Национальный исследовательский университет ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Вариант №16

Лабораторная работа №2.2

«Атака на алгоритм шифрования RSA методом повторного шифрования»

По дисциплине:

«Информационная безопасность»

Работу выполнила:

Студентка группы P34102

Никонова Наталья Игоревна

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Вариант

16	381864434327	1195459	163872954111 20331233144 247841893982 24077680684 186232454225 170708316287 287353419177
			53300545679 235380537126 229388042972 213972178887 351137706462 71827041797

Выполнение

В качестве зашифрованного текста я взяла самый первый блок из варианта, так как он был меньше N.

Итоговая фраза: размер экрана и отсутствие клавиатуры препятствуют _

Вывод

В ходе выполнения лабораторной работы я попробовала дешифровать текст, зашифрованный алгоритмом RSA, методом повторного шифрования. Правда из-за того, что всю работу за меня сделала программа (за это ей конечно спасибо

большое, так как шагов оказалось 56784) во время выполнения работы алгоритм постичь не удалось. Так что его удалось запомнить только через чтение дополнительных материалов, но не через моторную память.