Open access Journal International Journal of Emerging Trends in Science and Technology
IC Value: 76.89 (Index Copernicus) Impact Factor: 4.219 DOI: https://dx.doi.org/10.18535/ijetst/v4i8.41

Encoding and Decoding information with the help of Hill Cipher

Author
Archana[1], Ashish Vashisht[2]
[1]Student, Computer and Science, Kururkshetra Institute of Technology and Management, Kurukshetra, Harayana, India
[2]Assistant Professor, Kururkshetra Institute of Technology and Management Kurukshetra ,Harayana , India

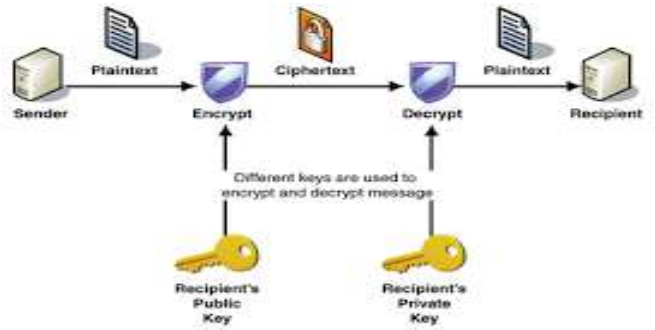
Abstract
The role of cryptographic part in today's world is very significant. It not only secures information mathematically by mailing massage with a key but also provides confidentiality which is the most important factor in today's world. Hill cipher is also one of the most famous symmetric cryptosystem which can be used to protect information from unauthorized party. This paper gives us dimensions of new technique in Hill cipher, here we are developing the complex procedure of key generation for the process of encryption of message to avoid any kind of data loss. Hill cipher is a matrix based poly graphic substitution which is an additional factor to the user.
A sender wants to transmit information to a receiver over an insecure channel that is a channel which may be tapped by any one. So, the information which is to be transferred, which we call the plaintext (actual message) which must be transformed (encrypt) to a cipher text, a form not legible by anybody other than the particular receiver. There must be given some way to decrypt the cipher text, i.e. get back the original message, while this must not be possible for receiver to read the information. This is where keys come into play; the receiver is considered to have a key at his disposal, let him to recover the actual message, a fact that distinguishes him from any data loss. This leads to the user for a secure account for user.
Key Words : Hill-Cipher, Encryption(Encode), Decryption(Decode), Data- Perturbation method.

Introduction

In today's world, the aim of transmitting contents securely not new issue. The last many years everyone had a need to keep their modes of communications private and secure. All people over the world are using internet as basic mode of communication. It is very important to secure our essential documents from unauthorized users as this can create a high security issue. Hence, Network security is blooming on the horizon as a potentially massive problem because of large number of unauthorized people. In this Info technical age, the Internet and other forms of communication become use -able, electronic security is becoming field to provide better security and each of them have their own merits and demerits. As a result researchers are still exploring new techniques in the field of cryptography to enhance the network based security for future. Cryptography is said to be the process of technology under which holding the principles and methods of transforming a plain text into the other form, (cipher text) and then re - generating that message back to its original form.

In modern world, cryptography is considered to be a branch of both fields of mathematics and computer science also is related closely with information theory. Cryptography is the science of

encryption (encoding), plays a very efficient role in sending private e-mails , mobile phone, communications, computer passwords, pay-TM, e-commerce, transmitting all information, security of ATM cards & pays attention on many aspects of our daily lives with the maximum support Various algorithms have been made in computer security and network processing with network transparency, and engineering and much wider parts too. The data transferred from one system to another system via public network that can be protected by means of encryption. In encryption the data is encoded by using the 'key'. Only the sender and receiver is having the path via which they can access to the same 'key' can decrypt the encoded data . It is same as covering data with packet by user and receiver can open it with the help of secret key.



Hill Cipher

Though Hill cipher's or we can say that linear block cipher is susceptible to cryptanalysis and minimum use in practice, still serves an important pedagogical role in both cryptology and linear algebra. The role of the linear algebra that raises several interesting questions which increases the curiosity in hill cipher. In general, the key space of the Hill cipher is precisely GL(r, Zm) the group of r * r matrices that are invertible over Zm for a predetermined modulus m. We first present a formula for the order of this group. We consider involuntary matrices, which eliminate the necessity of computing matrix inverses for Hill decryptions. Finally, we compare the total number of matrices with the number of invertible and involuntary matrices, identifying the effects of change in dimension and modulus on the order of the key space. It is fundamentally equivalent and is consistent with modern texts used in cryptography. A plaintext string over an alphabet of order m can be rewritten as a vector over Zm is using a natural correspondence. In either column major or row-major order, the vector is rewritten as a matrix P with d rows, where d is an arbitrarily chosen positive integer.

For a fixed n ϵ IN, the key space K is the set of all invertible n x n matrices in ZZnxn26 .P = C = ZZn26. Also, messages m ϵ ZZ* that are longer than n are split into blocks of length n and are encrypted block-wise. All arithmetic operations are carried out on modulo 26[1]. The Hill cipher is then defined as follows:

For each K ϵ K, defines as the encryption function.

