Лабораторна робота №1.

Гешування.

Мета.

Дослідити принципи роботи гешування.

Завдання.

Дослідити існуючі механізми гешування. Реалізувати алгоритм гешування SHA (будь-якої версії). Реализацію інших алгоритмів гешування слід омовити з викладачем. Довести коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями (напр. утилітою sha1sum).

Виконання.

SHA-1 – це алгоритм шифрування даних. Ідея алгоритму полягає в тому, щоб отримати фрагмент відкритого тексту і потім незворотно перетворити його на фрагмент (зазвичай меншого) зашифрованого тексту. Його також можна просто зрозуміти як отримання рядок вхідних кодів (називається попереднім відображенням або інформацією), і перетворити їх у коротку вихідну послідовність з фіксованою цифрою, яка є хеш-значення (також відоме як інформаційний дайджест або код автентичності інформації).

Довжина вхідного повідомлення алгоритму не обмежена і на виході виходить 160-бітний дайджест повідомлення. Вхід обробляється 512-бітовими групами. SHA-1 незворотний, запобігає зіткненням і має гарний лавинний ефект.

Метод шифрування вихідного тексту.

```
public class Sha {

  public static String shaEncode(String str) throws Exception{

         System.out.println ("исходная строка:" + str);

         MessageDigest sha=null;

         try{

          sha = MessageDigest.getInstance("SHA");

         }catch(Exception e){

          System.out.println(e.toString());

          e.getStackTrace();

          return  "";

         }

         byte[] byteArray = str.getBytes("utf-8");

         byte[] md5Bytes = sha.digest(byteArray);

         StringBuffer hexValue= new StringBuffer();

         for (int i = 0; i < md5Bytes.length; i++) {

          int val=((int)md5Bytes[i])& 0xff;

          if(val<16){

           hexValue.append("0");

          }

          hexValue.append(Integer.toHexString(val));

         }

          System.out.println ("Шифрование:" + hexValue.toString ());
```

```
        return  hexValue.toString();

}
```

Результати роботи програми.

```
вихідна строка:Вхідний текст
Шифрування:5fc54942d52b22ba802531ca89c860fd7b42ba33
```

Висновки.

Дослідили принципи роботи гешування.