

Improved Asymmetric Key Encryption Algorithm Using MATLAB

K.Sony¹, Desowja Shaik¹, B.Divya Sri², G.Anitha³

¹Assistant Professor, K L University, Vaddeswaram, Guntur District, AP

^{2,3,4}ECE Department, K L University, Vaddeswaram, Guntur District, AP

Abstract: In this paper, A new technique is deployed to improve Asymmetric Key Encryption Technique with multiple keys and Chinese remainder theorem(CRT) .The main aim of this Technique is to provide secure transmission of data between any networks through a channel. The Scope of this paper deals with Multiple Public and Private keys and its computation time. RSA algorithm is used to utilize asymmetric key encryption technique .In proposed model RSA will be implemented using MATLAB with original RSA Algorithm ,Proposed RSA Algorithm and RSA using Chinese Remainder Theorem(CRT). The Computational time and its mere effects are briefly dealt by varying the multiple number of keys .

Keywords: RSA, Multiple key, Chinese Remainder Theorem (CRT), Secure, MATLAB.

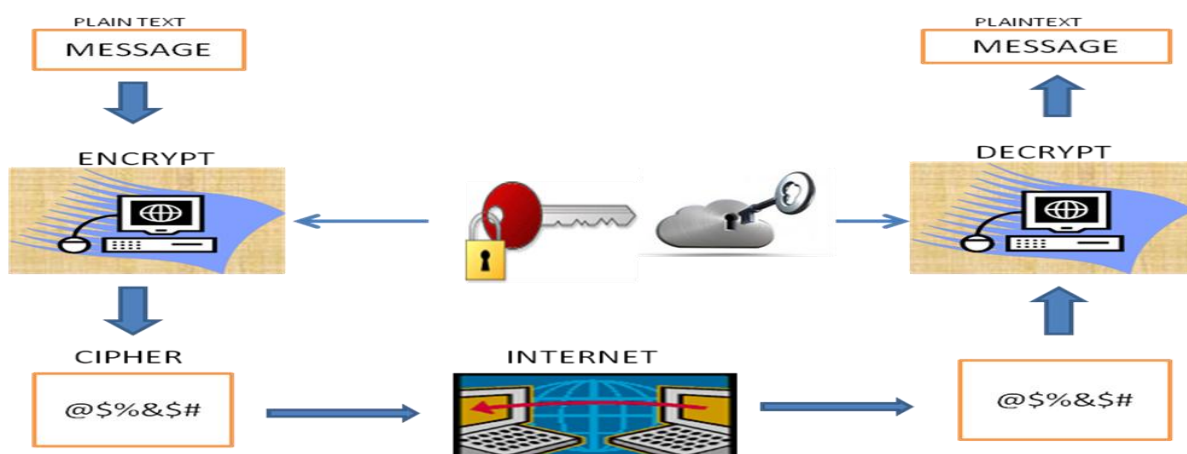
I. Introduction

In Communications regardless of the platform such as email, Voice messages or direct messages the end users ultimate motive is to send or receive the information without any intervention from the intruder. So a mechanism is to be deployed such that only the users should understand the information and for others it should be in the unreadable format .The process of encoding the plain text messages into cipher text is referred as Encryption and the reverse transforming process is decryption. In a Computer to Computer communications, the sender usually does the encryption and at the receiving end the decryption is done[1] .

Every encryption and decryption process has two primarily goals : Algorithm and the key generation .

Algorithm is made public to all the users an it's the key which makes the communication secure between the user domain. If the same key is used at both the ends then it is referred as Symmetric Key Cryptography and if different keys(Public and private key) are used at both the ends its Asymmetric key Cryptography[16]. The above mentioned process is depicted in the figure.

In this paper we deal about the Asymmetric key cryptography[3] since it overcomes the disadvantages of symmetric key cryptography such as key exchange and also digital signature can be deployed using this technique .It also deals about doing the encryption and decryption using two keys at both the ends so that the information can be sent more securely using the Modified RSA Algorithm and with Chinese Remainder Theorem .



II. RSA Crypto System

The RSA Algorithm was developed by Ron Rivest, Adi Shamir and Leonard in 1978[17]. The original RSA algorithm follows 4 phases: Key Generation, Encryption, Decryption and Digital signature [9].

Keygeneration

In key generation we typically need keys that are public and private keys. We will generate public and private key using below steps [2]. Public key is visible to both sender and receiver, where as private key is kept secret and is generated and made invisible to the end user. Public key is used during encryption process where as private key is used during decryption process. The steps to find out public and private key in key generation is given below.

