МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ
Кафедра интеллектуальных информационных технологий

Отчет
по дисциплине
«Современные методы защиты информации»
по лабораторной работе № 3
«Атака на алгоритм шифрования RSA»

Выполнил:
студент 4 курса
группы ИИ-22
Заречный А.О.
Проверила:
Хацкевич А.С.

Брест 2024

Цель: изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Постановка задачи:

Разработать приложение для декодирования зашифрованного текста, используя Китайскую теорему об остатках.

Вариант	Модуль			Блоки зашифрованного текста		
	N_1	N_2	N_3	C_1	C_2	C_3
21	570206339323	572010531679	573673162471	400967861722	400511331925	365230039044
				402921963995	359110439723	503139848290
				345366187498	156672928720	452112473725
				170749944344	81237697207	98832137945
				398474550143	446268495117	16750539498
				14128843304	567101402400	496867432761
				525338681306	380678770261	98372266130
				553357177665	405322363448	349596187748
				554714202377	250349383856	172522293935
				378737847392	480141604318	161623878001
				241207247252	201068876886	405142270947
				330231009566	160562856485	404286756199

Ход работы:

На языке Python реализовали требуемое приложение:

Рисунок 1 – Ссылка на исходные файлы

Вывод программы:

```
Исходные блоки:
0b11010000 0b11100101 0b11101010 0b11101110
0b11101100 0b11100101 0b11101101 0b11100100
0b11110011 0b11100101 0b11101100 0b00100000
0b11101111 0b11100101 0b11110000 0b11100101
0b11110101 0b11100010 0b11100000 0b11110010
0b11111011 0b11100010 0b11100000 0b11110010
0b11111100 0b00100000 0b00100001 0b11101100
0b11100101 0b11101101 0b11100101 0b11100101
0b00100000 0b00110001 0b00110010 0b00111000
0b00100000 0b11100001 0b11100000 0b11101001
0b11110010 0b00100000 0b11101111 0b11100000
0b11101010 0b11100101 0b11110010 0b11100000
Исходный текст:
Рекомендуем перехватывать !менее 128 байт пакета
```

Вывод: изучили и реализовали атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.