**Information Search and Analysis Skills**

**“ Implementation of Encryption MD5 using PHP”**

Written by : 1. Jasmine Nabila Novel (1610010037)

2. Yansiska (1610010045)

Faculty : Ms. Emma Yulianti, ST, MM

Semester : 4st (Four Semester)

Quarter : 8th (Eight Quarter)

Class : 4SC4

PREFACE

Praise be to the Lord of the universe for all the blessings, grace, and His guidance so that we can finish the ISAS with the title “Implementation of Encryption MD5 using PHP".

In the preparation of this ISAS, the authors derive a lot of help from various parties. The author wishes to thank Ms. Emma Yulianti college teacher preceptor who has provided guidance and direction so that we can finish this ISAS, as well as both parents, large family’s authors, and fellow college student CCIT-FTUI always pray and give motivation to the authors.

The authors recognize that there is still a lot of ISAS shortcomings. Therefore, the authors expect criticism and suggestions so this ISAS can be better. Final terms of reference the authors hope this paper can provide insight and knowledge to the readers in general and the author in particular.

Depok, May 2018

Writer

TABLE OF CONTENTS

[PREFACE](#_Toc513195829) i

[TABLE OF CONTENTS](#_Toc513195830) ii

[TABLE OF FIGURE](#_Toc513195831) iv

[CHAPTER I 1](#_Toc513195832)

[INTRODUCTION 1](#_Toc513195833)

[I.1 Background 1](#_Toc513195834)

[I.2 Writing Objective 2](#_Toc513195835)

[I.3 Problem Domain 2](#_Toc513195836)

[I.4 Writing Methodology 2](#_Toc513195837)

[I.5 Writing Framework 2](#_Toc513195838)

[CHAPTER II 4](#_Toc513195839)

[BASIC OF THEORY 4](#_Toc513195840)

[II.1 Definition of Cryptography 4](#_Toc513195841)

[II.2 The Definition and The Various Types of Encryption Methods 4](#_Toc513195842)

[II.2.1 Definition of Encryption 4](#_Toc513195843)

[II.2.2 Encryption Types 5](#_Toc513195844)

[II.3 Definition Of Hash Function 6](#_Toc513195845)

[II.4 Definition of Encryption MD5 7](#_Toc513195846)

[CHAPTER III 8](#_Toc513195847)

[PROBLEM ANALYSIS 8](#_Toc513195848)

[III.1 Implementation Algoritm MD5 8](#_Toc513195849)

[III.2 Implementation Programs Encryption Using PHP 9](#_Toc513195849)

[III.3 Advantages and Disadvantages Encryption MD5 12](#_Toc513195849)

[CHAPTER IV 15](#_Toc513195850)

[CONCLUSION AND SUGGESTION](#_Toc513195850)

[IV.1 Conclusion 15](#_Toc513195849)

[IV.2 Suggestion 15](#_Toc513195849)

[BIBLIOGRAPHY](#_Toc513195850)

TABLE OF FIGURE

[Figure 2.1 Diagram Blok Processing Encryption and Description 4](#_Toc508567105)

[Figure 2.2.2.1 Diagram Public Key of Asymmetic 5](#_Toc508567106)

[Figure 2.2.2.2 Diagram Private Key of Symmetrical 6](#_Toc508567107)

[Figure 3.1.3 Algorithm of MD5 9](#_Toc508567105)

[Figure 3.2.1 Register Account MD5 using PHP 10](#_Toc508567106)

[Figure 3.2.2 Database with Encryption Password 10](#_Toc508567107)

[Figure 3.2.3 Form Login Decryption Password MD5 11](#_Toc508567107)

[Figure 3.2.4 Form Sucessed Login 11](#_Toc508567107)

[Figure 3.2.5 Code MD5 using PHP 12](#_Toc508567107)

CHAPTER I

INTRODUCTION

I.1. Background

Technological developments are growing rapidly around the world. Technology has a very important role in human life today. Because of human presence, the presence of technology can make it easier for us to interact with others at any one time. Technology today is one of the most important things in the world today.

