

A Review of Modern Hill Cipher Techniques

Neha Sharma¹ Sachin Chirgaiya²

^{1,2} Department of Computer Science and Engineering

^{1,2} Oriental University, Indore, India

Abstract— In this paper, we are presenting some modern techniques for the encryption and decryption. Basically, all modern version of hill cipher are discussed in brief. This review research paper concentrates on the different kinds of encryption techniques that exist. The advantages and disadvantages of each method are also discussed in brief. In modern era, the use of information and communication technology is increasing day by day. It means that the information is travelling at a brisk pace. It is needed to be secured. We hope that our study will help in increasing the efficiency of popular encryption and decryption technique.

I. INTRODUCTION

Cryptography is the learning of mathematical practices related to features of information refuge such as confidentiality, information reliability, entity authentication, and information origin authentication. Cryptography is not the only way of providing information refuge, but rather one set of methods.

The security services include:

- 1) Data Confidentiality
- 2) Data Integrity
- 3) Authentication
- 4) Non repudiation
- 5) Access Management

A. Data Confidentiality:

Confidentiality has been defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access and is one of the cornerstones of information refuge. Confidentiality is one of the design goals for lots of cryptosystems, made possible in practice by the methods of modern cryptography. It is designed to protect information from disclosure attack. The service as described by X.800 is very broad and encompasses confidentiality of whole message or part of a message and also protection against traffic analysis. That is it is designed to prevent prying and traffic analysis [2,3]

B. Data Integrity:

Data Integrity is designed for the protection of data from unauthorized modification, insertion, deletion and replaying by an adversary. It can shield the whole message or the part of message.

C. Authentication:

This service provides the authentication of the party at the other end of the line. In the connection oriented communication, it provides the verification of the sender or receiver during the connection establishment (peer entity authentication). In connectionless communication, it

authenticates the source of data (also called data origin authentication).

D. Non-repudiation:

Non-repudiation service protects against repudiation by either the sender or the receiver of the data. In this, the receiver of the data can later prove the individuality of the sender if denied. In non-repudiation with the genuine proof of delivery the sender of the data can later on prove the data were delivered to the intended recipient [11, 12]. Non-repudiation is the concept of ensuring that a party in a dispute cannot deny, or refute the legality of a statement or contract. Although this theory can be applied to any broadcast, including television and radio, by far the most familiar application is in the proof and trust of signatures.

E. Access Control:

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access management system, within the area of physical refuge, is normally seen as the next layer in the security of a physical structure. It provides security against unauthorized access against data. The term access in this definition is very broad and can involve reading, writing, amending, executing programs. [2,3]

1) Classification

Cryptographic schemes are usually classified along three independent dimensions:

- 1) Type of procedures used for transforming plaintext to cipher text. All encryption algorithms stand on two general principles. Those are substitution, in which every element in the plain text is mapped into a different element and transposition in which elements in the plaintext are rearranged. The primary requirement is that no information be lost. Most schemes referred to as product systems, involved various stages of substitution and transposition.
- 2) The number of keys used: If sender and receiver make use of the identical key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender as well as the receiver each uses a diverse key the system is referred to as asymmetric, two key, or public-key encryption.
- 3) The way in which the plaintext is processed: A block cipher operates the input on block of elements at a moment, producing an output block for each input block. A stream cipher operates the input elements uninterruptedly, producing one output element at a moment, as it goes alongside.

2) Algorithms and Keys

A cryptographic algorithm, furthermore known as a cipher, is that the function used for encryption and decryption. (Generally, there are two connected functions: one for encryption and the other for decryption).

Terminology

If the security of an algorithm relies on keeping the manner that algorithm works a secret, it's a restricted algorithm. Restricted algorithms have historical interest, but are miserably inadequate by today's standards. An oversized or ever-changing cluster of users cannot use them, because every instance a user leaves the cluster everyone else must switch to a distinct algorithm. If somebody accidentally reveals the secret, everybody must modify their algorithm.

