Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)

КАФЕДРА «Информационная безопасность» (ИУ8)

ОТЧЁТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Тип практики: производственная

Название предприятия: НПО Эшелон

Студент:
Лоренц Нелли Анатольевна , группа ИУ8-62 (3 курс)

(подпись, дата)

Руководитель от предприятия:
Ведущий разработчик, Борзых Сергей Сергеевич

(подпись, дата)

Руководитель от кафедры:
доцент кафедры ИУ8 Зайцева Анастасия Владленовна

(подпись, дата)

Оценка: отлично

Москва, 2021

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)

КАФЕДРА «Информационная безопасность» (ИУ8)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Тип практики: производственная

Название предприятия: НПО Эшелон

Сроки практики: с 10 июля 2021 г. по 25 июля 2021 г.

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

За время прохождения практики студенту надлежит согласно программе практики:

- **Изучить** теорию об атаке Хастада на RSA.
- **Собрать** материал об атаке Хастада и её реализации для различных задач.
- **Получить практические навыки** в решении задач по заданной теме, взятых с сайта CTFtime.org

Студент:

Лоренц Нелли Анатольевна , группа ИУ8-62 (3 курс)

(подпись, дата)

Руководитель от предприятия:

Ведущий разработчик, Борзых Сергей Сергеевич

25.07.21

(подпись, дата)

Руководитель от кафедры:

доцент кафедры ИУ8 Зайцева Анастасия Владленовна

(подпись, дата)

Оглавление

Введение

Целью данной работы является приобретение навыков решения задач реализации атаки Хастада на RSA.

Объектом исследования является атака Хастада на RSA. Такая атака применяется в тех случаях, когда значения открытой экспоненты достаточно малы. Шифрование с открытыми ключами работают медленно, поэтому малые значения открытой экспоненты, начиная с e = 3, используются для увеличения скорости шифрования и проверки цифровой подписи. [1]. Существенным недостатком такого вида шифрования является возможность встретить повторяющиеся экспоненты, что позволит реализовать атаку с использованием китайской теоремы об остатках. В настоящий момент атака Хастада является одной из самых популярных атак на криптосистему RSA, поэтому важно изучить её реализацию и принципы, на которых построена эта атака как для успешной защиты от неё, так и для решения задач, связанных с ней.

Основная часть

1 Характеристика организации

НПО Эшелон – компания, основанная 22. 11. 2007, которая и в настоящее время является одним из лидеров российского рынка в сфере технологий информационной безопасности. [2]

Основная деятельность компании – это сертификация и испытание средств защиты информации, анализ утечек данных, проектирование систем с комплексной защитой информации, разработка стратегий по её реализации. [2] Компания считает своей целью задание высоких стандартов качества в области обеспечения безопасности для своих клиентов.

Продукты компании направлены на анализ текущего уровня защищенности информационных активов компании [3], а также решение проблем информационной безопасности, характерных как для малого бизнеса, так и для крупных компаний или государственных учреждений. Среди продуктов компании также встречаются защищенные тонкие клиенты, антивирусные системы и ПО для испытательных лабораторий, направленное на поиск дефектов исходного кода, мониторинга текущей защищенности и анализа безопасности кода. Продукты компании имеют сертификаты ФСТЭК России и Минобороны России и могут использоваться для защиты информации с грифом вплоть до «сов. Секретно». [2]

2 Теоретическая часть

2.1 Общие сведения об RSA

Сама RSA представляет собой криптосистему с открытым ключом, направленную на шифрование сообщения или цифровую подпись. На 2009 г. система шифрования считалась надежной, начиная с размера модуля N в 1024 бита. [1]

В криптографических системах с открытым ключом каждый участник имеет закрытый и открытый ключ, которые представляют собой пару целых чисел, взаимно обратных относительно друг друга.

В качестве подготовки к процессу шифрования текст представляется в виде упорядоченного набора чисел по некоторому модулю N. Например, использовать ASCII – кодировку, что применяется чаще всего. Далее выбираются случайные простые числа p и q, удовлетворяющие следующим условиям:

- они образуют группу чисел по модулю N = pq.

- эти числа не должны находиться близко друг к другу на числовой прямой, чтобы исключить возможность скомпрометировать друг друга.

- открытая экспонента e и секретная экспонента d должны быть взаимно просты по модулю (p-1)(q-1).

Таким образом получаем, что шифрование в криптосистеме RSA происходит по следующей формуле:

$$Y = M\text{^}e \bmod N$$

Y – передаваемый зашифрованный текст.

