A

Thesis Report

On

Optimization of Encryption Algorithm for Secured Communication

Submitted towards the fulfillment of requirement for the award of degree of

MASTER OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

Ajay Kumar

Roll. No. 801261002

Under the guidance of

Dr. Ajay Kakkar

(Assistant Professor)

Electronics and Communication Engineering Department

THAPAR UNIVERSITY

PATIALA-147004

DECLARATION

I hereby declare that the work which is being presented in this thesis entitled "**Optimization of Encryption Algorithm for Secured Communication**" in partial fulfillment of the requirement for the award of degree of ME (Electronics and Communication Engineering) at Thapar University, Patiala is an authentic record of my study carried out under the supervision of Dr. Ajay Kakkar (Assistant Professor), ECED during the year 2013-2014.

Date: 14/07/2014

Ajay Kumar
Roll No.801261002

It is certified that the above statement made by the student is correct to the best of my knowledge and belief.

Date: 14/07/2014

Dr. Ajay Kakkar
Assistant Professor
ECED,Thapar University

Contersigned By:

Dr. Sanjay Sharma
Head of Department
ECED, Thapar University

Dr. S. K. Mohapatra
Dean of Academic Affairs
Thapar University

ACKNOWLEDGENT

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar, Assistant Professor,** Electronics & Communication Engineering Department, Thapar University, Patiala for his patient guidance and support throughout the thesis. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to **Dr. Sanjay Sharma, Professor and Head of Department** as well as PG coordinator **Dr. Kulbir Singh, Associate Professor,** Electronics and Communication Engineering Department. I would like to thank entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Ajay Kumar

ABSTRACT

Data security is an essential component of an organization in order to keep the information safe from various competitors. It helps to ensure the privacy of a user from others. Secured and timely transmission of data is always an important aspect for organization. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and reduce the overheads of the system. Keeping in view the importance of dynamic keys for secure data transmission this work is carried out to optimize an encryption algorithm based upon dynamic key. Literature Survey has been carried out by incorporating key papers related to data encryption. From the literature survey gaps and observation have also been drawn. Encryption algorithm by Hill cipher was critically analyzed and key management has also been optimized. In proposed algorithm simulation results have been achieved using MATLAB 7.3 and proves that the algorithm is optimized in comparison to another Hill cipher technique in term of hacking and processing time. Finally, conclusion and future scope of work has also been stated the end of this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF GRAPHS

LIST OF ABBREVIATIONS

CT	Cipher Text
PT	Plain Text
SE	Symmetric Encryption
AE	Asymmetric Encryption
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
SKC	Secret Key Cryptography
PKC	Privet Key Cryptography
LAN	Local Area Network
HA	Hash Algorithm
MA	Modular Arithmetic
TEK	Traffic Encryption Key
CC	Central Controller
REK	Resource Encryption Key
RL	Resource Lists
DIFAC	Differential Access Control
GC	Group Controller
KEK	Key Encryption Keys
LME	Linear Maxima Edition
ATM	Automatic Teller Machine

LIST OF PUBLICATIONS

[1] Ajay Kumar and Ajay Kakkar, "A Review Paper on Encryption Algorithm for Data Security," International Conference on Emerging Technologies in Electronics and Communication, pp. 200-202, 2013.

Chapter 1: Introduction of Cryptography

1.1 Introduction

In current scenario number of problem arises with the security of documents, files and important data. So, there is a need to have a technique to protect the documents and which avoids the unauthorized access of data in an unsecure communication environment.

There are various techniques which are used to keep the data confidential from hackers. Some of these are passwords, cryptography and biometrics. Passwords are not so good for this task due to their low entropy. Biometrics technique produces harmful effects on the human beings and it is too costly. For these above problems cryptography is the best solution for security [9]. A plaintext is a message to be communicated in a secret way. Encryption is the process of creating a ciphertext (hidden data) from a plaintext and decryption is the reverse process of encryption, where cipher text is converted into plaintext.

The study of encryption and decryption is called cryptology and cryptography is the application of them. For encode a plaintext changes the plaintext into a series of bits or numbers alpha-numeric may be used which include A to Z and 0 to 9 values [29]. The most common method of encoding a message these days is to replace it with its ASCII value, which is an 8 bit representation for each symbol. The process of decoding turns bits or numbers back into plaintext is called decryption. Stream cipher operates on a message symbol by symbol or bit by bit. A block cipher operates on blocks of symbols. A transposition cipher is used to rearranges the letters symbols or bits in a plaintext. A substitution cipher is used to replaces the letters symbols or bits into plaintext with others or without changing the order. A product cipher alternates the transposition and substitution. The concept of stream cipher versus block cipher only applies to substitution and product ciphers not transposition ciphers.

1.2 Cryptography

Cryptography is best method to protect data and Important files from unauthorized parties. It is the science of writing the data in secret code and about the design and analysis of mathematical techniques that is enables secure communication in the presence of millions adversaries. Cryptography is the art of secret writing. The basic service provided by

cryptography is the ability to send information between participants in a way that prevents others from reading it [4]. Cryptographic systems involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms and it will allow reversible scrambling of information's.

1.3 Encryption

For achieving the data security encryption is the most effective way everywhere and everyplace where security is need. The process of hiding the contents of a message in such a way that the original information is recovered only through a decryption process is called encryption [29]. The purpose of Encryption is to prevent unauthorized parties from viewing crucial information. An encryption occurs when the data is passed through some substitute technique like shifting technique, table references or mathematical operations. A different form of data is generated through these processes. The unencrypted data is called plaintext and the encrypted data is called cipher text. This represents the original data in a difference form. Encryption key is use to encrypt the original message which depend upon key based algorithms.

There are two general categories for key based Encryption algorithm first one is called Symmetric Encryption (SE) which uses a single key to encrypt the message and decrypt the message. Second is Asymmetric Encryption (AE) which uses two different keys a public key to encrypt the message, and a private key to decrypt the message [4]. There are several different types of key based Encryption algorithms such as DES, RSA, PGP, Elliptic curve but all of these algorithms depend on high mathematical manipulations.

1.4 Keys

A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. For encryption, key is used called encryption key and for decryption, it is called decryption key. Key size is measured in bits, larger the key size more secure communication. Key can be used by two ways, private or publically. In Symmetric Encryption, key is used as private key or it is also called single key for encryption and decryption. In Asymmetric Encryption, key is used as private or public key one for encryption and second for decryption [16].

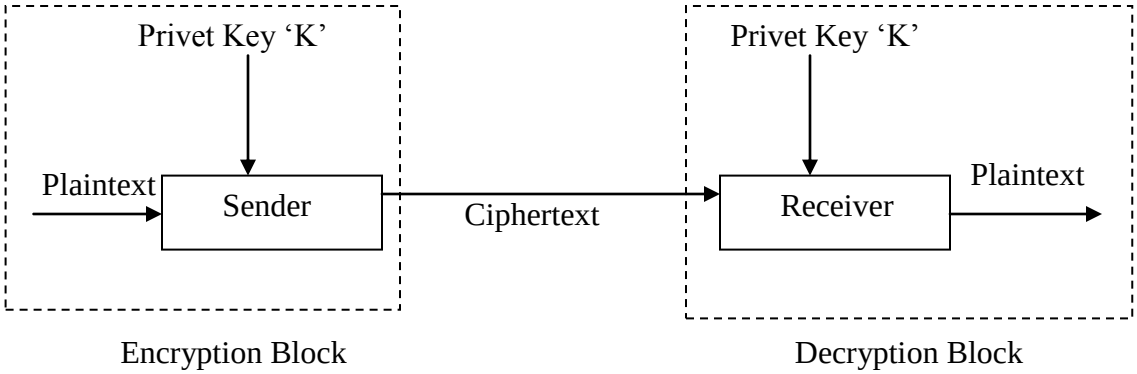


Figure 1.1: Private or Single Key for Encryption and Decryption Block

In Figure 1.1 Private Key ‘K’ is used for Encryption and Plaintext is converted into Ciphertext. Same Private Key ‘K’ is used for Decryption and Ciphertext is again converted back into Plaintext.

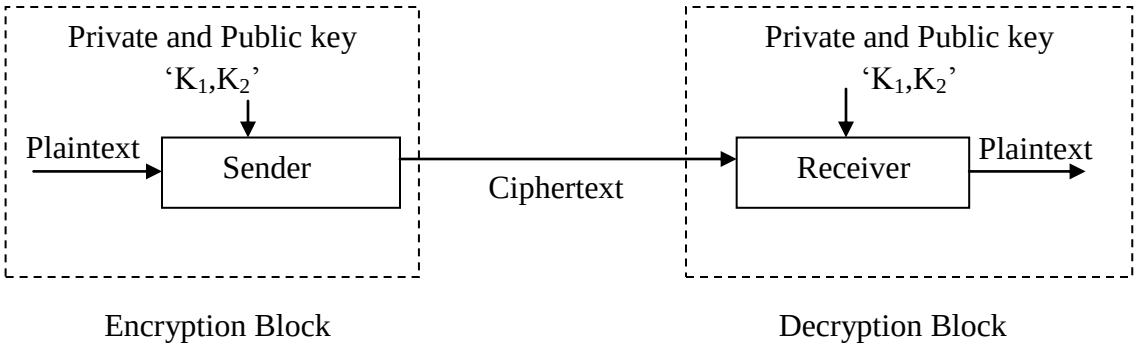


Figure 1.2: Private and Private Key for Encryption and Decryption Block

In Figure 1.2 Private and Public Key ‘K_1, K_2’ is used for Encryption and Plaintext is converted into Ciphertext. Same Key ‘K_1, K_2’ is used for Decryption and Ciphertext is again converted back into Plaintext. In this one key is publically distributed and another key is used as a private key.

1.5 Block Diagram of Cryptography

Figure 1.3 shows the basic building block of cryptography. Senders send information in the form of plaintext after the encryption algorithm and with the help of encryption key plaintext transformed into ciphertext. At the receiver side ciphertext is again transformed back into original plaintext with the help of inverse encryption algorithm and key.

