Experimental Analysis of Modified hill cipher to perform encryption and decryption for invertible and noninvertible matrices

Pooja Sharma[1], Tarun Dalal[2]

[1]M. Tech. Student, Department of CSE, CBS Group of Institutions, Jhajjar, Haryana
[2]Asst. Prof., Department of CSE, CBS Group of Institutions, Jhajjar, Haryana

Abstract

The Hill Cipher is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods. Cryptography is a security mechanism which caters the security services of world in perfect manner. In this paper, the author has studied and performed the experimental analysis of modified hill cipher to perform encryption and decryption for invertible and noninvertible matrices.

Keywords: Modified hill cipher, encryption, decryption, invertible and noninvertible matrices.

INTRODUCTION

The global society has faced many changes because of the digital revolution. Along with all, this has also increased the number of hackers and viruses. There is a need of a system which can control the curious eyes from getting in a harm way. In such a situation, steganography and cryptography emerge as a savior for such important information [1].

Cryptography is a Greek word for "hidden writing." The art and science of transforming (encrypting) information (plaintext) into a transitional form (cipher text) that stores information in storage or transit. The main feature of cryptography is to solve the problems, which are associated with verification, integrity and privacy. A protocol is the sequence of actions, which is designed with two or more sides, through which a goal can be fulfilled. Cryptography also, is associated with the meaning of protocol. Thus, a cryptographic protocol is a protocol that deals with the use of cryptography. This protocol uses cryptographic algorithm and intends to halt attempts of thefts and invasions [2].

In today's world, security is a major problem especially when it comes to hiding secret information from total strangers. So, converting a message into a form that cannot be easily cracked is an ultimate option for all. Due to the new and improved techniques used by hackers, sharing information on the internet is less secure now a days. To overcome such problems have evolved techniques like steganography and cryptography [3].

If we uncover the pages of history we find that in those times too, secret information was passed from one party to another via various means like invisible ink, tattoos and much more and that has become the brain child for the present techniques like cryptography where the online secret information sharing has become more secure for parties who have a sensitive information that cannot fall in wrong hands [4].

Cryptography

Cryptography is the art and science of achieving security by encrypting information to make them non-readable format [5].

Basic terms used in cryptography

- **Plain text-**Clear text is a readable format or original message understand by any person. For example, if A wants to send a message to B + "Hello" then here "hello" is a plain text message.

- **Cipher text-**It is unreadable message or after the encryption the resulting message is called cipher text. For example, "sd45@#$" is a Cipher Text produced for "hello".

- **Encryption-** Encryption is the process of converting plaintext into ciphertext. It is performed at the receivers side.

- **Decryption-**The process of cipher text converts plain text called decryption. Cryptography uses the decryption technique at the receiver side to obtain the original message from cipher text. The process of decryption requires two things- decryption algorithm and key. Generally the encryption and decryption algorithm are same, with the understood reverse concepts [6].

Key-There are basically, two types of Key Cryptographies:

1. Single key cryptography- Also called a private key cryptography, the encrypting and decrypting keys are similar.

2. Two key cryptography- It is also called a public key cryptography as the encrypting and decrypting keys are different. [7]

