A Novel version of Hill cipher Technique

Miss Anjali Saxena (Dept. of C.S.E, shree satay sai University, Sehore)
Mr. Harsh Lohiya (Dept. of C.S.E, shree satay sai University, Sehore)

Abstract

As Information Technology (IT) and network security becomes increasingly important in the era of cryptology. Competitive positions of firms, managers have grown more sensitive to their organization's overall security in IT or in every field. In this research area will concentrate on the development of a methodology for the cryptology in secure manner, analysis of encryption/decryption method and vulnerabilities within the context of security system. The aim of this research work is to propose a Novel version of Hill Cipher technique for System Security in cryptology. In this technique shows how encryption/decryption possible in when different typed of vulnerability arises which are harmful for any application or any organization. Distinguish the secure cryptography algorithm according to rating in network security environment due to dynamic and continuous risk on system security. Novel hill cipher technique is introduced for evaluating the vulnerability in secure manner. The potential of the proposed approach has been tested on different vulnerability and attacks. The result is compared with the conventional design method, is superior in terms of solution, quality, faster and reliable. This method is more secure, easy in mathematical computation and achieved known plain text attack. This research work solves the problem of vulnerability which occurred at the execution of decryption process.

I. INTRODUCTION

In this age of universal electronic communication, attackers and hackers, of electronic eavesdropping and electronic fraud, there is indeed needed to store the information securely. This, in turn led to a high awareness to secure information and resources from disclosure, to guarantee the integrity of information and messages, and to secure systems from network-based interruption attacks [2] cryptography, the art of encryption, plays a major role in cellular/mobile phone communications, pay-tv, e-commerce system, sending private emails, transforming financial information, security of ATM cards, system passwords, electronic commerce, digital signature and touches on many aspects of our daily lives. Cryptography is the concept of encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its original form [2]. In the new era, cryptography is considered to be a branch of both mathematics and computer technology, and is affiliated related with information theory, computer security, and engineering. Although in the history cryptography referred only to the encryption and decryption of message using secret keys. Nowadays, cryptography generally classified into two categories, the single key and asymmetric key [3].

The information transferred from one computer to another over secure public network can be protected by the method of encryption. On encryption, the information is encrypted/scrambled by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' cans decrypt/de-scramble the encrypted data. This method is known as private key (secret key) or single key cryptography. There are several standard single key algorithms explained for examples AES, 3DES etc [4].

II. BACKGROUND

Since the Hill Cipher serves as an important role in both cryptology and linear algebra, several researches have been done to improve the Hill cipher. Rushdi and Mousa (2009) had designed a robust cryptosystem algorithm for noninvertible matrices based on Hill cipher. Ismail *et al*. (2006) proposed a modified Hill cipher which used one-time-one key matrix to encrypt each plaintext unit. In this algorithm, each plaintext unit is encrypted by using its own key. This algorithm is proved to yield satisfied encryption quality. Bibhudendra (2006) also proposed an advanced Hill cipher algorithm (AdvHill, 2009) which is able to solve the non-invertible key matrix problem. To make sure every cipher text block can be decrypted; an involuntary key matrix is used for_ encryption. An involuntary 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 (Rangel-Romero *et al*., 2006).

III. METHODOLOGY

Novel Hill cipher provide better solution over previous hill cipher methods, because this will firstly find the inversion of non invertible key matrix and will detect the vulnerability and after that solve it.

From above it is clear that the decryption requires the inverse of the key matrix. But in some cases the inverse of a matrix does not exist. It is a well known fact in the field of mathematics that the entire matrix is not invertible. A matrix is non invertible if the determinant of a matrix is zero. Also if matrix is non invertible then in hill cipher, it is not possible to decrypt the cipher text. In order to overcome the above problem, it is suggested the use of setting offset. **If the determinant of a matrix is zero then set 1 as the offset value. If the determinant is negative then set -1 as the offset value.** First flow chart shows the process of encryption and second flow chart shows the process of decryption.Novel hill cipher is time consuming techniques for encryption and decryption because it is easy in mathematical computation but only for authorized person. This is very complicated to understand and breaking for hackers. Novel hill cipher more secure algorithm in easy manner rather than other complicated hill cipher algorithm. This technique prove that how vulnerability can be overcome of hill cipher without using the complicated mathematical computation. Because mathematical computation is very chaos to understand and implement so this is implemented in easy manner which user can prove how it is provide solution for vulnerability in hill cipher. Now flow chart shows the process of encryption step by step. With the help of flow chart novel hill cipher encryption algorithm is easy in understand and computed.

