A

Report On

**“Message Digest (MD5) Algorithm”**

**Under the subject**

**‘Network and Information Security [22620]’**

**Submitted by**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Enrollment No** | **Name of the student** |
| 1 | 1700100370 | Mr. Patil Pratik Kumar |
| 2 | 1800100002 | Mr. Kare Abhilash Sudam |
| 3 | 1800100392 | Mr. Pawar Vivek Appaso |

**Under the guidance of**

Mrs. Korade L. S.

Department of Computer Engineering

Government Polytechnic, Karad

**1.0 Rationale**

The MD5 message-digest algorithm is a widely used [hash function](https://en.wikipedia.org/wiki/Hash_function) producing a 128-[bit](https://en.wikipedia.org/wiki/Bit) hash value. Although MD5 was initially designed to be used as a [cryptographic hash function](https://en.wikipedia.org/wiki/Cryptographic_hash_function), it has been found to suffer from extensive vulnerabilities. It can still be used as a [checksum](https://en.wikipedia.org/wiki/Checksum) to verify [data integrity](https://en.wikipedia.org/wiki/Data_integrity), but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

In this project we have implemented MD5 algorithm using java. We used Security package of java which is specially designed for information security purpose. We used special type of class MessageDigest which is specially designed for MD5 algorithm. The program accepts a string and generates a hash code using MD5 algorithm.

**2.0 Aim of the project**

This micro-project aims were

1. To analyze working of Message Digest Algorithm.
2. To address importance of message encryption in network security.
3. To study Network and Information Security.
4. To implement Message Digest Algorithm using Java.

We have achieved all the aims which were decided at the start of the project. We have completed the project with achieving all the aims at the completion.

**3.0 Course Outcomes Achieved**

1. Identify risks related to Computer security and Information hazard in various situations.
2. Apply cryptographic algorithms and protocols to maintain Computer Security.

**4.0 Literature Review**

|  |  |  |
| --- | --- | --- |
| **Author (Publication)** | **Contribution** | **Conclusion** |
| Aradhna Sahu (ResearchGate) | This paper consisted of the information about hashing algorithms. | We used this paper to understand the concept of hashing algorithms. |
| Alok Kumar Kasgar (IJMEMR) | This paper explains the advantages and limitations of MD5 algorithm. | We used this paper to analyze advantages and limitations of MD5 algorithm. |
| Geeks for Geeks (Article) | This article consisted of java program for implementing MD5 algorithm. | We used this article to implement java program for MD5 algorithm. |
| Mary Cindy Ah Kioon (ResearchGate) | This paper explains the working of MD5 algorithm. | We used this paper to understand working of MD5 algorithm. |
| Shweta Mishra (IJSRD) | This paper explains the features of MD5 algorithm. | We used this paper to understand features if MD5 algorithm. |
| Prashant P. Pittalia(IJCSMC) | This paper consisted of comparative study of MD5 algorithm and SHA1 algorithm | We used this paper to understand difference between MD5 algorithm and SHA1 algorithm. |

**Table 1- Literature Review**

**5.0 Actual procedure followed**

Actual procedure followed during the project is mentioned in the table below with the planned start date and completed finish date.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Details of Activity** | **Planned Start Date** | **Completed Finish Date** | **Name of responsible Team Members** |
| 1. | Collecting information about MD5 algorithm. | 16/12/2019 | 25/12/2019 | 1. Patil Pratik  2. Pawar Viwek |
| 2. | Collecting information about Information Security. | 26/12/2019 | 02/01/2020 | 1. Pratik Patil  2. Kare Abhilash  3. Pawar Viwek |
| 3. | Understanding concepts of Java Programming Language | 03/01/2020 | 08/01/2020 | 1. Patil Pratik  2. Pawar Viwek |
| 4. | Developing logic of MD5 algorithm using java | 09/01/2020 | 20/01/2020 | 1. Pawar Viwek  2. Kare Abhilash |
| 5. | Implementing MD5 algorithm using java | 21/01/2020 | 03/02/2020 | 1. Pratik Patil  2. Kare Abhilash  3. Pawar Viwek |
| 6. | Observing Output | 05/02/2020 | 13/02/2020 | 1. Pratik Patil  2. Kare Abhilash  3. Pawar Viwek |
| 7. | Preparing final project report | 14/02/2020 | 22/02/2020 | 1. Patil Pratik  2. Kare Abhilash |

**Table 2- Actual procedure followed**

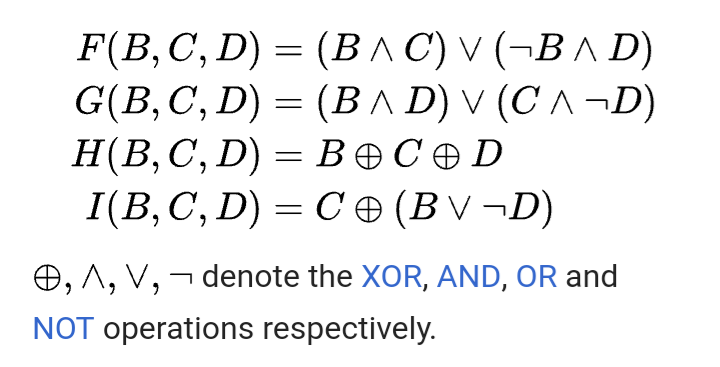
**General details about MD5 algorithm**

|  |  |
| --- | --- |
| **General** | |
| Designer | Ronald Rivest |
| First published | April 1992 |
| Series | MD2, MD4, MD5, MD6 |
| **Cipher detail** | |
| Digest sizes | 128 bits |
| Block sizes | 512 bit |
| Rounds | 64 |