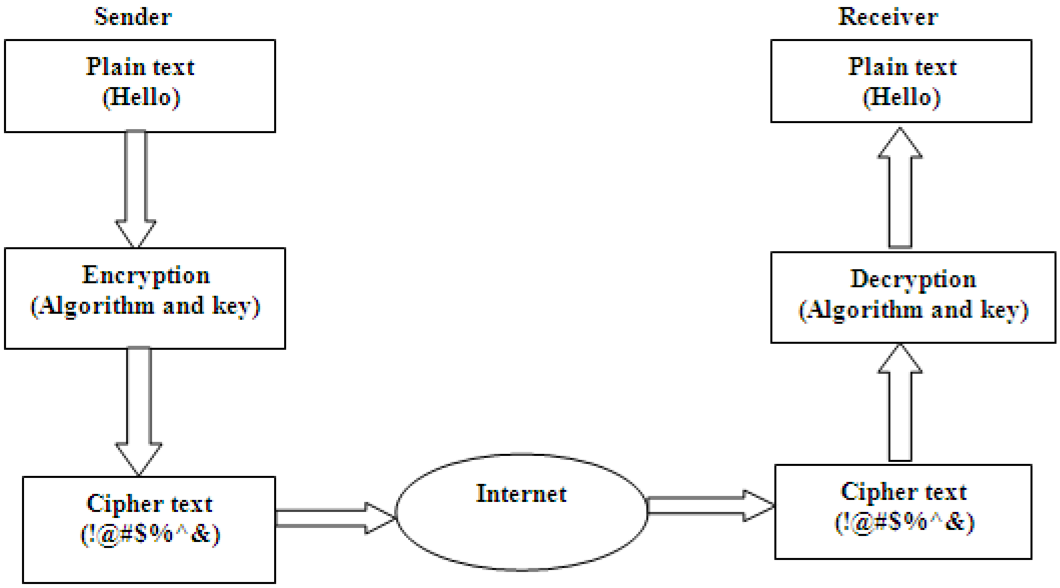
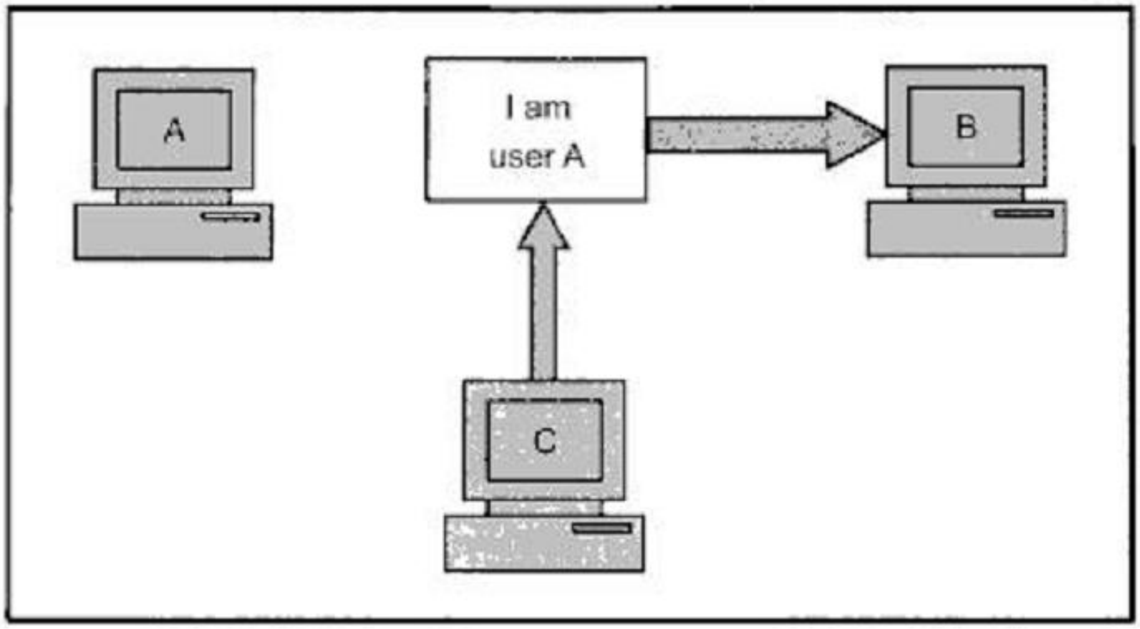


Figure 1: Model of Cryptography

SECURITY SERVICES & ATTACKS

Authentication

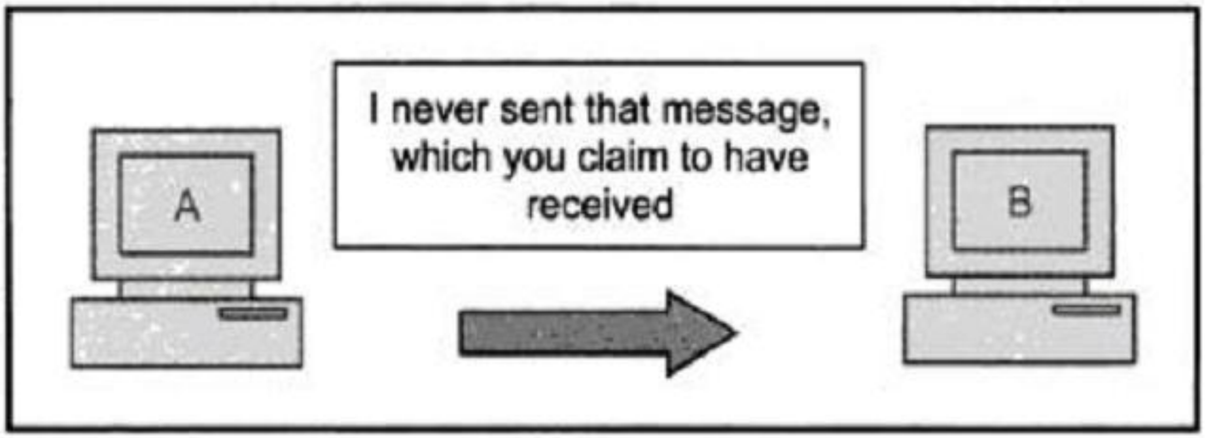
In the affiliation orienting communication, it provides the authentication of the sender or receiver throughout the affiliation institution (peer entity authentication) [4], it authenticates the source of data (also called data origin authentication) [8].



