Университет ИТМО

Факультет ФПИ и КТ

Отчёт

по лабораторной работе 2.3

«Иформационная безопасность»

Вариант 7

Студент:

Ляо Ихун

Гр.P34131

Преподаватель:

Маркина Татьяна Анатольевна

Цель работы:

изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Задача:

7	516439217617	1206433	1141277	400408320444	374984721363
				241545246801	438491303024
				282223079755	498951362977
				490328978748	218681974856
				350509811006	365827206348
				142356755075	175049781656
				109547314116	359111505460
				414823859933	297734746741
				330990395685	96963152197
				377471732609	362138584797
				44017319588	102758207364
				499241372980	37817394150
				171071879560	120430068125

Выполнение:

```
N = 516439217617
e1 = 1206433
e2 = 1141277

C1 = [
    400408320444,
    241545246801,
    282223079755,
    490328978748,
    350509811006,
    142356755075,
    109547314116,
    414823859933,
    330990395685,
    377471732609,
    44017319588,
    499241372980,
    171071879560
]

C2 = [
    374984721363,
    438491303024,
    498951362977,
    218681974856,
    365827206348,
    175049781656,
    359111505460,
    297734746741,
    96963152197,
```

```
    362138584797,
    102758207364,
    37817394150,
    120430068125
]


def gcd_extended(num1, num2):
    if num1 == 0:
        return num2, 0, 1
    else:
        div, x, y = gcd_extended(num2 % num1, num1)
    return div, y - (num2 // num1) * x, x

print(f"N = {N}")
print(f"e1 = {e1}")
print(f"e2 = {e2}")
print(f"C1 = {C1}")
print(f"C2 = {C2}")

message = ""

a, r, s = gcd_extended(e1, e2)

print(f" r = {r},\n s = {s}", "\n")

for i in range(len(C1)):
    c1r = pow(C1[i], r, N)
    c2s = pow(C2[i], s, N)
    m = (c1r * c2s) % N
    part = m.to_bytes(4, byteorder='big').decode('cp1251')
    message += part
    print(f"(C1^r) mod N = {c1r}")
    print(f"(C2^s) mod N = {c2s}")
    print(f"m = ({c1r} * {c2s}) mod {N} = {m} => text({m}) = {part}", "\n")

print(f"message = {message}")
```

Результат:

N = 516439217617

e1 = 1206433

e2 = 1141277

C1 = [400408320444, 241545246801, 282223079755, 490328978748, 350509811006, 142356755075, 109547314116, 414823859933, 330990395685, 377471732609, 44017319588, 499241372980, 171071879560]

C2 = [374984721363, 438491303024, 498951362977, 218681974856, 365827206348, 175049781656, 359111505460, 297734746741, 96963152197, 362138584797, 102758207364, 37817394150, 120430068125]

(e1 * r) + (e2 * s) = ±1

r = -339549,

s = 358934

(C1^r) mod N = 449048555821

(C2^s) mod N = 133166631220

m = (449048555821 * 133166631220) mod 516439217617 = 4024494821 => text(4024494821) = паке

(C1^r) mod N = 272249556170

(C2^s) mod N = 493391214558

m = (272249556170 * 493391214558) mod 516439217617 = 4075102446 => text(4075102446) = те о

(C1^r) mod N = 279867902071

(C2^s) mod N = 368042842534

m = (279867902071 * 368042842534) mod 516439217617 = 4025542116 => text(4025542116) = пред

(C1^r) mod N = 491332966409

(C2^s) mod N = 361810748405

m = (491332966409 * 361810748405) mod 516439217617 = 3857442285 => text(3857442285) = елен

(C1^r) mod N = 212320748879

(C2^s) mod N = 306613294135

m = (212320748879 * 306613294135) mod 516439217617 = 3991856110 => text(3991856110) = ного

(C1^r) mod N = 149174569946

(C2^s) mod N = 40115675459

m = (149174569946 * 40115675459) mod 516439217617 = 552526330 => text(552526330) = объ

(C1^r) mod N = 432509836867

(C2^s) mod N = 305238791918

m = (432509836867 * 305238791918) mod 516439217617 = 3857506336 => text(3857506336) = ема

(C1^r) mod N = 382564014075

(C2^s) mod N = 322788922809

m = (382564014075 * 322788922809) mod 516439217617 = 3839946221 => text(3839946221) = данн

(C1^r) mod N = 473459846372

(C2^s) mod N = 194598742520

m = (473459846372 * 194598742520) mod 516439217617 = 4227145812 => text(4227145812) = ых Т

(C1^r) mod N = 410740648785

(C2^s) mod N = 185093872245

m = (410740648785 * 185093872245) mod 516439217617 = 1129328160 => text(1129328160) = СР.

(C1^r) mod N = 28174939188

(C2^s) mod N = 513926609127

m = (28174939188 * 513926609127) mod 516439217617 = 3454070768 => text(3454070768) = Напр

(C1^r) mod N = 454142616657

(C2^s) mod N = 331984978122

m = (454142616657 * 331984978122) mod 516439217617 = 3907839472 => text(3907839472) = имер

(C1^r) mod N = 51171139201

(C2^s) mod N = 58868950333

m = (51171139201 * 58868950333) mod 516439217617 = 740302880 => text(740302880) = ,

message = пакете определенного объема данных TCP. Например,

Вывод:

В ходе выполнения работы мы реализовали атаку на алгоритм шифрования RSA посредством метода бесключевого чтения на языке python.