**Table 3. General details of MD5 algorithm**

**MD5 Algorithm:**

1. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.
2. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264.
3. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state.
4. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation.
5. Fig. 1 illustrates one operation within a round. There are four possible functions; a different one is used in each round:



**Fig 1. Four possible functions in MD5 algorithm**

**Code**

package project;

import java.math.BigInteger;

import java.security.MessageDigest;

import java.io.\*;

import java.security.NoSuchAlgorithmException;

public class Abc {

public static String getMd5(String input)

{

try {

MessageDigest md = MessageDigest.getInstance("MD5");

byte[] messageDigest = md.digest(input.getBytes());

BigInteger no = new BigInteger(1, messageDigest);

String hashtext = no.toString(16);

while (hashtext.length() < 32) {

hashtext = "0" + hashtext;

}

return hashtext;

}

catch (NoSuchAlgorithmException e) {

throw new RuntimeException(e);

}

}

public static void main(String args[]) throws Exception

{

System.out.println("Enter String to generate Hashcode");

BufferedReader br=new BufferedReader(new InputStreamReader(System.in));

String s=br.readLine();

System.out.println("Your HashCode Generated by MD5 is: " + getMd5(s));

}

}

**Advantages of MD5 algorithm:**

1. MD5 algorithms are useful because it is easier to compare and store these smaller hashes than to store a large text of variable length.
2. The MD5 algorithm is a widely used algorithm for one-way hashes that are used to without necessarily giving the original value.
3. It is very easy to generate a message digest of the original message using this algorithm.
4. MD5 algorithm can perform the message digest of a message having any number of bits, it is not limited to message in multiplies of 8, unlike MD5sum which is limited to octets.

**Limitations of MD5 algorithm**

1. MD5 has prone to hash collision weakness, i.e. it is possible to create the same hash function for two different inputs. MD5 does not provide security for this collision.
2. It is not suitable for digital signatures.
3. It is slow than optimized SHA algorithm.

