**Молдавский государственный университет**

**Факультет математики и информатики**

**Департамент Информатики**

**УПРАЖНЕНИЕ**

**Adler**

**Выполнил**: Гуцу Даниил.

**Группа:** IA2102

**Проверила:** др.,Чербу О.

Кишинев, 2023

**КИШИНЕВ – 2023**

Алгоритм Адлера (Adler-32) - это хеш-функция, используемая для вычисления контрольных сумм (хешей) для данных. Этот алгоритм часто применяется в сетевых протоколах и архиваторах для проверки целостности данных. Адлер-32 был разработан Марком Адлером в 1995 году.

Основная идея алгоритма Адлера заключается в том, чтобы вычислить два 32-битных значения, называемых "A" и "B", которые являются контрольными суммами для блока данных. Алгоритм принимает на вход массив байтов и последовательно обрабатывает каждый байт. Вначале A и B устанавливаются в начальные значения (обычно 1 для A и 0 для B). Затем для каждого байта данных выполняются следующие операции:

1. A увеличивается на значение байта.

2. B увеличивается на текущее значение A.

После обработки всех байтов данных, контрольная сумма Adler-32 вычисляется следующим образом:

1. Величина A сдвигается на 16 бит влево.

2. Затем к A добавляется значение B.

Полученное значение A является 32-битной контрольной суммой Adler-32 для входных данных.

Преимущество алгоритма Адлера-32 заключается в его простоте и относительной быстроте вычислений. Однако он не обеспечивает стойкость к коллизиям и не подходит для криптографических целей. Адлер-32 может использоваться для быстрой проверки целостности данных, но не для обеспечения безопасности данных от злоумышленников.

Код программы:

package adler;  
  
import java.math.BigInteger;  
import java.util.Scanner;  
  
public class Adler {  
 public static final int *MODULO\_CONSTANT* = 65521;  
  
 public static void main(String[] args) {  
 Scanner scanner = new Scanner(System.*in*);  
  
 System.*out*.println("Enter message to encrypt");  
 String plainText = scanner.nextLine();  
  
 System.*out*.println("Message is : " + plainText + " Hash: " + *createAdlerHash*(plainText));  
 plainText = "The quick brown fox jumps over the lazy dog";  
  
 System.*out*.println("Message is : " + plainText + " Hash: " + *createAdlerHash*(plainText));  
  
 scanner.close();  
 }  
  
 public static String createAdlerHash(String plainText) {  
 BigInteger a = BigInteger.*ONE*, b = BigInteger.*ZERO*;  
  
 for (int i = 0; i < plainText.length(); i++) {  
 a = a.add(BigInteger.*valueOf*(plainText.charAt(i)));  
 b = b.add(a);  
 }  
 b = b.mod(BigInteger.*valueOf*(*MODULO\_CONSTANT*));  
 a = a.mod(BigInteger.*valueOf*(*MODULO\_CONSTANT*));  
 return *convertToMyHex*(b) + *convertToMyHex*(a);  
  
 }  
  
 public static String convertToMyHex(BigInteger num) {  
 return String.*format*("%4s", num.toString(16)).replace(" ", "0");  
 }  
}

Вывод программы:

Enter message to encrypt

vlabla

Message is : vlabla Hash: 08c90273

Message is : The quick brown fox jumps over the lazy dog Hash: 5bdc0fda