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

Suman Chandrasekhar\textsuperscript{1}, Akash H.P\textsuperscript{2}, Adarsh.K\textsuperscript{3}, Mrs.Smitha Sasi\textsuperscript{4}

\textsuperscript{1}Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
\textsuperscript{2}Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
\textsuperscript{3}Department of Telecommunication Engineering, Dayananda Sagar College of Engineering Bangalore, Karnataka, India.
\textsuperscript{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

\begin{align}
C &= KP \mod 26 \quad (1.1) \\
P &= K^{-1}C \mod 26 \quad (1.2)
\end{align}

where P is the plaintext column vector, K the key matrix, C the cipher text, and \( K^{-1} \) 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

\begin{align}
C &= AP \mod N, \quad (1.3) \\
P &= AC \mod N \quad (1.4)
\end{align}

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

III. Generation Of Involutory Matrix

\[(AA^{-1}) \mod N = I, \quad (2.1)\]
\[AA^{-1} = A, \quad (2.2)\]

where \( A \) is a square matrix of size \( n \),

From (2.1) and (2.2) we get
\[A^2 \mod N = I, \quad (2.3)\]
in which \( I \) is an identity matrix.

From (2.3), the matrix \( A \) can be obtained by representing it in the form
\[A = [\begin{array}{cc} A_{11} & A_{12} \\ A_{21} & A_{22} \end{array}] \quad (2.4)\]
and taking
\[A_{11} = K, \quad \text{where } K \text{ is the key matrix.}\]

The relations governing, \( A_{22}, A_{12} \text{ and } A_{21} \) are given by
\[A_{22} = -K \quad (2.5)\]
\[A_{12} = [d(I - K)] \mod N, \quad (2.6)\]
\[A_{21} = [\lambda(I + K)] \mod N \quad (2.7)\]

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

The cipher is developed by using the relations
\[C = (AP + A_0) \mod N, \quad (2.9)\]
\[P = (A(C - A_0)) \mod N \quad (2.10)\]

where \( A_0 = [\begin{array}{cc} A_{22} & A_{11} \\ A_{12} & A_{11} \end{array}] \quad (2.11)\)
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 \( P' = (nP_{n+a} \mod 256) + P \) to the first four rows of the matrix, and \( P' = (nP_{n+1} \mod 256) + P \), 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. FLOWCHART

Algorithm for Encryption
1. Read n,P,K,a,d,j
2. $A_{11} = K, A_{22} = (-K)$
3. $A_0 = \text{permute}(A)$
4. $P = (AP + A_0) \mod 256$
5. For i=1 to j
   { 
     $P' = (nP_{n,a} \mod 256) + P$
     If i>4 
     $P' = (n+1P_{n+1,a} \mod 256) + P$
   }
6. $P'' = \text{Level 1 scramble}$
7. $P''' = \text{Level 2 scramble}$
8. \text{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. $A_0 = \text{permute}(A)$
4. \text{det} [P'''] verified
5. $C''' = \text{Level 2 de-scramble}$
6. $C'' = \text{Level 1 de-scramble}$
7. For i=1 to j
   { 
     $C' = (nP_{n,a} \mod 256) - P$
     If i>4 
     $C' = (n+1P_{n+1,a} \mod 256) - P$
   }
8. $P = (A(C - A_0) \mod 256)$
9. Write P
A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem

8. \( P = (A - A_0) \mod 256 \)
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]

ENCRIPTION

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

Key matrix
\[
\begin{bmatrix}
123 & 25 & 9 & 67 \\
134 & 17 & 20 & 11 \\
48 & 199 & 209 & 75 \\
39 & 55 & 85 & 92 
\end{bmatrix}
\]

Plain matrix:
\[
\begin{bmatrix}
201 & 163 & 64 & 136 & 129 & 162 & 64 & 148 \\
150 & 133 & 64 & 163 & 136 & 129 & 149 \\
64 & 244 & 214 & 214 & 107 & 214 & 214 & 214 \\
64 & 148 & 133 & 148 & 130 & 133 & 153 & 162 \\
64 & 137 & 149 & 64 & 148 & 150 & 153 & 133 \\
64 & 163 & 136 & 129 & 149 & 64 & 241 & 246 \\
214 & 64 & 131 & 150 & 164 & 149 & 163 & 153 \\
137 & 133 & 162 & 107 & 64 & 129 & 130 & 150 
\end{bmatrix}
\]

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

Determinant value:
2

Determinant symbol:
>

DECRYPTION

Received matrix:
\[
\begin{bmatrix}
152 & 239 & 222 & 237 & 8 & 92 & 35 & 15 \\
22 & 119 & 217 & 187 & 64 & 189 & 0 & 93 \\
245 & 87 & 110 & 61 & 122 & 253 & 68 & 47 \\
181 & 212 & 72 & 112 & 223 & 64 & 161 & 198 \\
85 & 249 & 23 & 55 & 25 & 93 & 99 & 149 \\
177 & 56 & 127 & 217 & 99 & 167 & 254 & 59 \\
41 & 184 & 148 & 135 & 28 & 184 & 31 & 32 \\
96 & 241 & 55 & 111 & 154 & 122 & 83 & 240 
\end{bmatrix}
\]
A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem

Received determinant symbol: 
> Determinant value: 2

SUCCESS

Final output matrix:

\[
\begin{bmatrix}
201 & 163 & 136 & 129 & 162 & 64 & 148 \\
150 & 153 & 133 & 64 & 163 & 136 & 129 & 149 \\
64 & 244 & 214 & 107 & 214 & 214 & 214 & 214 \\
64 & 148 & 133 & 148 & 130 & 133 & 153 & 162 \\
64 & 137 & 149 & 64 & 148 & 150 & 153 & 133 \\
64 & 163 & 136 & 129 & 149 & 64 & 241 & 246 \\
214 & 64 & 131 & 150 & 164 & 149 & 163 & 153 \\
137 & 133 & 162 & 107 & 64 & 129 & 130 & 150 \\
\end{bmatrix}
\]

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