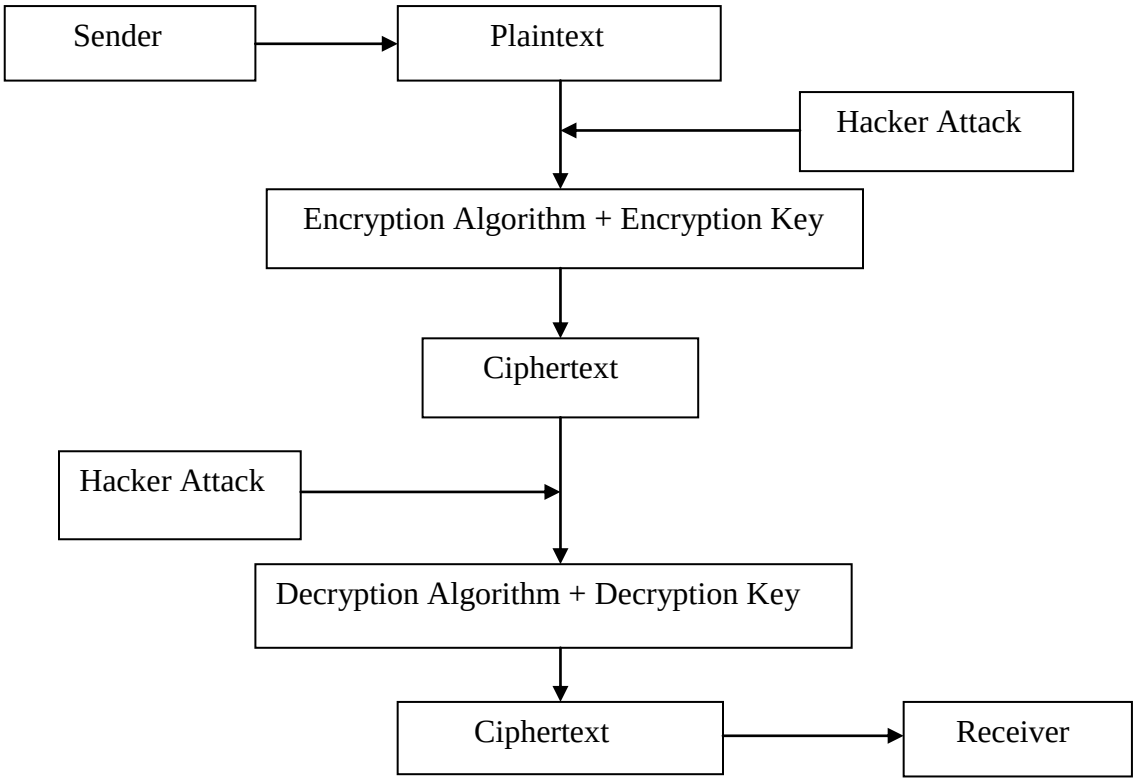


Figure 1.3: Basic Cryptographic Model.

1.6 Types of Attacks on Cryptography

There are following types of attacks on cryptography and these are:

If hacker wants to attack on the system, he has several goals in his mind. The primary goal is to detect the encryption and decryptions keys. Basically, there are four standard types of attacks on a cryptographic method are given below [9].

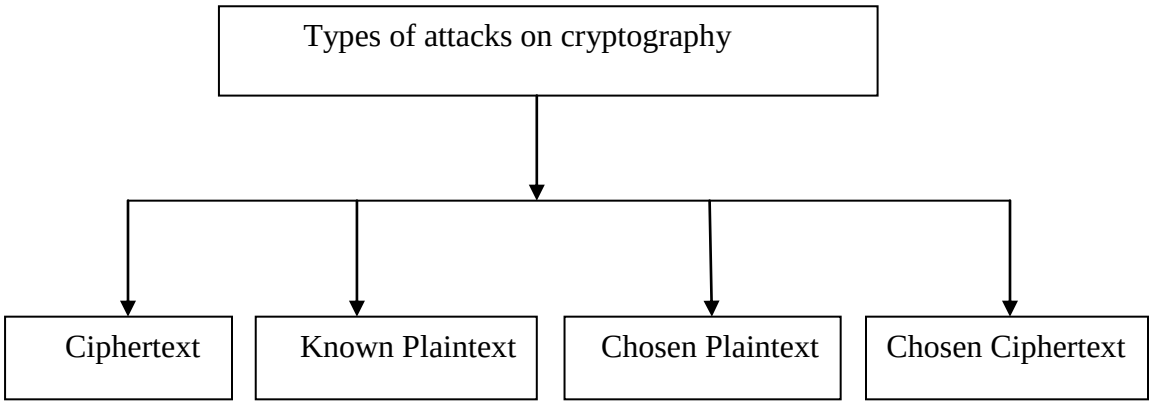


Figure 1.1: Different types of attacks on cryptography

1.6.1 Ciphertext

This type of attack occurs when the hacker has the ability to obtain ciphertexts. Even if hacker cannot perform the more sophisticated attacks described below. It is assumed that he can get access to encrypted messages. In the encryption method that cannot resist a ciphertext only attack is completely insecure [12].

1.6.2 Known Plaintext

This type of attacks occurs when hacker has a copy of the cipher text and the plaintext and encrypted with the same key, hacker not have the plaintext of the entire message. Suppose that sender always started his text to receiver with "Respected sir'' then hacker knows what is the first several letters of message and has the corresponding cipher text. It is known a crib on the portion of the plaintext message. It seems that knowing only the seven letters would be of little use to hacker but in many cases this would be enough information to construct the entire key [21].

1.6.3 Chosen Plaintext

This type of attacks occurs when the hacker temporally gains access to the encryption machine. Hacker has to carefully select some plaintext messages and sends them through the machine to obtain the corresponding cipher texts. Further, hacker can do a known plaintext attacks. If hacker chooses his plaintext messages correctly he will have an easier time to finding the key [22].

1.6.4 Chosen Ciphertext

This type of attacks occurs when hacker temporally gains access to the decryption machine carefully hacker select some cipher texts send them through the machine to obtain the corresponding plaintexts. Now hacker can do a known plaintext attacks and again if, he select his cipher text messages correctly hacker would have an easier time to finding the key. Cryptographic methods have their own strengths and weaknesses and these are depends upon the requirement. For the Hill Cipher known plaintext attacks on the system are used to find the key [24].

1.7 Types of Cryptographic Functions

There are three kinds of cryptographic functions; Secret key functions, Public key functions and Hash functions. Public key cryptography use two keys one public key and second key for data encryption [4]. Secret key cryptography uses one key. Hash functions involve the use of zero keys. Hierarchy of cryptographic functions has been defined below.

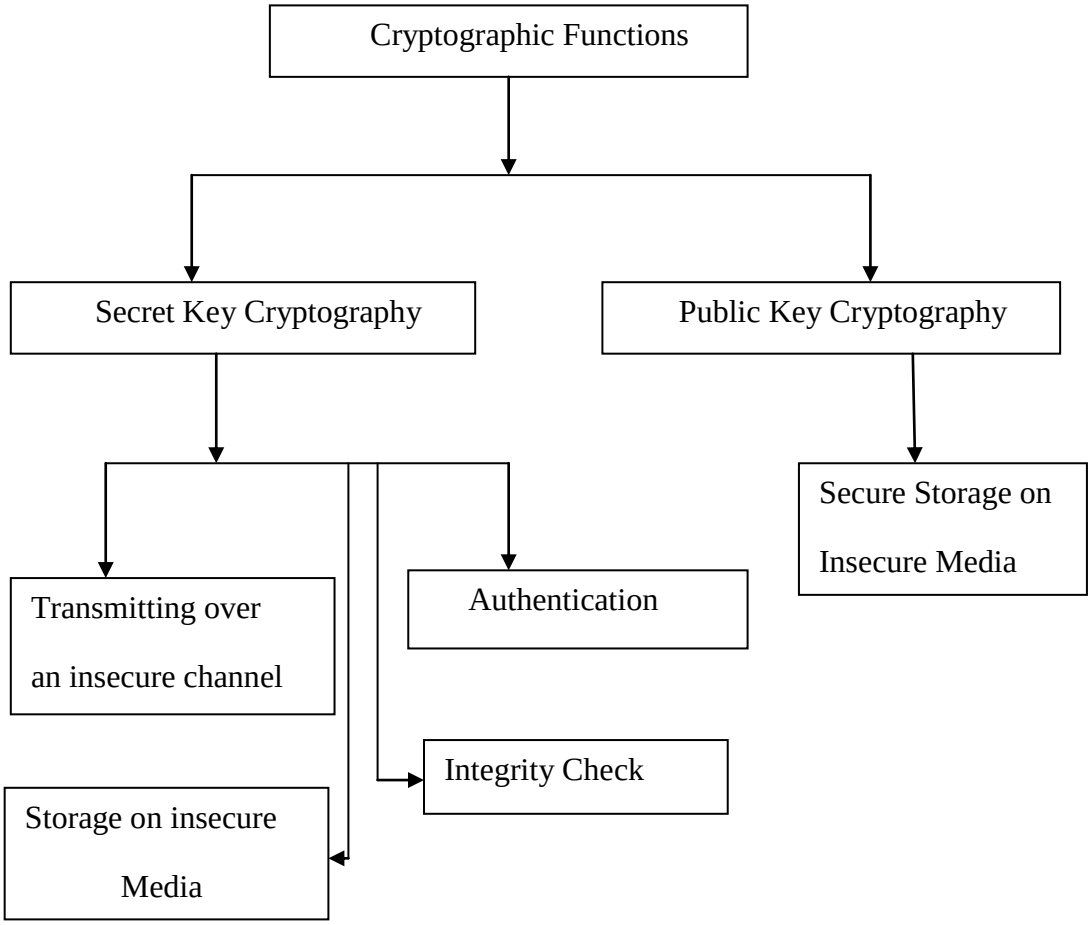


Figure 1.5: Hierarchy of cryptographic functions

1.7.1 Secret Key Cryptography (SKC)

Secret key cryptography involves the use of a single key for given a plaintext. The encryption key produces unintelligible which is same length of the plaintext. Decryption is the reverse of encryption, and uses the same key as used an encryption.

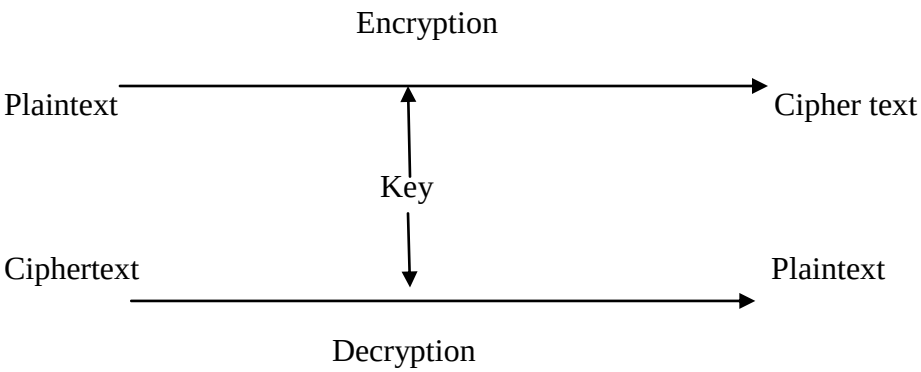


Figure 1.6: Secret Key Cryptography

Secret key cryptography is sometimes referred to as conventional cryptography or symmetric cryptography. The next sections describe the types of secret key cryptography.

1.7.1.1 Transmitting Over an Insecure Channel

It is impossible to prevent communication from eavesdropping when transmitting the information in an unsecure medium. A letter wants be intercepted when a massage transmitted on a LAN. If sender and receiver agree on a shared secret key, using secret key cryptography they could send messages to one another on same medium [28].

1.7.1.2 Secure Storage on Insecure Media

If senders have information and want to preserve it, he/she must be assumed that no could hacked the data. If sender invents a key and encrypts the information using this key, he can store it anywhere and it remains probably for long time [29].

1.7.1.3 Authentication

Strong authentication means that someone could prove knowledge of a secret without revealing it. This is possible only with cryptography and particularly useful when two computers are tries to communicate over an insecure network [30].

1.7.1.4 Integrity Check

In cryptography a secret key scheme could be used to generate a fixed length cryptographic checksum which are associated with a message. The original derivation of the term checksum comes from the operation of breaking a message into fixed length blocks. Finally the sum is

sent along with the message. The receiver adopt some approach and breaks up the message and repeats the addition the checks the sum [41].

