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

A Secure Cryptographic Algorithm Improving Security over Known Plaintext Attack Based on Hill Cipher

By

Khagendra Prasad Sah

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

SUEPRVISOR'S RECOMMENDATION

Mr. Khagendra Prasad Sah has carried out this research work entitled "A SECURE CRYPTOGRAPHIC ALGORITHM IMPROVING SECURITY OVER KNOWN PLAINTEXT ATTACK BASED ON HILL CIPHER" under my supervision and guidance. In my best knowledge this is an original work in computer science. I, therefore, recommend for further evaluation.

Prof. Dr. Shashidhar Ram Joshi

Head of Department
Department of Electronics and Computer Engineering
Institute of Engineering (IOE), Pulchowk, Lalitpur
Nepal

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 research work and in our opinion, it is satisfactory in the scope and quality as dissertation in the partial fulfillment for the requirement of the Master's Degree in Computer Science and Information Technology.

Evaluation Committee

Prof. Dr. Shashidhar Ram Joshi
(Supervisor)
Head of the Department
DECE, IOE, Pulchowk

Dr. Tanka Nath Dhamala
(Head)
CDCSIT
Tribhuvan University

Internal Examiner

External Examiner

ACKNOWLEDGMENTS

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

I would like to sincerely thank the following people for all their assistance during my studies.

Dr. Tanka Nath Dhamala, Head of Central Department of Computer Science and Information Technology, Tribhuvan University, Kirtipur, deserves my special thanks for bringing my supervisor and me together and his continuous support throughout my thesis work.

I would like to express my appreciation to my professors Suvarna Shakya, Sudarshan Karanjeet, my teachers Min Bahadur Khati, Samujjwal Bhandari for extremely insightful knowledge discussions on various topics.

I would like to thank to all faculties of the department for their suggestion and comments for the improvements of my thesis.

I would like to thank to all members of evaluation committees for going through such a long document and giving me valuable feedback.

Khagendra Prasad Sah

Kathmandu, Nepal

December, 2011

ABSTRACT

The secrecy of sensitive information against unauthorized access or deceitful changes has been of prime concern throughout the centuries. With the introduction of computer, the security of data or information (stored on a computer for a shared system or during their transmission in a distributed system) to maintain its confidentiality, proper access control, integrity and availability has been a major issue. The only way to address all these issues is cryptology.

Hill Cipher is one of the most famous symmetric cryptosystem that can be used to protect information from unauthorized access. Hill cipher is a multi-letter and polygraph substitution cipher. Although the Hill Cipher is resistant to frequency letter analysis and strong against ciphertext only attack, it succumbs to known-plaintext attack. The other disadvantage of the Hill Cipher is non invertible key matrix because all the matrices don't posses their inverses and this reduces the number of possible keys from actual number of possible keys and leads to the chances of brute-force attack. In the scheme that is going to be proposed, a variant of the Hill cipher is introduced that makes the Hill Cipher more secure and retains the efficiency. The scheme uses the Cipher Block Chaining (CBC) mode of operation and bitwise XOR operation that leads to diffusion and confusion and make the scheme strong against the known-plaintext attack.

TABLE OF CONTENTS

LIST OF FIGURES