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

Analysis of Dedicated Cryptographic Hash Functions – MD5 and SHA-1

By
SUDHIR GAUTAM

A dissertation submitted to the Central Department of Computer Science and Information Technology in partial fulfillment of the requirements for

the Master's Degree in Computer Science and Information Technology

December 2011

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

LETTER OF APPROVAL

We certify that we have read this dissertation work and in our opinion it is satisfactory in the scope and quality as a dissertation in the partial fulfillment for the requirement of Master of Science in Computer Science and Information Technology.

Evaluation Committee

_____

Dr. Tanka Nath Dhamala

Head, Central Department of Computer Science and Information Technology

Tribhuvan University

_____

Prof. Dr. Shashidhar Ram Joshi

Head, Department of Electronics and Computer Engineering, Institute of Engineering

Pulchowk, Nepal (Supervisor)

_____

External Examiner

_____

Internal Examiner

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

Supervisor's Recommendation

I hereby recommend that the dissertation prepared under my supervision by **Mr. Sudhir Gautam** entitled **"Analysis of Dedicated Cryptographic Hash Functions MD5 and SHA-1"** be accepted as fulfilling in partial requirements for the degree of M. Sc. in Computer Science and Information Technology.

Prof. Dr. Shashidhar Ram Joshi

Department of Electronics and Computer Engineering,

Institute Of Engineering, Pulchowk, Nepal

(Head)

ACKNOWLEDGEMENTS

It is a pleasure to thank many people who made this thesis possible.

I would like to express heartfelt regards to my supervisor Prof. Dr. Shashidhar Ram Joshi, Head of the Department of Electronics and Computer Engineering, Institute of Engineering (IOE), Pulchowk for his continuous guideline, support and inspiration throughout the thesis work.

Dr. Tanka Nath Dhamala, head of the Central Department of Computer Science and Information Technology, Kritipur deserves my special thanks as he has played vital role in bringing my supervisor and me together and his continuous support throughout the work.

I would like to express my appreciation to all faculties of the department for their suggestion and comments for the improvement of the thesis.

Sudhir Gautam

December, 2011

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Cryptography is the art and science of information security and Cryptographic hash functions are one of the most important tools used in modern cryptography. A hash function is a transformation function that maps strings of arbitrary length to strings of fixed length. For the last two decades, many types of hash functions have been defined but, the most widely used in many of the cryptographic applications currently are hash functions based on block ciphers and the dedicated hash functions. This dissertation shows how dedicated hash functions are constructed and what are their design principles and where they can be used. This dissertation also looks into a comparison between two dedicated hash algorithms. It has been observed that the MD5 algorithm is **slightly cheaper** to compute than SHA-1.

ABBREVIATION

CRHF	Collision Resistant Hash Function
OWHF	One Way Hash Function
MAC	Message Authentication Code
MDC	Manipulation Detection Code
SKC	Secrete Key Cryptography
PKC	Public Key Cryptography