1.7.2 Public Key Cryptography (PKC)

Public key cryptography involves two keys which are mathematically related and does not allow someone else to easily determine the other key. PKC uses a pair of different key and it is also called asymmetric cryptography. In public key cryptography one of the keys is designated the public key and advertised as the owner wants. The second key is designated the private key and never revealed to another party [11]. The public key should be distributed to each recipient. Everyone should be able to retrieve the public key. If a user wants to encrypt the data to a receiver it can decrypt the data by using the sender's public key. The advantage of public key algorithm is more computationally intensive than symmetric algorithms therefore encryption and decryption take longer time. This may not be significant for a short text message but certainly is for bulk data encryption.

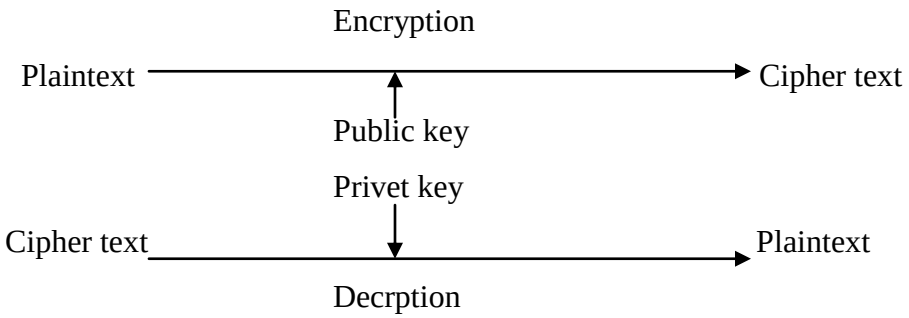


Figure 1.7: Public Key Cryptography

1.7.2.1 Secure Storage on Insecure Media

This is really the same as what one would do with secret key cryptography [13]. Encrypt the data with public key and then nobody can decrypt it except since decryption will require the use of the private key. It has the advantage over encryption with secret key technology that sender have to risk giving the private key to the machine that is going to encrypt the data. As with secret key technology if the private key lost the then data is irretrievably lost.

1.7.3 Hash algorithm

Hash algorithms are also known as message digests or one-way transformations. A cryptographic hash function is a mathematical transformation that takes a message of

arbitrary length (transformed into a string of bits) and computes from it a fixed-length (short) number [32]. It will call the hash of a message m, h(m).

It has the following properties:

a) For any message m, it is relatively easy to compute h(m). This just means that in order to be practical it can't take a lot of processing time to compute the hash.
b) Given h(m), there is no way to find an m that hashes to h(m) in a way that is substantially easier than going through all possible values of m and computing h(m) for each one.
c) Even though it's obvious that many different values of m will be transformed to the same value h (m).

1.7.4 Organization of this Thesis

The outline of thesis is as follows;

Chapter 1 shows the introduction of Cryptography and the function of Cryptography. A brief overview of data security is also included in this chapter.

Chapter 2 includes literature survey. This chapter involves the work done by the various researchers in the field of Cryptographic algorithm for data security. From the literature survey some observation have also been drawn and stated at the end of this chapter. Finally from the observation objectives of this work have also been derived.

Chapter 3 describe detailed description of mathematical definition, operational properties of Hill cipher an Encryption and Decryption procedure based on the Hill cipher. But the computation time is increased as file size is increased and main flaw in its existence of self repeating matrix. These drawbacks are overcome in next chapter.

Chapter 4 describe mathematical model for Encryption and Decryption for the optimization of Hill Cipher has been proposed in this chapter. This new Encryption and Decryption algorithms are time efficient and more secure than the existing algorithms.

Chapter 5 summarizes the simulation results obtained using proposed algorithms and their comparison with the existing methods on the basis of various experimental results. Different

parameters are defined to quantify the experimental results obtained from the execution of this algorithm.

Chapter 6 suggests conclusion and future scope of the work done in this thesis.

Chapter 2: Literature survey

This chapter involves the work done by the various researchers in the field of ryptographic algorithm for data security. From the literature survey, observation have been drawn and stated at the end of this chapter. Finally from the observation objectives of this work have also been derived.

2.1 Literature survey

Neal Koblitz *et al*. [30] proposed an elliptic curve cryptosystems for protecting the communication in unsecure network. Elliptic curves over finite fields of public key cryptosystems use the multiplicative group of a finite field. These elliptic curve cryptosystems were more secured because the analog of the discrete logarithm problem on elliptic curves harder than the classical discrete logarithm problem. Limitation of this scheme it was mainly based on the structure either of the multiplicative group or the multiplicative group of a finite field.

Hugo Krawczyk *et al.* [12] worked on the order of encryption and authentication scheme for protecting the communications. They composed a symmetric encryption and authentication scheme for building secured channels for the protection of communications over insecure networks. They also proved that the other method of composing encryption and authentication which includes the authentication encryption method was not so much secured against random attackers. Limitation of this was only forty bit key size can use in this scheme.

Laurent Eschenauer *et al*. [24] proposed a key management scheme for distributed sensor networks. Key management scheme designed to satisfy both operational and security requirements of distributed sensor networks. This scheme requires cryptographic protection of communications, sensor capture detection, key revocation and sensor disabling. So they present a key management scheme designed to satisfy both operational and security requirements of distributed sensor networks. Distributed sensor networks were Adhoc mobile networks and include sensor nodes with limited computation and communication capabilities. Limitation of this scheme it was less time efficient.

Jung.Wen Lo *et al.* [16] proposed an efficient key assignment scheme for access control in a large leaf class hierarchy. In which users were divided this into different security classes. They also proposed a new key assignment scheme for controlling the access right in a large partially ordered set hierarchy and reduce the required computation for key generation. Information retrieval and the number of leaf classes which were substantially larger than the number of non leaf classes.

Bharat B. Madan *et al*. [7] worked on various methods used for modeling and quantifying the security attributes of intrusion tolerant systems**.** Various issues related to quantifying the security attributes of an intrusion tolerant system were also addressed. Response of a security intrusion tolerant system to an attack was modeled as a random process. They facilitate the use of stochastic modeling techniques to predict the attacker behavior. They had also computed a security measure called the mean time to security failure and also compute probabilities of security failure due to violations of different security attributes.

Tariq Jamil *et al.* 42] worked upon rijndael algorithm for protecting sensitive unclassified government information. This algorithm was the new advanced encryption standard algorithms recommended by the US national institute of standards and technology. The performance of rijndael algorithm based on speed of encryption, decryption process and key set up time.

Ho Won Kim *et al*. [11] worked on Design and Implementation of a private and public key crypto processor and its application for security system. They present the design and implementation of a crypto processor. This special purpose microprocessor optimized for the execution of cryptography algorithms. This crypto processor can be used for various security applications such as storage devices, embedded systems, network routers, security.

Prosanta Gope *et al*. [33] proposed a new block cipher cryptographic symmetric key algorithm named TACIT encryption technique for secure routing. It used an independent approach with suitable mathematical which was assumed to be computationally secured. Key distribution system was being applied on a secure policy based routing. It was limited to conversion of text file.

Ismail .I.A *et al.* [14] worked on how to repair the hill cipher. This technique adjusts the encryption key to form a different key for each block encryption. This algorithm provides a method for adjusting the encryption key, thereby significantly increasing its resistance to various attacks such as a known plaintext attack and statistical attack.The proposed algorithm called HillMRIV cipher.

Yogesh Karandikar *et al*. [51] proposed on effective key management approach for differential access control in dynamic environment. In group communication each user accesses multiple resources and multiple users can access each resource. Each resource encryption key needs to be distributed to all subscribers of the resource and each subscriber must get the entire key. So they developed a new approach of keys management to enforce differential access control in highly dynamic environments for secure group communication framework. Limitation of this scheme was resources were independent and each resource needs to be encrypted by a different resource encryption key.

Yanchao Zhang *et al*. [50] worked on Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks. They worked on the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations. They developed LBK-based neighborhood authentication scheme to localize the impact of compromised nodes to their vicinity. The conclusion was that they presented a comprehensive set of location-based compromise tolerant security mechanisms for WSNs.

N. R. Potlapally *et al.* [31] worked on energy consumption characteristics of cryptographic algorithms and security protocols. They present a comprehensive analysis of the energy requirements of a wide range of cryptographic algorithms that form the building blocks of security mechanisms such as security protocols. They also discuss various opportunities for realizing energy efficient implementations of security protocols.

Darpan Anand *et al*. [8] explored identity based cryptography techniques and applications. They reviewed the identity based encryption applications in the field of various networks as ad-hoc networks. The scheme also used in mobile networks and other wireless networks. They also discussed that under what parameters identity based cryptography was used with

its benefits and limitations. The main limitation was that the available methods were restricted to fixed output block, which was a trace for crackers.

Wenbo He *et al.* [46] proposed a self contained public key management scheme for mission critical wireless Adhoc networks. This scheme was able to resist the Sybil attack achieves zero communication overhead for authentication and offers high service availability. In this scheme small numbers of cryptographic keys was stored at individual nodes before deployed in the network. For providing a good scalability in terms of number of nodes and storage space they utilize a combinatorial design of public private key pairs. This means that the nodes combine more than one key pair to encrypt and decrypt messages. Limitation of this scheme was every individual node use small no of cryptographic keys.

Ravindra Kumar Chahar *et al.* [36] worked on design of a new security protocol for providing integrity, confidentiality and authentication. This new security protocol for on line transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques. Limitation of this protocol was it uses elliptic curve cryptography for encryption, RSA algorithm for authentication and hash function for integrity.

Spyros T. Halkidis *et al*. [38] analyzed the architectural risk software systems based on security patterns. The first step was to determine to what extent specific security patterns shield from known attacks. This information is fed to a mathematical model based on the fuzzy-set theory and fuzzy fault trees in order to compute the risk for each category of attacks. The whole process was automated using a methodology that extracts the risk of a software system by reading the class diagram of the system under study. In this way security problems can be detected at an early stage that reduced the cost compared to the introduction of security during implementation. Extension to this work would be the automatic introduction of missing security patterns either at the design phase of a system being developed or in already implemented software systems.

Albert Tannous *et al*. [18] presented new side channels that leak password information during windows keyboard processing of password. Side channels were typically viewed as attacks which leak the cryptographic keys during cryptographic algorithm processing. They also proved that (a) side channels were not eliminated by removing accurate clocks or

hardware cache mechanisms (b) side channels were of continued concern for computer security as well as cryptographic processing.

Jason. H. Li *et al*. [19] proposed a scalable key management and clustering scheme for Adhoc networks. Scalability problem was solved by partitioning the communicating devices into subgroups. Further these were used to organize the subgroups into hierarchies. Each level of the hierarchy is called a tier or layer. Key generation distribution and actual data transmissions follow the hierarchy. Distributed efficient clustering approach provides robust clustering to form subgroups and used to obtain simulation results. These results proved that distributed efficient clustering approach was energy efficient and resilient against node mobility. This scheme was not suitable for large cluster size.

Jian Ren *et al.* [20] proposed generalized ring signature scheme based on the original ElGamal signature scheme. Instead of revealing the actual identity of the message signer and it specifies a set of possible signers. This scheme was secured against random adaptive message attacks. The main limitation of this schemes that the verifier was unable to indicate which member actually produced the signature.

Md. Nazrul Islam *et al.* [28] worked on effect of security increment to symmetric data encryption through Advanced Encryption Standard methodology. Protection of data during transmission and in storage may be necessary to maintain the confidentiality and integrity of the information. This algorithm defines the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. They showed the effect in security increment through AES methodology. Limitation of this algorithm was higher secure than rijndael algorithm but less efficient than that.

