UNIVERSITI TEKNOLOGI MARA

PERFORMANCE EVALUATION OF SYMMETRIC CRYPTOGRAPHY ALGORITHM FOR DATABASE SYSTEM

MARIAM AZWA BINTI YAZID

Dissertation submitted in partial fulfilment of the requirements
for the degree of
Master of Science in Computer Networking

Faculty of Computer and Mathematical Sciences

January 2015

ACKNOWLEDGEMENT

I would like to express the deepest appreciation to my Supervisor Dr Fakariah Hani Hj Mohd Ali for her advice, support and encouragement in carrying out this research. I would also like to thank to Course Coordinator Dr Nor Shahniza Kamal Bashah for her guidance and assistance in writing and preparing the dissertation. Without their help I might not be able to complete my studies and reports with ease.

My deepest thank go to my husband; Suhaib bin Khairuddin, my kids; Adeena Fatihah , Iman Syuhada and my precious that still in my womb, parents, family and colleagues for their support and encouragement during the process of completing this research.

ABSTRACT

PERFORMANCE EVALUATION OF SYMMETRIC CRYPTOGRAPHY ALGORITHM FOR DATABASE SYSTEM

Cryptography has been proven to be the best method to secure a database. However there are many types of cryptography algorithm that has been established in the market. To choose the best cryptography methods requires a research to suit it with the system requirement. Normally, the performance of the encryption and decryption process is the major consideration.

This research evaluates the performance of three different symmetric cryptography algorithms. A series of testing cycles has been carrier out to identify the fastest algorithm. There are three types of measurement parameters that have been used for the testing. A Database System Engine has been developed to measure the performance of the algorithm.

The result of the experiment shows that the AES is the fastest algorithm compared to TripleDES and RC4. This result might give a clear idea to any organisation that would like to adopt any cryptography technique as their database security approach.

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

1.0 Introduction

Database is an organized repository of an indexed data. The data was organized and designed to be easily accessed, managed and updated. Database can be classified as the heart of a system. Database Management System (DBMS) is a platform that being used to manage the database. There are four main types of DBMS that has been identified as follows:

a. Hierarchical DBMS
b. Network DBMS
c. Relational DBMS
d. Object-oriented DBMS

According to Basharat (2012), the data security has become the most critical and unsolved crime. The most important concern in data security is how to protect the private and confidential data from unauthorized activity. Providing the confidentiality, integrity and availability to the data stored in the database is the critical component in database security.

Database control should be in place in order to have a secured database. Figure 1.1 shows the example of controls that should be incorporated in the database.