



**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 possess 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

ABSTRACT

ACKNOWLEDGMENTS

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION	1
1.1 Introduction and Terminology	2
1.2 Shannon's Conventional System	3
1.3 Valuation of Secrecy System	5
1.4 Security Attacks	6
1.5 Motivation	7
1.6 Approach	8
2. LITERATURE REVIEW	9
2.1 History of Cryptography	10
2.2 Cipher Model	13
2.2.1 Types of Cipher	13
2.2.1.1 Substitution Cipher	13
2.2.1.2 Transposition Cipher	14
2.2.1.3 Running and Concealment Cipher	15
2.2.1.4 Steganography	16
2.3 Methods of Cryptography	17
2.3.1 Symmetric Cryptosystem	17

2.3.1.1 Caesar Cipher	19
2.3.1.2 Monoalphabetic Ciphers	20
2.3.1.3 Block and Stream Ciphers	20
2.3.1.3.1 Block Ciphers	21
2.3.1.3.2 Stream Ciphers	21
2.3.1.4 Polygraphic Ciphers	23
2.3.1.4.1 Playfair Ciphers	23
2.3.2 Asymmetric Model	25
2.4 Threat Models	27
2.5 Cryptanalytic Attacks	28
2.5.1 Ciphertext-only Attack	28
2.5.2 Known Plaintext Attack	28
2.5.3 Chosen Plaintext Attack	28
2.6 Brute-force Attack	28
2.7 Cryptographic Principles	29
2.7.1 Kerckhoff's Principle	29
2.7.2 Unconditionally Secure Scheme	29
2.7.3 Computationally Secure Scheme	29
2.8 Galois Field	29
3. ANALYSIS OF ALGORITHM	30
3.1 Background	30
3.2 Hill Cipher	31

3.3 Cryptanalysis of Hill Cipher	32
4. PROBLEM DEFINITION	34
5. PROPOSED SOLUTION	36
5.1 Cipher Block Chaining (CBC)	36
5.2 Development of Cipher	37
5.3 Algorithms	43
5.3.1 Algorithm for Encryption	43
5.3.2 Algorithm for Decryption	43
5.4 Implementation	44
5.4.1 Tools	44
5.4.1.1 Java	44
6. TESTING AND ANALYSIS	45
6.1 Testing of Proposed Scheme	45
6.2 Analysis of Proposed Scheme	46
6.2.1 Known-plaintext Attack	46
6.2.2 Brute-force Attack	46
6.2.3 Chosen Ciphertext Attack and Chosen Plaintext Attack	48
7. CONCLUSION AND FUTURE WORK	49
8. REFERENCES	
APPENDIX	



## LIST OF FIGURES

Figure 1: Shannon's Conventional Cryptosystem	4
Figure 2: Scytale used by the Spartans	10
Figure 3: Jefferson Disk	12
Figure 4: Enigma Machine	12
Figure 5: A Simplified Model of Symmetric Encryption	18
Figure 6: Stream Cipher	22
Figure 7: A Key Stream and Key are needed for Encryption and Decryption	22
Figure 8: A Playfair Cipher Matrix Box	23
Figure 9: Asymmetric Cryptogram	26
Figure 10: CBC Encryption	36
Figure 11: CBC Decryption	36