

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	1
ВВЕДЕНИЕ	3
ГЛАВА 1. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ	4
ГЛАВА 2. ВЫПОЛНЕНИЕ ЗАДАНИЙ НА ПРАКТИКУ	5
Анализ поставленной задачи	5
Решение	6
Алгоритм для решения задачи	8
ЗАКЛЮЧЕНИЕ	9
СПИСОК ЛИТЕРАТУРЫ	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 taska”.

Задачи учебной практики:

- Найти интересную задачу из архива сайта <https://cryptohack.org/>;
- Провести анализ “taska”;
- Составить математическое описание решения “taska”, 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 было 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 асимметричного 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 $flag^e \pmod n$;
- 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 посередине, Атака методом Ферма.

Нам дано:

$n=244763835677927607374458094434927896395325620139222478110201369235890107416442224202$
272063741974516389507714133409240963408377520432499377406617045523944979147585366956416253588
885709077986726822319783788631660063266767086897663942469623586448996093023152698369244176138
530843313059790379616617674818707024097241547830246025859935234520190046397558308729079363522
107256954185510841821733714610712531917958913646973734096619099449725558636764056503528744571
525202330491408008858276429974706205269484145325533900073632217708323012617330850220954685381
92372251696747049088035108525038449982810535032819511871880097702167

$enc_d=23851971033205169724442925873736356542293022048328010529601922038597156073052741$
135967263406916098353904000351147783737673489182435902916159670398843992581022424040234578709
904403027939686144718982884200573860698818686908312301218022582288691503272265090891919878763
225922888973146019154932207221041956907361037238034826284737842344007626825211682868274941550
017877866773242511532247005459314727939294024278155232050689062951137001487973659259356715242
237299506824804517181218221923331473121877871094364766799442907255801213557820110837044140390
668415470724167526835848871056818034641517677763554906855446709546993374

$enc_phi=398843967309312243364026809976003193275058956090101769461229423773499452844571$
128977652209432002972025090158947662274939694587511313457514895474564995640869812921144721773
839997099614623198750886321584010393846835171640348763620322422421194824842697934448818903991
281511042121906090159584515798955062673221285697254946519060971028844107523928972707993155880
866782098097806951206129753641454722442333793052918353783493442334740874705850631805259100708
271125800539487638800727986742572877759526397338769739141300839918049588522757043743915680176
7814674612719688588210328293559385199717899996385433488332567823928840559

$enc_flag=240336889107168136313340593495978359780664378742759781491979470482663602844142$
815042548426801281445665930253041226890624913620787546548452214413551734797927835680438658581
176834522662001590441803254850938796212700265691493644897935686331472701504442273844687636826
124722796728565848613885491641933499690306579291046433962252711836603974762069798993609494588
264089619110959941020022142510574094906745773239727179472697498170481459475787175195142537711
128205678288462821852080338316112864681279883737569493378131329609479076706819017423123841178
09682232325292812758263309998505244566881893895088185810009313758025764867

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 $d < d_{кр}$

$$\text{где } d_{кр} = n^{1/4} / \sqrt{(2a)}$$

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

$$h = p/q$$

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 e по модулю $\phi(n)$. Попробуем расписать этот факт.

$$e * d \equiv 1 \pmod{\phi(n)}$$

$$e * d = k_1 * \phi(n) + 1$$

Т. к. $d < n$ и $e = 3$ можем сделать вывод, что $0 < k_1 < 3$. Далее распишем d_{enc} используя сравнение выше.

$$d_{enc} \equiv d^3 \pmod{n}$$

$$e^3 * d_{enc} \equiv e^3 * d^3 \pmod{n}$$

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

$$27d_{enc} \equiv (k_1 * \phi(n) + 1) \pmod{n}$$

$$27d_{enc} \equiv (k_1^3 * \phi^3(n) + 3k_1^2 * \phi^2(n) + 3k_1 * \phi(n) + 1) \pmod{n}$$

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

$$27d_{enc} \equiv (k_1^3 * \phi_{enc} + 3k_1^2 * \phi^2(n) + 3k_1 * \phi(n) + 1) \pmod{n}$$

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

$$3k_1^2 * \phi^2(n) + 3k_1 * \phi(n) + k_1^3 * \phi_{enc} - 27d_{enc} + 1 \equiv 0 \pmod{n}$$

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.

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

$$\phi(n) \equiv -(p + q) + 1 \pmod{n}$$

Обозначим $x = p + q$, тогда

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

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

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

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

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:

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

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

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

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

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

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

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

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

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

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

Мы знаем все числа из b и c с 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 $k_2 \leq 84$, $k_2 \in \mathbb{Z}$. Таким образом мы можем перебрать все возможные k_2 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 $p * q = n$.

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

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

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

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

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

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

$$\text{Вычисляем флаг: } flag = enc_flag^d(\text{mod } n)$$

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 $k_1 \in \{1, 2\}$, а $k_2 \leq 84$. Используем `for` для перебора k_1 и k_2 . Обозначим коэффициенты квадратного уравнения a , b , c . Будем считать что k_1 , k_2 подобраны верно, если мы можем вычислить квадратный корень из детерминанта. Как только мы нашли подходящие k_1 и k_2 вычисляем x , ϕ 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 разобрался 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](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

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)

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

[illegible]

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.