Even a lot of damnatory, restricted algorithms permit no excellence control or standardization. Each cluster of users should have their own distinctive algorithm. Such a cluster can't use ready-made hardware or software products; an eavesdropper can purchase a similar product and learn the algorithm. They need to write down their own algorithms and implementations. If nobody within the cluster is a sensible cryptographer, then they won't recognize if they have a secure algorithm. In spite of this major weakness, restricted algorithms are vastly admired for low-security applications. Users either don't notice or don't care regarding the security problems inbuilt in their system.

Modern cryptography solves this dilemma with a key, denoted by K . This key can be anyone of an outsized quantity of values. The series of potential values of the key is known as the key space. Both the encryption and decryption processes use this key (i.e., they are reliant on the key and this reality is denoted by the K subscript), therefore the functions at this instant becomes:

$$Ek(M) = C$$

$$Dk(C) = M$$

Those functions have the characteristics that:

$$Dk(Ak(M)) = M$$

Some algorithms use a unique encryption key and decryption key. That is, the encryption key, $K1$, is completely different from the corresponding decryption key, $K2$. During this case:

$$Ek1(M) = C$$

$$Dk2(C) = M$$

$$Dk2(Ek1(M)) = M$$

All of the protection within these algorithms relies in the key (or keys); none of them relies in the details of the algorithm. This suggests that the algorithm may be revealed and examined. Products utilizing the algorithm can be off-the-shelf. It doesn't matter if an eavesdropper is aware of your algorithm; if she doesn't recognize your specific key, she can't examine your messages.

3) Symmetric Algorithms

There are two general forms of key-based algorithms: symmetric and public-key. Symmetric algorithms, generally known as standard algorithms, are algorithms wherever the encryption key is often calculated from the decryption key and contrariwise. In most symmetric algorithms, the encryption key and the decryption key are similar. These algorithms, conjointly known as secret-key algorithms, single-key algorithms, or one-key algorithms, need that the sender and receiver agree on a key before they can

communicate firmly. The refuge of a symmetric algorithm rests within the key; divulging the key implies that anyone might inscribe and decode messages. Because the communication has to stay secret, the key must stay secret. Encryption and decryption in a symmetric algorithm are symbolized by:

$$Ek(M) = C$$

$$Dk(C) = M$$

Symmetric algorithms are often divided into two classes. Some operate on a single bit plaintext (or generally byte) at a moment; these are known as stream algorithms or stream ciphers. Others operate the plaintext in clusters of bits. The clusters of bits are known as blocks, and also the algorithms are known as block algorithms or block ciphers. For contemporary PC algorithms, a typical block size is sixty four bits large enough to prevent analysis and minute enough to be feasible. (Before computers, algorithms typically operated on plaintext one character at a time. You will be able to think about this as a stream algorithm working on a stream of characters.)

4) Public-Key Algorithms

Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any affordable quantity of time) be calculated from the encryption key. The algorithms are known as "public-key" as a result of encryption key is created public: An entire outsider will use the encryption key to encipher a message, however solely a selected person with the corresponding decryption key can decipher the message. In these systems, the encryption key is typically known as the public key, and the decryption key is generally known as the private key. The private key is for the time being also known as the secret key, however to avoid confusion with symmetric algorithms, that label won't be used here.

Encryption using public key K is symbolized by:

$$Ek(M) = C$$

Even though the public key and private key are diverse, decryption with the analogous private key is symbolized by:

$$Dk(C) = M$$

Sometimes, messages are encrypted with the private key and decrypted with the public key; this is often utilized in digital signatures. Despite the potential confusion, these operations are symbolized respectively by:

$$Ek(M) = C$$

$$Dk(C) = M$$

5) Symmetric-key vs. public-key cryptography

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both. This section highlights variety of those and summarizes options noticed in previous sections.

Advantages of symmetric-key cryptography

- 1) Symmetric-key ciphers may be designed to own high rates of information outturn. Some hardware implementations reach encrypts rates of many megabytes per second, whereas software system implementations could achieve outturn rates within the megabytes per second series.
- 2) Keys for symmetric-key ciphers are comparatively short.