EK : ZZn26 -> ZZn26 by[1]

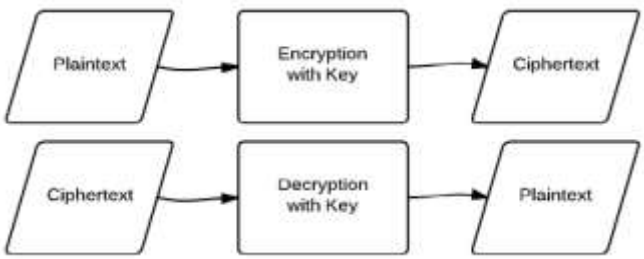
EK (p) = K . p mod 26 ……(1)

Where "." denotes matrix multiplication modulo 26[1].

Letting K-1 denote the inverse matrix of K, the decryption function DK-1: ZZn26 -> ZZn26 is defined by the values given below 2nd equation.

DK-1(c) = K-1 . c mod 26[1] ……...(2)

The value for K-1 can easily be computed from the value K, As the Hill cipher is a symmetric cryptosystem and is also the most of it have general linear block cipher. We must be aware about the Affine linear block ciphers are easy to break by known-plain-text attacks. That is for there is an attacker who knows some sample plain texts with the corresponding encryptions, it is not too hard to find the key used to encrypt these plain texts as already some of data is with attacker.So we generate a session key which remains active for few intervals of time for senders and recievers.



Data- Perturbation method

It is a mathematical method that gives approximate solutions to problems that cannot be solved exactly by starting from the exact solution of a related values but to nearer simpler problem. A critical feature of the technique is a middle step that breaks the problem into "solvable" and "perturbation" parts. Perturbation theory is applicable only on the problem if the problem at hand cannot be solved completely or can be terminated completely, but can be partially came to end by adding a "small" term to the mathematical description to transform it to the exactly solvable problem.

Perturbation theory gives us an expression for the required solution in terms of a formal power series in some of it is called as "small" parameter – known as a **perturbation series** – that quantifies the deviation from the exactly problem which is solvable. Leading the term present in the given values of the solution which is said to be exactly solvable problem, while further terms describe the deviation in the value of solution, due to the deviation from the initial problem. Formally, we are having the value for the v for the approximation to the full solution A, a series in the small parameter (here called ε), like the following:

- $A = A_0 + \varepsilon A_1 + \varepsilon^2 A_2 \ldots\ldots\ldots\ldots$

In this example, A_0 would be the known solution to the exactly solvable initial problem and A_1, A_2, ... represents the higher-order terms which may be found iteratively by some systematic procedure. For small ε these higher-order terms in the series become successively smaller. An approximate "perturbation solution" is obtained by truncating the series to get partially values, usually by keeping only the first two terms, the initial solution and the "first-order" perturbation correction

A. ENCRYPTION

1) Shared-Secret-Key: 3 Aenee is G00d..

2) One-time Session-Key: Nature Kals me..

3) Intermediate-Key:} 7"L4]

4) Input Text: My name is ARCHANA. I am working as a computer engineering student of college KITM. It is well known engineering college of Kurukshetra and 9km away from kurukshetra university .

5) Total No. of Characters: 130

6) Decimal format of the Input Text: 77 121 32 110 97 109 101 32 105 115 32 66 65 76 65 74 69 69 32 77 65 82 65 77 46 32 73 32 97 109 32 119 111 114 107 105 110 103 32 97 115 32 97 110 32 65 115 115 105 115 116 97 110 116 32 80 114 111 102 101 115 115 111 114 32 105 110 32 71 77 82 73 84 46 32 73 116 32 105 115 32 119 101 108 108 32 107 110 111 119 110 32 101 110 103 105 110 101 101 114 105 110 103 32 99 111 108 108 101 103 101 32 105 110 32 67 111 97 115 116 97 108 32 65 110 100 104 114 97 46

7) Now all the characters (Except.) in each sentence have been shuffled according to Double reflecting data perturbation method.

8) After shuffling the characters in the first sentence is like the following:

L y+8,4Y0&yWXMXOTTyLXGXL. In this way, all the characters present in each sentence will be shuffled according to Double reflecting data perturbation method.

9) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).

10) All matrices will be transposed.

11) All 4 characters in each row in every matrix will be shuffled according to Double-reflecting-data-perturbation method.

12) Now the characters present in 1st row, 2nd row, 3rd row and 4th row in 1st matrix will be arranged in form of paragraph. Then, from 2nd matrix and so on.

13) Now the first 16 characters are "<PX0MAG 4y4Uy+MU"

14) The first 16 characters are XOR ed with one-time Session-Key. So the first 16 characters are converted like the following: "r1,E?$gkU G u Ec{".

15) Next 16 characters are XORed by Intermediate-Key, and so on continues till all part is covered.

16) Now the Intermediate-Key is appended to cipher-text and transmitted to the receiver at destination point from senders point.