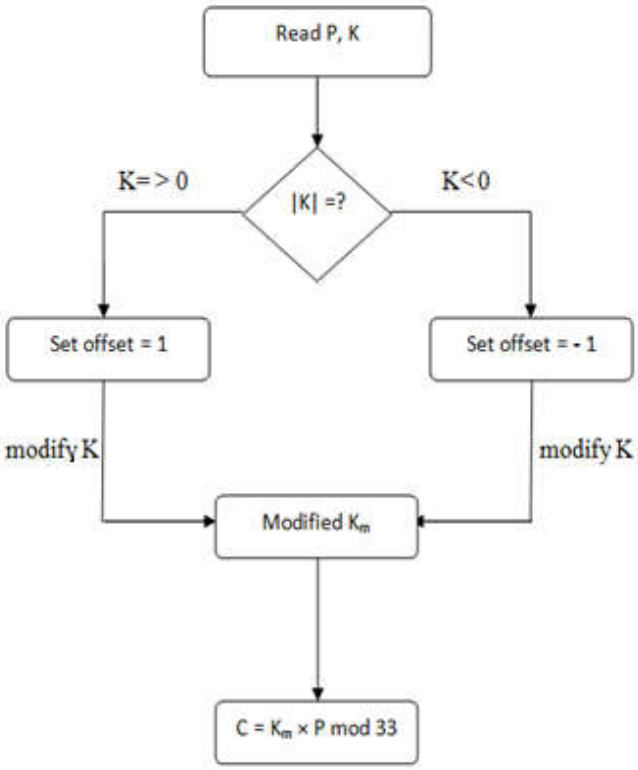

Fig: 1 Proposed Encryption Technique

A. *Proposed Algorithm for Encryption:*

Read Pj, Kij

for i= 0 to n do

for j= to n do

where P is the plain text matrix of order 1×N

K is the chosen key order of N×N

find the |K| = > 0 set offset =1 else offset= - 1

modified $Km_{ij} = K_{ij}$…….(i)

do encryption

$C[i] = C[i] + P_j \times Km_{ij}$ …….. (ii)

C[i] = C[i] mod 33…… (iii)

if C[i] <=0

do

C[i] = C[i] + 33

Generate C where C is the cipher text or encrypted text

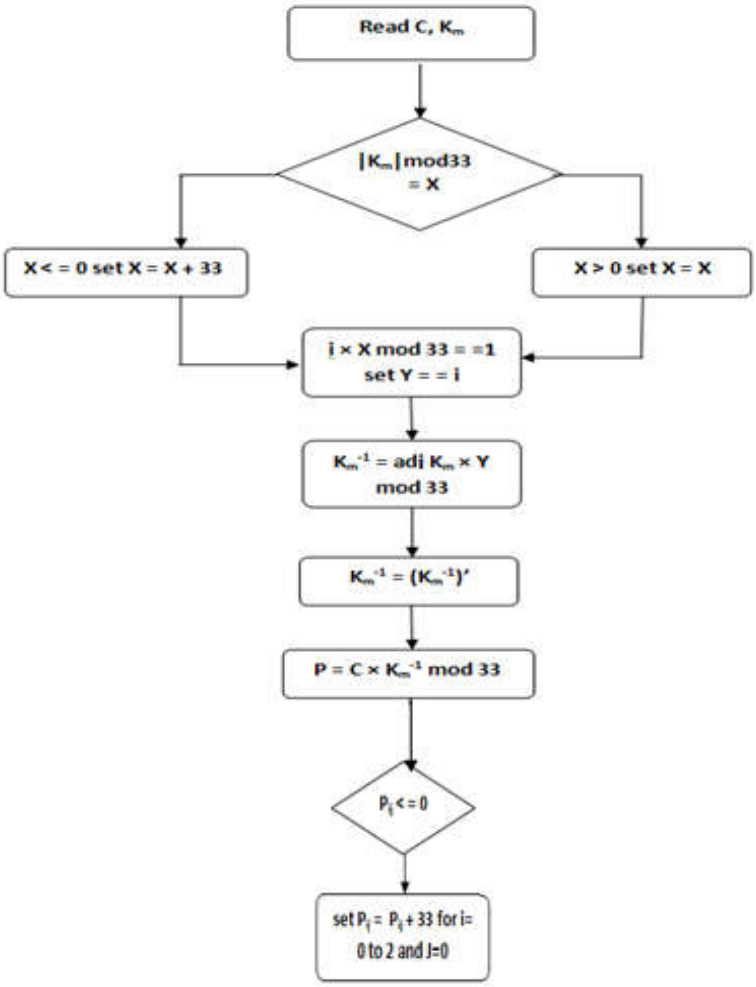

Fig: 2 Proposed Decryption Technique

B. *Proposed Algorithm for Decryption:*

Read C_i and Km_{ij}

where C is the cipher text and Km is modified key matrix

for i=0 to n and for j=0 to n do

find |Km| mod 33 = < 0 set Km = Km +33 else set Km = Km

set x = Km

if i × x mod 33 = = 1 set y = i for i=0 to n do

find Km^{-1} = [adj Km × y] mod 33

P[i] = P[i] + (Km^{-1} [i][j]) × C[j])…… (iii)

for i=0 to n and j = 0 to n do

if P[i] < = 0 do

P[i] = P[i] + 33

read P where P is the plain text.

