Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Лабораторная работа №3

За седьмой семестр

По дисциплине: «Современные методы защиты компьютерных систем»

Тема: «Атака на алгоритм шифрования RSA»

Выполнила:
Студентка 4 курса
Группы ИИ-21(II)
Соболева П.С.

Проверила:
Хацкевич А. С.

Брест 2024

Цель: изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Ход работы:

Вариант 1,7

Задание:

Варианты заданий к выполнению лабораторной работы 1

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
7	84032429242009	2581907	54879925681459 72167008182929 17828219756166 17814399744948 37136636080011 77223434260215 4272415279426 73759271926435 74021335775875 16903113250201 77520052156956 41247980943013

Результат:

```
Дешифрованное сообщение (числовое): 63765586526514
Дешифрованные байты: bytearray(b'9\xfe\x95"A2')
```

Вывод: в ходе лабораторной работы изучила атаку на алгоритм шифрования RSA посредством метода Ферма.