Для дешифрования полученного сообщения используется формула:

$$M = Y\text{^}d \bmod N$$

2.2 Теоретическое обоснование возможности реализации атаки Хастада

Атака Хастада относится к атакам с использованием китайской теоремы об остатках. Начальные условия выглядят следующим образом: Сторона А посылает зашифрованное сообщение M некоторому количеству пользователей (всего i пользователей). У каждого пользователя есть свой открытый ключ - модуль и открытая экспонента: (N_i, e). При чем $M < N_i$ для любых значений i. Пусть количество сообщений, которое было перехвачено, равно k. Если $k \geq e$, тогда исходное сообщение M может быть восстановлено. [1] Для доказательства данного утверждения воспользуемся следующими рассуждениями:

В случае с открытой экспонентой с малыми значениями составляют систему из e уравнений:

$$Y_j = M\text{^}e \bmod N_j \text{ для } \forall j \in [1, e] \quad (1)$$

Если все N_i взаимно простые числа, то может быть применена китайская теорема об остатках. Сама теорема рассматривает системы линейных сравнений вида:

В итоге получаем некоторое значение $Y_{иск}$ из (1):

$$Y_{иск} = M\text{^}e \bmod \prod_1^e N_j \quad (2)$$

Для восстановления исходного сообщения берем из (2) корень нужной степени:

$$M = Y_{отв} = \sqrt[e]{Y_{иск}}$$

Это равенство справедливо, так как M меньше любого N_i

3 Практическая часть

Для практической реализации атаки Хастада была выбрана задача с CTFtime «Quick Math». В неё используются сравнительно небольшие числа, которые будут удобны для дальнейшего анализа, приведенного в данной работе.

В задаче дано три модуля:

n1 = 86812553978993, n2 = 81744303091421, n3 = 83695120256591

и три зашифрованных текста:

c1 = 8875674977048, c2 = 70744354709710, c3 = 29146719498409. Необходимо найти оригинальное сообщение. [4]

В данной работе приведены два решения: при помощи вычислений и написания программы. Полученные результаты будут приведены ниже.

Решим задачу вычислительным методом:

Составим систему уравнений:

$$c_j = M\text{^}3 \ mod \ n_j \text{ для } \forall j \in [1, 3] \quad (3)$$

В числовом виде (3) представим как:

$$\begin{aligned} 8875674977048 &= M\text{^}3 \ mod \ 86812553978993 \\ 70744354709710 &= M\text{^}3 \ mod \ 81744303091421 \\ 29146719498409 &= M\text{^}3 \ mod \ 83695120256591 \end{aligned} \quad (4)$$

Общий модуль N = 593936706583013317449904263441604016328323

Применив китайскую теорему об остатках к системе уравнений (4), получаем:

$C_{иск}$ =M^3 =319222184729548122617007524482681344

Берем кубический корень из этого числа, получаем исходное сообщение, посланное пользователем: M=683435743464.

Ответ: 683435743464.

Первый вариант программной реализации атаки использует библиотеки языка python. В данном языке есть множество библиотек для работы с

различными форматами данных и удобной их обработки. Некоторые из них пригодны и для решения различных криптографических задач.

Для такого подхода к решению задачи требуется подключить библиотеки sympy и gmpy2. Программа (см. Приложение А) включает в себя использование уже готовой функции ctr из библиотеки sympy. Она принимает на вход два списка данных – n и c. Возвращает искомое C и общий модуль. Далее при помощи функции iroot из библиотеки gmpy2, получим искомое сообщение. Сама функция iroot принимает на вход два числа A и B, возвращая корень степени B из A, а также значение типа bool, указывающее на то, был ли корень извлечен точно.

Ответ: 683435743464.

Второй вариант реализации атаки Хастада на python был написан без использования библиотек (см. Приложение Б). Это необходимо для того, чтобы хорошо представлять, как действовать в том случае, если язык не располагает такими же средствами, как python, а также для проверки умение применять теоретические знания на практике.

В этой программе были реализованы три метода. Метод «gcd» – применение расширенного алгоритма Евклида разновидности «Ход Конем». Второй метод, «ChineseRemainderTheorem», применяет китайскую теорему об остатках к системе уравнений. На его вход подаются списки значений модуля и зашифрованных сообщений, на выходе получается число – решение системы уравнений. Третий метод, «root», получает на вход два числа n и pow. Вычисляет целый корень степени pow из числа n. Для вычисления корня сначала находится промежуток [maximum, minimum], в котором может находиться искомое число. Искомое число выбирается, как середина промежутка, который далее будет корректироваться в зависимости от значения, которое принимает текущее «искомое» число на каждом шаге.

