Криптографические системы

Лабораторная работа №2

Атака на алгоритм шифрования RSA методом повторного шифрования

ФИО студента: Готовко Алексей Владимирович
Вариант: 3
Учебная группа: P34101

1 Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

2 Вариант задания

По полученным исходным данным, используя метод перешифрования, определить порядок числа e в конечном поле $Z_{\varphi(N)}$ и, используя значение порядка экспоненты, получить исходный текст методом перешифрования.

Вариант	**Модуль,** N	**Экспонента,** e	**Блок зашифрованного текста,** C
3	385181864647	938573	331245775481 282425324609 65377570000 89972965825 264803627317 320989226085 324723654667 294634302620 142237555971 221994269576 209958712589 221718426295 163788492835

3 Исходный код программы

rsa_attacks.py

```python
def to_text(data: int) -> str:
    return data.to_bytes(length=4, byteorder="big").decode("cp1251")

def recipher(modulo: int, exponent: int, ciphertext: list[int]) -> str:
    result = ""
    exp_order = 1

    entry = ciphertext[0]
    cur = pow(entry, exponent, modulo)
    prev = cur

    while cur != entry:
        prev = cur
        cur = pow(cur, exponent, modulo)
        exp_order += 1

    print(f"Order of the exponent: {exp_order}\n")

    result += to_text(prev)

    for element in ciphertext[1:]:
        result += to_text(pow(element, pow(exponent, exp_order - 1), modulo))

    return result
```

4 Результат работы программы

```
Order of the exponent: 78300

Decrypted text: еще ошибками PCS (Frame Check Sequence, контрольная
```