Государственное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

09.03.02 200008 006

**«Защита информации»**

Семестр 4

Отчёт по лабораторной работе №3

Изображение выглядит как текст

Автоматически созданное описание

Преподаватель: Кибардин А.В.

      Студент: Киселев В.А.

       Группа: Фт-200008

Дата: 16.03.2022

Екатеринбург 2022 г.

**Задание 1 для отчета**

Пусть абоненты А и В выбрали простое число р=23 и каждый их них независимо от другого выбрал числа a=5 и b=7 соответственно.

Пусть абонент А отправляет сообщение m=17 абоненту В.

1. Найти вторые ключи и .

2. Вычислить значения , , , .

1. ,

2. ,

,

,

,

## **Задание 2 для отчета**

, – простые числа

, – простые числа

, – случайные числа, выбранные и соответственно.

Пусть абонент решает послать абоненту сообщение .

1. Вычислить секретные ключи.

2. Вычислить значения m1, m2.

1.Секретные ключи:

α ≡

β ≡

2. Значения m1, m2:

по определению.

## **Задание 3 для отчета**

Пусть банкир выбрал числа и , а вкладчик – и .

Банкир выбрал случайное число , а вкладчик – число .

Вкладчик дает поручение своему банкиру.

1. Вычислить секретные ключи вкладчика и банкира.

2. Вычислить значения .

1. Ключ вкладчика

Ключ банкира

2. Значения .