Data security and confidentiality issues are an important aspect of an information system. If talking about security issues related to the use of computers, it is difficult to separate them with cryptography. Cryptography aims to provide security services, including security to maintain passwords. The password data must be maintained or protected by its confidentiality. Do not let existing password data, fall into the hands of people who are not entitled or interested. Common passwords are used for authentication services, either authenticating the authenticity of the communicating party (user authentication or entity authentication) or identifying the authenticity of the data origin authentication.

To maintain password security can be done by encrypting the password (plaintext) into ciphertexts by encryption or enciphering (standard name according to ISO 7498-2). While the process of returning ciphertexts into plaintexts (password) was originally called decryption. In addition to using encryption, to maintain password security can also by using hash function In this ISAS, described about MD5 Encryption Implementation using PHP MySQL.

I.2.Writing Objective

This ISAS to knowing about :

1. Definiton of Cryptography
2. Definition and The Various Types of Encryption Methods
3. Definition of Hash Function
4. Definition Encryption MD5
5. Implementation Encryption MD5 Using PHP
6. Advantages and Disadvantages of MD5

I.3. Problem Domain

The problem domain based on the formulation in the differences can be said to be the problem as follows: " Implementation of Encryption MD5 using PHP "

I.4. Writing Methodology

The method used is the method of research with data collection techniques using literatur from reliable media. Including browsing and knowledge from friend.

I.5. Writing Framework

To facilitate the preparation of the ISAS, the use a writing framework as follows:

**Chapter I Introduction**

This section describes the background of the title with the writing objective, problem domain, writing methodology, writing framework.

**Chapter II Basic Theory**

Tell about Definition of Cryptography, Definition of Hash Function and Encryption of MD5.

**Chapter III Problem Analysis**

Analyzing and solve the problem that contained in problem domain.

**Chapter IV Conclusion and Suggestion**

This section describes about conclusion and suggestion.

CHAPTER II

BASIC THEORY

II.1 Definition of Cryptography

Cryptography is the study of encryption techniques where the "original text" (the plaintext) scrambled using an encryption key to be "random texts that are difficult to read" (ciphertext) by someone who does not have the decryption key.

In Cryptography a message that will be kept secret would be encoded using an algorithm. The message has been encoded called plaintext and posts that have been scrambled or encoded called ciphertext. The process to convert plaintext into ciphertext is called encryption (encrypt) and the process to recover the plaintext from the ciphertext is called decrypting (decrypt).

The block diagram, the process of with encryption and decryption can be described as follows:

D:\DATA KULIAH CCIT\4SC4\ISAS Q7\Revisi ISAS 4SC4\gbr 1.PNG

Figure 2.1 Diagram Blok Processing Encryption and Description

II.2 The Definition and The Various Types of Encryption Methods

**II.2.1 Definition of Encryption**

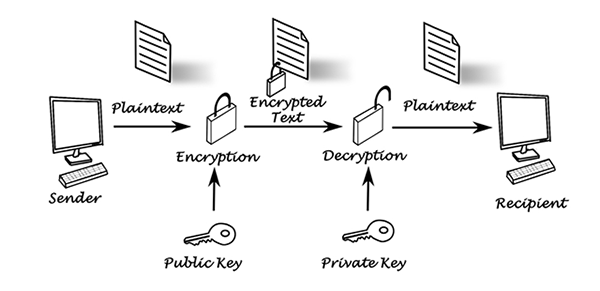
Information security on the internet prepared with a whole range of methods, you might not realize that the data you send is encrypted first. The data is sent in the form of raw (unencrypted) is called plaintext. The data is then encrypted using the encryption algorithm and encryption keys.

The process of generating a new form called chipertext. This Chipertext was only able to read when outlined in advance by using a key that fit her, the process of changing the form of chipertext into plaintext is called decryption.