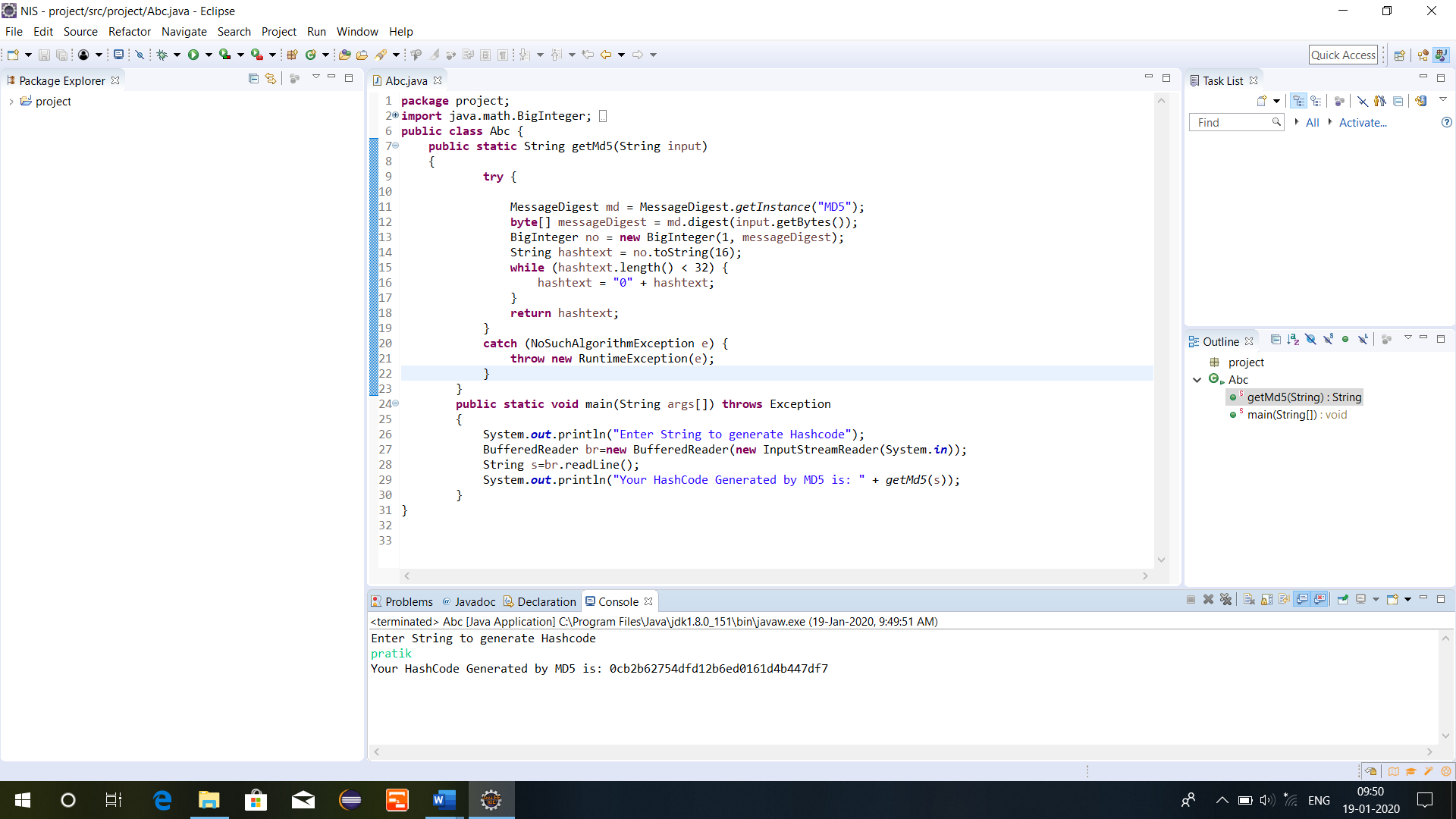
**6.0 Actual Resources Required**

The resources used during the completion of project are mentioned in the below table:

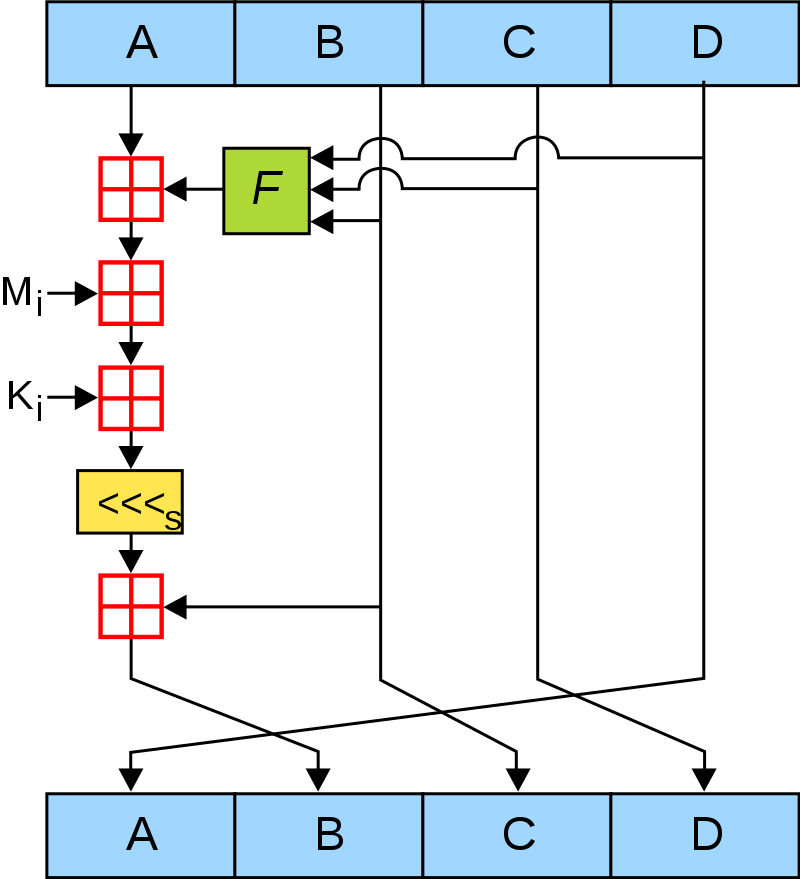
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Name of resources material** | **Specifications** | **Quantity** | **Remarks** |
| 1. | YouTube | MP4-file format, 640 x 360 pixels | 1 |  |
| 2. | Microsoft Word | 2010 version | 1 |  |
| 3. | Laptop | Dell, RAM 8 GB, Harddisk 1 TB, i3 processor | 1 |  |
| 4. | Eclipse | Oxygen | 1 |  |

**Table 3- Resources required**

**7.0 Outputs of the Micro-project**



**Fig 2. Output of the program**

****

**Fig 3. Working of MD5 algorithm**

**8.0 Skill Developed/ learning out of this Micro-Project**

We learnt,

1. Analyzing real world applications of Hash code generation.
2. Importance of Message Digest Algorithm.
3. Importance of Hash code generation algorithms in Information Security.
4. Efficient communication skills.
5. Working as a team.
6. Developing leadership qualities.

**9.0 Applications of the Project**

1. This project can be used in the understanding the importance of Hash code generation algorithm that is Message Digest (MD5) algorithm.
2. The project can be also used to make people aware about the information security.
3. The project can be used to generate hash code and original string using Message Digest (MD5) algorithm.

**Subject Teacher**

**Mrs. Korade L. S.**