Криптографические системы

Лабораторная работа №1

Атака на алгоритм шифрования RSA посредством метода Ферма

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

1 Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

2 Вариант задания

Используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:

- множители модуля (p и q);
- значение функции Эйлера для данного модуля $\varphi(N)$;
- обратное значение экспоненты по модулю $\varphi(N)$.

Дешифровать зашифрованный текст. Исходный текст должен быть фразой на русском языке.

Вариант	**Модуль,** N	**Экспонента,** e	**Блок зашифрованного текста,** C
3	93767386321457	2091619	62984326732858 22123186696272 24425203655789 45995309006047 8176196426076 12816278693250 27474201663022 86909026690842 20469575723850 29205116646939 21002901408912 79168478687790

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 fermat(modulo: int, exponent: int, ciphertext: list[int]):
    n = int(modulo ** 0.5) + 1

    t = n
    w = t ** 2 - modulo

    if n ** 2 != modulo:
        while w != int(w ** 0.5) ** 2:
            t += 1
            w = t ** 2 - modulo

    p = int(t + w ** 0.5)
    q = int(t - w ** 0.5)

    phi = int((p - 1) * (q - 1))
    d = pow(exponent, -1, phi)

    print("Fermat method parameters:\n"
          f"t   = {t}\n"
          f"w   = {w}\n"
          f"p   = {p}\n"
          f"q   = {q}\n"
          f"phi = {phi}\n"
          f"d   = {d}\n")

    result = ""

    for element in ciphertext:
        msg = pow(element, d, modulo)
        result += to_text(msg)

    return result
```

4 Результат работы программы

```
Fermat method parameters:
t   = 9683361
w   = 93934864
p   = 9693053
q   = 9673669
phi = 93767366954736
d   = 26651504610523

Decrypted text: исследователей с маршрутизацией от источника: __
```