# CHAPTER I

# PRELIMINARY

## 1.1 Background

Security is something that is very necessary for daily activities in all aspects. Almost every aspect of human activities requires security such as self-security, security in the world of work, security to safeguard personal assets, including the security of data. Before the 1970s, cryptographic technology was used only for military and diplomatic purposes. The development of science and communication technology such as the internet has made cybercrime more widespread because of the ingenuity of hackers or hackers who are increasingly good at committing crimes through the internet, such as sniffing, spoofing, tapping and others. So as to make users both individuals and businesses begin to realize the importance of protecting valuable information. Protection of data confidentiality is increasing. One way is to encode data so that the original form is no longer recognized.The use of computers is now connected to each other through networks with various transmission media. This opens up opportunities for important data used by other uses both legally and illegally.

To maintain important data stored in the computer user must be managed by grouping or collecting important data in a folder and folder that is protected or protected by an application that can prevent access to other unauthorized uses. Cryptography is an important technique that must be used to record data against third parties or eavesdroppers. Cryptography provides important aspects of information security such as data confidentiality, data integration, authentication, and non-repudiation. With this cryptography, it is expected that the stored data will be safer from the tapper.

But from the fast-growing era, data security, especially those already connected to the internet, are vulnerable to hacking. Because the algorithm technique used in securing data, especially those on a network, is too weak. By implementing the SHA-256 implementation it is hoped that the stored data will become safer. In this study, the author focused on securing Get parameters found on the web site.

## 1.2 Formulation of the problem

Based on the description of the background above, the problem can be formulated as follows:

1. How to design and use the hash algorithm SHA-256 GET parameters in a web.
2. How to implement the SHA-256 algorithm in the programming language PHP.

## 1.3 Initial hypothesis

The initial hypothesis of the formulation of the problem is obtained that:

Security SHA-256 algorithm will be more difficult in the breaks with SQL Injection Union Select. While security web site without the algorithm SHA-256 will easily inserted SQL Injection Union Select.

## 1.4 Scope of problem

Limitation of problems in this thesis is the Get parameter protection by applying the SHA-256 algorithm. Then compare in terms of power in the algorithm against SQL Injection attacks Union Select.

## 1.5 Research methods

The method of research conducted in several stages, namely:

1. Study of literature

   At this stage, a reference collection or needed in the research literature. This is done to obtain information and data necessary for the writing of this skirpsi. Reference or literature used can be books, journals, articles, and Internet sites related to Kriptografim hash function, and SHA256 algorithms.

2. Data Collection and Analysis

   At this stage the collection and analysis of data related to this study, such as the function of SHA256 algorithms can be implemented into the program, so that the author can determine the effectiveness and efficiency of the algorithm.

3. System planning

   Designing the system in accordance with a predetermined plan, which includes the initial interface design as the home page to display news or content of the web. That where there are two web, the web dummy and a web that has been implemented with SHA256 algorithms.

4. Application System

   At this stage of the manufacturing system has been completed and the results SHA256 add data into the system.

5. Testing Systems

   At this stage it will be tested against the system that has been developed.

6. Conclusions and Documentation System

   From the analysis, it will be made conclusions about the test results of the hash algorithm is applied to the system, as well as documentation of the system from the initial stage to the testing system, to then be made in the form of a research report (thesis).

## 1.6 Writing system

This thesis is divided into five chapters, namely:

a. Chapter 1 : Preliminary

   Contains background of the problem, objectives, problem definition, methodology and systematics writing.

b. chapter 2 : Base Theory

   Discussing security systems, cryptography, hash function, web based application, SQL Injection, and Secure Hash Algorithm 256.

c. Chapter 3 : Research methods

   Includes designing a system for testing, tools used, as well as testing methods.

d. Chapter 4 : Implementation and Discussion

   In this section the author presents the results of testing done on the system and analyze the results of such testing.

e. Chapter 5 Conclusion and Suggestions

   Conclusions and suggestions of this thesis.