**II.2.2 Encryption Types**

Encryption can be divided into two types, namely:

1. Public Key – Key of Asymmetric

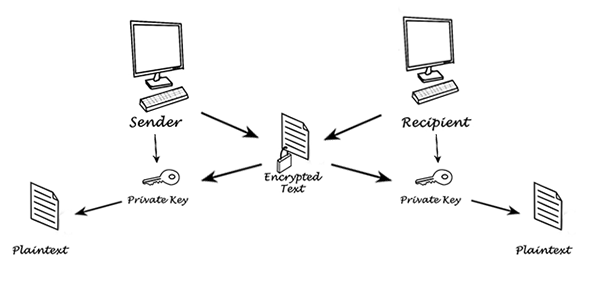


**Figure 2.2.2.1 Diagram Public Key of Asymmetic**

Asymmetric cryptography or also known as public-key cryptography, using two different keys: one public and one private related mathematically. The public key can be shared with everyone, whereas the private key must be kept secret. RSA asymmetric algorithm is the most widely used.

Example case: Boy (sender) will send a data to the Rose (recipient). Boy encrypts data with public key which he had, and then sends it to Rose. And only the Rose that is able to decrypt the data by using the private key that he had. In this scenario the public key used to encrypt the data, while the private key is used to decryption the data.

2. Private Key – Key Symmetrical



**Figure 2.2.2.2 Diagram Private Key Symmetrical**

Symmetric keys use the same key for encryption and decryption on the data. At the moment will decrypt, the sender must first share private keynya to be decrypted by the recipient. A symmetric key that is the most widely used is AES, which was created to protect the confidential information of the Government..

II.3 Definition Of Hash Function

One of the basic primitive things in cryptography modern is a frequent cryptographic hash function called a one-way hash function. Hash function is a function with a binary string input which is arbitrary and produces strings binary with a fixed length. The hash function is the most widely used in cryptography is for data integrity and digital signatures hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of length but output is always of fixed length values returned by a hash function are called message digest or simply hash values.

II.4 Definition of Encryption MD5

MD5 is one of a series of message-digest algorithms designed by Professor Ronald Rivest of the Massachusetts Institute of Technology (MIT). When analytic work indicates that MD5's MD4 predecessor was starting to be unsafe, then MD5 was then designed in 1991 in replacement of MD4. A 128-bit (16-byte) MD5 Hash, also known as the message's digest, is typically displayed in 32-digit hexadecimal digits. MD5 has been used in a variety of security applications and MD5 is also commonly used to perform data integrity testing.

CHAPTER III

PROBLEM ANALYST

III.1 Implementation Algoritm MD5

MD5 algorithm is an algorithm that uses the one-way hash function created by Ron Rivest.

  The cryptographic work of the MD5 algorithm is to receive input in the form of a message of any size and generate a message diggest that has a length of 128 bits. Here's an illustration of the drawing of message diggest generation on MD5 algorithm cryptography

1. The addition of padding bits. The first process is to add a message with a number of bit wedge so that the length of the message (in units of bits) congruent with 448 modulo 512. This means after adding bits of booster, now the length of the message is 64 bits less than a multiple of 512. The thing to remember is the 512 number appears because the MD5 algorithm processes messages in blocks of size 512.
2. Increase the value of the original message length. Then the next process is the message added again with 64 bit which states the length of the original message. If the message length is greater than 264 then the length is taken in modulo 264. in other words, if initially the message length is equal to K bit, then 64 bit adds K modulo 264. so that after the second process is done then the message length now is 512 bits.

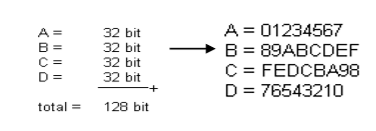
3. Initialize buffer (MD) buffer. In the MD5 algorithm it takes four buffers, the four buffer names are A, B, C and D, respectively. Each buffer is 32 bits long. The total length of the buffer is 4 '32 = 128 bits. These four buffers accommodate the intermediate and final results so that the total length is 128 bits.