B. DECRYPTION

1) After receiving the cipher-text, the receiver extracts the last 16-bytes (Intermediate-Key) so that decoding becomes easy and avoids hacking issue.

2) Now the receiver can calculate the Session-Key by using Shared-Secret-Key and Intermediate-Key.

3) The first 16 characters are XORed with one-time Session-Key. So the first 16 characters are converted like the following: "r1,E?$gkU G u Ec{".

4) Next 16 characters are XORed by Intermediate-Key, and so on.

5) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).

6) All 4 characters in each row in every matrix will be shuffled according to Double-reflecting-data-perturbation method.

7) All matrices will be transposed.

8) Now all the characters in each row of each matrix including left-over characters are arranged in the form of paragraph.

9) All the characters in each row (dot is delimiter for each row) will be reshuffled according to Double-reflecting-Data-Perturbation method.

Conclusions

As of now, there are many algorithms and technologies have been proposed by many researchers in the world. But till today, it is very difficult to provide security to the information which is being passed through Internet. So this proposed paper tries to give one more new algorithm for Information Security. It is a Symmetric Encryption only.

This technique is used by maximum number of higher institution so that there is least chance of loss of data as well as privacy concern will b maintained well to avoid any future contradiction. Also, crypto don't work individually it work with some systems so here that platform we used is hill cipher. Under this, third party can never attack the data because there are so many keys are available for the given set and to check for each individual key it will not be only time consuming but also very hectic. The chances of data or information loss are nearly equal to zero. In this research we came to know about how the security is being modified from the previous one. Even in ancient times, the data is being delivered with high privacy. Also, there are several methods of conventional cryptography, and since it is not possible to present all the methods, very important and popular methods were presented.

The algorithm is modified so it provides great security thus no one in between sender and receiver will hack the data because it will require the key. Key is the part which is used for the decoding the encoded data which is having large permutation number and hacking that key from this is quite hectic and time consuming. This makes the security level too high.

Advantages In Proposed System

1) For even sentences, the Session-Key is applicable and for odd sentences, the Intermediate-Key is applicable. So, the two

consecutive sentences will be encrypted differently.

2) No need to send both the keys i.e. Session-Key and Intermediate-Key to one person. Firstly judge the person whether he/she is eligible for this then, enact over the situation of giving key authority.

Future Scope

The main achievement is the correctly functional tool of hill cipher. Unfortunately the time constraints have meant that not all the originally mentioned objectives were accomplished. The various compression techniques may be applied for efficient utilization of bandwidth & storage. This system can be extended to work on the files containing Unicode characters as well leads to the formation of minor codes. This application can be extended to work with other file formats. By addition of transferring of data from one system to another, system can be enhanced.

References:

1. W. Stallings; "Cryptography and Network Security", 2nd Edition, Prentice Hall,1999
2. Bruce Schneir: Applied Cryptography, 2nd edition, John Wiley & Sons, 1996
3. A. Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.
4. N. Koblitz, "Elliptic Curve Cryptosystems", Journal of Mathematics of Computation. Published by American Mathematical Society, Vol. 48, No. 177, pp. 203-209, 1987.
5. H. Krawczyk, "The Order of Encryption and Authentication for Protecting Communications", http://eprint.iacr.org/2001.
6. L. Eschenauer, V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks", ACM conference on Computer Security, Vol.2, pp. 41-47, 2002.
7. Jung. W. Lo, M. S. Hwang, 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.
8. 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
9. Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167-186, 2004.
10. Stallings. W, "Cryptography and Network Security", 4th edition, Prentice Hall, 2005 [4] A. Viji Amutha Mary, Dr. T. Jebarajan, A Novel Data Perturbation Technique with higher Security, IJCET, Vol:3, Issue:2, pp:126-132,2012
11. http://aix1.uottawa.ca/~jkhoury/cryptography.htm) [6] Maram Balajee, Challa Narasimham, "Double-reflecting Data Perturbation Method for Information Security", ISSN: 0974-6471 December 2012, Vol. 5, No. (2):Pgs. 283-288
12. *William E. Wiesel (2010). Modern Astrodynamics. Ohio: Aphelion Press. p. 107. ISBN 978-145378-1470.*
13. Martin C. Gutzwiller, "Moon-Earth-Sun: The oldest three-body problem", Rev. Mod. Phys. 70, 589 – Published 1 April 1998
14. *Cropper, William H. (2004), Great Physicists: The Life and Times of Leading Physicists from Galileo to Hawking, Oxford University Press, p. 34, ISBN 978-0-19-517324-6.*
15. L. A. Romero, "Perturbation theory for polynomials", Lecture Notes, University of New Mexico (2013)
16. Sergei Winitzki, "Perturbation theory for anharmonic oscillations", Lecture notes, LMU (2006) Michael A. Box, "Radiative perturbation theory: a review",

Environmental Modelling Software 17 (2002) 95–106

17. *Bransden, B. H.; Joachain, C. J. (1999). Quantum Mechanics (2nd ed.). p. 443. ISBN 978-0582356917.*