International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 7 Issue 5, May-2018, Impact Factor: 3.578

Study of encryption and decryption for matrices using Modified hill cipher

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 backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. 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.

Introduction

The network security becomes more important with the development of various techniques of network development. With the growth in the use of world wide web, this has become even more important as the users can access tools and edit the information. While communicating any information via an unsecure channel to its righteous owner, security issue becomes important. To avoid such problem, cryptography and steganography are the main ways of communicating such information in a stealth mode without anyone knowing what it is.

With the increase in the content on the web, the increase of viruses and bad eyes in the form of hakers, privacy has become an important issue among many. In such situation, Image Steganography has many important roles and application. Specially, when two parties want to communicate secretly.

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.

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 steganography where the online secret information sharing has become more secure through images and other imaging techniques for parties who have a sensitive information that cannot fall in wrong hands.

Cryptography System Classified in to Category

There square measure 2 cryptography mechanisms, counting on what keys square measure used. If an identical secret is employed for coding and secret writing, we tend to tend to call the mechanism as Symmetric key cryptography. On the various hand, if 2 fully totally different keys square measure used in science mechanism, then we tend to tends to call mechanism as uneven Key or asymmetric key [4].

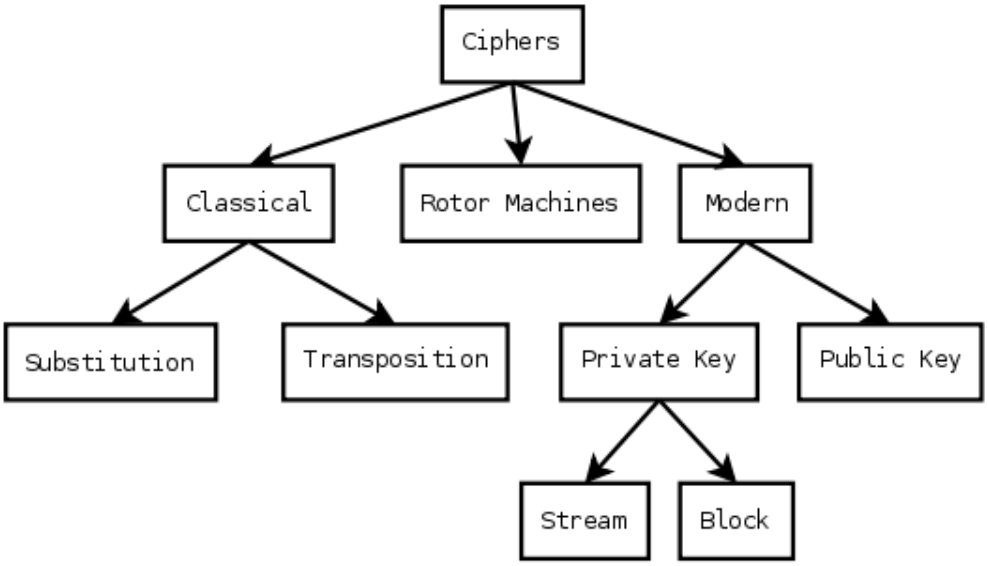

Figure 1: Cryptography Classification

LITERATURE REVIEW

Yang Ren-er, ZhengZhiwei, Tao Shun, Ding Shilei[4] , have presented DES algorithm for encryption along with LBS algorithm so that the hidden information is given a dual protection and the information is compressible and invisible to anyone else. Problem of the research was DES algorithm. Now days it is easily breakable.

Mr. Madhusudhan Mishra, Mr. Gangadhar, Tiwari, Mr.Arun Kumar Yadav,,[5] the authors has used a new technique. The author has used RSA algorithm for encryption along with F5 algorithm. To hide the encrypted message in the lower image, the author has also used a two tier security layers- first using cryptography key and second using stego key.

Manu Devi, Nidhi Sharma, [6] the proposed system the author has used LBS steganography for image embedding. The author has calculated the PSNR for the better quality of the image and how it is calculated has also been mentioned. The higher the PSNR value, the better is the quality of the stego image. The main aim of the research was developing a new and enhanced technique of hiding the data. The main motive was to make the encrypted message totally unbreakable from the inside.

Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R.[1]has proposed model gives two tier security to secret data. Further our proposed method gives high embedding capacity and high quality stego imagesusing advanced encryption standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with least-significant-bit (LSB) substitution is used to hide encrypted message into true color RGB image.