User C is that user C has exhibit as user A once he sent this document to user B. However, the issue would user B grasp that the message has returned from user C, World Health Organization is sitting as user A? a true life example of his can be the case of a user C, sitting as a user A causation a funds transfer request (from A's account to C's account) to bank B. The bank may with happiness transfer the funds from A's account to C's account-after all, it'd suppose that user A has requested for the funds transfer. This idea is shown in figure 1.5. This type of attack is understood as fabrication [9].

Non repudiation

Non-repudiation service protects against repudiation by either the sender or the receiver of the Data. In this with the proof of origin, the receiver of the data can later prove the identity of the Sender. If denied. In non-repudiation with the real proof of delivery the sender Of the data can later prove the data were delivered to the intended recipient [10].



User A performs the funds transfer as per A's instruction, a may claim that whenever sent the funds transfer instruction to the bank. Thus, A repudiates, or denies, his fund transfer instruction. The principle of non-repudiation defeats such prospects of denying instruction, once sent. Non repudiation doesn't enable the sender of a message to refute the claim of not causation that message [11].

Access Control

Access management could be a system that permits associate degree authority to regulate access to areas and resources during a given physical facility or computer-based data system. Associate degree access system, with within the field of physical security [12].

Book Code Attack

Brute force attacks are not effective on encryption algorithm that uses the chaos function. In encryption if they are using chaos function technique it is impossible to decrypt the information. The chaos in hiding information is that it is extremely sensitive in the initial condition. Even a minute of changes can bring a drastic change. In book code attack, attacker applying all possible changes in cover image and stego image using random keys after the analysis. [13]

Cipher Text Only Attack

In a Ciphertext only Attack, Donald must access to just some ciphertext. He tries to seek out the corresponding key and therefore the plaintext.
The assumption is that Donald is aware of the formula and may intercept the ciphertext.

Known Plain Text Attack

In A best-known Plain Text Attack, Donald Has Access To Some Plaintext/Ciphertext Pairs additionally To The Intercepted Ciphertext That He needs to interrupt.The plaintext/ciphertext pairs are collected earlier.

Chosen-Plaintext Attack

The chosen-plaintext attack is analogous to the known-plaintext attack, however the plaintext/ciphertext combines are chosen by offender herself.

PROPOSED METHODOLOGY

Encryption Algorithm:

The steps of the encryption algorithm are as follows:
Step1: Start
Step 2: Input: Plaintext, Key Matrix,
Step 3: Convert the plaintext characters in to matrix form P
Step 3: Perform Encryption using

