TRIBHUVAN UNIVERSITY
INSTITUTE OF SCEINCE AND TECHNOLOGY
CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
KIRTIPUR, KATHMANDU
NEPAL

ENHANCED SECURITY ENCRYPTION FOR DATA STORAGE USING MULTIPLE KEYS

BY:

SUSHIL NEPAL

A thesis submitted to the Central Department of Computer Science and Information Technology in partial fulfillment of the requirement for the Master's Degree in Computer Science and Information Technology

December, 2010

TRIBHUVAN UNIVERSITY
INSTITUTE OF SCEINCE AND TECHNOLOGY
CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
KIRTIPUR, KATHMANDU
NEPAL

CERTIFICATION

Mr. Sushil Nepal has carried out this thesis entitled **"Enhanced Security Encryption for Data Storage using Multiple Keys"** under my supervision and guidance. In the best of my knowledge this is an original work done by him in computer science. I, therefore, recommend for further evaluation.

……

Prof. Dr. Shashidhar Ram Joshi

Institute of Engineering

Pulchowk Campus,

Lalitpur,

Nepal

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor Prof. Dr. Shashidhar Ram Joshi for his guidance, encouragement, and optimism. His patience, support and confidence have been driving force of this thesis work. Furthermore, I would like to thank Dr. Brian Gladman for his support on the implementation of Secure Hash Algorithm which has been a key part for the completion of my thesis work.

I am also thankful to all members of my preliminary and final examination committees for going through the document and giving me valuable feedback. I am thankful to the staff at the University for their Cordial Support.

My gratitude goes to my teachers Prof. Subarna Shakya, Mr. Min Bdr. Khati, Mr. Samujjwal Bhandari, and to all my teachers at the Central Department of Computer Science and Information Technology. Special thanks go to my friends Mr. Laxman Thapa, Mr. Bhogendra Mishra, and Mr. Thaneshwor Pd. Paneru whose support, motivation and inspiration has been a key factor to complete my thesis work.

Last but not the least, this work would have been impossible without mentioning my dear friends Mr. Bharat Sharma, Mr. Suresh Khatiwada, Mr. Suraj Karki, Mr. Bhojraj Ghimire, Mr. Yogaraj Joshi, Mr. Kiran Shrestha, Mr. Sushil Dahal, Ms. Yamuna Ghimire and Miss Manita Aryal for their generous support in completion of this work.

Sushil Nepal

ABSTRACT

Encryption of data has been a key issue in the global market as the technology advancement has brought high risk through unauthorized access, alteration, degradation, destruction, and other threats to the information that is being shared. For the solution to these problems, many algorithms have been designed to overcome the potential threats.

My research also focuses on encrypting the data through efficient use of algorithm to make it secure. For this the use of multiple keys is an essential part. Key1 is a high entropy source where as key2 is a a pass phrase. Key1 is seeded with PRNG to generate 32 byte block which is then added to the beginning of the message.

Encryption algorithm is designed to provide some protection for the user who re-uses the same pass phrase when encrypting various files. The algorithm will generate different cipher text even if it is invoked on the exact same plain text with the same pass phrase. This is accomplished by cascading a stream cipher with a block cipher. The block cipher is not cryptographically secure. Its purpose is to avalanche changes throughout the file. The first block is XORed with the hash of the pass phrase, the hash of the subsequent blocks are calculated from the plain text of the previous block concatenated with the hash used in the previous block. The stream cipher is a simple XOR against the next PRNG return and an XOR against the sum of all previous plain text modulo 256. Before starting encryption, the PRNG is seeded with high entropy data and used to generate a first block.

TABLE OF CONTENTS

LIST OF FIGURES