- 3) Symmetric-key ciphers may be used as primitives to construct varied crypto logical mechanisms as well as pseudorandom number generators, hash functions, and computationally proficient digital signature schemes, to call simply some.
- 4) Symmetric-key ciphers may be composed to provide stronger ciphers. Straight forward transformations that are simple to evaluate, however on their own fragile, may be used to construct sturdy product ciphers.

The high growth in the networking technology leads a common culture for interchanging of the digital images very drastically. Hence it is more vulnerable of duplicating of digital image and re-distributed by hackers. Therefore the images have to be protected while transmitting. All the sensitive information like email, credit cards, personal information banking transactions and identity number need to be protected. To do the same many encryption techniques exist which are used to avoid the information theft. The encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. There are many encryption techniques, which are used to protect the confidential data from unauthorized use. Encryption is also a very common technique for the image security. There are many areas where the encryption and decryption techniques are used. Some of the popular areas are as follows: Image encryption, chaos based encryption, video encryption etc. They have applications in many fields including the internet communication, medical imaging, multimedia systems, Tele-medicine and military Communication etc. Therefore encryption is a heart favorite topic for many researchers. The new methods of encryption techniques are discovered frequently. This paper presents some of those recent existing encryption techniques and their security issues. Their performances are studied and discussed in later chapters of the paper.

Hill Cipher Encryption [1]

The Hill cipher was developed by the mathematician Lester Hill in 1929. The encryption algorithm of Hill cipher takes m successive plaintext letters as input and substitutes for them m cipher text letters. The substitution is performed by m linear equations in which each character is assigned a numerical value. Core of hill cipher is matrix manipulation. For, the system can be described as follows:

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

Decryption requires the inverse of matrix. The inverse K^{-1} of a matrix K is defined by the equation.

$$KK^{-1} = I \text{ Where } I \text{ is the identity matrix of order } N \times N.$$

NOTE: The inverse of a matrix doesn't always exist, but when it does it satisfies the preceding equation.

In general terms we can write as follows:

$$\text{For encryption: } C = KP$$

$$\text{For Decryption: } P = K^{-1}C = K^{-1}KP = P$$

II. LITERATURE SURVEY

Here, we are discussing some new modifications of the Hill cipher. The Hill cipher [7] uses interlacing and iteration and [8] uses interweaving, it means transposition of the binary bits of the plaintext letters and iteration in both encryption and decryption.

The work done in [9] uses a pair of key matrices. In [10], a key on one side of the plaintext matrix and its inverse on the other side are used. In method of the work done in [7, 8] each letter of the plaintext is represented into a binary form under consideration in terms of ASCII code and 128 is used as a fundamental operation. In proposed method the interweaving and interlacing is a type of bit-level permutations and 16 iterations are used. The result analysis that is the cryptanalysis and the avalanche effect of these ciphers has indicated that ciphers cannot be broken by any cryptanalytic attack.

One more modification of the Hill cipher is proposed in [9] by introducing a pair of key matrices. First key is used on the left side of plaintext matrix and second on the right side of plaintext is used as matrix multiplications. Every letter of the plaintext is converted into a binary form under consideration in terms of EBCDIC code and 256 is used as a fundamental operation. Then an iterative process which includes a bit-level permutation on the matrix transformation is used. The results of avalanche effect and cryptanalysis clearly show that the cipher can be strong one. This strength is obtained by the pair of the key matrices one on the left side of the plaintext and the other key on the right side of the plaintext and the process of permutation.

The recently modified Hill cipher is presented in [10]. By having a key on one side of the plain text matrix and its inverse on the other side. In the proposed cipher bit-level permutation which named Mix process is applied. Mix process is used for mixing the plaintext at every stage of the iteration. Every cipher has its own avalanche effect and its own strong and weak points.