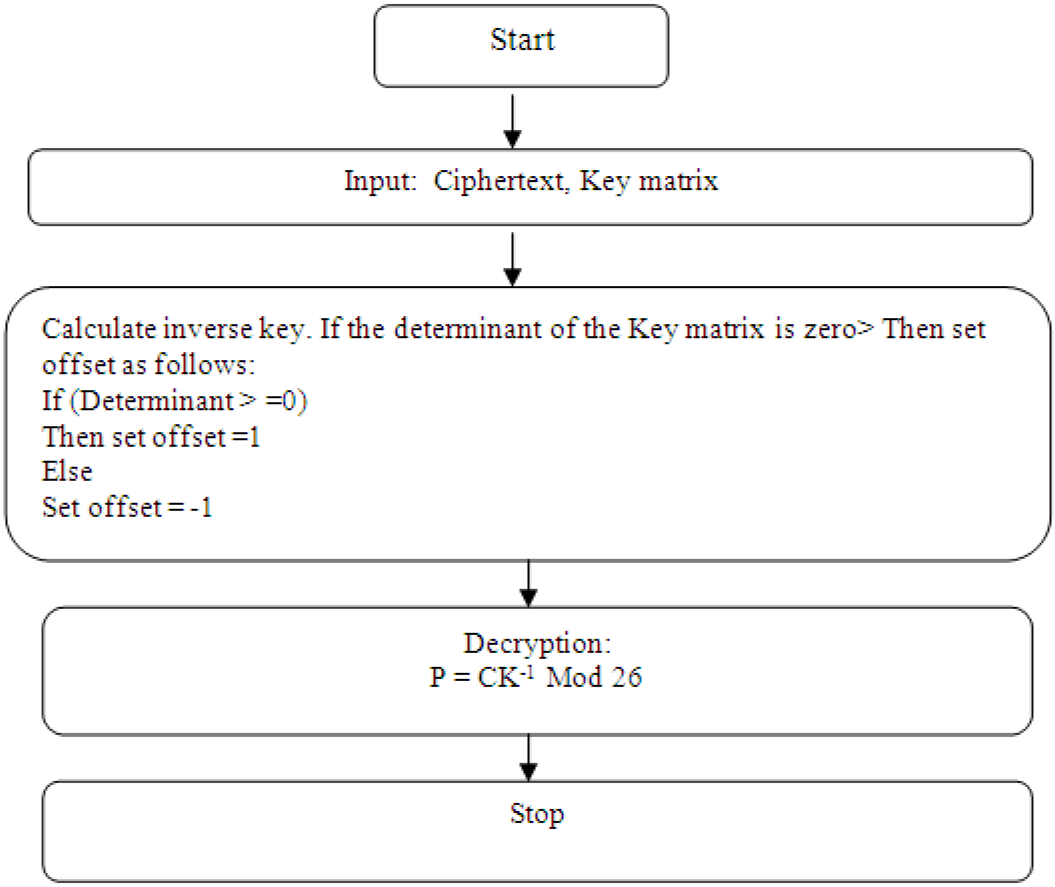
$$C = KP \text{ MOD } 26$$

Where C & P are the matices of order 1 X N. Also K is a matrix of the order NXN.

Decryption Algorithm:

The steps of the Decryption algorithm are as follows:
Step1: Start
Step 2: Input : Ciphertext, Key matrix
Step 3: Calculate inverse key. If the determinant of the Key matrix is zero> Then set offset as follows:
If (Determinant > =0)
Then set offset =1
Else
Set offset = -1
Step 4: Decryption:
$P = CK^{-1}$ Mod 26

Encryption:
The steps of the proposed method are as follows:


Start
Input: Ciphertext, Key matrix
Calculate inverse key. If the determinant of the Key matrix is zero> Then set offset as follows:
If (Determinant > =0)
Then set offset =1
Else
Set offset = -1
Decryption:
P = CK^{-1} Mod 26
Stop

IMPLEMENTATION

The basic design of the entire image retrieval concept is prepared. in this chapter the proposed model implementation is demonstrated. Therefore the required tools and techniques, implemented and referenced classes and the implemented GUI is described in detail.

Tools and Techniques

The implementation required for this software and hardware on the development side system:

(A) Tools-
User Interface Design (UI Design)-Net Beans IDE 6.7.1
(B) Technology/Framework-
Framework-JDK 1.6
(C) Hardware Specifications-
3 GB storage disk
512 MB RAM
Intel P4 Processor
(D) Software Specifications-
Linux or
Windows based platform

NETBEANS IDE 6.7.1

Net Beans Integrate Development Environment (IDE) is a modular, standards-based IDE, inscribed in the Java encoding skill. The Net Beans project consists of an open source IDE inscribed in the Java encoding skill and an application platform, which can be recycled as a standard structure to construct any sympathetic of application.

JDK

Java Platform, Standard Edition (Java SE 8) which code-named “Mustang” is the new name and future version of what previously known as J2SE. The new liberate will be identified as product version 8, and developer version 1.8.0. Java SE 8 has two products brought under the name of the platform, that’s Java SE Development Kit 8 (JDK 8) and Java SE Runtime Environment 8 (JRE 8).Java SE 8 has a greater level of maturity, stability, scalability and security of Java implementations. Java SE 8 has a lot of new characteristics, enhancements and improvements, especially better GUI performance and better handling of the behavior of GUI applications, plus improvements and new features in server-side core and Java core. Enhancements to the JVM Tool interface.

