Национальный исследовательский университет ИТМО

Факультет программной инженерии и компьютерной техники

Направление программная инженерия
Образовательная программа системное и прикладное программное обеспечение
Специализация системное программное обеспечение

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2.3

курса «Информационная безопасность»

по теме: «Криптографические системы с открытым ключом»

Вариант № 26

Выполнил студент:
Тюрин Иван Николаевич
группа: P33102

Преподаватель:
Маркина Т.А.,
Рыбаков С.Д.

Санкт-Петербург, 2025 г.

Содержание

Лабораторная работа № 2.3 Криптографические системы с открытым ключом

1. Описание

Цель работы. Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Порядок выполнения работы: – ознакомьтесь с теорией, в подразделе («Бесключевое чтение»); – получите вариант задания у преподавателя; – по полученным данным определите значения r и s при условии, чтобы $e_1 \cdot r - e_2 \cdot s = 1$. Для этого необходимо использовать расширенный алгоритм Евклида; – используя полученные выше значения r и s, запишите исходный текст; – результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

Задание варианта № 26:

Вариант	Модуль, N	Экспоненты e_1	e_2	Блок зашифрованного текста C_1	C_2
26	199463062753	419513	830477	177528135337	63508097139
				131197957980	142467940607
				181321285074	131649552179
				96738779356	182684157712
				127632416974	22912524157
				161779284378	94825501208
				148599198368	189716623763
				2033602084	86236434624
				141914496373	94875774697
				105405878640	120252092430
				120038779975	26215384541
				7139491789	53782670605

2. Выполнение задания

Для расшифровки текста использовался метод бесключевого чтения. Метод использует теорию чисел и расширенный алгоритм Евклида для поиска обратного числа в конечном поле остатков. Результат дешифрации можно видеть на изображении 1.1.

```
D:\Projects\itmo-info-sec\crypto\lab-2_3> python main.py
message = 'монопольно захватить одна из станций, постоянно '
D:\Projects\itmo-info-sec\crypto\lab-2_3>          12/23/2024 06:42:00 PM
```

Рис. 1.1: Результат работы утилиты

```python
#!/usr/bin/env python

from argparse import ArgumentParser

N = 199463062753
E1 = 419513
E2 = 830477

C1 = '''
177528135337
131197957980
181321285074
96738779356
127632416974
161779284378
148599198368
2033602084
141914496373
105405878640
120038779975
7139491789
'''

C2 = '''
63508097139
142467940607
131649552179
182684157712
22912524157
94825501208
189716623763
86236434624
94875774697
120252092430
26215384541
53782670605
'''
```

```python


def gcd_ext(a: int, b: int) -> tuple[int, int, int]:
    if a == 0:
        return b, 0, 1
    else:
        div, x, y = gcd_ext(b % a, a)
    return div, y - (b // a) * x, x

def hack_RSA(
    N: int, e1: int, e2: int, c1: list[int], c2: list[int], debug=False
) -> str:
    message = []

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

    if debug:
        print(f"{N=}", f"{e1=}", f"{e2=}", f"{c1=}", f"{c2=}", sep="\n")
        print("(e1 x r) - (e2 x s) = +-1")
        print(f"{r=},")
        print(f"{s=}")

    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.append(part)
        if debug:
            print(f"C1[{i}]^r (mod N) = {c1r}")
            print(f"C1[{i}]^s (mod N) = {c2s}")
            print(f"m{i} = ({c1r} x {c2s}) (mod {N}) = {m} => text({m}) = {part}", "\n")

    return "".join(message)


def main():
    parser = ArgumentParser(description="Чтение сообщения зашифрованного с помощью RSA без ключа")
    parser.add_argument("--debug", action="store_true", help="Добавить отладочную информацию в вывод")
    args = parser.parse_args()

    c1 = list(map(int, C1.split()))
    c2 = list(map(int, C2.split()))
    e1 = E1
    e2 = E2

    message = hack_RSA(N, e1, e2, c1, c2, debug=args.debug)
```

```
85
86      print(f"message = '{message}'")
87
88
89  if __name__ == "__main__":
90      main()
```

Листинг 1.1: Код скрипта выполняющего расшифрование текста методом безключевого чтения RSA

3. Вывод

В результате выполнения работы изучили метод безключевого чтения текста зашифрованного по средствам RSA. Реализовали алгоритм расшифровки на языке Python.