MINOR PROJECT 2

MID SEM REPORT

on

INFORMATION SECURITY USING SALTING,

HASHING AND ENCRYPTION

Submitted By :

|  |  |  |
| --- | --- | --- |
| **Name** | **Roll No** | **Branch** |
| Vibhor Jain | R100216094 | CSE OSOS |
| Shashi Kumar | R100216076 | CSE OSOS |
| Yash Kumar | R100216097 | CSE OSOS |

Under the guidance of Dr. Adarsh Kumar Associate Professor

Department of Systemics



School of Computer Science UNIVERSITY OF PETROLEUM AND ENERGY STUDIES Dehradun-248007

2017-18

Approved By

(Dr. Adarsh Kumar) (Dr. Monit Kapoor)

Project Guide Department Head

ABSTRACT

Information Security using hashing, salting and encryption development using java. Salting and hashing are used for password protection and cryptography. We will use Java to use hashing and salting techniques with their algorithms to perform various operations such as input validation, validation of basic languages, encrypt the messages using salt and store some passwords in high security. This project shows the security measures which are used in today’s world to keep our data safe.We are completing two different tasks in one code which allows user to complete their work a little bit faster. One is handling invalid input while other is encrypting and decrypting messages (cryptography) using salting. Thus user can encrypt messages while their input will automatically get validated without any manual work. We are applying salting technique to make it more secure. Thus we are making sure that data entered is valid and then encrypt it and using salting to make sure that the security of user data is maintained throughout the flow of the process. It has a lot of advantages the foremost being security of data which everyone wants to have .In today’s world data leaks are very common and can be really harmful .We are making our project to create a sense of security for the user.

TABLE OF CONTENTS

Contents

1 Introduction ………………………………………………………………………..5

2 Objective …………………………………………………………………………5

3 Design ………………………………………………………………………...5

4 Implementation …………………………………………………………………………8

4.1 Pseudocode ……………………………………………………………………….8

4.2 Output Screen ……………………………………………………………………..9

A APPENDIX I PROJECT CODE

LIST OF FIGURES

List of Figures

1. Flowchart . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .6
2. Use-case ……………………………………………………………………………..7

1 Introduction

In today’s world everybody wants their data safe and data leaks are becoming more and more harmful everyday with all of our important and personal information stored electronically. So, everybody wants there data safe and various techniques were developed for keeping data safe from hackers who intercept the messages and claim the user’s personal data. Thus encryption, decryption ,cryptography etc came into the picture and ever since then new techniques have been developing to protect data from being stolen .We will be showcasing two of these techniques. These techniques are used throughout the world to keep our data safe and create security for the user .Info validation using hashing salting and encryption advancement using java .Salting and hashing are utilized for secret phrase assurance and cryptography.

2 **Objective**

Encrypting and Decrypting messages (cryptography) using salting and hashing.

Creating a UI for user’s input and output

Input will automatically get validated without any manual work.

**Sub-objectives:-**

Encrypt the messages using salt

Decrypt the encrypted code

To make it user friendly

Validating the user Input

Providing high security level

3 **DESIGN**

The code is programmed in such a way that it can detect errors and encrypt or decrypt data for safety reasons. We will be designing user interface for input and output. AES is one of the best techniques for encrypting the messages and keeping it secure. where Salting and hashing are utilized for secret phrase assurance and cryptograph Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

TEXT

**FLOWCHART**

Encryption process

Encryption process

Import data from text

Encrypt text using alogorithm

Encrypted Text

Import data from encryted text

Decryption process

Decrypt Text using algorithm

Text

Figure no.1-

(Flowchart of encryption and decryption)