SYSTEM DOMAIN

Implementation of the required system utilize software and hardware for successfully implementation is listed in this section.

Recommended

- 2.0 GHz Processor required (Pentium 4 and above)
- Minimum 2 GB RAM
- 25 GB hard disk space

Software

- Operating System (Windows XP and above)
- Netbeans
- Jdk

SOFTWARE CONFIGURATION:

✓ **Operating System**	**: Windows XP**
✓ **Programming Language**	**: JAVA**
✓ **Java Version**	**: JDK 1.6 & above.**

CONCLUSION

In this paper, the basic design of the entire image retrieval concept is prepared. Also the proposed model implementation is demonstrated. Therefore the required tools and techniques implemented and referenced classes and the implemented GUI is described in detail. Comparison has been done between the proposed encryption algorithm, New Hill and a few others previous Hill algorithms. New Hill has features which obviously overcome some of the vulnerabilities in the existing Hill algorithms.

REFERENCES

[1]. William Stallings “ Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.

[2]. National Bureau of Standards, “ Data Encryption Standard,” FIPS Publication 46, 1977.

[3]. Prashant Sharma, “Modified Integer Factorization Algorithm using V-Factor Method”, 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.

[4]. Prof.Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh ,“Enhanced Method for RSA Cryptosystem Algorithm” 2012International Conference on Advanced Computer Science Applications and Technologies, IEEE 2012.

[5]. V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[6]. Shashi Mehrotra Seth, 2Rajan Mishra,” Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.

[7]. Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms",

[8]. G. jai Arul jose, research scholar,sathyabama University,Chennai-possible Attack on RSA Signature.

[9]. Vitthal S., BhosaleRajkumar S., Panhalkar Archana R A Novel Security Scheme for Secret Data using Cryptography and Steganography. DOI: 10.5815/ijcnis.2012.02.06

[10]. Manjunath N, S.G. HiremathImage and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique ISSN : 2347-2820, Volume -3, Issue-5 2015.

[11]. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena Security Improvisation in Image Steganography using DES 978-1-4673-4529-3/12/_c 2012 IEEE

[12]. Yang Ren-er, ZhengZhiwei, Tao Shun, Ding ShileiImage Steganography Combined with DES Encryption Pre-processing 978-1-4799-3434-8/14 © 2014 IEEE DOI10.1109/ICMTMA.2014.80

[13]. Mr. Madhusudhan Mishra, Mr. GangadharTiwari, Mr.Arun Kumar YadavSecret Communication using Public key Steganography [978-1-4799-4040-0/14/$31.00 ©2014 IEEE

[14]. Manu Devi Nidhi Sharma Improved Detection of Least Significant Bit SteganographyAlgorithms in Color and Gray Scale Images 978-1-4799-2291-8/14/$31.00 ©2014 IEEE

[15]. D. B. Rane, Swetal R.Gund, Chandreshwari B. Pawar, Jyoti F. Ukande , " Hardware Implementation of RC4 Stream Cipher using VLSI", IJCTEE, Vol. 3, pp. 8184, March 2013.

[16]. Poonam Jindal and Bramhajit Singh, "A survey on RC4 stream cipher," IJCNIS, Vol. 7, pp. 37–45, Jun. 2015.

[17]. Rajendar Racherla and S. Nagakishor Bhavanam, "Design and simulation of enhancing RC4 stream cipher for Wi-Fi security using Verilog HDL," IJERA, vol. 1, Issue 3, pp. 653–659.

[18]. Sultan Weatherspoon, "Overview of IEEE 802.11b security," Network Communication Group, Intel Technology Journal Q2, 2000.

[19]. P.kitsos, G. Kostopoulos, N. Sklavos and O. Koufopavlou, IEEE Std 802.11. IEEE Standard: Hardware implementation of the RC4 stream cipher, IEEE, Vol. 4, pp. 13631366, 2004.

[20]. Claude E. Shannon. Communication theory of secrecy systems. Bell Systems Technical Journal, Vol. 4, pp. 656–715, 1949.

[21]. Description of BluetoothTM. Bluetooth specification, E0 encryption algorithm. Technical Journal Vol 2, pp. 1072–1081, June 2010.

[22]. Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: A practical attack on Bluetooth encryption. In Victor Shoup, editor, CRYPTO, Springer Vol 3621, pp. 97–117, 2005.