Its two main keys are used i.e. in encryption and decryption. RSA is an algorithm based in the theorem of factoring two large prime numbers. [3, 5].

Advance Encryption Standard (AES)

The Advance Encryption Standard algorithm described by AES is a Symmetric-Key Algorithm, meaning the same key is used for encrypting and decrypting the data.

The algorithm was invented by Joan Daemen and Vincent Rijmen. AES can process 128 bit data block and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be referred to as AES-128, AES-192 and AES-256 respectively. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides resistance against all known attacks, simple in design and good speed of computation.

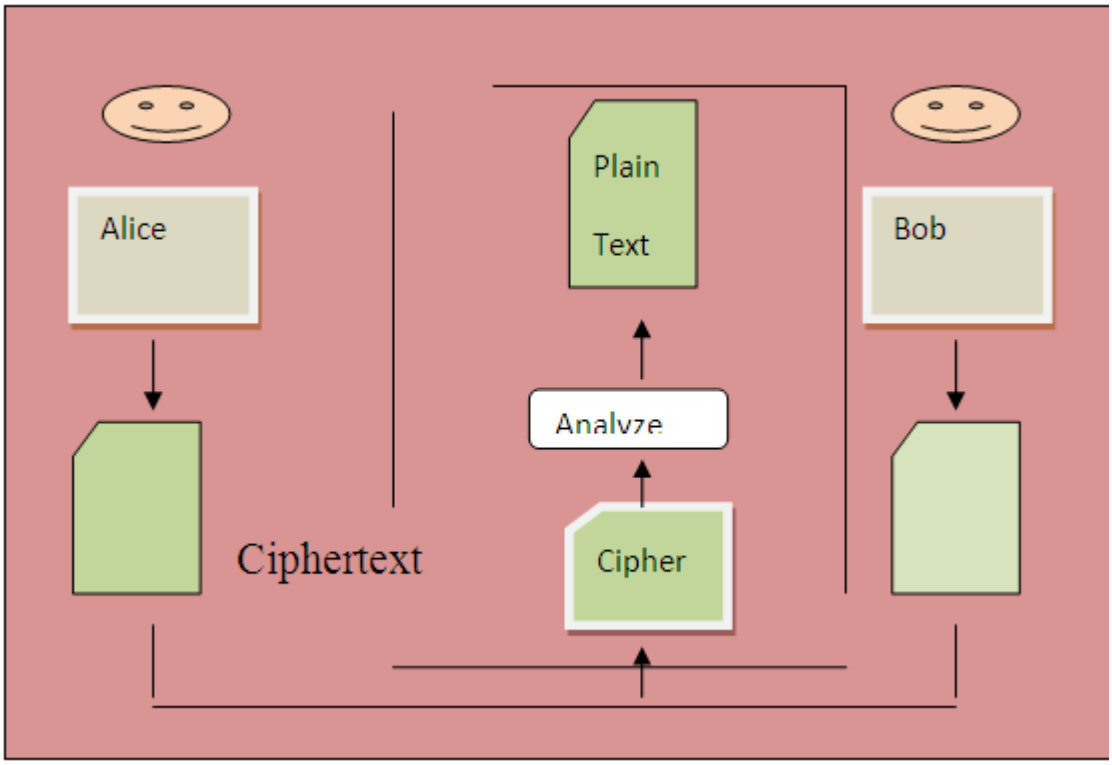

Fig 2: A broad level steps in IDEA

AES Algorithm has following steps.

1) Key Expansion—Expand the key to get the actual key block to be used
2) Initial Round—Each byte of the state is combined with the round key using bitwise XOR.
3) Rounds
a) Sub Bytes—A non-linear substitution step where each byte is replaced with another according to a lookup table.
b) Shift Rows—A transposition step where each row of the state is shifted cyclically a certain number of steps.
c) Mix Columns—A mixing operation which operates on the columns of the state, combining the four bytes in each column.
d) Add RoundKey
4) Final Round (no Mix Columns)
a) Sub Bytes
b) Shift Rows
c) Add RoundKey
Advantages of using AES algorithm
1) Very Secure.
2) Reasonable Cost.
3) Main Characteristics
i) Flexibility, ii) Simplicity

Peak Signal to Noise Ratio(PSNR)

