MainPage/Info Security/Encript Lab 2.1

Университет ИТМО
Факультет ФПИ и КТ

Отчёт по лабораторной работе 2.1

«Атака на алгоритм шифрования RSA посредством метода Ферма»

по дисциплину

«Информационная безопасность»

Студент: Чжоу Хунсян
Группа: P34131
Преподаватель:

Санкт-Петербург 2024

Цель работы

изучить атаку на алгоритм шифрования RSA посредством метода Ферма

Варианты заданий

> Вариант: 23

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
23	888532740131	508097	251133768996 359801014616 557356431645 75854873865 768478933532 624174758081 306027834198 586384787006 155294489444 358096762086 197284968232 498688500894 467532994504

Исходный код

```python
# Определение начальных значений
N = 888532740131  # Модуль
e = 508097  # Показатель
C = [  # Зашифрованные сообщения
    251133768996,
    359801014616,
    557356431645,
    75854873865,
    768478933532,
    624174758081,
    306027834198,
    586384787006,
    155294489444,
    358096762086,
    197284968232,
    498688500894,
    467532994504
]


def decrypt_message(c, e, N):
    """
    Расшифровывает одно зашифрованное сообщение.
    :param c: зашифрованное сообщение
    :param e: показатель
    :param N: модуль
    :return: расшифрованное сообщение в виде строки
    """
    yi = pow(c, e, N)  # Вычисление yi
    res = 0
    while yi != c:  # Пока yi не совпадает с исходным c
        res = yi
        yi = pow(yi, e, N)  # Обновляем yi
    return res.to_bytes(4, byteorder='big').decode('cp1251')  # Преобразование в строку


if __name__ == "__main__":
    print(f"N = {N}")
    print(f"e = {e}")
```

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

    # Расшифровка каждого сообщения в списке
    for c in C:
        decrypted_message = decrypt_message(c, e, N)
        print(decrypted_message, end='')
```

Результаты работы программы

Пример Usage

```
N = 888532740131
e = 508097
C = [251133768996, 359801014616, 557356431645, 75854873865, 768478933532, 624174758081, 3
интенсивность ошибок, а также определить основные __
Process finished with exit code 0
```

Вывод

В ходе выполнения работы мы реализовали метод Ферма для атаки на алгоритм шифрования RSA на языке python.