится как “Много людей в CTF ошибочно шифруют p, q в RSA. Но в этот раз…”. В этом задании нам было дано:

* (n, e) - публичный ключ;
* enc\_flag - зашифрованное сообщение, или ;
* enc\_phi - зашифрованная функция Эйлера от n;
* enc\_d - зашифрованная секретная экспонента.

Последние два значения, обычно никому не передаются и не шифруются в криптосистеме RSA, их знает только владелец криптосистемы. Следовательно, скорее всего, нам придется воспользоваться ошибкой владельца криптосистемы и с помощью enc\_phi и enc\_d дешифровать сообщение.

# ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ

## Анализ поставленной задачи

Для начала проведем анализ данных нам чисел и проверим криптосистему на уязвимость к изученным нами атакам, в числе которых: Атака повторным шифрованием, Атака Винера, Атака встреча поседение, Атака методом Ферма.

Нам дано:

n=24476383567792760737445809443492789639532562013922247811020136923589010741644222420227206374197451638950771413340924096340837752043249937740661704552394497914758536695641625358888570907798672682231978378863166006326676708689766394246962358644899609302315269836924417613853084331305979037961661767481870702409724154783024602585993523452019004639755830872907936352210725695418551084182173371461071253191795891364697373409661909944972555863676405650352874457152520233049140800885827642997470620526948414532553390007363221770832301261733085022095468538192372251696747049088035108525038449982810535032819511871880097702167

enc\_d=23851971033205169724442925873736356542293022048328010529601922038597156073052741135967263406916098353904000351147783737673489182435902916159670398843992581022424040234578709904403027939686144718982884200573860698818686908312301218022582288691503272265090891919878763225922888973146019154932207221041956907361037238034826284737842344007626825211682868274941550017877866773242511532247005459314727939294024278155232050689062951137001487973659259356715242237299506824804517181218221923331473121877871094364766799442907255801213557820110837044140390668415470724167526835848871056818034641517677763554906855446709546993374

enc\_phi=3988439673093122433640268099760031932750589560901017694612294237734994528445711289776522094320029720250901589476622749396945875113134575148954745649956408698129211447217738399970996146231987508863215840103938468351716403487636203224224211948248426979344488189039912815110421219060901595845157989550626732212856972549465190609710288441075239289727079931558808667820980978069512061297536414547224423337930529183537834934423347408747058506318052591007082711258005394876388007279867425728777595263973387697391413008399180495885227570437439156801767814674612719688588210328293559385199717899996385433488332567823928840559

enc\_flag=24033688910716813631334059349597835978066437874275978149197947048266360284414281504254842680128144566593025304122689062491362078754654845221441355173479792783568043865858117683452266200159044180325485093879621270026569149364489793568633147270150444227384468763682612472279672856584861388549164193349969030657929104643396225271183660397476206979899360949458826408961911095994102002214251057409490674577323972717947269749817048145947578717519514253771112820567828846282185208033831611286468127988373756949337813132960947907670681901742312384117809682232325292812758263309998505244566881893895088185810009313758025764867

А также e = 3. Упрощая, нам дано n длиной 2048 бит. Также мы знаем, что длина p и q равна 1024 бита. Очевидно, что разложить n на множители вряд ли будет эффективным решением.

Атака “встреча посередине” не была успешна, обычно она срабатывает при малой длине сообщения (l<64 бит) и наличии разложения на два примерно равных множителя, битовая длина которых меньше l/2. Атака методом Ферма также не принесла результата, данная атака могла бы быть успешна, если p и q “близкие” друг к другу числа (половина старших цифр числа равны). Атака Винера гарантированно успешна, при d<dкр

где dкр =

a =

h =

Как мы можем заметить, для вычисления dкр требуется знать p и q, а мы их пока что не знаем, но мы знаем точно, что попытка атаки Винера не принесла результата.

Атака повторным шифрованием также не дала быстрого результата, из чего можем сделать вывод, что порядок e по модулю сообщения достаточно велик.

## Решение

Из алгоритма работы RSA мы знаем, что d это обратное число к e по модулю phi(n). Попробуем расписать этот факт.

Т. к. d < n и e = 3 можем сделать вывод, что 0 < k1 < 3. Далее распишем denc используя сравнение выше.

Заменим на , так как e = 3, а сравнение выполняется по модулю n, также как и шифрование.

Перенеся всё в одну сторону можно получить квадратное сравнение от

Все переменные кроме даны. Однако, т. к. n не является простым числом, то решить такое сравнение можно только через систему сравнений по модулям множителей n, но в нашем случае множители неизвестны[1]. Поэтому попробуем расписать для упрощения решения.

Обозначим , тогда

(1)

Далее зная что , можем сделать вывод что гораздо меньше . Допустим .

Зная что p, q сгенерированы длиной 1024 бит, . Можем записать такое неравенство:

, следовательно . А также

Используя коэффициент a из квадратного сравнения (1) распишем неравенство для .

, так как .

Мы знаем все числа из b и c коэффициентов неравенства выше, делаем вывод что b и c отрицательны, поэтому меняем знак на строгий.

,

где Таким образом мы можем перебрать все возможные k2 чтобы решить уравнение, корнем которого будет , .

