IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 10-14
www.iosrjournals.org

A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem

Suman Chandrasekhar[1], Akash H.P [2] ,Adarsh.K[3], Mrs.Smitha Sasi[4]

[1]Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
[2] Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
[3]Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
[4]Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.

Abstract : *In the present era of Information Technology, Transmission of information in a secured manner is the primary concern of all agencies. Security is highly essential, as intruders are very keen to rob the information with all their might and intelligence. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. The objective of this paper is to encrypt a text using a technique different from the conventional Hill Cipher. The Advanced Hill Cipher uses an involutory matrix and permuted key. In this paper, we implement a second level of encryption using permutation approach, which makes the cipher highly secure. This encryption scheme is highly reliable as it uses tamper detection of the cipher text ensuring successful decryption of the cipher. All of these functions and transformations that are introduced ensure that this cipher is a very strong one and it cannot be broken by any cryptanalytic attack.*

Keywords - *Advanced Hill Cipher, Decryption, Encryption, Public Key Cryptosystem, Permuted key, and Tamper detection.*

I. INTRODUCTION

` Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth. Cryptographic algorithms are broadly divided into two categories namely Symmetric and Asymmetric key algorithms. In Symmetric scheme, a common key is shared between the sender and the receiver. Asymmetric schemes involve a pair of keys (both public, private) which are mathematically related. The Hill cipher is the first polygraph cipher, which has a few advantages in data encryption. However, it is vulnerable to known plaintext attack. Besides, an invertible key matrix is needed for decryption. It may become problematic since an invertible key matrix does not always exist. The Advanced Hill cipher algorithm uses an Involutory key matrix, Permuted key for encryption. The objective of this paper is to enhance the Advanced Hill Cipher algorithm by making the cipher more secure by further encrypting it and adding a tamper detection method, which ensures the original cipher, is received for intelligible decryption.

II. EXISTING SYSTEM

In the case of the classical Hill cipher, the basic equations governing the cipher are

$$C = KP \bmod 26 \qquad (1.1)$$

$$P = K^{-1}C \bmod 26 \qquad (1.2)$$

where P is the plaintext column vector, K the key matrix, C the cipher text, and is the modular arithmetic inverse of K. It may be noted here that we have to make use of the modular arithmetic inverse of the key matrix in the process of decryption.

In the Advanced Hill cipher, the basic equations governing the encryption and the decryption are given by

$$C = AP \bmod N, \qquad (1.3)$$

$$P = AC \bmod N. \qquad (1.4)$$

where A is an involutory matrix which includes the key matrix. Since A is an involutory matrix, we have A^{-1} = A, where A^{-1} is the modular arithmetic inverse of A. Thus in the case of this cipher, we need not compute the modular arithmetic inverse of A separately, once A is known to us.

In the present paper, our objective is to modify the Advanced Hill cipher and develop a enriched block cipher which includes an involutory matrix and a set of functions for creating confusion and diffusion, thus transforming the plaintext to a secure cipher.

III. Generation Of Involutory Matrix

(AA^{-1}) mod N = I, (2.1)

$AA^{-1} = A$, (2.2)

where A is a square matrix of size n,

From (2.1) and (2.2) we get

A^2 mod N = I, (2.3),

in which I is an identity matrix.

From (2.3), the matrix A can be obtained by representing it in the form

$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ (2.4)

and taking

$A_{11}=K$, where K is the key matrix.

The relations governing, A_{22}, A_{12} and A_{21} are given by

$A_{22} = -K$ (2.5)

$A_{12} = [d(I-K)]$ mod N, (2.6)

$A_{21} = [\lambda(I+K)]$ mod N (2.7)

where $(d\lambda)$ mod N =1. (2.8).

The cipher is developed by using the relations

$C = (AP + A_0)$ mod N, (2.9)

$P = (A(C - A_0))$ mod N (2.10)

here $A_0 = \begin{bmatrix} A_{22} & A_{21} \\ A_{12} & A_{11} \end{bmatrix}$ (2.11)

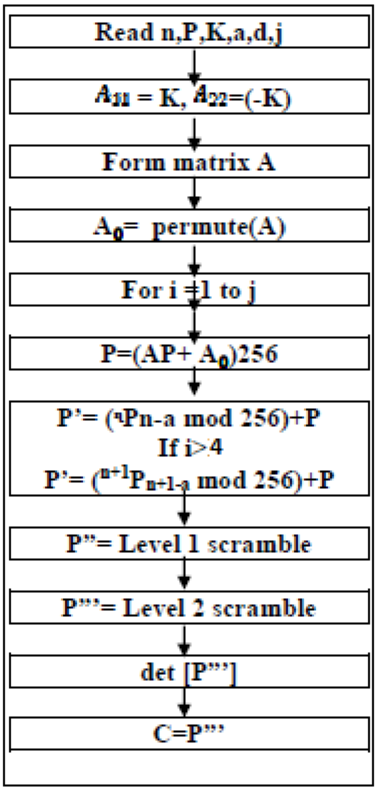
is obtained by permuting the sub matrices of A.