One more newly developed technique is discussed in [11]. Several modifications of Hill Cipher have appeared in the literature of Cryptography. In all those modifications the modular arithmetic inverse of a key matrix plays a vital role in the processes of encryption and decryption. Now, It is well known that the Hill Cipher containing the key matrix on the left side of the plaintext as multiplicand can be broken by the known plaintext attack. To overcome this drawback, the papers have developed a block cipher which includes a key matrix on both the sides of the plaintext matrix. They have discussed the avalanche effect and cryptanalysis, and have shown that. The proposed cipher is a strong one. In the present algorithm, the objective is to modify the Hill Cipher by including a pair of key matrices. On the left side of the plaintext matrix and another one on the right side of the plaintext matrix as multiplicands. The strength of the cipher becomes highly significant. We represent each character of the plaintext under consideration in terms of EBCDIC code and use mod 256 as a fundamental operation. The security of the cipher is expected to be more as we have two keys.

A lot of the research works have been done with an aim to improve the security of Hill cipher. A method HCM-PT found in [5] tries to make Hill cipher secure by using dynamic key matrix K obtained by random permutations M . This method is also vulnerable against the known-plaintext attack on the plaintext. This motivated [13] to modify HCM-PT. The modified cipher of HCM-PT called SHC-M found in [13] works the same way as HCM-PT but does not

transfer the permutation vector. Both the sender and the receiver use a pseudo-random permutation generator=*PRPG seed n* and only the number of the necessary permutation is transferred to the receiver.

Yi-Shiung Yeh [15] presented a new polygraph substitution algorithm based different bases. Their algorithm uses two co-prime base numbers that are securely shared between the participants. Although their algorithm thwarts the known plaintext attack, involves several mathematical manipulations. It is time consuming and is not efficient for dealing bulk data. Sadeenia [13] tried to make Hill cipher safe and sound by using dynamic key matrix obtained by random permutations of columns and rows of the master key matrix and transfers an encrypted plaintext and encrypted permutation vector to the receiving facet. The numbers of dynamic keys are generated $n!$ Where n refers the scale of the key matrix. Every plaintext is encrypted by a novel key matrix that forestalls the known-plaintext attack on the plaintext but however it is susceptible to known-plaintext attack on permutation vector, the similar vulnerability of original Hill cipher. [7] Proposed a modification to [13] that works similar to Hill cipher permutation method, but it does not transfer permutation vector, instead both sides use a pseudo-random permutation generator, and only the number of the necessary permutation is transferred to the receiver. The number of dynamic keys is the same as [13]. Lin Ch [10] claimed that taking random numbers and using one-way hash function thwarts the known-plaintext attack to the Hill cipher but their scheme is vulnerable to chosen-ciphertext attack. Mohsen Toorani [11,12] proposed a symmetric cryptosystem based on affine transformation. It uses one random number and generates other random numbers recursively using HMAC in chain. Ahmed Y Mahmoud [15] proposed a modification to Hill cipher based on Eigen values HCM-EE. The HCM-EE generates dynamic encryption key matrix by exponentiation with the help of Eigen values but it is time consuming.

Rushdi and Mousa (2009) had designed a robust cryptosystem algorithm for noninvertible matrices based on Hill cipher. The noninvertible key matrix problem is solved by converting each plaintext character into two cipher text characters. So with the decryption, the process involves the conversion of two cipher text characters into one plaintext character. Even though this algorithm solved the non-invertible key hitch, it is time-consuming as the decryption method engaged the computation of an inverse key matrix. It will surely delay the decryption procedure mainly when it involved high dimensional key matrix.

Ismail et al. (2006) proposed a modified Hill cipher which used one-time-one key matrix to encrypt every plaintext blocks. In this algorithm, every plaintext block is encrypted by using its own key. This unique key is computed by multiplying the current key with a secret Initial Vector (IV). The multiplying operation is carried out row by row, thus the algorithm is named as Hill Multiplying Rows by Initial Vector (Hill MRIV). This algorithm is proved to yield better encryption quality.

