УНИВЕРСИТЕТ ИТМО

ФГАОУ ВО «Национальный исследовательский университет ИТМО»

Факультет программной инженерии и компьютерной техники

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лабораторная работа №4

Вариант 7

Лабушев Тимофей

Группа P3402

Санкт-Петербург

2021

Лабораторная работа №4. Атака на алгоритм шифрования RSA методом бесключевого чтения

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Задание

Вариант 7:

- Модуль n: 516439217617
- Экспоненты e: 1206433 1141277
- Блок зашифрованного текста $C1$: 400408320444 241545246801 282223079755 490328978748 350509811006 142356755075 109547314116 414823859933 330990395685 377471732609 44017319588 499241372980 171071879560
- Блок зашифрованного текста $C2$: 374984721363 438491303024 498951362977 218681974856 365827206348 175049781656 359111505460 297734746741 96963152197 362138584797 102758207364 37817394150 120430068125

Алгоритм шифрования RSA

1. Выбираются два больших простых числа p и q, вычисляется $n = pq$.
2. Вычисляется $\phi(n) = (p-1)(q-1)$.
3. Находится любое число e, которое является взаимно простым $\phi(n)$: $\{e \in \mathbb{Z} \mid \gcd(e, \phi(n)) = 1, 1 < e < \phi(n)\}$.
4. Вычисляется такое число d, что de сравнимо с единицей по модулю $\phi(n)$: $\{d \in \mathbb{Z} \mid de \equiv 1 \pmod{\phi(n)}\}$.

Пара (n, e) является публичным ключом, который используется для шифрования. Сообщение разделяется на блоки $t, t < n$, для каждого из которых вычисляется $c = t^e \mod n$.

Пара (n, d) является секретным ключом, который используется для дешифрования: $t = c^d \mod n$.

Атака на алгоритм RSA

Известны (n, e) — публичный ключ, c — зашифрованные данные. Необходимо найти d путем факторизации n, т.е. нахождения p и q. При правильном выборе чисел данная задача является вычислительно сложной.

Однако если известны два зашифрованных сообщения, $c_1 = t^{e_1} \pmod{n}$, $c_2 = t^{e_2} \pmod{n}$, содержание t которых одинаково и при шифровании которых использовался один и тот же модуль n, но разные экспоненты e_1 и e_2, то исходное сообщение t может быть восстановлено методом бесключевого чтения.

Атака основывается на наблюдении, что e_1 и e_2 взаимно просты, т.е. можно найти такие целочисленные r и s, что $re_1 + se_2 = 1$ (соотношение Безу для взаимно простых чисел). В таком случае $c_1^r \cdot c_2^s = t^{re_1 + se_2} = t \pmod{n}$.

```
Given n = 516439217617
Given public key exponents e1 = 1206433, e2 = 1141277

Computed r = 801728, s = -847499 for r*e1 + s*e2 = 1

Decoding C:
c1 = 400408320444, c2 = 374984721363, c1^r = 253379909020, c2^s = 295184394587
t = c1^r * c2^s (mod n) = 4024494821 = ef e0 ea e5 = |пакe|
c1 = 241545246801, c2 = 438491303024, c1^r = 260323309898, c2^s = 297807813622
t = c1^r * c2^s (mod n) = 4075102446 = f2 e5 20 ee = |те o|
c1 = 282223079755, c2 = 498951362977, c1^r = 376310539447, c2^s = 262920734020
t = c1^r * c2^s (mod n) = 4025542116 = ef f0 e5 e4 = |пред|
c1 = 490328978748, c2 = 218681974856, c1^r = 443795639236, c2^s = 397949876247
t = c1^r * c2^s (mod n) = 3857442285 = e5 eb e5 ed = |елен|
c1 = 350509811006, c2 = 365827206348, c1^r = 092543709642, c2^s = 123830137291
t = c1^r * c2^s (mod n) = 3991856110 = ed ee e3 ee = |ного|
c1 = 142356755075, c2 = 175049781656, c1^r = 241385074792, c2^s = 312002657785
t = c1^r * c2^s (mod n) = 0552526330 = 20 ee e1 fa = | объ|
c1 = 109547314116, c2 = 359111505460, c1^r = 394448339357, c2^s = 251358506177
t = c1^r * c2^s (mod n) = 3857506336 = e5 ec e0 20 = |ема |
c1 = 414823859933, c2 = 297734746741, c1^r = 359127075448, c2^s = 451648360081
t = c1^r * c2^s (mod n) = 3839946221 = e4 e0 ed ed = |данн|
c1 = 330990395685, c2 = 096963152197, c1^r = 246454332586, c2^s = 038124395171
t = c1^r * c2^s (mod n) = 4227145812 = fb f5 20 54 = |ых T|
c1 = 377471732609, c2 = 362138584797, c1^r = 471934614857, c2^s = 396719558963
t = c1^r * c2^s (mod n) = 1129328160 = 43 50 2e 20 = |CP. |
c1 = 044017319588, c2 = 102758207364, c1^r = 388658832651, c2^s = 481853440946
t = c1^r * c2^s (mod n) = 3454070768 = cd e0 ef f0 = |Напр|
c1 = 499241372980, c2 = 037817394150, c1^r = 258637941765, c2^s = 163563348305
t = c1^r * c2^s (mod n) = 3907839472 = e8 ec e5 f0 = |имер|
c1 = 171071879560, c2 = 120430068125, c1^r = 220495130798, c2^s = 324422260341
t = c1^r * c2^s (mod n) = 0740302880 = 2c 20 20 20 = |,   |

Decoded message:
пакете определенного объема данных TCP. Например,
```

```
with_terminal() do
    r, s = solve_rs(task_e1, task_e2)

    print("Given n = $(task_n)\n")
    print("Given public key exponents e1 = $(task_e1), e2 = $(task_e2)\n\n")
    print("Computed r = $(r), s = $(s) for r*e1 + s*e2 = 1\n\n")
    print("Decoding C:\n")

    msg = []

    for (c1, c2) in zip(task_c1, task_c2)
        c1_r::BigInt = powermod(c1, r, task_n)
        c2_s::BigInt = powermod(c2, s, task_n)
        t = mod(c1_r*c2_s, task_n)

        # Each block contains four 8-bit characters encoded as windows-1251
        chars = [(t >> 24) % UInt8, (t >> 16) % UInt8, (t >> 8) % UInt8, t % UInt8]
        textchars = decode(chars, "WINDOWS-1251")

        @printf("c1 = %012d, c2 = %012d, c1^r = %012d, c2^s = %012d\n",
            c1, c2, c1_r, c2_s)
        @printf("t = c1^r * c2^s (mod n) = %010d = %s = |%s|\n",
            t, join(map(n -> string(n, base=16), chars), " "), textchars)

        append!(msg, textchars)
    end

    print("\nDecoded message:\n$(join(msg))")
end
```

```
solve_rs (generic function with 1 method)
```

```
# Finds Bézout coefficients for coprime e1 and e2,
# i.e. a pair of (r, s) such that e1*r + e2*s = 1.
# For positive e1 and e2, r will be positive and s will be negative
function solve_rs(e1, e2)::Tuple{Int64,Int64}
    r = 0
    while true
        # e1*r + e2*s = 1
        r += 1
        s = (1 - e1*r)/e2
        if isinteger(s)
            return (r, s)
        end
    end
end
```

Вывод

В ходе выполнения лабораторной работы были рассмотрены на практике последствия использования одного и того же параметра n для шифрования одинаковых сообщений с применением алгоритма RSA: атакующий может восстановить содержание без знания секретного ключа за небольшое число шагов.