Для решения таска нам нужно знать , оно находится с помощью выражения ниже, но мы также можем подсчитать p и q чтобы проверить наше решение .

, домножим на p и перенесем всё в одну сторону.

Решением данного квадратного уравнения будут p и q. Далее мы можем проверить выражение и переходить к финальному шагу.

Вычисляем

Вычисляем флаг:

С помощью функции long\_to\_bytes вычисляем текстовое значение флага, которое равно:

b"HackTM{Have you warmed up? If not, I suggest you consider the case where e=65537, although I don't know if it's solvable. Why did I say that? Because I have to make this flag much longer to avoid solving it just by calculating the cubic root of enc\_flag.}"

## Алгоритм для решения задачи

Как мы уже выяснили ранее , а . Используем for для перебора k1 и k2. Обозначим коэффициенты квадратного уравнения a, b, c. Будем считать что k1, k2 подобраны верно, если мы можем вычислить квадратный корень из детерминанта. Как только мы нашли подходящие k1 и k2 вычисляем x, phi и проверяем p\*q=n.

Код программы можно просмотреть на нашем гитхабе по ссылке: https://github.com/DKuligin/practice2023/blob/main/chall\_solve1.py, или в приложении к отчету.

# ЗАКЛЮЧЕНИЕ

В процессе обучения студенты получают огромное количество теоретической информации, которая составляет основу для будущих знаний и умений. Но если не использовать полученные знания на практике, то студент не будет получать умения необходимые для будущей работы.

Задачи CTF являются специально созданными заданиями для обучающихся информационной безопасности и чаще всего представляют собой криптосистему с какой-то конкретной уязвимостью, которую нужно обнаружить и воспользоваться ей. В нашем таске уязвимость была не похожа на те, что мы проходили в течении курса, но я разобралися в решении и получил ценные практические навыки.

В ходе практики я справился со всеми задачами и достиг поставленных целей. Я усовершенствовал свое умение программировать на Python. Кроме того, я повысил свой уровень владения LaTeX, Git и GitHub. Я также развил навыки самоорганизации и поиска нужной информации.

# СПИСОК ЛИТЕРАТУРЫ

**Перечень учебной литературы, необходимой для проведения практики**

1. Мир программирования. Перевод с английского С.А. Кулешова под редакцией С.К. Ландо. Н. Смарт Криптография Москва: Техносфера, 2005. 528 с. ISBN 5-94836-043-1.
2. The CrypTool Book: Learning and Experiencing Cryptography with CrypTool and SageMath. Prof. Bernhard Esslinger and the Development Team of the Open-Source Software CrypTool. Edition 12 (2018). - https://www.cryptool.org
3. Elementary Number Theory: Primes, Congruences, and Secrets. William Stein (January 23, 2017)
4. Криптоанализ RSA. Сонг Ян, 2011 год. ISBN 978-5-93972-873-7.
5. Ю.Ф. Болтнев, М.В. Алешникова, Е.В. Козьминых “ИССЛЕДОВАНИЕ УСЛОВИЙ ПРИМЕНИМОСТИ АТАКИ ВИНЕРА НА КРИПТОСИСТЕМУ RSA”

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

1. Математика криптографии и теория шифрования. Лекция 13: Квадратичное сравнение. https://intuit.ru/studies/courses/552/408/lecture/9370
2. Криптографические атаки: объяснение для смятённых умов. https://habr.com/ru/articles/462437/
3. 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
4. Математические формулы в LaTeX - https://ru.wikibooks.org/wiki/Математические\_формулы\_в\_LaTeX
5. Условие решаемой задачи - https://cryptohack.org/challenges/ctf-archive/

**Приложения**

n = 2447638356…

enc\_d = 2385197103…

enc\_phi = 3988439673…

enc\_flag = 2403368891…

e=3

for k1 in range(1, 3):

a = 3\*(k1^2)

b = -(6\*(k1^2)+3\*k1)

c = 3\*(k1^2) + 3\*k1 + (k1^3)\*enc\_phi - 27\*int(enc\_d) + 1

#f = a\*(x^2) + b\*x + c

det = b^2 - 4\*a\*c

for k2 in range(85):

c -= n

det = b^2 - 4\*a\*c

if(is\_square(det)):break

if(is\_square(det)):break

qrs\_det = sqrt(b^2 - 4\*a\*c)

print("qrs\_det=", qrs\_det)

cand\_x = (-1\*b + qrs\_det)/(2\*a) #x=p+q

phi = n - cand\_x + 1

print("phi=", phi)

p = ((n + 1 - phi) + sqrt(((n + 1 - phi) ^ 2) - 4 \* n))/ 2

q = n // p

print("p: ", type(p), p)

print("q: ", type(q), q)

assert(p\*q == n)

d = pow(e, -1, phi)

print("flag=", (pow(enc\_flag, d, n)))

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**

Борзенко Михаил Андреевич 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)** |
| **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 | 20.06.2023 | Пройден инструктаж по технике безопасности |  |
| 2 | 26.06.2023 | Получение индивидуального задания |  |
| 3 | 26.06.2023-07.07.2023 | Выполнение задания по практике |  |
| 4 | 07.07.2023 | Оформление отчета по практике |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**4. Отзыв руководителя практики**

Борзенко Михаил Андреевич, 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 Борзенко Михаил Андреевич 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.