Лабораторная работа 2
Атака на алгоритм шифрования RSA посредством метода Ферма
Вариант 1

Выполнила: Батомункуева Виктория

Группа: P34101

Цель работы:

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Вариант:

Модуль – 99595193774911
Экспонента, e – 1908299
Блок зашифрованного текста –
75790643190143 36869061035180 38422576553598 68899435645717 16193161920958
98487458352335 34167725433806 96613844267045 26583768908805 73052827576371
94695336463618 69092596694070

Листинг:

```
import math

import math

N = 99595193774911
e = 1908299
C = '''
75790643190143
36869061035180
38422576553598
68899435645717
16193161920958
98487458352335
34167725433806
96613844267045
26583768908805
73052827576371
94695336463618
69092596694070
'''

def get_factors(N):
    approx = int(math.sqrt(N)) + 1
    inc = 0
    while True:
        inc += 1
        temp_factor = approx + inc
        diff = temp_factor ** 2 - N
        if math.sqrt(diff).is_integer():
            sqrt_diff = int(math.sqrt(diff))
            return temp_factor + sqrt_diff, temp_factor - sqrt_diff
```

```
def get_key(e, phi):
    return pow(e, -1, phi)

def decrypt_text(cipher_text, decryption_key, N):
    decrypted_text = ""
    for char_code in cipher_text.split():
        numeric_char = pow(int(char_code), decryption_key, N)
        decrypted_char = numeric_char.to_bytes(4,
byteorder='big').decode('cp1251')
        decrypted_text += decrypted_char
    return decrypted_text

def decrypt_message(N, e, cipher_text):
    p, q = get_factors(N)
    print(f"p - {p}, q - {q}")
    phi = (p - 1) * (q - 1)
    dkey = get_key(e, phi)
    print(f"d - {dkey}")
    decrypted_text = decrypt_text(cipher_text, dkey, N)
    return decrypted_text


message = decrypt_message(N, e, C)
print(f"Decrypted message - {message}")
```

Результаты программы:

```
p - 9989569, q - 9969919
d - 65973656360291
Decrypted message - Для работы алгоритма маршрутизации от источника_
```