Figure 3.1.3 Algorithm of MD5

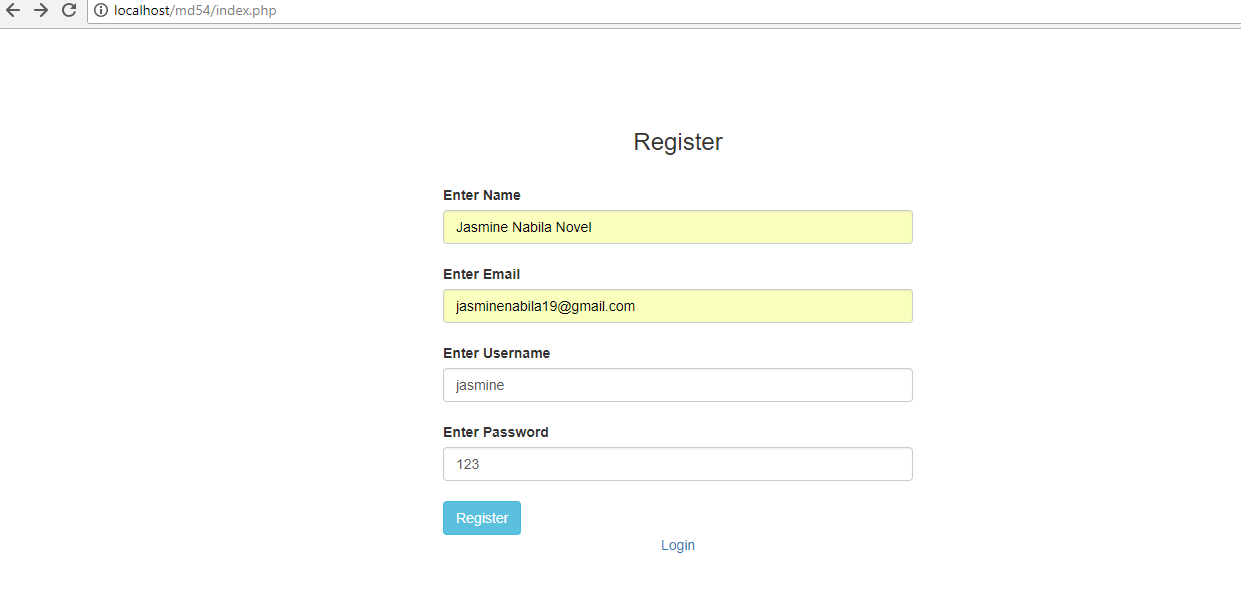
The four buffers above accommodate the intermediate and final results. Each buffer is initialized with values (in Hexadecimal notation).

III.2 Implementation Programs Encryption Using PHP

In the implementation phase, secure the database login by using encryption on user password data . languages used are php language and mysql database.

1. Form Register

Before login, the user register first to enter the database. Here is how it looks

****

**Figure 3.2.1 Register Account MD5 using PHP**

1. Database Design

Because only for login and register only, enough with one table that is table register consists name, username, password. here is the contents of the table register

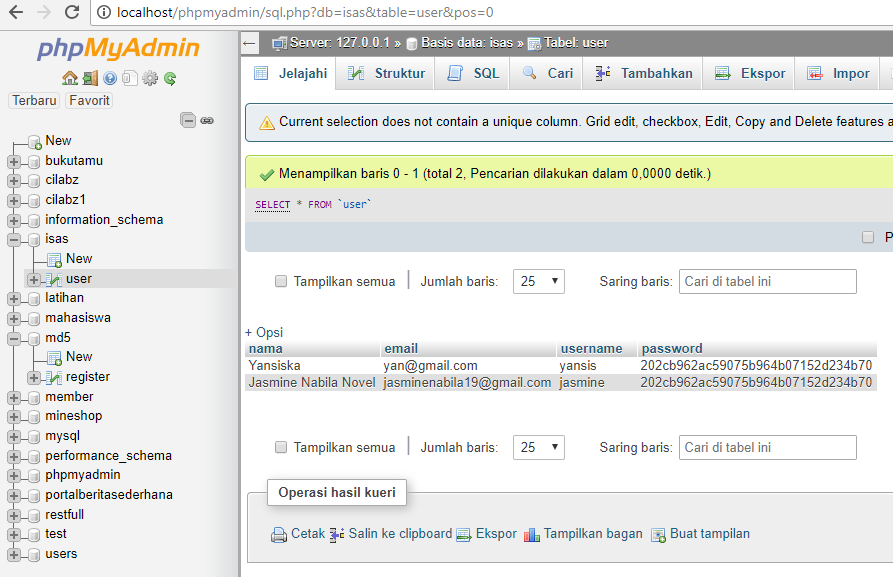


Figure 3.2.2 Database with Encryption Password

1. Form Login

The login form is used by the user to log into the system. User / user fill in username and password in accordance with the data that has been filled at the time of registration, then click Login. If the username and password are entered according to the one in the database, it will go into the data list. But if the username and password do not match, will remain in the login page.