For a plaintext input, on using the involutory matrix, and (2.9), (2.10), (2.11), we get a 8x8 matrix.

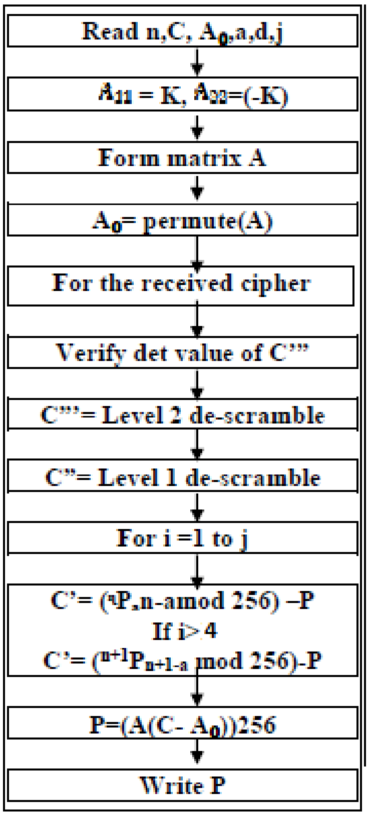
To the 8x8 matrix, we add the resulting value of the equation $P' = ({}^{n}P_{n-a} \bmod 256)+P$, to the first four rows of the matrix, and $P' = ({}^{n+1}P_{n+1-a} \bmod 256)+P$, to the bottom four rows of the 8x8 matrix, where 'n' is the randomly generated public key of receiver and 'a' is the private key. After the calculation of P', the 8x8 matrix is scrambled twice by two unique and distinct patterns for better diffusion of the contents to get P"'. Further, we calculate the determinant of the P"' matrix and represent it in a symbol and transmit it to the receiver. The receiver again calculates the determinant from the transmitted cipher and compares it with the symbol transmitted earlier.If a match is found, it ensures that no data has been tampered by the adversary and the user authentication is successfully carried out.

If there is a mismatch with the transmitted and the calculated value of determinant by the receiver, then the packet re-transmission request is sent.

III. FLOWCHARRT



ENCRYPTION PROCESS



DECRYPTION PROCESS

Algorithm for Encryption

```
1.      Read n,P,K,a,d,j
2.      $A_{11} = K, A_{22} =(-K)$
3.      $A_0$ = permute(A)
4.      $P=(AP+A_0)mod256$
5.      For i=1 to j
        {
          $P' = ({}^{n}P_{n-a} \bmod 256) +P$
          If i>4
              $P' = ({}^{n+1}P_{n+1-a} \bmod 256) +P$
   6.  .P"= Level 1 scramble
   7.   P"'= Level 2 scramble
   8.  det [P"'] calculated

   9. C=P"'
```

Algorithm for Decryption

```
        1. Read n,C,$A_0$,a,d,j
        2.  $A_{11} = K, A_{22} =(-K)$
3. $A_0$ = permute(A)
4. det [P"'] verified
     5. C"'= Level 2 de-scramble
6.C"= Level 1 de-scramble
7. For i=1 to j
 {
     $C' = ({}^{n}P_{n-a} \bmod 256)-P$
  If i>4
 $C' = ({}^{n+1}P_{n+1-a} \bmod 256)+P$
    }
```

```
8.P=(A(C-$A_0$))mod256
9.Write P
```

VI. ILLUSTRATION OF OUR METHOD.

Public key:
119

Enter the message:
It has more than 400,000 members in more than 160 countries, about 51.4% of whom reside in the United States.[2][3]

ENCRYPTION

Here, we consider a block of 64 alphanumeric characters per iteration from the message.

```
      Key matrix
123    25     9    67
134    17    20    11
48   199   209    75
39     55    85    92
```

```
                      Plain matrix:
  201   163    64   136    129  162    64     148
  150   153   133    64    163  136   129    149
    64   244   214   214    107  214   214    214
    64   148   133   148    130  133   153    162
    64   137   149     64    148  150   153    133
    64   163   136   129    149    64   241    246
  214     64   131   150    164  149   163    153
  137   133   162   107     64   129   130    150
```

```
Cipher text :
152   239   222   237     8      92     35     15
 22   119   217   187    64    189      0     93
 245     87   110     61   122   253     68     47
 181   212     72   112   223     64   161   198
  85   249     23     55     25     93     99   149
  177     56   127   217     99   167   254     59
  41   184   148   135     28   184     31     32
   96   241     55   111   154   122     83   240
```

