|  |
| --- |
| https://lh6.googleusercontent.com/QcftzNtI05T0Y6fjdSh1Rr2rt8oqZ1IvnLvbn1jLJ7CCyteVir3k-xBLv4SL1wAgWJsRhmmJSR0UW-RP63_GQenE4vVWv05BRoZTsmIcBccVTnfxwmsnNMvjg599x9SqZd8E3dkd |
| МИНОБРНАУКИ РОССИИ |
| **Федеральное государственное бюджетное образовательное учреждение****высшего образования**"МИРЭА **-** Российский технологический университет"РТУ МИРЭА |

Институт Информационных Технологий

Кафедра Вычислительной Техники (ВТ)

**Отчет по лабораторой работе №2**

по дисциплине

**«Защита Информации»**

Выполнил: Нани М.Б.

ИВБО-04-15

Руководитель: Воронков С.O.

Москва 2018

**Цель:**

**Цель:**  
Сформировать общий ключ для двух пользователей, используя общие параметры A, P, и закрытого ключа X.  
  
**Пункты выполнения:**  
1. Получение пользователями общих параметров и формирование закрытого ключа с помощью генератора случайных чисел;  
2. Вычисление пользователями числа Y по формуле Y = Ax mod P;  
3. Обмен пользователей полученными значениями числа Y;  
4. Формирование общих ключей по формулам:  
Z1 = (Y2) x1 mod P;  
Z2 = (Y1) x2 mod P;  
  
**Вывод:**  
Общие ключи были вычислены пользователями, не передаваясь друг другу.

**Ссылка:**

https://github.com/Maximovix/Lab2\_ZI