Bibhudendra Acharya *et al.* [5] proposed an involutory, permuted and reiterative key matrix sgeneration methods to overcome the weakness of the hill cipher system. Involutory matrix generation method solves the key matrix inversion problem.This meant that same machinery could be used both for encryption and decryption of massages no additional hardware would be needed to compute inverses before decrypting permuted and reiterative key matrix generation method generates “different" key for each block of data encryption and increases the hill system's security.

Saroj Kumar *et al.* [23] proposed an image encryption using advanced hill cipher algorithm for encrypt an image. The proposed advanced hill algorithm was more secure to brute force attacks as compared to original hill cipher algorithm. The proposed scheme was resistant against known plaintext attacks.

Kirtiraj B hatele *et al.* [6] worked on design of new hybrid security protocol architecture for online transaction. This new security protocol for on line transaction can be designed using the combination of both symmetric and asymmetric cryptographic techniques which was known as hybrid cryptography. This protocol serves three important cryptographic primitives, integrity, confidentiality and authentication. This hybrid security protocol architecture was can be easily upgraded and the protocol becomes more immune against the attacks and at the same time it becomes more time efficient.

Mao.Yin Wang *et al.* [27] worked on a Single and Multi core advanced encryption standard architectures for flexible security. The architecture for advanced encryption standard encryption major building blocks was a group of advanced encryption standard processor. Each processor provides block cipher schemes with new key expansion design for the original advanced encryption standard algorithm. In multi core architecture the memory controller of each advanced encryption standard processor was designed for the maximum overlapping between data transfer and host processor. This design used for high speed systems and data paths reduce the input output and bandwidth problem. Limitation of this scheme was each standard processor need separate memory controller.

Aqeel Khalique *et al.* [2] worked on a password authenticated key agreement scheme based on ECC Using Smart Cards. It is one of the best public key techniques for its small key size and high security. It is also suitable for secure access of smart cards due to the implementation on smart cards.

J. Lan *et al.* [18] proposed a Random Number Generator (RNG) for low power cryptographic applications. It was widely used in cryptographic systems as the cryptographic keys generator. These keys were most important component in the system because the security of the cryptographic system relies entirely on its quality. They also presented the good statistical quality and low energy consumption RNG including a serial-to-parallel shift register, a 32-bit

register and a pseudo random number generator (PRNG) module which could be suitable for low-power, flexible cryptographic applications. They also suggested that it could be implemented completely in digital circuit and required no external components.

Mao Yin Wang *et al*. [26] worked on a mesh structured scalable internet protocols security processor used for protect the data over the Internet. They developed a parallel mesh structured internet protocols security processor and execute the protocols for Internet security applications. They developed several areas where efficient cryptographic internet protocols security processor embedded in mesh structured internet protocols security processor. They also proposed mesh structured internet protocols security processor was suitable for transport mode.

S. Pradheep kumar *et.al* [40] proposed a secured grid based route public key cryptography scheme for heterogeneous sensor network. They show that homogeneous sensor networks were poor security, connectivity, performance and scalability. Under the dynamic condition of sensor node implementation grid based coordinate scheme was highly adaptable for public key management scheme. They also compare the energy and throughput efficiency for dynamic position of sensor nodes. The proposed method was compared with the existing routing techniques and it was more secure.

Dhruti Sharma *et al*. [10] proposed an identity based secure key generation protocol scheme was exciting alternative to public key Cryptography. They use a distributed protocol to generate the private key for users and this scheme entails significant communications overhead. The proposed scheme involves less number of authorities in the computation of the public, private key pair and hence was more efficient. The main drawback with identity based cryptography was key escrow.

Joan Arnedo *et al*. [17] proposed a secure communication setup for peer to peer communications. They proposed a security framework for cryptographic data setup in order to secure juxtapose overlay communications. The main features were including a completely modular approach which may cater to a broad set of scenarios, an effective secure key distribution method, and a hybrid key authenticity scheme.

Levente Buttyan *et al.* [23] proposed detection and recovery scheme from pollution attacks in coding based distributed storage schemes. In a pollution attack the adversary maliciously alters some of the stored encoded packets which results in the incorrect decoding of a large part of the original data. So they propose an algorithm to detect and recover the data from such attacks. The proposed algorithms were suitable for practical systems especially in wireless sensor networks.

R. H. Torres *et al.* [35] proposed an identification of keys and cryptographic algorithms using genetic algorithm and graph theory. Identification of presented keys and cryptographic algorithm uses the calisnkiharabasz index as its evaluation function and graphs techniques. The method used to identify patterns in cryptograms generated by cryptographic algorithms certified by National Institute Standard Technology.

Dongyang Xu *et al.* [47] proposed a key management scheme for segment based document protection. The practical key management scheme for segment based document was a new extensible markup language based document format. This scheme was not only efficient for key generation and key derivation but also secure against collusion attack, reverse attack and key modification attack.

Yi Sheng Shiu *et.al* [52] worked on physical layer security in wireless network for security of information transfer via wireless networks. Security methods on cryptographic techniques employed at the upper layers of a wireless network known as physical layer. Physical layer security techniques can be classified into five major categories theoretical secure capacity, power, code, channel, and signal detection approaches.

Septimiu Fabian Mare *et al.* [41] worked on secret data communication system using steganography, AES and RSA. They show new secret data communication system that employs the use of two cryptographic algorithms RSA and AES together with steganography. The joining of these three techniques builds a robust steganography based communication system capable of withstanding multiple types of attacks. The key used for the data encryption uses a combination between a random generated sequence and a hash function. Limitation of this scheme was the secret data and the key used for encryption both

were passed through multiple levels of security checks that assure the integrity, authenticity and security and making this a reliable communication.

Shurbhi Khar *et al.* [37] presented an implementation and enhanced modified hill cipher by P-box and M-box technique. They were showing a new encryption key model as well as encryption algorithm model which will improving avalanche effect as compare various encryption algorithm it was not any known security weak points and this makes it an excellent candidate to be considered as a standard encryption working model..

Tao Ma *et al.* [43] worked on an assurance of energy efficiency and data security for Electrocardiographic transmission in body area sensor networks. Technological advancement in body area sensor networks low cost high quality electrocardiographic diagnosis systems was becomes important equipment for healthcare service providers. They investigate the properties of compressed electrocardiographic data for energy saving. Encryption mechanism provides simple and effective security solution for an electrocardiographic. Limitation of this scheme was energy consumption and data security with electrocardiographic systems in body area sensor networks was still two major challenges to tackle.

Suyash Verma *et al*. [39] proposed an efficient symmetric key cryptography algorithm for information security. This block encryption algorithm was much faster and offers the enhanced security features compared to other symmetric key algorithms. It helps in achieving confidentiality as well as message authentication. It produces better performance than other common encryption algorithms used in terms of time consumption, whenever there is a change in packet size. It was also good whenever there was a change in data type such as image, audio or video instead of text. By changing key size it also proved that higher key size leads to change in the battery and time consumption.

Kazuo Sakiyama *et al.* [22] proposed an information theoretic approach for optimal differential fault analysis used to check the optimality of the differential fault analysis attacks. They presented a comprehensive analysis of differential fault analysis attacks on the advanced encryption standard. The injecting fault into cryptosystems was categorized as an active attack and attackers induce an error in operations to retrieve the secret information.

Some of the attacks were not optimal and can be improved especially for advanced encryption standard.

Xiaojiang Du *et al.* [48] worked on routing driven Elliptic Curve Cryptography key management scheme for heterogeneous sensor networks. In this scheme they adopt heterogeneous sensor network model for better performance and security and gave a routing driven key management scheme and establishes a shared keys for neighbor sensors that communicate with each other. The performance evaluation and security analysis show that this key management scheme provides better security, storage space and energy consumption than other key management schemes.

Qian Wang *et al.* [34] worked on cooperative secret key generation from phase estimation in narrowband fading channels for providing privacy in communication. They developed a cooperative key generation protocol to facilitate high rate key generation in narrowband fading channels. In this two keying nodes extract the phase randomness of the fading channel with the aid of relay node. Performance of this scheme shows that the key rate can be improved by a couple of orders of magnitude compared to the existing approaches.

ZhiguoWan *et al*. [53] worked on a hierarchical attribute based solution for flexible and scalable access control in cloud computing. Cloud computing was one of the most influential paradigms in the IT industry. Attribute based encryption was proposed for access control of outsourced data in cloud computing. This scheme was not only achieves scalability due to its hierarchical structure but also inherits flexibility.

Hung Min Sun *et al.* [13] proposed dual RSA algorithm and also analyzed the security of the algorithm. They presented new variants of RSA whose key generation algorithms output two distinct RSA key pairs having the same public and private exponent's two applications for Dual RSA were blind signatures and authentication. The main disadvantage of using dual RSA was that the computational complexity of the key generation algorithms was also increased.

Pavan. N *et al.* [32] proposed an image steganography scheme based on hill cipher for key hiding. They implement hill cipher algorithm for hiding a text behind the cover image and decrypt the cover image to get original text. The highlight of this paper was that the key was

encrypted and scrambled within the cover image scheme eliminates the use of key distribution system and making the system highly secure for various network applications

Vivek Mhatre *et al.* [44] worked on a minimum cost heterogeneous sensor network with a lifetime constraint. In heterogeneous sensor network nodes was to be deployed over a unit area for the purpose of surveillance. An aircraft visits the area periodically and gathers data about the activity in that area from the sensor nodes. There were two types of nodes that were distributed over the area using two dimensional homogeneous poison points. A) Nodes with intensity. B) Battery energy. Nodes use multi hopping to communicate with their closest cluster heads. They determine the optimum node intensities and node energies that guarantee connectivity and coverage the surveillance area with a high probability. Limitation of this scheme was every node in the network need separate battery.

Xuhong Li *et al.* [49] presented a novel convertible authenticated encryption schemes without using hash functions. An authenticated encryption scheme allows a designated recipient to recover the message and verify its authenticity while keeping the message secret from the public. Hence a convertible authenticated encryption scheme enables the recipient to convert the signature to an ordinary one. The limitation was if the recipient could not reveal the converted signature, any third party cannot check the validity of the message even though he gets the message.

2.2 Gaps in Study and Observations

From the following literature survey observations have been drawn:

a) Single key of short length is not capable to provide secured cryptographic model. On the other hand if long length key is used for encryption of data, more processing time is resulted which will give a fair chance to hacker to break the cryptographic model.
b) In order to keep the data secured from hacker dynamic keys will be used.
c) Key should be generated from the available data which avoids the need of transmitting keys over a secured channel.

2.3 Objectives

From the observation it is concluded that there is a need to develop cryptography model which are based upon the dynamic keys for data security. So, objectives have been derived

from the observations obtained from literature survey. Providing privacy in unsecure communication is not only objective of cryptography it also provides solutions for other problems. The objectives are given as:

a) To study various encryption algorithm used for data security.
b) To study different soft computing tools used to achieve secured cryptographic model.
c) To design an optimized algorithm based upon dynamic keys for encryption.
d) Comparison of our approach with existing ones.

Chapter 3: Hill Cipher Algorithm

It includes a detailed description of mathematical definition, operational properties and applications of Hill cipher an encryption and decryption procedure based on the Hill cipher. These methods are analyzed on the basis of their quality of encryption decryption and computation time.