Peak Signal to Noise Ratio (PSNR) is calculated to measure the stego image's quality. The quality of a digital image or video is assessed through this statistical measurement method. The larger the PSNR value is smaller will be the possibility of a visual attack by a human. [8]

Bluetooth TM is one of the major modern technologies for wireless communication, prevalent in an array of practical devices. In 1998, the Bluetooth special interest group (SIG) developed the technology. The technology has been

embraced by all companies in the communication business ever since. The E0 stream cipher is used as a pseudorandom key stream generator for confidentiality in Bluetooth transmission [16]. The cipher follows the standard design model of a combiner generator by the use of linear feedback shift registers, where the key length is typically of 128 bits. Since 1999, several attacks have been mounted on E0, resulting in practical and near-practical breaches [17][18][19][20].

A5/1 and A5/2 stream ciphers, designed around late 1980's, are used to provide privacy in the GSM cellular network. A5/2 is a (deliberately) weakened version of A5/1, created for certain export regions. Both the ciphers A5/1 and A5/2, initially kept secret, became public in 1994 through leaks and reverse engineering [21].

3GPP LTE advanced [22] is the leading contender in the race towards 4G mobile technologies. For LTE advanced technology, the chosen security algorithms for encryption and authentication employ two different stream ciphers – snow 3G [21] and ZUC [23].

Common Problems in Existing RSA Variants [8]:

- The main disadvantage of RSA decryption is its slower speed
- Not secure against wiener's attack
- Problem arise to common modulus attack
- known plaintext attack are possible
- Low decryption exponent attack if we know the decryption exponent.
- The decryption time slow.

SECURITY SERVICES & ATTACKS

Data Confidentiality

The principal of confidentiality specifies solely the sender and meant recipient(s) ought to be ready to access the content of the message. Confidentiality has been defined by the International

Organization for Standardization (ISO) in ISO-17799 as "ensuring that info is accessible solely to those licensed to possess access "and is one at all The cornerstones of data security. Confidentiality is one in all the planning goals for several cryptosystems, created doable in the follow by the techniques of contemporary cryptography. It is designed to shield the knowledge from revelation attack.

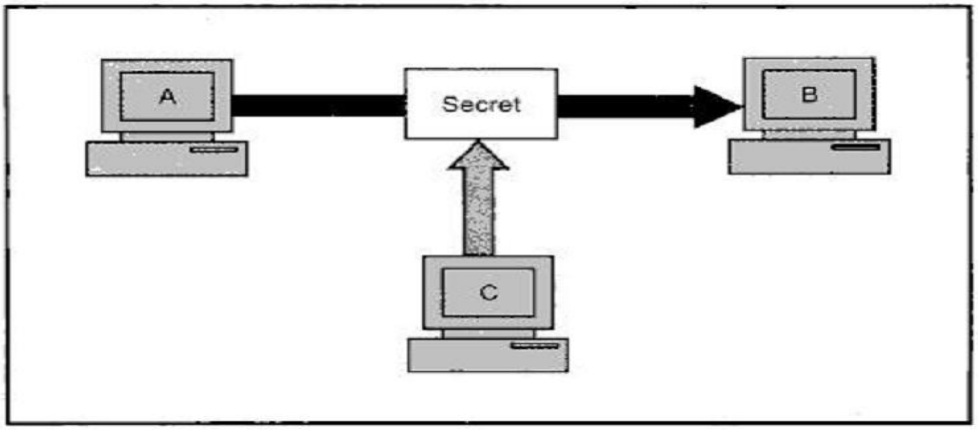

Figure 3: Data Confidentiality

The service as outlined by X.800 is incredibly broad and encompasses confidentiality of whole message or a part of a message and additionally protection against traffic analysis. That's it's designed to stop snooping and traffic analysis [3].

Data Integrity

Data Integrity is intended for the protection of knowledge from unauthorized modification, insertion, Deletion associate degrees replaying by an informant. It will defend the complete message or the part of the message. User c tampers with a message originally sent by user A, which is truly destined for user B. User C somehow manages to access it, amendment,

it contents, and send the amendment message to user B. User B has no method of knowing that the content of massage was amended once user A had sent it. User A conjointly doesn't knowing concerning this variation. This kind of attack is thought as modification.

