Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 5s (2024)

Some Results of Data Encryption and Decryption using Euler's Totient Function

Gobburi Rekha[1], V. Srinivas[2]
1 Department of Humanities and Sciences, Malla Reddy College of Engineering and Technology
[2] Department of Mathematics, Osmania university

Article History:

Received: *10-05-2024*

Revised: *20-06-2024*

Accepted: *02-07-2024*

Abstract:

In this paper, we discuss about the Hill Cipher cryptosystem, the RSA public-key cryptosystem, developed by Rivest, Shamir, Adleman for text encoding and decoding. To encrypt and decrypt the message, we use the Euler Phi-function, congruences, and matrix multiplication. Further, we employ two keys for coding and decoding.

Introduction: In present, computer networks, internet and mobile communications are important and inevitable part of our society and security of information from hackers is a big task. One of the most widely used applications for information security is Cryptography. Usually in Hill cipher there are two keys, of which one acts as encryption key and the other one acts as decryption key. In this paper we discuss about Hill Cipher using only one key for data encryption and data decryption. Further, we extend our result with dual encryption and decryption process which is explained by using the RSA public key cryptosystem and Hill Cipher and they together execute a powerful cryptosystem to secure the data.

Objectives: The purpose of this paper is to obtain and compare the result of data encryption and data decryption using:

- A matrix which is invertible.
- A matrix which is Involutory.
- An RSA cryptosystem which is applied for Hill Cipher where the matrix is Involutory.

Methods: Using Hill Cipher and thereafter Hill Cipher - RSA together we have encrypted and decrypted the data under modulo 255.

Results: The text message is converted to coded message and then original message is retrieved by using the three different techniques.

Conclusions: As the paper involves two stages of encryption and decryption where public key and private key which are unthinkable by the third parities, the security of information is highly appreciable.

Keywords: Cryptography, Congruence, Euler-Phi function, Hill Cipher, RSA cryptosystem and matrix, ASCII code.

1. Introduction

In present, computer networks, internet and mobile communications are important and inevitable part of our society and security of information from hackers is a big task. One of the most widely used applications for information security is Cryptography. Usually in Hill cipher there are two keys, of which one acts as encryption key and the other one acts as decryption key. In this paper we discuss about Hill Cipher using only one key for data encryption and data decryption. Further, we extend our paper with dual encryption and decryption process which is explained using the RSA public key cryptosystem and Hill Cipher cryptosystem which together execute a powerful cryptosystem technique to secure the data. This paper extends the result of [1] by using involutory matrix for RSA cryptosystem.

2. Standard Definitions

Plain Text: The message which is to be converted for the purpose of security.

Cipher Text: The message which is in unreadable language.

Encryption: Encryption is a form of data security in which information is converted to ciphertext.

Decryption: Decryption is the process of converting encrypted data into recognizable information.

Hill Cipher: Invented by Lester S. Hill which is a polygrahic substitution cipher based on linear algebra.

Involutory Matrix: Any square matrix, A which satisfies the condition $A^2 = I$.

Linear Congruence: A linear congruence is a congruence relation of the form ax ≡ b (mod m) where a, b, m $\in Z^+$ and m > 0. A solution is an integer x which makes the congruence relation true and x is a least residue (mod m) (that is, 0 ≤ x ≤ m−1).

RSA: The Rivest-Shamir-Adleman (RSA) encryption algorithm is an asymmetric encryption algorithm. Asymmetric encryption uses a key pair that is linked to encrypt and decrypt data. A public key is generated and made available to everybody, while the private key is kept confidential and known only to the person who generated the key pair.

Euler -Phi function: Euler’s phi (or totient) function of a positive integer *n* is the number of integers in {1,2, 3..., n} which are relatively prime to *n* which is denoted $\emptyset(n)$.

Let n be the product of two individual primes p and q.

Let us define K = (n,p,q,e,d):ed≡1(mod($\emptyset(n)$)).

We define $e_k(x) \equiv x^e (\text{mod } n)$ and $d_k(y) \equiv y^e (\text{mod } n)$ where p, q and d are used as public keys.

3. Methods

In this we discuss three different methods for encryption and decryption of the data.