3.1 Hill Cipher Algorithm

Hill cipher was described in 1929 by a mathematician Lester S. Hill [25]. Hill cipher was the polytrophic cipher in which plaintext is divided into groups of adjacent letters of the same fixed length 'n' (n is an integer) and then each such group is transformed into a different group of 'n' letters. It increased the speed and throughput of hill cipher. Matrix manipulation is also used and it the core of hill ciphers. Its linear algebra equation is represented as

$C = K \times P\,(mod\, m)$. Where '$C$' represents the cipher text block 'P' represents the plaintext block and 'K' is the key. The key 'K' is in the form of matrix. Therefore decryption an inverse of the key matrix 'K^{-1}' is needed. [5]

For encryption and decryption the Hill cipher assigns numerical values to each letter of an alphabet as shown in table 3.1. Therefore it is important to recognize that the above alphabet is a linear space

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 3.1: Numerical values for each letter of an alphabet

Steps of Hill cipher are defined as;

1. Finally the alphabet has a zero element. In the above shown table 3.1 zero element is 'A' and its numerical value is called as $\alpha + A = \alpha$.

2. Each alphabet is closed under modulo addition. The addition operator " $+$ " is defined as modulo addition. In second formula it becomes$\alpha + n$. When 'n' is the alphabet and varies from 26 to 36.

3. Each alphabet is closed under modulo scalar multiplication. Here $\alpha\beta = \gamma$ where γ is the remainder of the product of α and β divided by the size of the alphabet.

For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. Each character in the Hill cipher assigned a numerical value like this

A=0

B=1

…..

…..

Z=25

By the substitution of cipher text letters in place of plaintext leads to m linear equations. For

m=1 to n the system is described as follows:

$$C_1 = (K_{11}P_1 + K_{12}P_2 \ldots + K_{1n}P_n)MOD26 \quad (3.1)$$

$$C_2 = (K_{21}P_1 + K_{22}P_2 \ldots + K_{2n}P_n)MOD26 \quad (3.2)$$

.

.

.

.

$$C_m = (K_{m1}P_1 + K_{m2}P_2 \ldots + K_{mn}P_n)MOD26 \quad (3.3)$$

Equation 3.3 can also be written as;

$$C = KP \quad (3.4)$$

Where 'C' and 'P' are column vectors of length 'n' representing the plaintext and the cipher text and 'K' is an 'n*n' matrix which is the encryption key. All operations are based upon MOD 26 here. Decryption procedure requires the inverse of encryption matrix 'K'. The inverse 'K^{-1}' of a matrix 'K' is defined by the equation. $K\ K-1=\ I$ Where 'I' is an Identity matrix. Finally inverse of encryption key K^{-1}' is applied to the cipher text, and then the plain text is recovered. In general terms it can written as follows:

For encryption: $C = Ek(P) = Kp$ (3.5)

For decryption*:* $P = Dk(C) = K^{-1}Kp = P$ (3.6)

3.2 Modular Arithmetic (MA)

The mod of arithmetic operation used in this approach is addition, subtraction, unary operation, multiplication and division. Based on there the self invertible matrix for Hill cipher algorithm is generated [25].

There are following modulo operator's properties describes as:

1. $a \equiv b\ mod\ p\ if\ n(a-b)$

2. $(a\ mod\ p) = (b\ mod\ p) => a \equiv b\ mod\ p$

3. $a \equiv b\ mod\ p => b \equiv a\ mod\ p$

4. $a \equiv b\ mod\ p\ and\ b \equiv a\ mod\ p => a \equiv c\ mod\ p$

Let $Zn = [0,1, \ldots . . p-a]$, the set of residues modulo$p$. If modular arithmetic is performed within this set Zn, the following equations present the arithmetic operations:

1Addition: $(a+b)modp = [(a\ mod\ p) + (b\ mod\ p)]mod\ p$

2 Negations:$-a\ mod\ p = p - (a\ mod\ p)$

3. Subtraction: $(a-b)mod\ p = [(a\ mod\ p) - (b\ mod\ p)]mod\ p$

4. Multiplication: $(a*b)mod\ p = [(a\ mod\ p) * (b\ mod\ p)]mod\ p$

5. Division: $\left(\frac{a}{b}\right) mod\ p = c\ when\ a = (b*c)mod\ p$

6. Multiplicative inverse: $a^{-1} = c\ if\ there\ exists\ (c*z)mod\ p = 1$

SL. No.	Property	Expression
1	Commutative Law	$(w + x) \bmod p = (x + w) \bmod p$ $(w * x) \bmod p = (x * w) \bmod p$
2	Associative Law	$[(w + x) + y] \bmod p = [w + (x + y)] \bmod p$
3	Distributive Law	$[w * (x + y)] \bmod p = [w * x + w * y] \bmod p$ $[w * (x * y)] \bmod p$ $= [\{w * x \bmod p\} * \{(w * y) \bmod p\}] \bmod p$
4	Identities	$(0 + a) \bmod p = a \bmod p$ $and\ (1 * a) \bmod p = a \bmod p$
5	Inverse	For each X belongs to Zp , there exists y such that (x + y) mod p =0 then $y = -x$ For each X belongs to Zp, there exists y such that $(x * y)$ mod $p = 1$

Table 3.2: Properties of modulo arithmetic

3.3 Encryption with the Hill Cipher

As we know alphabet is a linear space perform linear transformations. So encrypting text key using the hill cipher is accomplished by breaking a given plaintext into blocks of size 'n' (where n is an integer) writing these blocks as column vectors and multiplying these column vectors by any invertible $n * n$ matrix has been used. The encryption matrix should be invertible because its inverse is used to decrypt the cipher texts created with the Hill cipher [1]. The inevitability of the encryption matrix ensures that its determinant must not be 0. The determinant of the encryption matrix should also be relatively prime to the size of the alphabet. The proposed work for encryption matrix system chooses must have a determinant which is relatively prime to 26. This condition allows for a randomized distribution of letters in the cipher text. In order to encrypt the plaintext "MY NAME IS AJAY" with $n = 2$, the process is as follows:

1. Choose a 2x2 encryption matrix. For this example, we will use the matrix $\begin{vmatrix}2 & 1\\3 & 4\end{vmatrix}$. This matrix has the determinant$(2 * 4) - (3 * 1) = 8 - 3 = 5$. Since$5\ are\ \neq\ 0$, this matrix is invertible. 5 are also relatively prime to 26. These two qualities satisfy the requirements listed previously, making this encryption matrix a valid choice for use in the Hill cipher.

2. Split the plaintext into blocks of size 2 (ignoring spaces), determine the letters' numerical values, and align these as column vectors [5]. If the length of the plaintext is not evenly divisible by 2, add a previously decided character to the end of the string until the plaintext is evenly divisible by 2.

$\begin{vmatrix}M\\Y\end{vmatrix}=\begin{vmatrix}12\\24\end{vmatrix}$

$\begin{vmatrix}N\\A\end{vmatrix}=\begin{vmatrix}13\\0\end{vmatrix}$

$\begin{vmatrix}M\\E\end{vmatrix}=\begin{vmatrix}12\\4\end{vmatrix}$

$\begin{vmatrix}I\\S\end{vmatrix}=\begin{vmatrix}8\\18\end{vmatrix}$

$\begin{vmatrix}A\\J\end{vmatrix}=\begin{vmatrix}0\\9\end{vmatrix}$

$\begin{vmatrix}A\\Y\end{vmatrix}=\begin{vmatrix}0\\24\end{vmatrix}$

3. Multiply each of these column vectors by the encryption matrix $A = \begin{bmatrix}2 & 1\\3 & 4\end{bmatrix}$ and take modulo 26 of the result

$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}12\\24\end{vmatrix}=\begin{vmatrix}48\\132\end{vmatrix}$ (mod26) = $\begin{vmatrix}22\\2\end{vmatrix}$

$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}13\\0\end{vmatrix}=\begin{vmatrix}26\\39\end{vmatrix}$(mod26) = $\begin{vmatrix}0\\13\end{vmatrix}$

$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}12\\4\end{vmatrix}=\begin{vmatrix}28\\52\end{vmatrix}$ (mod26) = $\begin{vmatrix}2\\0\end{vmatrix}$

$$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}8\\18\end{vmatrix} = \begin{vmatrix}34\\96\end{vmatrix} \text{ (mod26) } = \begin{vmatrix}8\\18\end{vmatrix}$$

$$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}0\\9\end{vmatrix} = \begin{vmatrix}9\\36\end{vmatrix} \text{ (mod26) } = \begin{vmatrix}9\\10\end{vmatrix}$$

$$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix} * \begin{vmatrix}0\\24\end{vmatrix} = \begin{vmatrix}24\\96\end{vmatrix} \text{ (mod26) } = \begin{vmatrix}24\\18\end{vmatrix}$$

4. Convert each of the matrices obtained in step 3 to their alphabetical vectors and combine them to produce the cipher text.

$$\begin{vmatrix}22\\2\end{vmatrix} = \begin{vmatrix}W\\C\end{vmatrix}$$

$$\begin{vmatrix}0\\13\end{vmatrix} = \begin{vmatrix}A\\N\end{vmatrix}$$

$$\begin{vmatrix}2\\0\end{vmatrix} = \begin{vmatrix}C\\A\end{vmatrix}$$

$$\begin{vmatrix}8\\18\end{vmatrix} = \begin{vmatrix}I\\S\end{vmatrix}$$

$$\begin{vmatrix}9\\10\end{vmatrix} = \begin{vmatrix}J\\K\end{vmatrix}$$

$$\begin{vmatrix}24\\18\end{vmatrix} = \begin{vmatrix}Y\\S\end{vmatrix}$$

Cipher text: [WCANEAISJKYS]

This completes the process of the Hill cipher's encryption by matrix multiplication. It is observed that the plaintext "MY NAME IS AJAY" encodes to "WCANEAISJKYS." It is important to note that the Hill cipher overcomes the frequency distribution problem associated with simple substitution ciphers. Since the encryption is not simply based on replacing certain characters with others but instead on linear transformations of blocks of characters, the frequencies of each letters appearance in the language have been masked.