Ответ: 683435743464

Все три ответа, полученные различными способами, совпали между собой и ответом, приведенным автором задачи. Осуществим последнее

преобразование с числом при помощи метода fromhex для получения сообщения.

Итоговый результат: h45t4d.

Данная программа подходит для решения и других задач по заданной теме. Возьмем, для примера, задачу «Illuminati Confirmed» с сайта CTFtime. В ней нам даны 3 значения модуля (n1-n3). И 3 зашифрованных сообщения (c1-c3). Требуется найти исходное переданное сообщение, содержащее в себе время встречи. [5]

На выходе программы получится искомое сообщение: 104101108108111044084104101110101201161091011011161051101031051150971160490480480731101151161051161171161010821001111100871011001101011151000971210770971210490510440500480500480460531121090460681111101160981011080971161010870800731230671040491100511150510950820510770641051101000510820950841040510481140511090950330951250 46.

Из него не понятно, какой будет ответ на задачу, поэтому проведем ещё несколько преобразований. Алгоритм их будет таков: разобьем это число на отрезки длиной 3, а затем, используя таблицу кодировки ASCII, переведем в понятное для нас сообщение.

Полученное сообщение:

hello,Thenextmeetingisat100InstituteRdonWednesdayMay13,2020.5pm.DontbelateWPI{Ch1n3s3_R3M@ind3R_Th30r3m_!_}.

Ответ: *Wednesday May 13, 2020. 5pm*

Заключение

В результате выполнения практики были реализованы поставленные цели и задачи:

- Были приобретены навыки решения задач по заданной теме.
- Была изучена информация по заданной теме, рассмотрены различные способы решения схожих практических задач.
- Был получен опыт в написании программ для криптоанализа RSA, в частности, с использованием атаки Хастада.
- Проведено сравнение вычислений аналитическим методом, программным методом с использованием библиотек и с написанием собственных функций. Полученные результаты совпали.

Список использованных источников

1) Википедия. Криптоанализ RSA. [Электронные ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Криптоанализ_RSA (Дата обращения: 15.07.2021)
2) Официальный сайт национальной библиотеки им. Н. Э. Баумана. «НПО Эшелон» [Электронный ресурс]. – Режим доступа: https://ru.bmstu.wiki/НПО_Эшелон (Дата обращения: 15.07.2021)
3) Официальный сайт НПО Эшелон. «Крупный бизнес» [Электронный ресурс]. – Режим доступа: https://npo-echelon.ru/solutions/enterprise/ (Дата обращения: 15.07.2021)
4) CTFtime. Задание «Quick Math». Электронный ресурс]. – Режим доступа: https://ctftime.org/task/12445 (Дата обращения: 15.07.2021)
5) CTFtime. Задание «Illuminati Confirmed». Электронный ресурс]. – Режим доступа: https://ctftime.org/task/11302 (Дата обращения: 15.07.2021)

Приложение А

```
from sympy.ntheory.modular import crt
from gmpy2 import iroot

n = [86812553978993, 81744303091421, 83695120256591]
c = [8875674977048, 70744354709710, 29146719498409]
EX = 3
C_search, N = crt(n, c)
answer, is_accurate = iroot(C_search, EX)
print(answer)
```

Приложение Б

e = 3

N = [86812553978993, 81744303091421, 83695120256591]

C = [8875674977048, 70744354709710, 29146719498409]

```
def gcd(num1, num2):
    a, b, a1, b1 = 0, 1, 1, 0

    while num2:
        num1, new_num, num2 = num2, num1 // num2, num1 % num2
        a, a1 = a1 - new_num * a, a
        b, b1 = b1 - new_num * b, b
    return num1, a1, b1


def ChineseRemainderTheorem(C, N_m):
    NAll = 1
    res = 0
    for n in N_m:
        NAll = NAll * n

    for i in range(0, len(N_m)):
        n = N_m[i]
        a = C[i]
        m = NAll // n
        nod, first, second = gcd(n, m)
        if nod != 1:
            raise Exception("value error")
        res += a * second * m
```

```
    return res % NAll


def root(n, pow):
    maximum = 1
    while maximum ** pow < n:
        maximum = maximum * 2
    minimum = maximum // 2
    while maximum > minimum:
        cur = (maximum + minimum) // 2
        if minimum < cur and cur ** pow < n:
            minimum = cur
        elif maximum > cur and cur ** pow > n:
            maximum = cur
        else:
            return cur
    return cur + 1


res = ChineseRemainderTheorem(C, N)
res = root(res, 3)
print(res)
```