**Молдавский государственный университет**

**Факультет математики и информатики**

**Департамент Информатики**

**УПРАЖНЕНИЕ**

**Создание ключей с помощью Диффи-Хеллмана**

**Выполнил**: Гуцу Даниил.

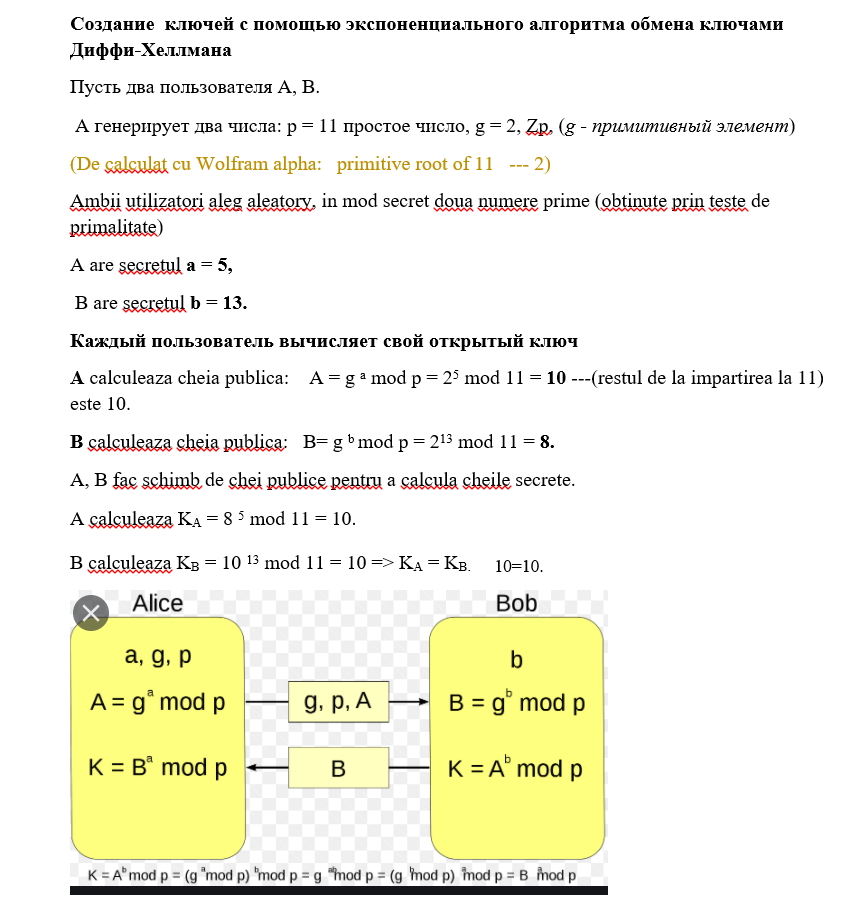
**Группа:** IA2102

**Проверила:** др.,Чербу О.

Кишинев, 2023

**КИШИНЕВ – 2023**

Алгоритм:



Код программы:

public class Hellman {  
 public static void main(String[] args) {  
 KeyProvider provider1 = new KeyProvider(23, 5, 3);  
 KeyProvider provider2 = new KeyProvider(23, 5, 7);  
  
 System.*out*.println("encrypt1: " + provider1.encryptPublicKey());  
 System.*out*.println("encrypt2: " + provider2.encryptPublicKey());  
  
 System.*out*.println("decrypt1: " + provider1.decryptPublicKey());  
 System.*out*.println("decrypt2: " + provider2.decryptPublicKey());  
 }  
}  
  
class KeyProvider {  
 private Integer p, g, a;  
 private Integer publicKey;  
  
 public KeyProvider(Integer p, Integer g, Integer a) {  
 this.p = p;  
 this.g = g;  
 this.a = a;  
 }  
  
 private Double calculatePublicKey(Integer g, Integer a) {  
 return Math.*pow*(g, a);  
 }  
  
 public Integer encryptPublicKey() {  
 return publicKey = calculatePublicKey(this.g, this.a).intValue() % p;  
 }  
  
 public Integer decryptPublicKey() {  
 return calculatePublicKey(publicKey, a).intValue() % p;  
 }  
}

Вывод программы:

encrypt1: 10

encrypt2: 17

decrypt1: 11

decrypt2: 20