Лабораторная работа 3
Атака на алгоритм шифрования RSA методом бесключевого чтения
Вариант 1

Выполнила: Батомункуева Виктория

Группа: P34101

Цель работы:

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Вариант:

Модуль – 420882327013
Экспоненты, e1 – 1372369, **e2** – 961447
Блок зашифрованного текста:
C1 – 373413138774 142492164990 181970101695 71400620884 83588687662 111752930680 154836140461 191336073909 186412386345 303121580659 167437105893 279265271451
C2 – 105783140624 384545054504 91022339898 266856044417 106548952403 160772152396 128969469496 242028887287 256618243529 47586486979 306022591934 419219258598

Листинг:

```
N = 420882327013
e1 = 1372369
C1 = '''
373413138774
142492164990
181970101695
71400620884
83588687662
111752930680
154836140461
191336073909
186412386345
303121580659
167437105893
279265271451
'''
e2 = 961447

C2 = '''
105783140624
384545054504
91022339898
266856044417
106548952403
160772152396
128969469496
242028887287
256618243529
47586486979
306022591934
419219258598
```

```
'''


def get_gcd(first, second):
    if first == 0:
        return second, 0, 1
    else:
        gcd, bezout_x, bezout_y = get_gcd(second % first, first)
    return gcd, bezout_y - (second // first) * bezout_x, bezout_x


def decrypt_message_block(block1, block2, N, r, s):
    decrypted1 = pow(block1, r, N)
    decrypted2 = pow(block2, s, N)
    decrypted = (decrypted1 * decrypted2) % N
    return decrypted.to_bytes(4, byteorder='big').decode('cp1251')


def decrypt_combined_message(N, e1, e2, encrypted_message1,
encrypted_message2):
    list_encrypted_blocks1 = list(map(int, encrypted_message1.split()))
    list_encrypted_blocks2 = list(map(int, encrypted_message2.split()))
    decrypted_message = ""

    gcd, bezout_r, bezout_s = get_gcd(e1, e2)

    for i in range(len(list_encrypted_blocks1)):
        decrypted_part = decrypt_message_block(
            list_encrypted_blocks1[i],
            list_encrypted_blocks2[i],
            N,
            bezout_r,
            bezout_s
        )
        decrypted_message += decrypted_part

    return decrypted_message


decrypted_message = decrypt_combined_message(N, e1, e2, C1, C2)
print(decrypted_message)
```

Результаты программы:

```
Протоколы определяют синтаксис-семантику данных.
```