UNIVERSITI TEKNOLOGI MARA

IMPLEMENTATION OF AES ALGORITHM INTO INFORMATION INVESTIGATION AUTOPSY (IIA)

AHMAD WAFIY BIN AHAMAD ZAKI

BACHELOR OF SCIENCE (Hons.)
DATA COMMUNICATION AND NETWORKING

JULY 2013

ACKNOWLEDGEMENTS

"By the name of Allah, the Most Gracious and Most Merciful"

The research presented in this report could not been done without the support, encouragement and cooperation of many people. First of all, I would like to express my gratitude to my supervisor, Dr. Fakariah Hani binti Hj. Mohd Ali, who has always given valuable advice and encouragement to me. I also would like to thank him for giving this opportunity to learn and work under guidance, which has been memorable experience.

Special thanks to Dr. Nor Shahniza Kamal Bashah for her guidance to write this thesis report and her thoughtful suggestion at each stage in preparation of this project. Also thanks to all of my lecturers, which guide me to make this project paper successful. Without their cooperation, I would not be able to finish this project.

I also would like to thank to our entire family for their encouragement, knowledge and their constant prayer for me. Last but not least, thanks to my friends and associated for their encouragement, criticism and support for this project.

ABSTRACT

Information Investigation Autopsy (IIA) is the tools that can captured the information needed on the Local Area Network environment and later needed to be secured, the IIA need a module that can to secure the evidence captured from any harm. The objectives of this project are to apply the encryption algorithm into these tools for securing the information collected by keystroke logging mechanism. Therefore the Advance Encryption Standard (AES) algorithm is being implemented to secure the evidence captured. AES use high level description of algorithm that based on a design formula as a substitution permutation and fast implementation on software. AES also have 128 bits fixed on block size with the key size of 256, 192, or 128 bits and operates on 4 times 4 column byte matrix. The result of this project later will benefit the user.

TABLE OF CONTENT

ACKNOWLEDGEMENTS iv
ABSTRACT v
LIST OF ABBREVIATIONS viii
LIST OF TABLES ix
CHAPTER 1 1
INTRODUCTION 1
1.0 Background of Study 1
1.1 Problem Statement 2
1.2 Research Questions 2
1.3 Objectives 2
1.4 Project Scope 3
1.5 Outline of the Thesis 3
1.6 Research Significance 3
CHAPTER 2 4
LITERATURE REVIEW 4
2.0 Introduction 4
2.1 Cryptography 4
2.1.1 Encryption 4
2.1.2 Decryption 5
2.1.3 Symmetric-key 5
2.1.4 Public-key 5
2.1.5 Block cipher 5
2.1.6 AES Algorithm 6
2.2 Related Works 8
2.2.1 Pipelined Statistical Cipher Feedback: A New Mode for High-Speed Self-synchronizing Stream Encryption 8
2.2.2 Design of a New Block Cipher based on Conditional Encryption 9
2.2.3 Pseudo-Random Functions and Parallelizable Modes of Operations of a Block Cipher 10
2.2.4 Impossible differential cryptanalysis of reduced–round Camellia–256 11
2.2.5 Block Cipher Design: Generalized Single-Use-Algorithm Based on Chaos 12

CHAPTER 1

INTRODUCTION

1.0 Background of Study

Traditional information security solutions focus on securing IT systems against breached from outside the boundary. But, in today's combined and connected world, where there really are no longer openly defined perimeters, we have to place a great deal of faith in the awareness and integrity of trusted insiders and associates. However, while trusting our employees, suppliers and partners, we still have a responsibility to protect sensitive material. Only technology can realistically afford protection in difficult technical environment (Assuria, 2012).

Data encryption refers to the progress of altering electronic evidence into a scrambled form that can only be read by someone who knows how to decode. Encryption is significant in the business world because it is the easiest and most useful method of shielding data that is stored, processed, or transmitted electronically. It is vital to electronic business, for example, because it allows merchants to protect customers' credit card numbers and personal. It is also usually used to defend legal contracts, subtle documents, and private messages that are directed over the Internet. Without encryption, this information could be caught and altered or misused by unknowns. In addition, encryption is used to scramble sensitive information that is stored on business computer networks, and to create digital signatures to verify e-mail and other types of messages sent between businesses. (G. Cengage, 2002)