Method I: Using Invertible matrix

- Let us consider nxn invertible matrix say A in which the matrix A acts as an encryption key and its inverse acts as a decryption key.
- Convert the original plain text into numbers using the ASCII values and arrange the numbers in matrix form say P.
- Let E≡AP (mod 255).
- Now, on converting the numbers in the matrix E into alphabets and symbols we get the encrypted message which is to be sent.

- To decode the message which is sent by the sender, let us convert the alphabets and symbols in the matrix E into numbers.
- Let D ≡ $A^{-1}E$ (mod 255), we get the original plaintext.

Method II: Using Involutory matrix

- Now we shall continue the explanation of encrypting and decrypting the data by using an involutory matrix where we use only one key for encryption and the same key for decryption.
- Let us consider a nxn involutory matrix say A which acts as an encryption and decryption key.
- Convert the plaintext in numbers using the latest ASCII values and arrange the numbers in matrix form say P.
- Let E = AP, adjusting the values under modulo 255 we get the encrypted message.
- Hence, after converting the numbers in E into symbols under the ASCII values, we get the Cipher text.
- To decode the message let us write E in matrix form and multiply by the key A.
- Let D = AE. Since, A is an involutory matrix where $A^2 = I$ which can also be written as $A = A^{-1}$.
- Now, adjusting the values of D under modulo 255 we can retrieve the original text.

Method III: Dual encryption and decryption of data using Euler's totient function in Hill cipher

- Let us consider a nxn involutory matrix say A such that $A^2 = I$
- Convert the plaintext in numbers using the latest ASCII values and arrange the numbers in matrix form say P.
- Let E = AP, adjusting the values under modulo 255 which gives the first stage of encryption.
- For further safety purpose let us encrypt E using RSA cryptosystem we define $e_k(x) \equiv x^e (\text{mod } n)$.
- To decrypt the message using RSA cryptosystem we define $d_k(y) \equiv y^e (\text{mod } n)$ which gives the first stage of decryption.
- Arrange the above decrypted codes in the form a matrix say M and multiply by A^{-1} we get D.
- On adjusting the values of D under modulo 255 we can retrieve the original text.

4. Results

To see how the methodology works, let us consider the following illustrations.

Illustration I: Let the plaintext to be sent to the receiver by the sender is **"Estimation".**

Using the ASCII values convert the alphabets into numbers "=34, E = 69, s = 115, t = 116, i = 105, m = 109, a =97, t = 116, i = 105, o = 111, n = 110 and" = 34.

Encryption:

Let P = $\begin{bmatrix} 34 & 69 & 115 & 116 \\ 105 & 109 & 97 & 116 \\ 105 & 111 & 110 & 34 \end{bmatrix}$.

Let A = $\begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{bmatrix}$ be an invertible matrix.

Therefore, $A^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{bmatrix}$.

Let E = AP.

E = $\begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{bmatrix}\begin{bmatrix} 34 & 69 & 115 & 116 \\ 105 & 109 & 97 & 116 \\ 105 & 111 & 110 & 34 \end{bmatrix}$.

E $\equiv \begin{bmatrix} -71 & -42 & 5 & 82 \\ -71 & -40 & 18 & 0 \\ -34 & -71 & -128 & -34 \end{bmatrix}$ (mod 255).

E =AP = $\begin{bmatrix} 184 & 213 & 5 & 82 \\ 184 & 215 & 18 & 0 \\ 221 & 184 & 127 & 221 \end{bmatrix}$.

On converting the numbers in matrix E into symbols we get **¸ÕENQR¸×DC2 NULÝ¸DELÝ** which acts as the cipher text.

Decryption:

Let the cipher text be transformed into numbers under the ASCII values.

Let E = $\begin{bmatrix} 184 & 213 & 5 & 82 \\ 184 & 215 & 18 & 0 \\ 221 & 184 & 127 & 221 \end{bmatrix}$.

Now let D = A^{-1}E.

D = $\begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{bmatrix}\begin{bmatrix} 184 & 213 & 5 & 82 \\ 184 & 215 & 18 & 0 \\ 221 & 184 & 127 & 221 \end{bmatrix}$.

D $\equiv \begin{bmatrix} -221 & -186 & -140 & -139 \\ -405 & -401 & -158 & -139 \\ -405 & -399 & -145 & -221 \end{bmatrix}$ (mod 255).