C. *Novel codes for mod 33*

In this novel code of table 33 codes are using. This table contains 26 alphabets that are placed 1- 26 and 7 special symbols placed 27 to 33. This code are very helpful to find the new variant of plain text and cipher text, because now plain text and cipher text can not only contain the alphabets but also contain the special symbols for example "WHAT?" This is plain text which contains alphabets and special symbols. Alphabets are "WHAT" and special symbol is? So with the help of Novel code it can be possible to encrypt in easy way.

A=1	B=2	C=3	D=4	E=5	F=6	G=7	H=8	I=9	J=10
K=11	L=12	M=13	N=14	O=15	P=16	Q=17	R=18	S=19	T=20
U=21	V=22	W=23	X=24	Y=25	Z=26	,=27	.=28	_=29	-=30
?=31	\=32	:=33							

Table: novel codes

IV.CONCLUSION

In novel version of Hill cipher technique encryption and decryption process implemented successfully and its impact are satisfy the process of encryption/decryption. Comparison has been done between the proposed encryption/decryption algorithm and few others previous Hill cipher algorithms. Novel Hill cipher has features which obviously overcome some of the vulnerabilities in the existing Hill cipher algorithms. Now consideration on overall impact of Novel version of hill cipher it's have ability to encrypt/decrypt messages in secure manner. If talking about network security or information security so researcher can't be imagine that how many types of vulnerabilities are there which breaking the system in every moment of life. So security is the dangerous factor of cryptology not everyone can imagine its power. Researcher and hackers trying to encoded and decoded the systems. So in daily life or in at high risk zone security is most important factor.

ACKNOWLEDGMENTS

First of all I would like to express my heartiest to my guide Mr. Harsh lohiya, for her all time guidance, support, and valuable suggestion.

I would like to express my gratitude towards Prof. Harsh lohiya, Head of the Department, C.S.E., Satay sai sehore.

REFRENCES

[1] Al-Saidi, N.M.G., M.R.M.: "A new approach in cryptographic systems using fractal image coding". Journal of Mathematics & Statistics, Vol. 5 Issue 3, 2009, pp183.189

[2] Rushdi, A.H. and F. Mousa: Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher. IJCSNS, Vol. 9, May 2009,

[3] Eisenberg, M.: Hill ciphers and modular linear algebra. Mimeographed notes. University of Massachusetts. 1998.

[4] Ziedan, I.E., M.M. Fouad and D.H. Salem: "Application of data encryption standard (DES) to bitmap and JPEG images, ieeexplore. Proceedings of the 20th National Radio Science Conference, Mar. 18-20, 2003, pp: 1-8.

[5] Stindon, D.R.,: Cryptography Theory and Practice. 3rd Edn. Chapman and Hall/CRC, ISBN: 1584885084, 2006 pp: 593.

[6] Ismail, I.A., M. Amin and H. Diab,: How to repair the hill cipher. J. Zhejiang University. Science Academy, 7: 2022- 2030. DOI: 10.1631/jzus.2006.A2022

[7] Rangel-Romero, Y., G. Vega-García, A. Menchaca- Méndez, D. Acoltzi-Cervantes and L. Martínez- Ramos *et al*.: Comments on How to repair the Hill cipher. J. Zhejiang Univ. Sci. DOI: 10.1631/jzus.A072143

[8] Bibhudendra, A.,: Novel methods of generating self-invertible matrix for hill cipher algorithm. International Journal of Security, Volume 1: Issue (1), 2009 pp 4 21.

[9] Bibhudendra, A., K.P. Saroj, K.P. Sarat and P. Ganapati,: Image encryption using advanced hill cipher algorithm. International Journal in Recent Trends Eng., 2009, pp1: 663-667.

[10] Pour, D.R., M.R.M. Said, K.A.M. Atan and M. Othman: The new variable-length key Symmetric cryptosystem. Journal Mathematical Statics, DOI: 10.3844/jmssp,2009,pp24.312009.