

**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

ABSTRACT.....	9
ACKNOWLEDGEMENTS.....	4
ABBREVIATION.....	10
TABLE OF CONTENTS.....	5
LIST OF FIGURES.....	7
LIST OF TABLES.....	8
CHAPTER I.....	1
INTRODUCTION.....	1
1. Cryptography.....	1
1.1 Secret Key Cryptography.....	Error! Bookmark not defined.
1.2 Public-Key Cryptography.....	Error! Bookmark not defined.
2. Hash Function.....	Error! Bookmark not defined.
2.3 One-way hash function (OWHF).....	Error! Bookmark not defined.
2.4 Collision resistant hash function (CRHF).....	Error! Bookmark not defined.
2.5 Message Authentication Code (MAC).....	Error! Bookmark not defined.
3. Hash functions based on block ciphers.....	Error! Bookmark not defined.
4. Dedicated hash functions:.....	Error! Bookmark not defined.
4.1 MD5.....	Error! Bookmark not defined.
4.2 SHA-1.....	Error! Bookmark not defined.
5. Motivation.....	Error! Bookmark not defined.
6. Problem Statement.....	Error! Bookmark not defined.
CHAPTER II.....	Error! Bookmark not defined.

BACKGROUND AND LITERATURE REVIEW	Error! Bookmark not defined.
1. Cryptography	Error! Bookmark not defined.
1.1 Privacy protection with symmetric cryptology	Error! Bookmark not defined.
1.2 Authentication with symmetric cryptology.....	Error! Bookmark not defined.
2. Applications of hash function in cryptography.....	Error! Bookmark not defined.
2.1. Digital Signature	Error! Bookmark not defined.
2.2. Data Integrity	Error! Bookmark not defined.
2.2. Password tables	Error! Bookmark not defined.
3. Merkle-Damgard Construction.....	Error! Bookmark not defined.
6.1. Birthday attack	Error! Bookmark not defined.
6.2. Differential attack.....	Error! Bookmark not defined.
7. The MD5 hash Algorithm.....	Error! Bookmark not defined.
8. Security of MD5	Error! Bookmark not defined.
9. The SHA-1 Algorithm	Error! Bookmark not defined.
10. Security of SHA-1.....	Error! Bookmark not defined.
Chapter III.....	Error! Bookmark not defined.
Implementation	Error! Bookmark not defined.
1.1. General Model.....	Error! Bookmark not defined.
1.2. MD5 Algorithm	Error! Bookmark not defined.
1.3. SHA-1 Algorithm	Error! Bookmark not defined.
1.3.1. High Level Design.....	Error! Bookmark not defined.
CHAPTER V	Error! Bookmark not defined.
TESTING AND ANALYSIS	Error! Bookmark not defined.
1.2. Algorithm comparison	Error! Bookmark not defined.
CHAPTER V	Error! Bookmark not defined.
SUMMARY AND FURTHER WORK	Error! Bookmark not defined.
Chapter VI	Error! Bookmark not defined.
References	Error! Bookmark not defined.

LIST OF FIGURES

Figure 1: A taxonomy for cryptographic hash functions.....	Error!
Bookmark not defined.6	
Figure 2: Model of symmetric encryption system.....	13
Figure 3: A hash function.....	15
Figure 4: Merkle-Damgard structure.....	18
Figure 5: The MD5 compression of a single 512-bit message block.....	24
Figure 6: The Architecture of Cryptographic hash model.....	31
Figure 7: Detailed view of Cryptographic hash model.....	32
Figure 8: The MD5 Algorithm.....	33
Figure 9: Flow chart of SHA-1 Algorithm.....	34
Figure 10: Chart showing speed in Mbits/s for MD5 and SHA-1.....	39

LIST OF TABLES

Table 1: The primitive functions of MD5 compression fuction.....	23
Table 2: Primitive logic functions used in SHA-1.....	27
Table 3: Definition of the operations for dedicated hash functions.....	27 Error!
Bookmark not defined.	
Table 4: The four additive constants used in SHA-1 algorithm.....	37
Table 5: Average running speed of MD5 and SHA-1.....	40

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