МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

Кафедра ИИТ

ОТЧЁТ
По лабораторной работе №3
«Атака на алгоритм шифрования RSA посредством метода бесключевого чтения»

Выполнил:
Студент группы ИИ-22
Кузьмич В.Н.
Проверила:
Хацкевич А.С.

Брест 2024

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения

Ход работы

Исходные данные: $N = 357114156277$; $e_1 = 1025537$; $e_2 = 722983$; $C_1 = 68639736967$; $C_2 = 204258645263$.

Код программы:

```
N = 357114156277
e1 = 1025537
e2 = 722983
C1 = 68639736967
C2 = 204258645263

r = 286243
s = 406030

result_check = e1 * r - e2 * s
print("Проверка уравнения e1 * r - e2 * s =", result_check)

result1 = pow(C1, r, N)
print("C1^r mod N =", result1)

result2 = pow(C2, -s, N)
print("C2^(-s) mod N =", result2)

m = (result1 * result2) % N
print("Результат дешифрации (m mod N) =", m)

try:
    decoded_message = m.to_bytes((m.bit_length() + 7) // 8, 'big').decode()
    print("Сообщение в текстовом виде:", decoded_message)
except UnicodeDecodeError:
    print("Сообщение не может быть корректно преобразовано в текст.")
```

Результат работы:

```
Проверка уравнения e1 * r - e2 * s = 1
C1^r mod N = 189703239311
C2^(-s) mod N = 104340380259
Результат дешифрации (m mod N) = 1381187873
Сообщение в текстовом виде: RSA!
```

Вывод: изучил атаку на алгоритм шифрования RSA посредством метода бесключевого чтения