3.4 Decryption with the Hill Cipher

Hill cipher use matrix multiplication and any encryption matrix used in the Hill cipher must be invertible. For three $n * n$ matrices $A, B,$ and C where $AB = C$ and A is invertible, we know that $B = A^{-1}C$. Using this we can decrypt an encoded message by multiplying it by the inverse of the encryption matrix [1]. Due to the modulo arithmetic involved in this cipher we needs to find A^{-1} such that $AA^{-1} = In \, mod \, 26$.The cipher text is split into blocks of size 'n' and multiplied by the inverse matrix. The process is the same as encryption, but with the inverse matrix instead of the original encryption matrix. Decryption of the cipher text "WCANEAISJKYS" with the $2x2$ encryption matrix previously defined would go as follows:

1. Find A^{-1}

$$A = \begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix}$$

$$A^{-1} = \begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix}$$

2. Split the cipher text into blocks of 2, determine the letters numerical values and align these as column vectors.

$$\begin{vmatrix} W \\ C \end{vmatrix} = \begin{vmatrix} 22 \\ 2 \end{vmatrix}$$

$$\begin{vmatrix} A \\ N \end{vmatrix} = \begin{vmatrix} 0 \\ 13 \end{vmatrix}$$

$$\begin{vmatrix} C \\ A \end{vmatrix} = \begin{vmatrix} 2 \\ 0 \end{vmatrix}$$

$$\begin{vmatrix} I \\ S \end{vmatrix} = \begin{vmatrix} 8 \\ 18 \end{vmatrix}$$

$$\begin{vmatrix} J \\ K \end{vmatrix} = \begin{vmatrix} 9 \\ 10 \end{vmatrix}$$

$$\begin{vmatrix} Y \\ S \end{vmatrix} = \begin{vmatrix} 24 \\ 18 \end{vmatrix}$$

3. Multiply each of these column vectors by the decryption matrix calculated in step 1 and take modulo 26 of the result.

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 22 \\ 2 \end{vmatrix} = \begin{vmatrix} 142 \\ 362 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 12 \\ 24 \end{vmatrix}$$

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 0 \\ 13 \end{vmatrix} = \begin{vmatrix} 65 \\ 208 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 13 \\ 0 \end{vmatrix}$$

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 2 \\ 0 \end{vmatrix} = \begin{vmatrix} 12 \\ 30 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 12 \\ 4 \end{vmatrix}$$

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 8 \\ 18 \end{vmatrix} = \begin{vmatrix} 138 \\ 408 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 8 \\ 18 \end{vmatrix}$$

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 9 \\ 10 \end{vmatrix} = \begin{vmatrix} 104 \\ 295 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 0 \\ 9 \end{vmatrix}$$

$$\begin{vmatrix} 6 & 5 \\ 15 & 16 \end{vmatrix} * \begin{vmatrix} 24 \\ 18 \end{vmatrix} = \begin{vmatrix} 234 \\ 648 \end{vmatrix} \text{mod} 26 = \begin{vmatrix} 0 \\ 24 \end{vmatrix}$$

3. Convert each of the matrices obtained in step 3 to their alphabetic vectors and combine them to produce the original plaintext.

$$\begin{vmatrix} 12 \\ 24 \end{vmatrix} = \begin{vmatrix} M \\ Y \end{vmatrix}$$

$$\begin{vmatrix} 13 \\ 0 \end{vmatrix} = \begin{vmatrix} N \\ A \end{vmatrix}$$

$$\begin{vmatrix} 12 \\ 4 \end{vmatrix} = \begin{vmatrix} M \\ E \end{vmatrix}$$

$$\begin{vmatrix} 8 \\ 18 \end{vmatrix} = \begin{vmatrix} I \\ S \end{vmatrix}$$

$$\begin{vmatrix} 0 \\ 9 \end{vmatrix} = \begin{vmatrix} A \\ J \end{vmatrix}$$

$$\begin{vmatrix} 0 \\ 24 \end{vmatrix} = \begin{vmatrix} A \\ Y \end{vmatrix}$$

Original plaintext: MYNAMEISAJAY

The cipher text has been decrypted into the original plaintext, minus the original spaces. Spaces can be added by the recipient at the receiver. For example, the character "_"could be added to our alphabet as having the numerical value 26 and all of modulo functions would change to modulo 27 to adjust for the fact there would now be 27 characters in the alphabet. This modified alphabet would allow for encryption of the space character within messages.

3.5 Outcome

From this chapter we found that it, describe detailed description of mathematical definition, operational properties of Hill cipher an encryption and decryption procedure based on the Hill cipher. But the computation time is increased as file size is increased and main flaw in its existence of self repeating matrix. These drawbacks are overcome in next chapter.

Chapter 4: Proposed Work

A mathematical model for encryption and decryption for the optimization of Hill Cipher has been proposed in this chapter. Further, the detailed discussion about the computation complexity of these algorithms has also been done.

4.1 Proposed Work

Hill cipher decryption requires the inverse of key matrix. So, problem arises there is the inverse of key matrix doesn't always exist. If the key matrix is not invertible, encrypted text cannot be decrypted. In order to surmount this problem, the use of self repetitive matrix needed. This matrix if multiplied with itself for a given mod value results in an identity matrix after 'n' multiplications. So after $n + 1$ multiplication the matrix will repeat itself.

The Modification in Hill cipher algorithm generates the different key matrix for each block encryption instead of keeping the key matrix constant [15]. It increases the secrecy of data and algorithm also checks the matrix used for encrypting the plaintext whether that is invertible or not. If the encryption matrix is not invertible, the algorithm modifies the matrix such a way that it's inverse exist. The new matrix obtained after modification of key matrix is called known as Encryption matrix. In order to generate different key matrix each time the encryption algorithm randomly generates the seed number and from this key matrix is generated [5].

Key matrix,

$$K=\begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix}$$

Where,

$$K_{11} = \text{seed number}$$

$$K_{12} = (\text{seed number} * m) \bmod n$$

$$K_{11} = (12K * m) \bmod n$$

$$K_{11} = (13K * m) \bmod n$$

$K_{11} = (32K * m) \bmod n$

Where m is successive numbers of plaintext letters taken at a time for encryption and 'n' is length of the lookup table or we can set this 'n' value as per requirement. Then with the help of key matrix encryption matrix'E' is generated. For self repetitive matrix, matrix should be square and it should be non-singular [52].

4.2 Generation of a self repetitive Matrix for an 'n'.

If the matrix is of dimension greater than $5 * 5$ and with mod index greater than 91, the methods of brute force are not performed. It takes very long time and 'n' value may be in the range of millions and 'n' is the value where the matrix becomes an identity matrix. If the computations will be $15 * 15$ matrixes or more a normal Pentium 4 machine takes more processing time [7].

Hence, it would be comfortable to know the value of 'n' and then generate a random matrix. This can be done as follows:

1. First a diagonal matrix 'A' is chosen and then the values powers of each individual element when they reach unity is calculated and denoted as $n1, n2$, and $n3$ .... Now taking the LCM of these values gives the value of 'n'.
2. Now the next step is generate a random square matrix whose n value is same as the n calculated in the previous step.
3. Pick up any random invertible square matrix'E'.
4. Generate $c = E^{-1}AE$
5. The 'n' value of 'C' is also 'n'

4.3 Mathematical proof generation of a self repetitive matrix for an'n'.

$(E^{-1}\ AK)n = \ (E^{-1})\ n * (A)\ n * (E)\ n$

$AN = I$ as calculated before as it is a diagonal matrix and 'n' is the LCM of all elements

$(E^{-1}\ E) * (E^{-1}\ * E) \ldots\ldots n\ times = I$

4.4 Ciphertext Development

First take plaintext and represent this in the form of a matrix, given by

B=input ('Enter the block of string')

$P = [pij], I = 1\ to\ n, j = 1\ to\ n.$ (Public key)

Let us choose a secret key matrix K,

$K = [kij], I = 1\ to\ n, j = 1\ to\ n,$

and

$E = [eij], i = 1\ to\ n, j = 1\ to\ n,$ Obtained by key matrix an increments in diagonals element in K

Here, we assume that the determinant of E is not equal to zero and it is an odd number. In view of this fact the modular arithmetic inverse of E can be obtained by using the relation

$(EE - 1)MOD97 = I$

On assuming that eij, the elements of the matrix E are odd numbers lying in [1-97], we get the decryption key matrix E^{-1} in the form

$E^{-1} = Inv\ [E],$

Where e_{ij} and d_{ij} are governed by the relation

$(eij \times dij)\ mod\ 97 = 1$

Here, it is to be noted that dij also turn out to be odd numbers in [1-97].

The basic equations governing the encryption and the decryption are given by

$P = (pij)$

$E = [eij \times pij]\ mod\ 97, i = 1\ to\ n, j = 1\ to\ n,$

$C = E * B$

and

$C = [cij] = [dij \times cij]\ mod\ 97, i = 1\ to\ n, j = 1\ to\ n$

$P = (E^{-1}C)mod\ 97.$

The corresponding algorithms for the encryption and the decryption are as follows.

4.5 Algorithm for Encryption

1. $Read\ B, P, E, K, n, r$
2. $For\ k = 1\ to\ r\ do$

{

3. $P = pij$
4. $For\ i = 1\ to\ n\ do$

{

5. $E = eij$

6. $For\ j = 1\ to\ n\ do$

{

7. $E = (pij \times eij)\ mod 97$

} }

8. $C = [E * B]$

}

9. $C = [cij]$

10. $Write(C)$

4.6 Algorithm for Decryption

1. $Read\ C, E, K, n, r$

2. $E^{-1} = Inv\ (E)$

3. $For\ k = 1\ to\ r\ do$

{

4. $C = [cij]$

5. $B = E^{-1}C)\ mod\ 97$

}

6. $Write\ (B)$

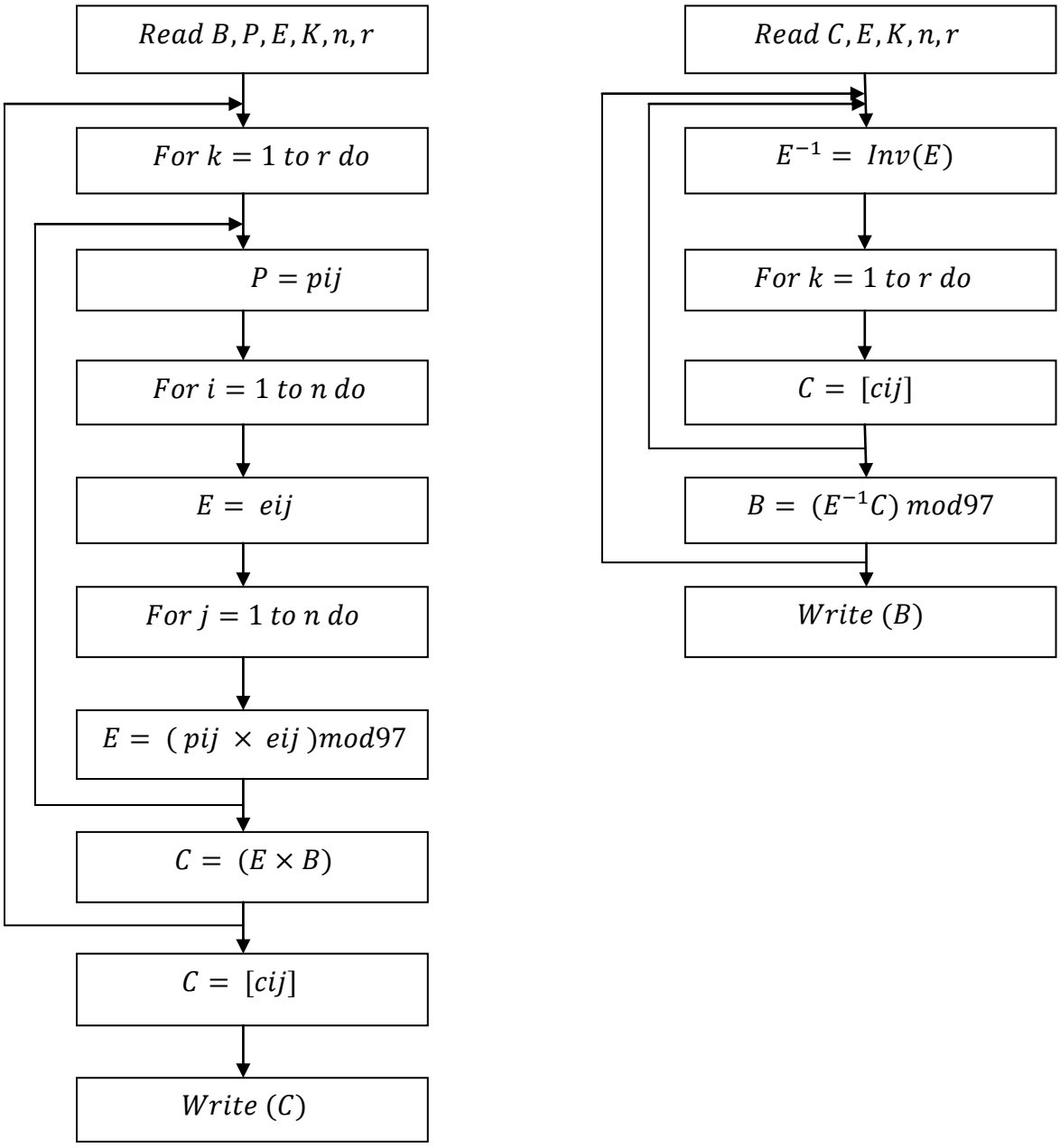


Figure 3.1: Flow chart of Encryption and Decryption Algorithm

4.7 Outcome

After studying Hill cipher algorithm, it has been found that there are many flaws in it. The main flaw was in its existing inverse of encryption matrix. To overcome this flaw, we proposed a new algorithm that gives the better solution for it and make it more efficient than other algorithms.

