УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

**Лабораторная работа №2.4**

*Атака на алгоритм шифрования RSA, основанная на Китайской теореме об остатках*

*Вариант 22*

Студент

*Патутин В. М.*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Исходные данные:

е = 3

*N1 =* 582980801989

*N2 =* 585089367091

*N3 =* 586408807447

C1 =   
428799001102   
417746620458   
233652090970   
425829696584   
132807280253   
540064099057   
191642450251   
364237792802   
294540030550   
287338190886   
8030576378   
562848664519

C2 =

330278110381

413803169370   
399528613141   
431344022162   
133251402314   
579394141601   
339286468279   
235332969532   
1036448642   
400656499573   
47204841232   
249621210713

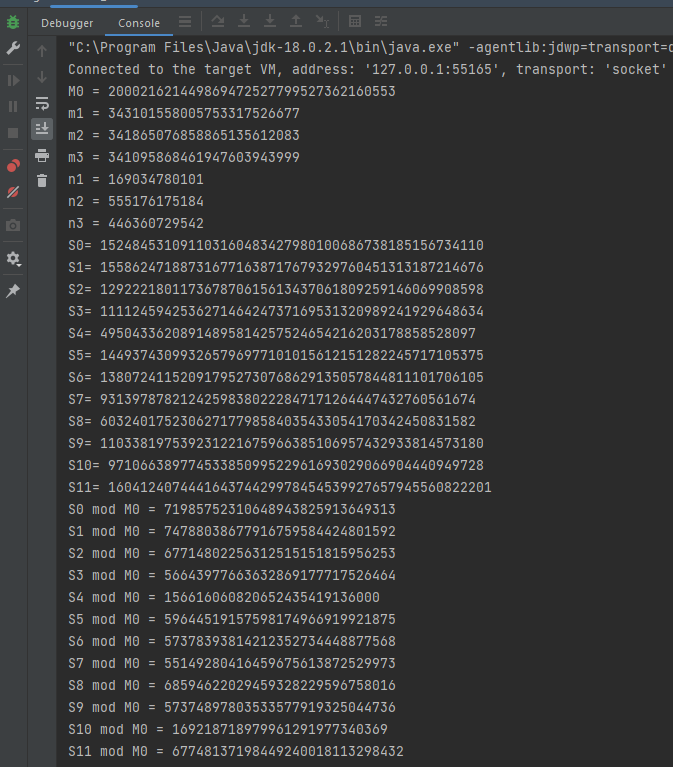
C3 =

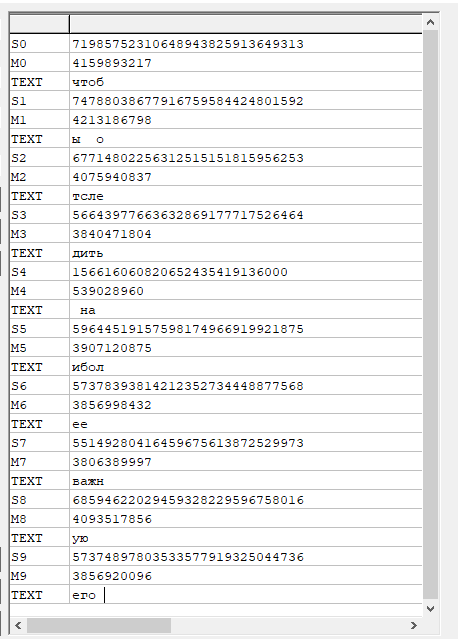
426468615928   
348743875265   
261688856582   
29957256669   
108448874326   
23970225383   
410917339855   
179638698652   
282723305676   
115801357719   
575898855271   
528022904569

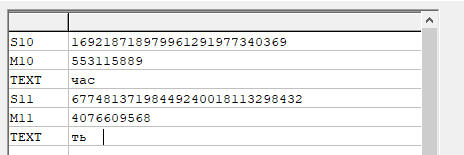
Алгоритм выполнения

1. Вычисляем M0 = N1∙N2∙N3;
2. Вычисляем m1 = N2∙N3;
3. Вычисляем m2 = N1∙N3;
4. Вычисляем m3 = N1∙N2;
5. Вычисляем n1 = m1^ (–1) mod N1;
6. Вычисляем n2 = m2^ (–1) mod N2;
7. Вычисляем n3 = m3^ (–1) mod N3;
8. Вычисляем S = c1∙n1∙m1 + c2∙n2∙m2 + c3∙n3∙m3;
9. Вычисляем S mod M0;
10. Вычисляем M = (S mod M0)^(1/e);
11. Получаем исходный текст.

Выполнение работы







Вывод программы

чтобы отследить наиболее важную его часть

Выводы

В данной лабораторной работе я изучил *атаку на алгоритм шифрования RSA, основанная на Китайской теореме об остатках*