МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА
ПО ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЕ НА ТЕМУ

«Механизмы контроля целостности данных»

ОП.09 « Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. _____14.10.2020_____ _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель: исследование порядка вычисления и проверки ЭЦП (электронной цифровой подписи)
Задание вариант 2

p	q	e	d	M
17	11	7	23	8866

8866 -> 8*8*6*6 =2304
N = p*q=17*11=187
r = (p-1)*(q-1)=(17-1)*(11-1)=160
e = 7
d = 23
N = 187
r = 160
Cipher = (Msg)^e mod N = 121
Msg = (Cipher)^d mod N=77
Поскольку 8866> N надо воспользоваться ASCII
Сообщение, преобразованное в код ASCII: 56,56,54,54
Значит по формуле message^E % N мы получаем: 177,177,142,142
Дешифрация_message^D % N мы получаем 56,56,54,54
Что равно сообщению в ASCII коде

Вывод: в ходе работы было выведено способ шифрации и дешифрации данных, а также был изучен порядка вычисления и проверки ЭЦП