Chapter 5: Simulation Results and Discussion

This chapter summarizes the simulation results obtained by MATLAB 7.3, using proposed algorithms and their comparison with the existing methods on the basis of various experimental results. Different parameters are defined to quantify the experimental results obtained from the execution of this algorithm.

5.1 Simulation Results and Discussion

Example 1 Following example shows the transmission & reception with any length of string. Let we enter a string “my name is ajay kumar” then it received the string with following procedure:

A =

0 9 14 7 1 9 0 4 1

B1 =

30

2

57

26

14

E is the encryption key obtained by the multiplication of B1 and secret key.

E =

1 48 73 96 24

74 12 34 18 4

93 14 9 44 75

57 63 82 93 51

17 68 35 0 28

Code is obtained by the multiplication of E and B1. Procedure will be same till we get final code value.

Code =

38

50

93

39

26

A =

0 15 4 3 6 12 0 11 7

B1 =

30 46

2 27

57 25

26 48

14 5

E =

1 48 73 96 24

74 12 34 18 4

93 14 9 44 75

```
    57    63    82    93    51
    17    68    35     0    28
Code =
    38
    30
    93
    34
    44
A =
     1     8    15    14     6     7     6     4     1
B1 =
    30    46    75
     2    27    76
    57    25    16
    26    48    30
    14     5    60
E =
     1    48    73    96    24
    74    12    34    18     4
    93    14     9    44    75
    57    63    82    93    51
```

17 68 35 0 28

Code =

93

26

35

26

50

A =

0 8 2 9 6 5 3 8 5

B1 =

30 46 75 24

2 27 76 72

57 25 16 50

26 48 30 43

14 5 60 40

E =

1 48 73 96 24

74 12 34 18 4

93 14 9 44 75

57 63 82 93 51

17 68 35 0 28

Code =

93

36

46

38

26

A =

1 7 10 12 10 11 12 2 2

B1 =

30 46 75 24 71

2 27 76 72 76

57 25 16 50 14

26 48 30 43 2

14 5 60 40 63

E =

1 48 73 96 24

74 12 34 18 4

93 14 9 44 75

57 63 82 93 51

17 68 35 0 28

Code =

43

43

93

93

93

After the whole procedure at transmission block entered string has been transformated in the matrix form multiplied by the encryption key matrix and at the reception block inverse of encryption key matrix again transformated it in original form.

Ans = my name is ajay kumar

5.2 Performance Evaluation Parameters

Performance measurement criteria are time taken by the algorithms to perform the encryption and decryption of the input text file that is encryption computation time and decryption computation time.

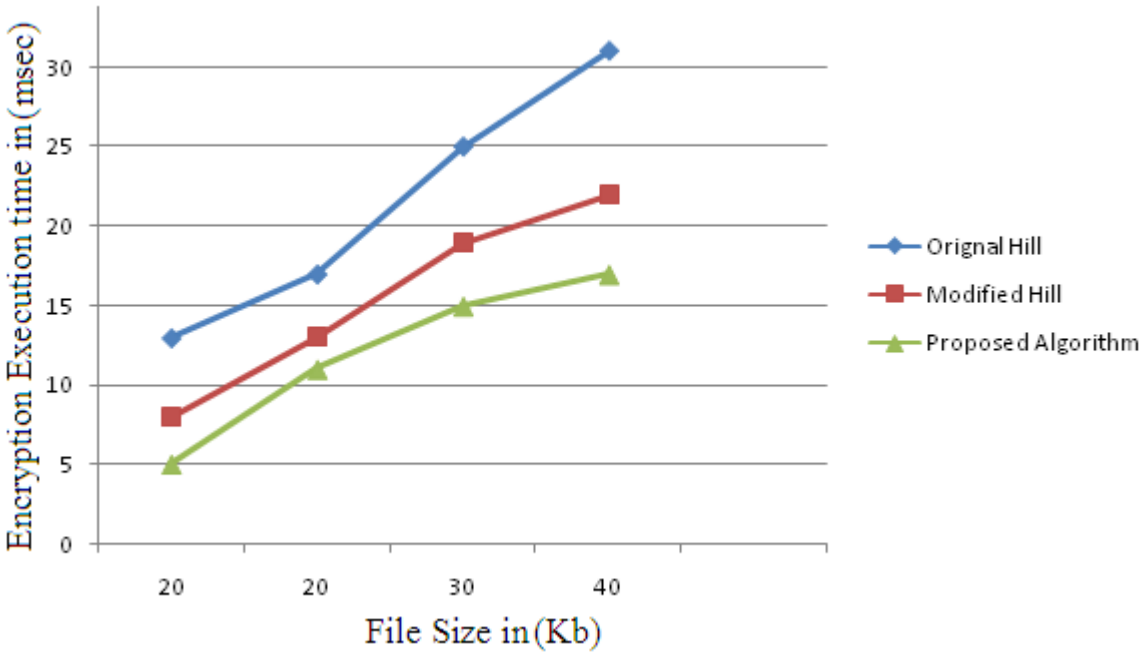
5.2.1 Encryption Computation Time

The encryption computation time is the time which is taken by the algorithms to produce the cipher text from the plain text. The encryption time can be used to calculate the encryption throughput of the algorithms.

Input File	**Original Hill Cipher**	**Modified Hill Cipher**	**Proposed Algorithm**
File Size (Kb)	Encryption Execution time (msec)	Encryption Execution time (msec)	Encryption Execution time (msec)
10	13	8	5
20	17	13	11
30	25	19	15
40	31	22	17
Total 100 Kb	**86 msec**	**62 msec**	**48 msec**

Table 5.1: Encryption Execution Time for Different File Sizes

For the file of 10Kb in size the encryption execution time for original Hill cipher, Modified Hill cipher and proposed algorithm are 13, 8 and 5 msec respectively and for file size of 100 kb the encryption execution time are 86, 62 and 48 msec respectively. Since it is shown that proposed algorithm consumes less time for all types of file sizes. With the help of the table we are able to plot the graph showing how the encryption execution time depends on the file size and we are able to compare Hill Cipher with various algorithms.



Graph 5.1: Encryption Execution Time for Different File Sizes

5.2.2 Decryption Computation Time

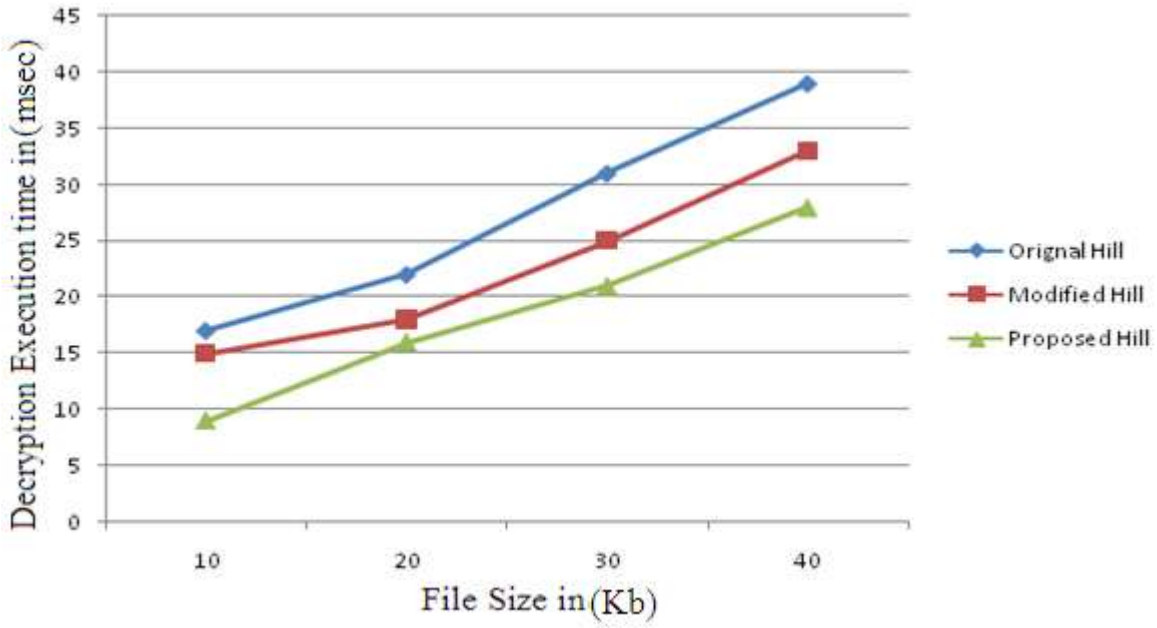
The decryption computation time is the time taken by the algorithms to produce the plain text from the cipher text. The decryption time can be used to calculate the decryption throughput of the algorithms.

Input File	Original Hill Cipher	Modified Hill Cipher	Proposed Algorithm
File Size (Kb)	Decryption Execution time (msec)	Decryption Execution time (msec)	Decryption Execution time (msec)
10	17	15	9
20	22	18	16

30	31	25	21
40	39	33	28
Total Size 100 Kb	**109 msec**	**91 msec**	**74 msec**

Table 5.2: Decryption Execution Time for Different File Sizes

and for file size of 100Kb the decryption execution time are 109, 91 and 74 msec respectively. Since it is shown that proposed algorithm consumes less time for all types of file sizes. With the help of the table we are able to plot the graph showing how the decryption execution time depends on the file size and we are able to compare Hill Cipher with various algorithms.



Graph 5.1: Encryption Execution Time for Different File Sizes

5.2 Outcome

From the simulation result, it shows that when the cipher text is decrypted with the help of public or private keys we get the same plaintext. It can be observed that proposed approach provides less commutation time for all types of file sizes when compared to other algorithms. The proposed algorithm is optimized compared to other algorithms in terms of hacking and

processing time. So the accuracy and secrecy of proposed algorithm is better than other existing algorithms.

