MES Wadia College of Engineering Pune-01

Department of Computer Engineering

Name of Student:	**Class: TE Comp**
Semester/Year: 6th	**Roll No:**
Date of Performance:	**Date of Submission:**
Examined By: Prof(Dr.)S.K.Wagh	**Experiment No: Part 2-IS-06**

PART 2- LPII-ELII-IS-ASSIGNMENT NO: 06

AIM:
Calculate the message digest of a text using the MD5 algorithm in JAVA.

OBJECTIVES:

1. Understanding Hash Functions

- Gain a comprehensive understanding of hash functions, their properties, and how they are used in information security.
- Learn about the characteristics of cryptographic hash functions, including determinism, quick computation, pre-image resistance, small changes in input drastically change the output, and collision resistance.

2. Grasping the MD5 Algorithm

- Understand the specifics of the MD5 (Message Digest Algorithm 5) hashing algorithm, including its purpose, operation, and structure.
- Study the steps involved in the MD5 hashing process: padding, appending the length, initializing MD buffer, processing the message in 16-word blocks, and outputting the final digest.

3. Implementing MD5 in Java

- Learn how to use Java's cryptographic library to implement the MD5 algorithm.
- Develop skills in utilizing Java's Message Digest class for generating a message digest from an input string.

APPRATUS:

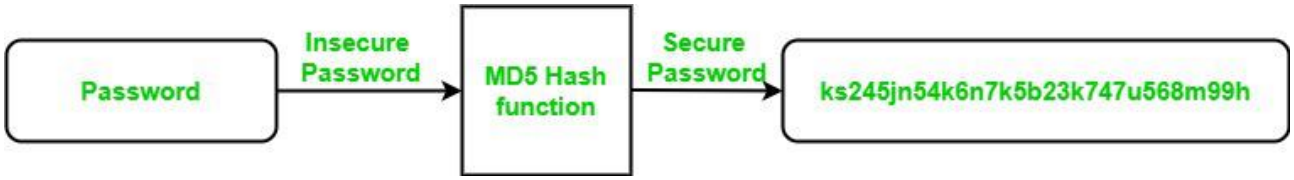
- Operating System recommended: 64-bit Open source Linux or its derivative.

THEORY:

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always 128 bits. MD5 was developed in 1991 by Ronald Rivest.

Use of MD5 Algorithm:

- It is used for file authentication.
- In a web application, it is used for security purposes. E.g. secure password of users etc.
- Using this algorithm, we can store our password in 128 bits format.



Working of the MD5 Algorithm:

MD5 algorithm follows the following steps

1. Append Padding Bits: In the first step, we add padding bits in the original message in such a way that the total length of the message is 64 bits less than the exact multiple of 512.

Suppose we are given a message of 1000 bits. Now we have to add padding bits to the original message. Here we will add 472 padding bits to the original message. After adding the padding bits the size of the original message/output of the first step will be 1472 i.e. 64 bits less than an exact multiple of 512 (i.e. 512*3 = 1536).

Length(original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. Append Length Bits: In this step, we add the length bit in the output of the first step in such a way that the total number of the bits is the perfect multiple of 512. Simply, here we add the 64-bit as a length bit in the output of the first step.

i.e. output of first step = 512 * n – 64

length bits = 64.

After adding both we will get 512 * n i.e. the exact multiple of 512.

3. Initialize MD buffer: Here, we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.

- J = 0x67425301

- K = 0xEDFCBA45

- L = 0x98CBADFE

- M = 0x13DCE476

4. Process Each 512-bit Block: This is the most important step of the MD5 algorithm. Here, a total of 64 operations are performed in 4 rounds. In the 1st round, 16 operations will be performed, 2nd round 16 operations will be performed, 3rd round 16 operations will be performed, and in the 4th round, 16 operations will be performed. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2nd G function, 3rd for the H function, and 4th for the I function.

We perform OR, AND, XOR, and NOT (basically these are logic gates) for calculating functions. We use 3 buffers for each function i.e. K, L, M.

- F(K,L,M) = (K AND L) OR (NOT K AND M)

- G(K,L,M) = (K AND L) OR (L AND NOT M)

- H(K,L,M) = K XOR L XOR M

- I(K,L,M) = L XOR (K OR NOT M)

After applying the function now we perform an operation on each block. For performing operations we need

add modulo 232

M[i] – 32 bit message.

K[i] – 32-bit constant.

<<<n – Left shift by n bits.

Now take input as initialize MD buffer i.e. J, K, L, M. Output of K will be fed in L, L will be fed into M, and M will be fed into J. After doing this now we perform some operations to find the output for J.

In the first step, Outputs of K, L, and M are taken and then the function F is applied to them. We will add modulo 232 bits for the output of this with J.

In the second step, we add the M[i] bit message with the output of the first step.

Then add 32 bits constant i.e. K[i] to the output of the second step.

At last, we do left shift operation by n (can be any value of n) and addition modulo by 232.

After all steps, the result of J will be fed into K. Now same steps will be used for all functions G, H, and

I. After performing all 64 operations we will get our message digest.

Output:

After all, rounds have been performed, the buffer J, K, L, and M contains the MD5 output starting with the lower bit J and ending with Higher bits M.

Application Of MD5 Algorithm:

- We use message digest to verify the integrity of files/ authenticates files.
- MD5 was used for data security and encryption.
- It is used to Digest the message of any size and also used for Password verification.
- For Game Boards and Graphics.

Advantages of MD5 Algorithm:

- MD5 is faster and simple to understand.
- MD5 algorithm generates a strong password in 16 bytes format. All developers like web developers etc use the MD5 algorithm to secure the password of users.
- To integrate the MD5 algorithm, relatively low memory is necessary.
- It is very easy and faster to generate a digest message of the original message.

Disadvantages of MD5 Algorithm:

- MD5 generates the same hash function for different inputs.
- MD5 provides poor security over SHA1.
- MD5 has been considered an insecure algorithm. So now we are using SHA256 instead of MD5
- MD5 is neither a symmetric nor asymmetric algorithm.

CONCLUSION:

We have successfully studied MD5 algorithm.

QUESTIONS:

1. What are vulnerabilities and limitations of the MD5 algorithm, including susceptibility to collision attacks?

2. Discuss why MD5 is no longer recommended for cryptographic security purposes and where it can still be appropriately used (e.g., checksums for file integrity verification).