D = $\begin{bmatrix} 34 & 69 & 115 & 116 \\ 105 & 109 & 97 & 116 \\ 105 & 111 & 110 & 34 \end{bmatrix}$.

The matrix D is same as that of matrix P.

Therefore, on converting the numbers of matrix D into alphabets we get the message as **"Estimation".**

Illustration 2:

Let the message to be sent is **"Taste of life"** using the ASCII values covert the alphabets into numbers as "= 34, T = 84, a = 97, s = 115, t = 116, e = 101, space = 32, o = 111, f = 102,

space = 32, l = 108, I = 105, f = 102, e = 101 and"=34.

Encryption:

Let P = $\begin{bmatrix} 34 & 84 & 97 & 115 & 116 \\ 101 & 32 & 111 & 102 & 32 \\ 108 & 105 & 102 & 101 & 34 \end{bmatrix}$

Let A = $\begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix}$ be an involutory matrix such that $A^2 = I$.

$A^2 = \begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix}\begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Therefore E = AD

E = $\begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix}\begin{bmatrix} 34 & 84 & 97 & 115 & 116 \\ 101 & 32 & 111 & 102 & 32 \\ 108 & 105 & 102 & 101 & 34 \end{bmatrix}$

E = $\begin{bmatrix} -978 & -676 & -1373 & -1391 & -836 \\ 607 & 412 & 846 & 855 & 508 \\ 128 & 43 & 217 & 218 & 146 \end{bmatrix}$.

Adjusting the values under modulo 255.

E ≡ $\begin{bmatrix} -978 & -676 & -1373 & -1391 & -836 \\ 607 & 412 & 846 & 855 & 508 \\ 128 & 43 & 217 & 218 & 146 \end{bmatrix}$ (under mod 255).

We get E = $\begin{bmatrix} 42 & 89 & 157 & 139 & 184 \\ 97 & 157 & 81 & 90 & 253 \\ 128 & 43 & 217 & 218 & 146 \end{bmatrix}$.

On converting the numbers in E into alphabets we get ***Y□‹¸a□QZý€+ÙÚ'**

Which acts as Cipher text.

Decryption:

Let the cipher text be transformed again into numbers under the ASCII values.

Let E = $\begin{bmatrix} 42 & 89 & 157 & 139 & 184 \\ 97 & 157 & 81 & 90 & 253 \\ 128 & 43 & 217 & 218 & 146 \end{bmatrix}$.

Now let D = AE.

D = $\begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix}\begin{bmatrix} 42 & 89 & 157 & 139 & 184 \\ 97 & 157 & 81 & 90 & 253 \\ 128 & 43 & 217 & 218 & 146 \end{bmatrix}$.

D ≡ $\begin{bmatrix} -986 & -1701 & -1433 & -1415 & -2944 \\ 611 & 1052 & 876 & 867 & 1817 \\ 108 & 360 & 102 & 101 & 544 \end{bmatrix}$ (under mod 255).

D = $\begin{bmatrix} 34 & 84 & 97 & 115 & 116 \\ 101 & 32 & 111 & 102 & 32 \\ 108 & 105 & 102 & 101 & 34 \end{bmatrix}$.

On converting the numbers of matrix D into alphabets we get the message as **"Taste of life".**

Illustration3:

We continue the result by applying hill cipher and RSA cryptosystem simultaneously. Now let us discuss the illustration which includes dual encryption and decryption of involutory matrix using Euler Totient function.

Step 1: Let A be a square matrix of order 3x3 which is an involutory matrix.

Let A = $\begin{bmatrix} 4 & 3 & 3 \\ -1 & 0 & -1 \\ -4 & -4 & -3 \end{bmatrix}$ then $A^2 = \begin{bmatrix} 4 & 3 & 3 \\ -1 & 0 & -1 \\ -4 & -4 & -3 \end{bmatrix}\begin{bmatrix} 4 & 3 & 3 \\ -1 & 0 & -1 \\ -4 & -4 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Step 2: Transform each plaintext into a column vector B by taking the ASCII values.

Let us consider the message to be encrypted as **Now or Never.**

P = 78 111 119 32 111 114 32 78 101 118 101 114 which is written in matrix form as

P = $\begin{bmatrix} 78 & 111 & 119 & 32 \\ 111 & 114 & 32 & 78 \\ 101 & 118 & 101 & 114 \end{bmatrix}$.

