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

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 $flag^e (mod\ n)$;
- 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=39884396730931224336402680997600319327505895609010176946122942377349945284457112897765220943200297202509015894766227493969458751131345751489547456499564086981292114472177383999709961462319875088632158401039384683517164034876362032242242119482484269793444881890399128151104212190609015958451579895506267322128569725494651906097102884410752392897270799315588086678209809780695120612975364145472244233379305291835378349344233474087470585063180525910070827112580053948763880072798674257287775952639733876973914130083991804958852275043743915680176781467461271968858821032829355938519971789999638543348833256782392884055978146746127196885882103282935593851997178999963854334883325678239288405599

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 $d<d_{кр}$

где $d_{кр} = n^{1/4}/\sqrt{(2a)}$

a = $(h + 1)/\sqrt{}(h)$

h = p/q

Как мы можем заметить, для вычисления $d_{кр}$ 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.

$$e * d \equiv 1 \ (mod \ \phi(n))$$

$$e * d = k1 * \phi(n) \ + 1$$

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

$$d_{enc} \equiv d^3 \ (mod \ n)$$

$$e^3 * d_{enc} \equiv e^3 * d^3 \ (mod \ n)$$

$$27d_{enc} \equiv (e * d)^3 \quad (mod \ n)$$

$$27d_{enc} \equiv (k1 * \phi(n) \ + 1) \ (mod \ n)$$

$$27d_{enc} \equiv (k1^3 * \phi^3(n) + 3k1^2 * \phi^2(n) + 3k1 * \phi \ \ (n) \ + 1) \ (mod \ n)$$

Заменим $\phi^3(n)$ на ϕ_{enc}, так как e = 3, а сравнение выполняется по модулю n, также как и шифрование.

$$27d_{enc} \equiv (k1^3 * \phi_{enc} + 3k1^2 * \phi^2(n) + 3k1 * \phi \ \ (n) \ + 1) \ (mod \ n)$$

Перенеся всё в одну сторону можно получить квадратное сравнение от $\phi \ \ (n)$

$$3k1^2 * \phi^2(n) + 3k1 * \phi \ \ (n) + k1^3 * \phi_{enc} \ - 27d_{enc} + 1 \equiv 0 \ (mod \ n)$$

Все переменные кроме $\phi \ \ (n)$ 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 $\phi \ \ (n)$ для упрощения решения.

$$\phi \ \ (n) = (p - 1) * (q - 1) = pq - p - q + 1 = n - p - q + 1$$

$$\phi \ \ (n) \equiv -(p + q) + 1 \ (mod \ n)$$

Обозначим $x = p + q$, тогда

$$3 * k1^2 * \phi^2(n) + 3 * k1 * \phi\ \ (n) + k1^3 * \phi_{enc}\ - 27d_{enc} + 1 \equiv 0\ (mod\ n)$$

$$3 * k1^2 * (1 - x)^2 + 3 * k1 * (1 - x) + k1^3 * \phi_{enc}\ - 27d_{enc} + 1 \equiv 0\ (mod\ n)$$

$$3 * k1^2 * (1 - 2x + x^2)^2 + 3 * k1 * (1 - x) + k1^3 * \phi_{enc}\ - 27d_{enc} + 1 \equiv 0\ (mod\ n)$$

$$3k1^2 * x^2 + (-6k1^2 - 3k1) * x + (3k1^2 + 3k1 + k1^3 * \phi_{enc} - 27d_{enc} + 1) \equiv 0\ (mod\ n)\ \ (1)$$

Далее зная что $x = p + q$, можем сделать вывод что x гораздо меньше n. Допустим $p > q$.

$$x^2 = (p + q)^2 = p^2 + q^2 + 2 * p * q = p^2 + q^2 + 2 * n$$

Зная что p, q сгенерированы длиной 1024 бит, $p/q < 2$. Можем записать такое неравенство:

$p \leq 2 * q$, следовательно $p^2 \leq 4 * q^2$. А также $q^2 \leq n$

$$p^2 + q^2 + 2 * n \leq 4 * q^2 + q^2 + 2 * n$$

$$x^2 \leq 5 * q^2 + 2 * n$$

$$x^2 \leq 5 * n + 2 * n$$

$$x^2 \leq 7 * n$$

Используя коэффициент a из квадратного сравнения (1) распишем неравенство для x^2.

$3k1^2 * x^2 \leq 3 * 2^2 * x^2$, так как $k1 \leq 2$.

$$3k1^2 * x^2 \leq 12 * 7 * n$$

$$3k1^2 * x^2 \leq 84 * n$$

$$3k1^2 * x^2 + (-6k1^2 - 3k1) * x + (3k1^2 + 3k1 + k1^3 * \phi_{enc} - 27d_{enc} + 1) < 84n$$

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

$3k1^2 * x^2 + (-6k1^2 - 3k1) * x + (3k1^2 + 3k1 + k1^3 * \phi_{enc} - 27d_{enc} + 1) = k2 * n$,

где $k2 \leq 84, k2 \in Z$. Таким образом мы можем перебрать все возможные k2 чтобы решить уравнение, корнем которого будет x, $x = p + q$.

Для решения таска нам нужно знать $\phi\ \ (n)$, оно находится с помощью выражения ниже, но мы также можем подсчитать p и q чтобы проверить наше решение $p * q = n$.

$\phi\ \ (n) = n - p - q + 1$, домножим на p и перенесем всё в одну сторону.

$$pn - p^2 - pq + p - p * \phi\ \ (n) = 0$$

$$p^2 - pn - p + p * \phi\ \ (n) + n = 0$$

$$p^2 - p * (n - \phi\ \ (n) + 1) + n = 0$$

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

Вычисляем $d = e^{-1}(mod\ \phi\ \ (n))$

Вычисляем флаг: $flag = enc\_flag^d(mod\ n)$

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 $k1 \in \{1, 2\}$, а $k2 \leq 84$. 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.