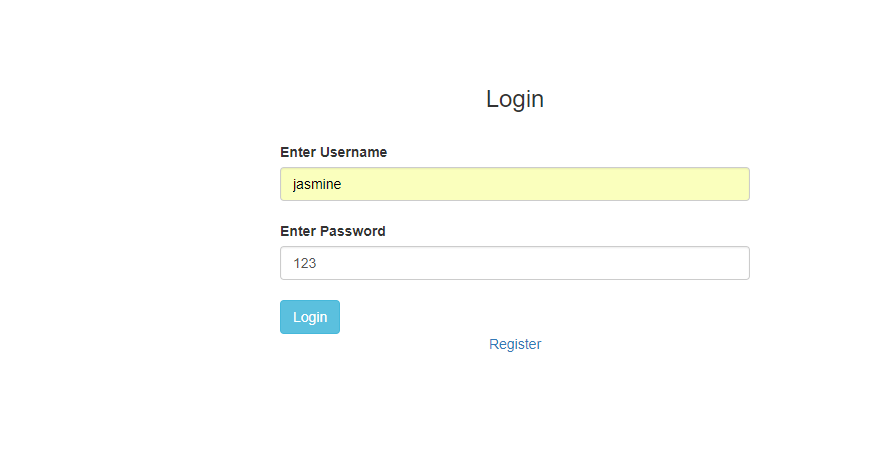


Figure 3.2.3 Form Login Decryption Password MD5

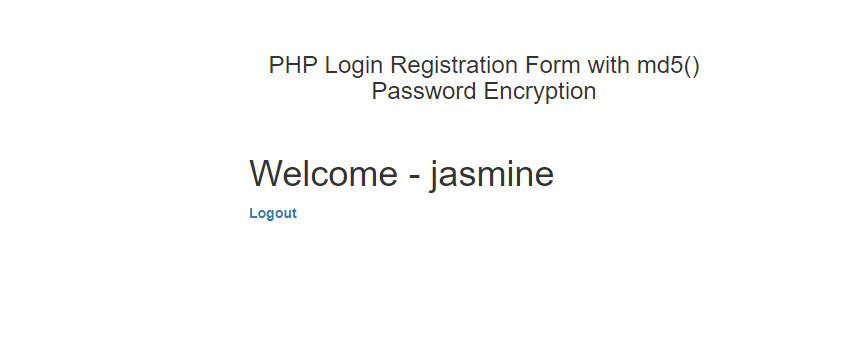


Figure 3.2.4 Form Succesed Login

1. Implementation Code PHP

The following code to use md5 password only write md5 and connect to the database.