1^{st} stage of encryption

Step 3: To encrypt the message, multiply the plaintext matrix P by matrix A to form the matrix

E = [AP] (modulo 255).

E = AP = $\begin{bmatrix} 4 & 3 & 3 \\ -1 & 0 & -1 \\ -4 & -4 & -3 \end{bmatrix}\begin{bmatrix} 78 & 111 & 119 & 32 \\ 111 & 114 & 32 & 78 \\ 101 & 118 & 101 & 114 \end{bmatrix}$.

E ≡ $\begin{bmatrix} 948 & 1140 & 875 & 704 \\ -179 & -229 & -220 & -146 \\ -1059 & -1254 & -907 & -782 \end{bmatrix}$ (mod 255).

E = $\begin{bmatrix} 183 & 120 & 110 & 194 \\ 76 & 26 & 35 & 109 \\ 216 & 21 & 113 & 238 \end{bmatrix}$.

Step 4: For further safety we will code the cipher text E into another text with the help of Euler -Phi function:

E = $\begin{bmatrix} 183 & 120 & 110 & 194 \\ 76 & 26 & 35 & 109 \\ 216 & 21 & 113 & 238 \end{bmatrix}$.

2^{nd} stage of encryption

Now we use RSA encoding system in the matrix E

E= (183 120 110 194 76 26 35 109 216 21 113 238).

For further safety let us consider three primes where N = P *Q* R

Let P = 11, Q = 13, R= 17 where N = 2431

Therefore, $\emptyset(\mathrm{N}) = (\mathrm{P}-1) * (\mathrm{Q}-1) * (\mathrm{R}-1)$.

= 10.12.16 =1920.

≡1921 = 113*17.

Assume the enciphering proponent to be k then the recapture element the individual integer j fulfilling the congruence kj $\equiv 1 \bmod (\emptyset(\mathrm{N})$.

Here k = 113 and j = 17

To code N we require each part of N to be an integer less than 2431

Let us find encrypted value for the first element

$183 \equiv 183 \bmod 2431$

$183^4 \equiv 443 \bmod 2431$

$183^8 \equiv 1769 \bmod 2431$

$183^{16} \equiv 664 \bmod 243$

$183^{32} \equiv 885 \bmod 2431$

$183^{64} \equiv 443 \bmod 2431$

Therefore,$183^{113} \equiv 1509 \bmod 2431.$

Now, we find for

$120 \equiv 120 \bmod 2431$

$120^4 \equiv 562 \bmod 2431$

$120^8 \equiv 2245 \bmod 2431$

$120^{16} \equiv 562 \bmod 2431$

$120^{32} \equiv 2245 \bmod 2431$

$120^{64} \equiv 562 \bmod 2431$

Therefore, $120^{113} \equiv 1803 \bmod 2431.$

Similarly, we get the remaining elements as

$110^{113} \equiv 1419 \bmod 2431$

$194^{113} \equiv 1520 \bmod 2431$

$76^{113} \equiv 1385 \bmod 2431$

$26^{113} \equiv 1131 \bmod 2431$

$35^{113} \equiv 2109 \bmod 2431$

$109^{113} \equiv 109 \bmod 2431$

$216^{113} \equiv 1542 \bmod 2431$

$21^{113} \equiv 21 \bmod 2431$

$113^{113} \equiv 1303 \bmod 2431$

$238^{113} \equiv 816 \bmod 2431.$

Therefore, the total coded message sent by the sender is:

(1509 1803 1419 1520 1385 1131 2109 109 1542 21 1303 816).

To decode the coded message the receiver uses RSA cryptosystem.

Step 5: Now we will decode the message by using recapture element j = 17.

1st stage of decryption

Now, let us decode the coded values

First, we find

$1509 \equiv 1509 \bmod 2431$

$1509^2 \equiv 1665 \bmod 2431$

$1509^3 \equiv 1262 \bmod 2431$

$1509^4 \equiv 885 \bmod 2431$

$1509^5 \equiv 846 \bmod 2431$

Therefore, $1509^{17} \equiv 183 \bmod 2431$.