However, it is proved by Rangel-Romero et al. (2006) that this proposed algorithm is still vulnerable towards known-plaintext attack. Besides, Ismail et al. (2006) does not tackle the non-invertible key matrix problems which may lead to

failure in decryption. Bibhudendra (2006) also proposed an advanced Hill cipher algorithm (AdvHill) which is able to solve the non-invertible key matrix problem. To make sure every ciphertext block can be decrypted; an involutory key matrix is used for encryption. An involutory key matrix is a key which can be used for both encryption and decryption. It means an inverse key matrix is not needed for decryption and this definitely simplify the computational complexity and save the computational time. However, this algorithm still contains some of the major drawbacks of the original Hill cipher such as the vulnerability to known-plaintext attack. Besides, this algorithm is also not suitable to encrypt all-zeroes plaintext as C will always equals zero when P equals zero

One more modification to the Hill cipher is found in [6] which try to improve the security of Hill cipher by using a one-time-one key matrix to encrypt each plaintext block. The unique key is computed by multiplying the current key with a secret Initial Vector. But the author in [12] shows that the method is prone to a known-plain text attack. The proposed method presented here works the same way as SHC-M but our method requires that the master key matrix be MDS. An MDS master key has the key space bigger than that of SHC-M and our method can be used to encrypt plaintext blocks of variable length.

III. CONCLUSION

In this paper the modern variants of hill cipher are considered and analyzed well to advance the performance of the cryptography strategies additionally to confirm the protection proceedings. To sum up, all the techniques are helpful for real-time cryptography. Every technique is exclusive in its own manner, which could be appropriate for various applications. Everyday new cryptography technique is evolving thus quick and secure standard cryptography techniques will constantly work out with high rate of security.

REFERENCES

- [1] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
- [2] Bibhudendra, A., K.P. Saroj, K.P. Sarat and P. Ganapati, 2009. Image encryption using advanced hill cipher algorithm. *Int. J. Recent Trends Eng.*, 1: 663-667.
<http://www.ijrte.academypublisher.com/vol01/no01/ijrte0101663667.pdf>
- [3] Eisenberg, M., 1998. Hill ciphers and modular linear algebra. Mimeographed notes. University of Massachusetts. <http://www.apprendre-enligne.net/crypto/hill/Hillciph.pdf>
- [4] Ismail, I.A., M. Amin and H. Diab, 2006. How to repair the hill cipher. *J. Zhejiang Univ. Sci. A.*, 7: 2022- 2030. DOI: 10.1631/jzus.2006.A2022
- [5] Shahrokh Saeednia, "How to Make Hill cipher Secure," *Cryp- tologia* 24:4, pp. 353-360, Oct 2000.
- [6] Ismail I A, Amin Mohammed, Diab Hossam, "How toRepair the Hill Cipher," *Journal of Zhejiang UniversityScience*, 7(12), pp. 2022-2030, 2006.

- [7] V.U.K. Sastry and N. Ravi Shankar, "Modified Hill Cipher with Interlacing and Iteration", *Journal of Computer Science*, vol. 3, no. 11, pp. 854-859, 2007.
- [8] N. Ravi Shankar, S. Durga Bhavani and V. Umakanta Sastry, "A Modified Hill Cipher Involving Interweaving and Iteration", *International Journal of Network Security*, vol. 10, no. 3, pp. 210-215, 2010.
- [9] A. Varanasi, S.U daya Kumar and V.U.K. Sastry, "A Modified Hill Cipher Involving a Pair of Keys and a Permutation", *International Journal of Computer and Network Security*, vol. 2, no. 9, pp. 150-108, 2010.
- [10] D. S. R. Murthy, S. Durga Bhavani and V. U. K. Sastry, "A Block Cipher Having a Key on One Side of the Plaintext Matrix and its Inverse on the Other Side", *International Journal of Computer Theory and Engineering*, vol. 2, no. 5, pp. 805-810, 2010.
- [11] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", *International Journal of Computational Science*, 2, No. 6, 815-826, Dec. 2008.
- [12] Romero, Y. R. Garcia, R. V. et al., "Comments on How to Repair the Hill Cipher," *J. Zhejiang Univ. Sci. A* 9(2): pp. 211-214, 2008.
- [13] Chefranov, A. G., "Secure Hill Cipher Modification," *Proc. Of the First International Conference on Security of Information and Network (SIN2007)* 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 3437, 2007.

