Университет ИТМО

Факультет ФПИ и КТ

Отчёт

по лабораторной работе 2.4

«Иформационная безопасность»

Вариант 7

Студент:

Ляо Ихун

Гр.P34131

Преподаватель:

Маркина Татьяна Анатольевна

Цель работы:

изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Задача:

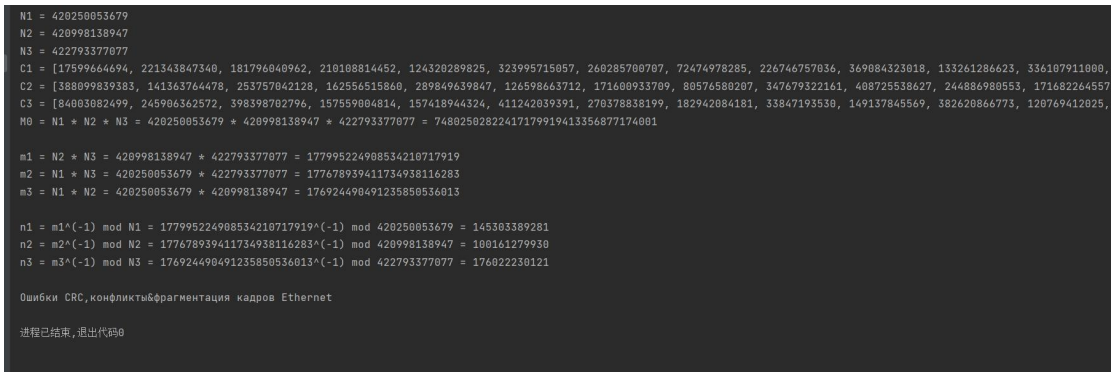
7	420250053679	420998138947	422793377077	17599664694	388099839383	84003082499
				221343847340	141363764478	245906362572
				181796040962	253757042128	398398702796
				210108814452	162556515860	157559004814
				124320289825	289849639847	157418944324
				323995715057	126598663712	411242039391
				260285700707	171600933709	270378838199
				72474978285	80576580207	182942084181
				226746757036	347679322161	33847193530
				369084323018	408725538627	149137845569
				133261286623	244886980553	382620866773
				336107911000	171682264557	120769412025
				303767221006	366784660912	272019119100

Выполнение:

```
from decimal import Decimal

N1 = 420250053679
N2 = 420998138947
N3 = 422793377077

C1 = [
    17599664694,
    221343847340,
    181796040962,
    210108814452,
    124320289825,
    323995715057,
    260285700707,
    72474978285,
    226746757036,
    369084323018,
    133261286623,
    336107911000,
    303767221006
]

C2 = [
    388099839383,
    141363764478,
    253757042128,
    162556515860,
    289849639847,
    126598663712,
    171600933709,
    80576580207,
```

```
    347679322161,
    408725538627,
    244886980553,
    171682264557,
    366784660912
]

C3 = [
    84003082499,
    245906362572,
    398398702796,
    157559004814,
    157418944324,
    411242039391,
    270378838199,
    182942084181,
    33847193530,
    149137845569,
    382620866773,
    120769412025,
    272019119100
]


print(f"N1 = {N1}")
print(f"N2 = {N2}")
print(f"N3 = {N3}")
print(f"C1 = {C1}")
print(f"C2 = {C2}")
print(f"C3 = {C3}")

message = ""

M0 = N1 * N2 * N3
m1 = N2 * N3
m2 = N1 * N3
m3 = N1 * N2
n1 = pow(m1, -1, N1)
n2 = pow(m2, -1, N2)
n3 = pow(m3, -1, N3)

print(f"M0 = N1 * N2 * N3 = {N1} * {N2} * {N3} = {M0}", "\n")
print(f"m1 = N2 * N3 = {N2} * {N3} = {m1}")
print(f"m2 = N1 * N3 = {N1} * {N3} = {m2}")
print(f"m3 = N1 * N2 = {N1} * {N2} = {m3}", "\n")
print(f"n1 = m1^(-1) mod N1 = {m1}^(-1) mod {N1} = {n1}")
print(f"n2 = m2^(-1) mod N2 = {m2}^(-1) mod {N2} = {n2}")
print(f"n3 = m3^(-1) mod N3 = {m3}^(-1) mod {N3} = {n3}", "\n")

for i in range(len(C1)):
    S = (C1[i] * n1 * m1) + (C2[i] * n2 * m2) + (C3[i] * n3 * m3)
    SmodM0 = S % M0
    M = round(SmodM0 ** (Decimal(1 / 3)))
    part = M.to_bytes(4, byteorder='big').decode('cp1251')
    message += part
print(message)
```

Результат:



```
N1 = 420250053679
N2 = 420998138947
N3 = 422793377077
C1 = [17599664694, 221343847340, 181796040962, 210108814452, 124320289825, 323995715057, 260285700707, 72474978285, 226746757036, 369084323018, 133261286623, 336107911000,
C2 = [38809839383, 141363764478, 253757042128, 162556515860, 289849639847, 126598663712, 171600933709, 80576580207, 347679322161, 408725538627, 244886980553, 171682264557
C3 = [84003082499, 245906362572, 398398702796, 157559004814, 157418944324, 411242039391, 270378838199, 182942084181, 33847193530, 149137845569, 382620866773, 120769412025,
M0 = N1 * N2 * N3 = 420250053679 * 420998138947 * 422793377077 = 74802502822417179919413356877174001

m1 = N2 * N3 = 420998138947 * 422793377077 = 177995224908534210717919
m2 = N1 * N3 = 420250053679 * 422793377077 = 177678939411734938116283
m3 = N1 * N2 = 420250053679 * 420998138947 = 176924490491235850536013

n1 = m1^(-1) mod N1 = 177995224908534210717919^(-1) mod 420250053679 = 145303389281
n2 = m2^(-1) mod N2 = 177678939411734938116283^(-1) mod 420998138947 = 100161279930
n3 = m3^(-1) mod N3 = 176924490491235850536013^(-1) mod 422793377077 = 176022230121

Ошибки CRC,конфликты&фрагментация кадров Ethernet

进程已结束,退出代码0
```

Вывод:

В ходе выполнения работы мы реализовали атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках на языке python.