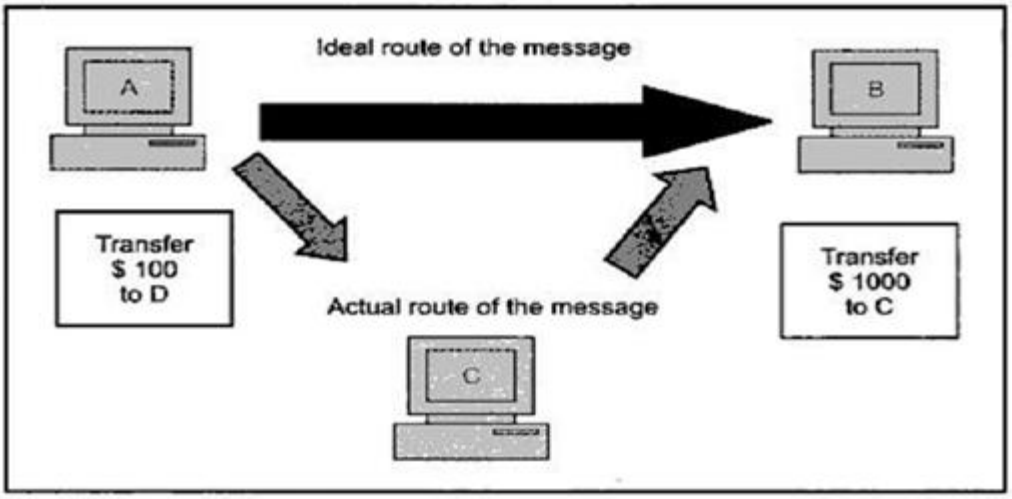

Figure 4: Data Integrity

Encryption algorithm and key

Every encryption and decryption process has two aspects:

- Algorithm
- key

There are two types of keys in cryptography

Symmetric key - Symmetric key uses a single key for both encryption and decryption.
Asymmetric key - Asymmetric key uses one key for encryption and another key for decryption.

Comparison of various Symmetric Key Cryptography Algorithms

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

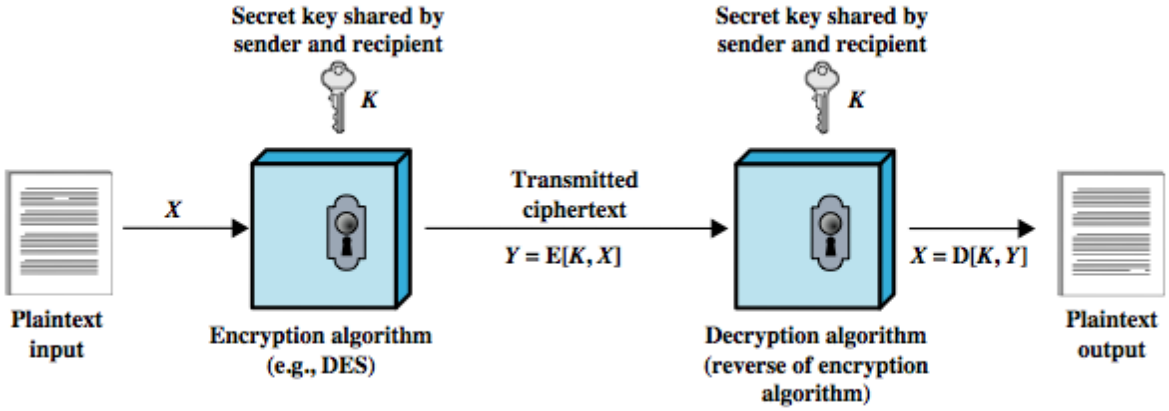

Figure 5 : symmetric key encryption

Table 1: Different symmetric key encryption algorithm

Algorithm Name	Maximum size of KEY	Use of algorithm/Security
DES	56 bits	Insecure
3DES	168 bits	Replaced by AES
AES	128,192, or 256 bits	US Govt classified information
IDEA	128 bits	Used in PGP, very secure
BLOWFISH	32 to 448	Public domain
RC5	Up to 2040	Secure for 72-bits or more

CONCLUSION

In this paper, the author has studied about the encryption and decryption for matrices using Modified hill cipher. Comparison Analysis between the proposed encryption algorithm, New Hill and a few others previous Hill algorithms has been also studied. New Hill has features which obviously overcome some of the vulnerabilities in the existing Hill algorithms. However, New Hill still have the ability to encrypt the plaintext effectively even if k equals zero.

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.