

УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

Лабораторная работа №2.2

Атака на алгоритм шифрования RSA методом повторного
шифрования

Вариант 22

Студент

Патутин В. М.

P33101

Преподаватель

Маркина Т. А.

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Исходные данные:

$N = 914022837691$

$e = 517823$

Блок текста C:

133088999278

758078110965

705889026842

98403371042

768948684522

78137927374

383272719045

341665550116

407871370619

382219973835

653544166840

658599075370

825218892763

Алгоритм выполнения

1. Определяем порядок экспоненты при помощи программы PS. Для этого значение модуля помещаем в поле N, экспоненты в поле e, в поле Y записывается произвольное число. В поле X появится значение, равное корню e степени от числа Y по модулю N, а в поле i – порядок e.
2. Дешифруем зашифрованный текст. В область редактирования поля C поместить блоки зашифрованного текста, значение модуля в поле N, экспоненты в поле e и порядка экспоненты в поле i. Получаем исходный текст в области редактирования M.

Выполнение работы

The screenshot shows a software window titled "PS" with standard Windows window controls (minimize, maximize, close). The interface is divided into several sections:

- Исходные данные:** A row of input fields for N, e, and Y. N contains "914022837691", e contains "517823", and Y contains "12213". To the right is a checkbox labeled "Show results".
- Intermediate values:** Below the inputs are fields for Y^{i-1} and Y^i , both currently empty.
- Calculated values:** Below those are fields for X and i. X contains "573188840917" and i contains "75012".
- Buttons:** A button labeled "Запуск повторного шифрования" (Start re-encryption) is highlighted with a dashed border. To its right is a "Pause" button.
- Text Areas:** At the bottom, there are two large text areas labeled "C" and "M". Above them is a tab labeled "Дешифрация" (Decryption). Both text areas are currently empty.

PS

Исходные данные: $N =$ 914022837691 $e =$ 517823 $Y =$ 12213 ☐ Show results

$Y_{i-1} =$ $Y_i =$

$X =$ 573188840917 $i =$ 75012

С М

133088999278
758078110965
705889026842
98403371042
768948684522
78137927374
383272719045
341665550116
407871370619
382219973835
653544166840
658599075370
825218892763

активные серверы, измерить загруженность сети и ____

Исходный текст:

активные серверы, измерить загруженность сети и ____

Выводы

В данной лабораторной работе я изучил атаку на алгоритм шифрования RSA посредством повторного шифрования.