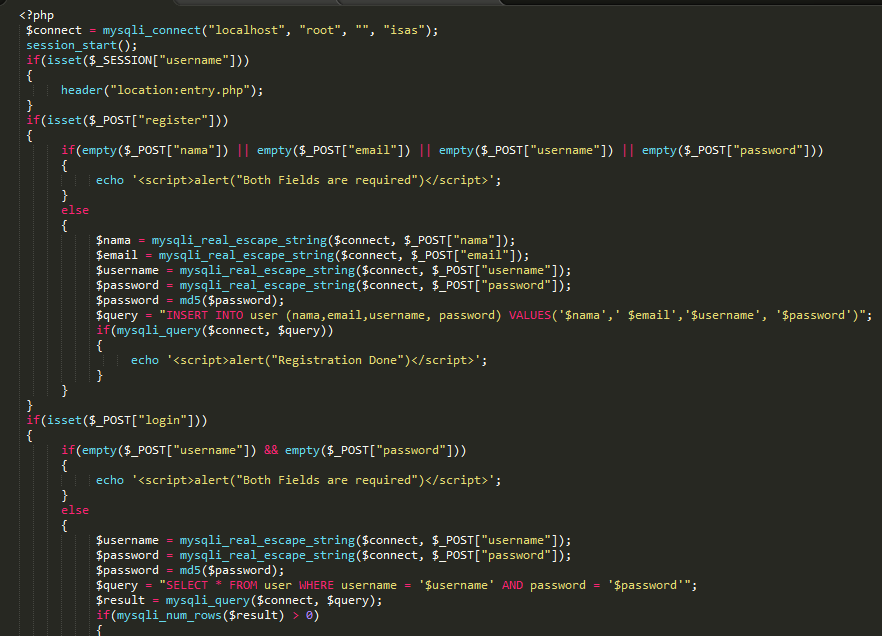


Figure 3.2.5 Code MD5 using PHP

III.3 Advantages and Disadvantages Encryption MD5

* Advantages

1. For file integrity verification

The authenticity of the file, whether the file has been changed or not. Usually when downloading a file from internet md5 acts as an algorithm used to prove whether the downloaded file is still original or not.

1. Md5 excess as a detector of file changes

for example on tripwire on linux. This is from an instruction detection system where if any file is changed its hash value then IDS will turn on the alarm that there has been a change of file.

1. The password storage on MD5 is more efficient
2. The md5 algorithm is very sensitive in the smallest data changes.

The MD 5 algorithm with its hash function is very sensitive to message changes, so the MD5 algorithm is suitable for applications that maintain the integrity of a data.

* Disadvanatages

1. Collision Attack

Md5 tends to be susceptible to collision attacks where events of 2 different values can have the same hash value. This cacusion is used to enter fake SSL network certificates.

1. Vulnerable Preimage Attack

Preimage attacks are generally more complex than collision attacks and it is not uncommonly the only alternative to do this attack is to use brute force.

1. Further cryptanalysis against MD5

In about 5 years after its launch, a warning is then issued not to rely on MD5 for uses that require collision resistance. A completely different input can also be relatively easily adjusted so that its hash value is the same as any other message, provided that there is a snippet of both messages whose collision has been found.

1. The process of changing the original data into MD5 takes a relatively long time (hardware resources)

md5 hash process first to convert plaintext data to chiper, then Once accepted so that data can be read and understood by data recipient, data must go through md5 hash process of converting chiper to plaintext After data through process of converting chiper to plaintext. The process of changing the original data into MD5 takes a relatively long time (hardware resources)

CHAPTER IV

CONCLUSION AND SUGGESTION

IV.1 Conclusion

MD5 cryptography algorithm with its own encryption capability can be a recommendation for data security and computer system network. The MD5 cryptography algorithm can be exploited in a variety of security applications, whether for document files, database or network security. Although this is not the only magical solution and may not necessarily solve all security issues, but as much as possible reduce the many security risks facing the organization. The MD5 cryptographic application can be developed with other programming languages as well as a combination of other methods to strengthen the integrity of the document. The MD5 cryptography algorithm will not affect or disturb the authenticity of a document.

IV.2 Suggestion

Database encryption techniques can be developed using other cryptographic algorithms to establish better data security and then This system works on text data, so hopefully further research can be implemented on image data, voice, or video.

BIBLIOGRAPHY

1. Tjiharjadi, Semuil and Chandra Wijaya, Marvin,21 Mei 2009, *“Pengamanan Data Menggunakan Metoda Enkripsi Einstein”,* UPN ”Veteran” Yogyakarta, Indonesia.
2. <https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/> [03-05-2018]
3. <https://www.nesabamedia.com/pengertian-enkripsi/> [03-05-2018]
4. <https://www.scribd.com/mobile/document/43964955/Definisi-Kriptologi> [03-05-2018]
5. <https://steemit.com/cryptography/@bosbandet/pengertian-dan-contoh-kriptografi-dengan-proses-enkripsi-dan-deskripsi-36ec6defefcb3> [03-05-2018]