Determinant value:
2

Determinant symbol:
>

DECRYPTION

```
Received matrix:
  152   239   222   237     8    92    35    15
    22   119   217   187    64   189     0    93
  245     87   110     61   122   253    68    47
  181   212     72   112   223     64   161   198
    85   249     23     55     25     93     99   149
  177     56   127   217     99   167   254     59
    41   184   148   135     28   184     31     32
    96   241     55   111   154   122     83   240
```

```
Received determinant symbol:
>
Determinant value:
2

SUCCESS
Final output matrix:
   201  163   64  136  129  162   64   148
   150  153  133   64  163  136  129  149
    64  244  214  214 107  214  214  214
    64  148  133  148 130  133  153  162
    64  137  149   64  148  150  153  133
    64  163  136  129 149   64  241   246
   214   64  131  150 164  149  163  153
   137  133  162  107   64  129  130   150
```

IV. CONCLUSION

In this paper, we have proposed a novel Asymmetric block cipher technique using EBCDIC to represent the plaintext. The computations are carried out by writing the programs for encryption and decryption in Matlab.The cryptanalysis carried out in [1], ensures us that the cipher is indeed a strong one.

In addition to this, our second level of encryption is based upon a random value of public key associated with a modular arithmetic function. Also, the cipher is scrambled twice by two unique and different patterns before transmission to ensure higher randomness.

Another highlight of this paper is the use of symbols to represent the determinant which in turn performs user authentication and detection of tampered cipher text.

Thus, with all the above techniques implemented, we justify that the cipher is highly robust and secure. To date, we have modelled our technique for the encryption and decryption of alphanumeric text as input.

Further, it can be implemented for image and video encryption and decryption .And also in steganography applications involving encryption and decryption

REFERENCES

[1] A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation, V.U.K.Sastry, Aruna Varanasi and S.Udaya Kumar *Journal of Global Research in Computer Science,* Volume 2, No. 4, April 2011

[2] A Modern Advanced Hill Cipher Involving XOR Operation and Permuted Key,A Research paper by V.U.K.Sastry, Aruna Varanasi and S.Udaya Kumar Journal of Global Research in Computer Science, Volume 2, No. *4, April 2011*

[3] Advanced Hill Cipher Involving a Pair of Keys, V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar," International Journal of Computational Intelligence and Information Security, Vol.2 No.1, pp 100-108, January2011

[4] A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes, 1A.F.A. Abidin, 1O.Y. Chuan and 2M.R.K. Ariffin, Journal of Computer Science 7 (5): 785-789, 2011ISSN 1549-3636© 2011 Science Publications[5]A Modified Hill Cipher Involving Interweaving and Iteration. V. Umakanta Sastry, N. Ravi Shankar, and S Durga Bhavani, International Journal of Network Security, Vol.11, No.1,2010.

[5] A Modified Hill Cipher Involving Interweaving and Iteration. V. Umakanta Sastry, N. Ravi Shankar, and S Durga Bhavani, International Journal of Network Security, Vol.11, No.1,2010.

[6] Public key cryptosystem and a key exchange protocol using tools of non-abelian group, Dr. H.K. Pathak et. al./ International Journal on Computer Science and Engineering Vol. 02, No. 04, 2010, 1029-1033

[7] A New Knapsack Public-Key Cryptosystem Based on Permutation Combination Algorithm, Min-Shiang-Hwang, Cheng-Chi Lee, and Shiang-Feng Tzeng, World Academy of Science, Engineering and Technology 33 2009

[8] Recommendation for Cryptographic Key Generation,NIST Special Publication,July 2011.

[9] Advanced Hill Cipher Involving Permutation and Iteration", V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar International Journal of Advanced Research in Computer Science, Vol.1, No.4, pp. 141- 145, Nov-Dec. 2010.

[10] Image Encryption Using Advanced Hill CipherAlgorithm, Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, ACEEE International Journal on Signal and Image Processing Vol 1, No. 1, Jan 2010

[11] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, *International Journal of Security*, Vol 1, Issue 1, 2007, pp. 14-21.

[12] Cryptography and Network Security by William Stallings , Fourth Edition,