**USECASE DIAGRAM**

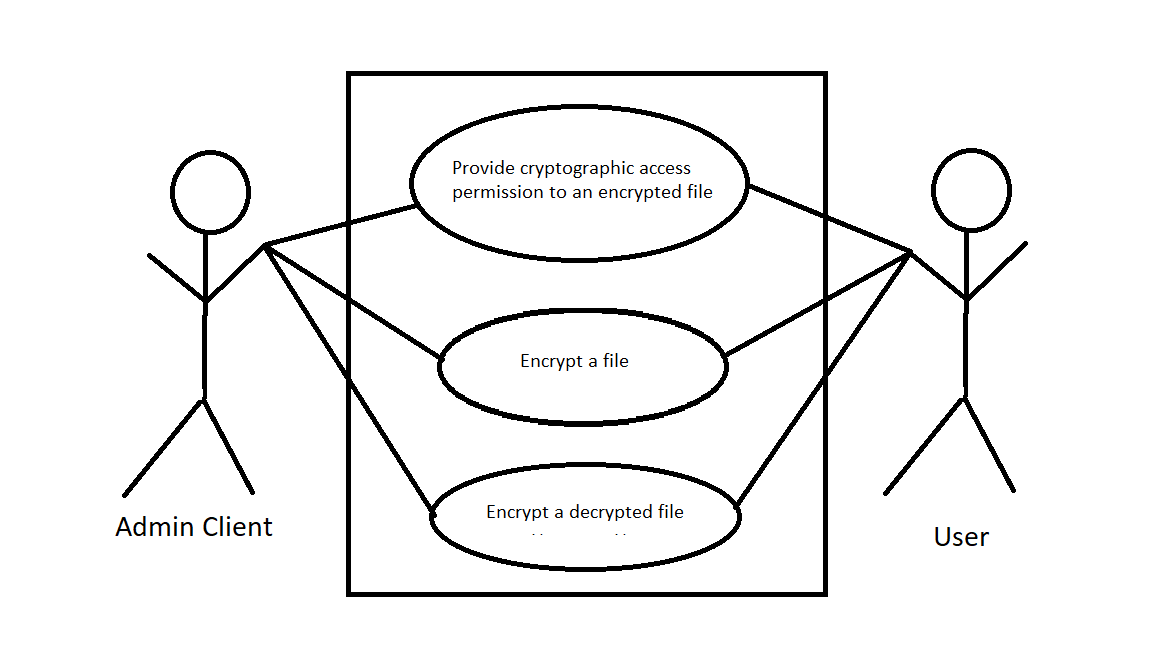


Figure no.2 –Usecase of Encryption and Decryption

4 **Implementation**

The text editor is programmed in such a way that it can detect errors and encrypt or decrypt data for safety reasons . AES is one of the best techniques for encrypting the messages and keeping it secure.[1][2]

4.1 **Pseudocode**

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster.

These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.

2. Initialize state array and add the initial round key to the starting state array.

3. Perform round = 1 to 9 : Execute Usual Round.

4. Execute Final Round.

5. Corresponding cipher text chunk output of Final Round Step

**i *Usual Round :*** Execute the following operationswhich are described above.

* 1. Sub Bytes
  2. Shift Rows
  3. Mix Columns
  4. Add Round Key , using K(round)

**ii *Final Round:*** Execute the following operationswhich are described above.

* + 1. Sub Bytes
    2. Shift Rows
    3. Add Round Key, using K(10)

**iii *Encryption :*** Each round consists of the followingfour steps:

1. Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
2. Shift Rows : In the encryption, the transformation is called Shift Rows.
3. Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
4. Add Round Key : Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the “Mix columns” step. [4]

***iv Decryption:*** Decryption involves reversing all thesteps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the “Inverse mix columns” step.

4.2 Output Screen

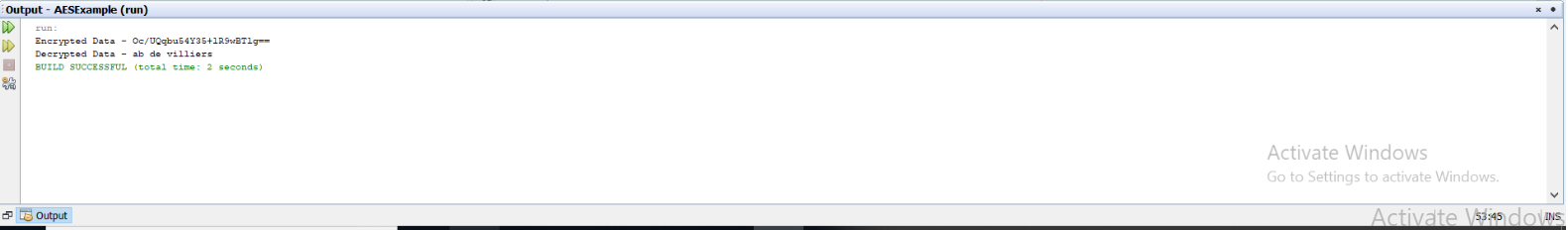
1. 

Figure no-3(output1)

2.

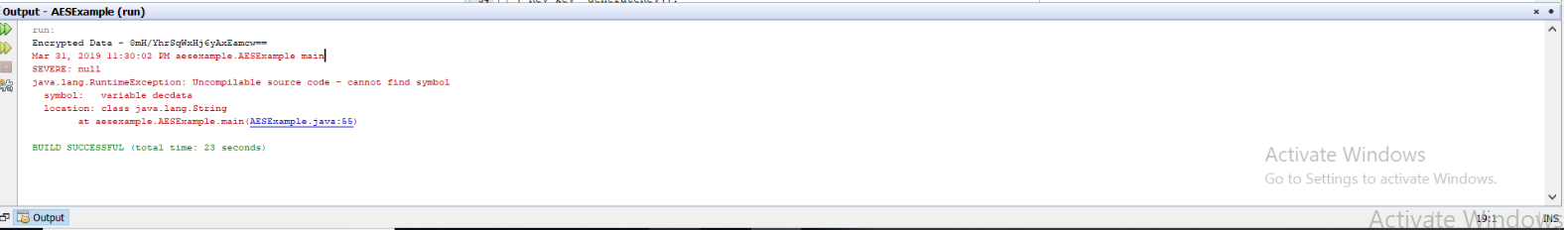


Figure no-4(output2)

References

1. Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. “Analyzing the speed of combined cryptographic algorithms with secret and public key”. International Journ a l of Engineering Research and Development ,e- ISSN : 2278 - 067X, p - ISS N : 2278 - 800X, www.ijerd.com Volume 8, Issue 2 (August 2013) , pp. 45

2. Chehal Ritika, Singh Kuldeep. “Efficiency and Security of Data with Symmetric Encryption Algorithms”. Internat ional Journ a l of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 8, August 2012, pp. 1.

8