IT8761 - SECURITY LAB

DATE : 21/12/20
SESSION : FN

NAME : SWETHA SRI T S
REG NO. : 312217104175
DEPT : CSE - 'C'

Develop a Java Program to implement the MD5 Algorithm

AIM :

To develop a java program to implement the MD5 Algorithm.

ALGORITHM :

Step 1 : Read the Plaintext message as input

Step 2 : Divide the plaintext message into 512 bit blocks

Step 3 : Append Padding bits, A single '1' bit is appended to the message, and then '0' bits are appended so that the length in bits of the padded message equals to 448 mod 512

Step 4 : Append Length, a 64-bit representation of length of message is appended

Step 5 : Initialise MD buffers, A, B, C, D, E

Step 6 : Invoke the compress function for four times

Step 7 : Display the message digest from the buffers

METHODS USED :

1. String messageDigest (String input)

- Input of this method is string message of any length.
- Output of this method is 32 bit hexadecimal string which is the 512 bit message digest.

2. public static void main (String [] args)

- This is the main function
- It accepts string input from user
- Prints message digest string as output

PACKAGES AND FUNCTIONS USED :

1. Big Integer

- java.math.Biginteger is math package in java used to store numbers with greater values.

2. Message Digest

- java.security.MessageDigest is present in security package of java
- used to create a messagedigest instance of MD5 using getinstance() method with arguement 'MD5'.
- used to convert input bytes into byte[] digest using MessageDigest.digest() function.

SAMPLE INPUT AND OUTPUT :

Enter Input String : annauniversity

Message digest : 9f9e9e27766l9eaa4794181eb62b

Output is a 32 length (128 bits) hexadecimal string.

RESULT :

Thus a Java program to implement MD5 algorithm was executed successfully

NAME: Swetha sri T S
REG NO: 312217104175

SSN College of Engineering
University Practical Examinations
IT 8761 Security Laboratory

CODE:

```
class Main {
 public static String messageDigest(String input){
   try{
     BigInteger numberFromDigest;
     MessageDigest m = MessageDigest.getInstance("MD5");
     byte[] digest = m.digest(input.getBytes());
     numberFromDigest = new BigInteger(1,digest);
     String hexText = numberFromDigest.toString(16);
     while(hexText.length()<32){
       hexText="0"+hexText;
     }
     return hexText;
   }catch(NoSuchAlgorithmException e){
     throw new RuntimeException(e);
   }
 }
 public static void main(String[] args) {
   Scanner sc=new Scanner(System.in);
   System.out.println("Enter Plaintext: ");
   String inputMessage=sc.nextLine();
   System.out.println();
   System.out.println("MessageDigest: "+messageDigest(inputMessage));
   System.out.println();
   sc.close();
 }
}
```

OUTPUT:

Example 1:

```
javac -classpath .:/run_dir/junit-4.12.jar:target/dependency/* -d . Main.java
java -classpath .:/run_dir/junit-4.12.jar:target/dependency/* Main
Enter Plaintext:
annauniversity

MessageDigest: 9f9e9e2776619eaa4794181eb62be833
```

Example 2:

```
javac -classpath .:/run_dir/junit-4.12.jar:target/dependency/* -d . Main.java
java -classpath .:/run_dir/junit-4.12.jar:target/dependency/* Main
Enter Plaintext:
Betty bought some butter

MessageDigest: 3ba3432359fc04814097ee1f4728f5b8
```