Chapter 6: Conclusions and Future Work

From the introduction it has been concluded that the Cryptography provides the confidentially, privacy and secrecy in unsecure communication channel. Literature Survey has been successfully carried out and objectives have also been drawn. Cryptography provides solution for data integrity, authentication and non-reproduction. The Hill cipher technique using a novel method of self-repetitive matrix and it has been successfully implemented. From the experimental results it has been shown that the modified Hill Cipher is easy to implement and difficult to crack. This technique becomes more secure by using modular arithmetic. The block size which is specified as 64 bit is expandable as per requirement, thus gives flexibility in message string length. It generates key of 56 bits which is enhance the security aspect of this algorithm and make them more secure than other encryption algorithms. Due to the following facts it has been concluded that it takes very less time for execution as compare to other Hill Cipher algorithm. Using the Hill Cipher, performance will be appropriate in much kind of applications where it is suitable. The proposed algorithm has been compared with other algorithms and found that throughput of proposed algorithm is greater than other encryption algorithms. More several systems can also be optimizing if multiple keys can be used. Future work will be carried out to decrease the complexity of the proposed algorithm.

References

[1] A. Bibhudendra, "Novel Methods of Generating Self Invertible Matrix for Hill Cipher Algorithm", International Journal of Security, Vol. 1, no. 1, pp. 14-21, 2006.

[2] A. Khalique, K. Singh and S. Sood, " A Password Authenticated Key Agreement Scheme Based on ECC Using Smart Cards", International Journal of Computer Applications, Vol. 2, No.3, pp. 26-30, 2010.

[3] A. Tannous, J. Trostle, M. Hassan, S. E. McLaughlin and T. Jaeger, "New Side Channels Targeted at Passwords", Annual Computer Security Applications Conference, Vol. 2, pp. 45-54, 2008.

[4] A. Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.

[5] B. Acharya, S.K. Patra and G. Panda, "Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System", International Journal of Recent Trends in Engineering, Vol. 1, No.4, pp. 106-108, 2009.

[6] B. Acharya, S. K. Panigrahy, S. K. Patra and G. Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, pp. 663-667, 2009.

[7] B. B. Madan, K. G. Popstojanova, K. Vaidyanathan and K.S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167-186, 2004.

[8] D. Anand, V. Khemchandani and R. K. Sharma, "Identity Based Cryptography Techniques and Applications", International Conference on Computational Intelligence and Communication Networks, Vol. 1, pp. 343-348, 2013.

[9] D. R. Stinson, "Cryptography Theory and Practice", 3rd edition Chapman Hall, Vol. 1, pp. 13-37, 2006.

[10] D. Sharma and D. Jinwala, "Identity Based Secure Key Generation Protocol", International Conference on Computer & Communication Technology, Vol. 9, pp. 416-421, 2011.

[11] H.W. Kim and S. Lee, “Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System”, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 214-224, 2004.

[12] H. Krawczyk, “The Order of Encryption and Authentication for Protecting Communications, http://eprint.iacr.org/2001.

[13] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, “Dual RSA and Its Security Analysis”, IEEE Transactions on Information Theory, Vol. 53, No. 8, pp. 2922-2933, 2007.

[14] I. I.A, A. Mohammed and D. Hossam, “How to repair the Hill cipher”, Journal of Zhejiang University Science, Vol. 1, pp. 2022-2030, 2006.

[15] I. A. Ismail, M. Amin and H. Diab, “How to repair the Hill Cipher”, Journal of Zhejiang University Science A, Vol. 7, no. 12, pp. 2022-2030, 2006.

[16] Jung. W. Lo, M. S. Hwang and C. H. Liu, “An efficient key assignment scheme for access control in a large leaf class hierarchy”, Journal of Information Sciences Elsevier Science, Vol. 4, pp. 917-925, 2003.

[17] J. A. Moreno, K. Matsuo, L. Barolli and F. Xhafa, “ Secure Communication Setup for a Peer to Peer Communication”, IEEE Transaction on Industrial Electronics, Vol. 58, No. 6, pp. 2086-2096, 2011.

[18] J. Lan, W. L. Goh, Z. H. Kong and K. S. Yeo, “A Random Number Generator for Low Power Cryptographic Application” ISOCC, Vol. 1, pp. 328-331, 2010.

[19] J. H. Li, B. Bhattacharjee, M. Yu and Levy, “A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks”, Journal of Future Generation Computer Systems, Elsevier Science Publishers, Vol. 24, pp. 860-869, 2008.

[20] J. Ren and L. Harn, “Generalized Ring Signatures”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 155-163, 2008.

[21] K. Wang, “An Encrypt and Decrypt Algorithm Implementation on FPGAs”, International Conference on Semantics, Knowledge and Grid, Vol. 1, pp. 298-301, 2009.

[22] K. Sakiyama, Y. Li, K. Ohta and M. Iwamoto, “Information Theoretic Approach to Optimal Differential Fault Analysis”, IEEE Transactions on Information Forensics and Security, Vol. 2, pp. 109-120, 2012.

[23] L. Buttyan, L. Czap and I. Vajda, “Detection and Recovery from Pollution Attacks in Coding Based Distributed Storage Schemes”, IEEE Transaction on Dependable and Secure Computing, Vol. 8, No. 6, pp. 824-838, 2011.

[24] L. Eschenauer and V. D. Gligor, “A Key Management Scheme for Distributed Sensor Networks”, ACM conference on Computer Security, Vol.2, pp. 41-47, 2002.

[25] Lester. S. Hill, “Cryptography in an algebraic alphabet”, Amer. Math, Vol. 1, pp. 306-312, 1936.

[26] M.Y. Wang and C.W. Wu, “A Mesh Structured Scalable IPsec Processor”, IEEE Transaction on Very Large Scale Integration System, Vol. 18, No. 5, 2010.

[27] M. Y. Wang, C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, “Single and Multicore Configurable AES Architectures for Flexible Security”, IEEE Transactions on Very Large Scale Integration Systems, Vol. 2, pp. 541-552, 2010.

[28] M. N. Islam, M. M. H. Mia, M.F. I. Chowdhury and M.A. Matin, “Effect of Security Increment to Symmetric Data Encryption through AES Methodology”, International Conference on Software Engineering, Artificial Intelligence Networking and Parallel Distributed Computing, Vol. 1, pp. 291-294, 2008.

[29] M. Alqdah and L.Y. Hui, “Simple Encryption and Decryption Algorithm”, International Journal of Computer Science and Security, Vol. 1, pp. 14-17, 2008.

[30] N. Koblitz, “Elliptic Curve Cryptosystems”, Journal of Mathematics of Computation. Published by American Mathematical Society, Vol. 48, No. 177, pp. 203-209, 1987.

[31] N. R. Potlapally, S, Ravi, A. Raghunathan and N. K. Jha, “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols”, IEEE Transaction on Mobile Computing, Vol. 5, No. 2, pp. 128-143, 2006.

[32] Pavan. N, Nagarjun G. A, Nihaar N, G. S Gaonkar and P. Sharma, “Image Steganography Based On Hill Cipher with Key Hiding Technique”, IOSR Journal of Computer Engineering, Vol. 11, pp. 47-50, 2013.

[33] P. Gope, A. Singh, A Sharma and N. Pahwa, “An Efficient Cryptographic Approach for Secure Policy Based Routing”, IEEE Journal on Selected Areas in Communications, Vol. 1, pp. 359-363, 2013.

[34] Q. Wang, K. Xu and K. Ren, “Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels”, IEEE Journal on Selected Areas in Communications, Vol. 30, No. 9, pp. 1666-1674, 2012.

[35] R. H. Torres, G. A. Oliveira, J. A. M. Xexeo,W. A. R. Souza and R. Linden, “Identification of Keys and Cryptographic Algorithms using Genetic Algorithm and Graph Theory”, IEEE Latin America Transactions, Vol. 3, pp. 178-183, 2011.

[36] R. K. Chahar, G. Datta and N. Rajpal, “Design of a New Security Protocol”, IEEE International Conference on Computational Intelligence and Multimedia Applications, Vol. 4, pp. 132-134, 2007.

[37] S. Khar, N. Bhargawa, R. Shukla and M. Shukla, “Implementation and Enhanced Modified Hill Cipher by P-box and M-box technique”, International Journal of Information Technology and Knowledge Management , Vol. 5, No.1, pp. 53-58, 2012.

[38] S. T. Halkidis, N. Tsantalis and A. Chatzigeorgiou, “Architectural Risk Anaylisis of Software Systems Based on Security Patterns”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 129-142, 2008.

[39] S. Verma, R. Choubey and R. Soni, “An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security”, International Journal of Emerging Technology and Advanced Engineering, Vol. 1, pp. 18-21, 2012.

[40] S.P. Kumar, R. Fareedha, M. Jenieferkavetha, A. Geanremona and R. Juliajoyce, “Secured Grid Based Route Public Key Cryptography Scheme for Heterogeneous Sensor Network”, International Journal of Grid Computing & Applications Vol. 1, No.2, pp. 15-25, 2010.

[41] S. F. Mare, M. Vladutiu and L. Prodan, “Secret data communication system using Steganography, AES and RSA”, International Symposium for Design and Technology in Electronic Packaging, Vol. 2, pp. 339-344, 2011.

[42] T. Jamil, “The Rijndael Algorithm”, IEEE Potential, Vol.1, pp. 1-4, 2004.

[43] T. Ma, P. L. Shrestha, M. Hempel, D. Peng, H. Sharif and H.H. Chen, "Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs", IEEE Transactions on Biomedical Engineering, Vol. 59, No. 4, pp. 1041-1048, 2012.

[44] V.P. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar and N. Shroff, "A Minimum Cost Heterogeneous Sensor Network with a Lifetime Constraint" , IEEE Transactions on Mobile Computing, Vol. 4, No. 1, pp. 4-15, 2005.

[45] V. U. K. Sastry and K. Shirisha, "A Block Cipher Involving a Key Matrix and a Key Bunch Matrix, Supplemented with Permutation", The International Journal of Engineering and Science, Vol. 1, pp. 40-47, 2012.

[46] W. He, Y. Huang, K. Nahrsted and W. C. Lee, "A Self contained Public Key Management Scheme for Mission Critical Wireless Ad Hoc Networks", IEEE International Conference on Pervasive Computing and Communications, Vol. 1, pp. 1- 10 2007.

[47] X. Dongyang, Z. Tang and Y. Yinyan, "An Efficient Key Management Scheme for Segment based Document Protection", IEEE Conference on Consumer Communications and Networking Conference, Las Vegas, Vol. 1, pp. 896-900, 2011.

[48] X. Du, M. Guizani, Y. Xiao and H. Chen, "A Routing Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1223-1229, 2009.

[49] X. Li, W. Zhang, X. Wang and M. Li, "Novel Convertible Authenticated Encryption Schemes without Using Hash Functions", International Conference on Advanced Communication Control and Computing Technologies, Vol. 1, pp. 504-508, 2012.

[50] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location Based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.

[51] Y. Karandikar, X. Zou and Y. Dai, "An Effective Key Management Approach to Differential Access Control in Dynamic Environments", Journal of Computer Science, Vol. 1, pp. 542-549, 2006.

[52] Y.S. Shiu, S. Y. Chang, H.C. Wu, S. C.H. Huang and H.H. Chen, " Physical Layer Security In Wireless Networks", IEEE Wireless Communications, Vol. 1, pp. 66-74, 2011.

[53] Z. Wan, J. Liu and R. H. Deng, "A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transaction on Information Forensics and Security, Vol. 7, No. 2, pp. 743-754, 2012.