$1803 \equiv 1803 \bmod 2431$

$1803^2 \equiv 562 \bmod 2431$

$1803^3 \equiv 1990 \bmod 2431$

$1803^4 \equiv 2245 \bmod 2431$

$1803^5 \equiv 120 \bmod 2431$

Therefore, $1803^{17} \equiv 120 \bmod 2431$.

Similarly, we get the remaining elements as

$1419^{17} \equiv 110 \bmod 2431$

$1520^{17} \equiv 194 \bmod 2431$

$1385^{17} \equiv 76 \bmod 2431$

$1131^{17} \equiv 26 \bmod 2431$

$2109^{17} \equiv 35 \bmod 2431$

$109^{17} \equiv 109 \bmod 2431$

$1542^{17} \equiv 216 \bmod 2431$

$21^{17} \equiv 21 \bmod 2431$

$1303^{17} \equiv 113 \bmod 2431$

$816^{17} \equiv 238 \bmod 2431$

Now the decoded message after introducing RSA is

M = ($183\ \ 120\ \ 110\ \ 194\ \ 76\ \ 26\ \ 35\ \ 109\ \ 216\ \ 21\ \ 113\ \ 238$).

Step 6: Now, we shall apply the hill cipher cryptosystem for M which is obtained in step 5.

2^{nd} stage of decryption

Let us write M in the form a matrix.

M = $\begin{bmatrix} 183 & 120 & 110 & 194 \\ 76 & 26 & 35 & 109 \\ 216 & 21 & 113 & 238 \end{bmatrix}$.

Now we can recapture the text by using inverse matrix $D = A^{-1}M$

D = $\begin{bmatrix} 4 & 3 & 3 \\ -1 & 0 & -1 \\ -4 & -4 & -3 \end{bmatrix}\begin{bmatrix} 183 & 120 & 110 & 194 \\ 76 & 26 & 35 & 109 \\ 216 & 21 & 113 & 238 \end{bmatrix}$.

$\equiv \begin{bmatrix} 1608 & 621 & 884 & 1817 \\ -399 & -141 & -223 & -432 \\ -1684 & -647 & -919 & -1926 \end{bmatrix}$ (mod 255).

= $\begin{bmatrix} 78 & 111 & 119 & 32 \\ 111 & 114 & 32 & 78 \\ 101 & 118 & 101 & 114 \end{bmatrix}$ which is equal to matrix P.

Hence, the total decoded message is P = (28 14 15 23 27 15 18 27 14 5 22 5 18 29 27 27) retrieved as **Now or Never.**

5. Conclusion

The present paper involves three different methods to encrypt and decrypt the message where the first two methods involved Hill cipher using invertible matrix and involutory matrix. Whereas, the third method involves two stages of encryption and decryption where public key and private key which are untraceable by the third parities, as it is involves large prime numbers which provides security of information.

References

[1] Mohiuddin Ahmed and Md. Ashik Iqbal, (2020). International Journal of Material and Mathematical Sciences, 2(6), 99-103, 2020.

[2] Rao, GAV Rama Chandra, P.V. Lakshmi and N. Ravi Shankar. “A New Modular Multiplication Method in Public Key Cryptosystem.” International Journal of network Security15.1(2013):23-27.

[3] Rao, GAV Rama Chandra, P.V. Lakshmi and N. Ravi Shankar. “A Novel Modular Multiplication Algorithm and its application to RSA Decryption”, IJCSI International Journal of Computer Science Issues, Vol.9, Issue 6, No 3, November 2012.

[4] B. Persis Urbana Ivy, Purushotam Mandiwa, Mukesh Kumar, (2012). International Journal of Engineering and Computer Science ISSN:2319-7242 Vol1 Issue2 Nov 2012 Page No.63-66.

[5] Adhikari M.R and Avishek Adhikari, (2007). Introduction to linear algebra with application to basic cryptography, (New Delhi 2007).

[6] Koblitz N. (1998). Algebraic Aspects of Cryptography, Springer.

[7] Cohen H. (1994). A course in computational Algebraic Number theory, Springer.

[8] Lester, S.H (1992). Cryptography in an algebraic alphabet. The American mathematical monthly,36:306-312.

[9] Rivest R., Adleman L.M and Shamir A. (1978). A method for obtaining digital signature and public key cryptosystems (Comm. Of ACM21(1978)120-126).