- 1). Select two random prime numbers: r, s and find $n=r*s$.
- 2). Compute the value of $\phi(n)=(r-1)*(s-1)$
- 3). Select a random integer e[12], such that $1<e<n$ and $\gcd(e, \phi(n))=1$.
- 4). Compute value of d, such that $d*e \equiv 1 \pmod{n}$.
- 5). Public Key {e, n}, Private key {d, n}

Encryption

We generated public and private keys using Key generation. Now, we have to encrypt the message using Public key. The process is dealt as given below

- 1). Take the message which represents Plain text. The Plain text should be encrypted using public key e. If a sender wants to transmit the information to receiver, the receiver should send the public key to the sender, and then the sender will encrypt the message(M) with a Public key(e).
- 2). Now calculate the cipher text (C) by using given formula.

$$C=M^e \pmod{n}$$

Decryption

In decryption we will find out decrypted message(M) by using cipher text(C) and Private key(d). Then Compare if the original message is equal to decrypted message[5]. If it is equal then algorithm is proven .

$$M=C^d \pmod{n}$$

Digital Signature

In order to find whether the process we followed in designing the algorithm is accurate or not we use the concept of digital signature[6]. Here we will find signature(s) using private key(d) and H(m). And we will find verification m'' using signature(s) and public key(e) where H is the hash function. If $m''=H(m)$ then our signature is correct[7]. The following formula are given below:

$$s = (H(m)^d) \pmod{n}$$
$$m'' = (s^e) \pmod{n}$$

2.1 Modified RSA Algorithm Using Multiple Keys

Here in Modified RSA algorithm we will generate multiple public and private keys. In modified RSA algorithm the computational time is more due to multiple keys but security is more compared to original RSA algorithm[10]. In modified RSA algorithm we are using two public and private keys it is less subjected to brute force attack. Here in this we are having 3 phases are: key generation, encryption, decryption[14].

Key Generation In Modified RSA Algorithm

In key generation process we will generate multiple public and private keys using below steps. Here in order to increase security we are generating multiple keys. Here public keys are visible to both sender and receiver. And private keys are kept secret and. The following steps for key generation process in given below:

- 1). Select two set random numbers say p, q and r, s.
- 2). Find the value of n, z i.e., $n=p*q$, $z=r*s$
- 3). Compute the value of $\phi(n)=(p-1)*(q-1)$, $k(z)=(r-1)*(s-1)$.
- 4). Select a random integer e, g such that $1<e<n$, $1<g<z$ and $\gcd(e, \phi(n))=1$ $\gcd(e, k(z))=1$
- 5). Compute value of d, T such that $d*e \equiv 1 \pmod{n}$ and $t*g \equiv 1 \pmod{z}$
- 6). Public Key {e, g, n, z}, Private key {d, t, n, z}

Encryption

We have generated multiple public and private key in above key generation. Now we will encrypt using public keys. Since we will do two times encryption such a way reliability will be more compared to that

of original RSA algorithm. We take message(M) and first public key(e) during encryption and find out $C1=M^e \text{ mod}(n)$. By using c1 and second public key(g) we will find cipher text in encryption process.

$$C=C1^g \text{ mod}(z)$$

Decryption

In decryption we decrypt original message using private keys d, g. Here first we will decrypt using first private key (d) which is $m1=C^d \text{ mod}(n)$.

And we will find out decrypted message using second private key (t).

$$M=m1^t \text{ mod}(z)$$

2.3 RSA Algorithm Using Chinese Remainder Theorem

By using Chinese remainder theorem(CRT)[4] we will increase processing time and security of algorithm. By using CRT an efficient implementation of RSA algorithm can be implemented. Chinese remainder theorem(CRT) states that, if input M, raise it to the e^{th} (or d^{th}) power modulo P and modulo Q the intermediate results are then combined through multiplication and addition with some pre defined constant to compute final result. By using CRT in RSA algorithm it requires four times less processing time compared and smaller amount of memory for final decoded result. By Using Multi Prime Concept[19] we implement RSA using CRT. They are 3 operations present in RSA using CRT are:

Key Generation Operation

The steps included in the key generation operation of multi-prime RSA-CRT are illustrated as:

- i. Select three large prime r, s and w at random, each of which is n/3-bit in length.
- ii. Set $N = r \times s \times w$ and $\phi(N) = (r-1) \times (s-1) \times (w-1)$.
- iii. Randomly pick an odd integer e such that $\text{gcd}(e, \phi(N)) = 1$.
- iv. After that compute $d = e^{-1} \text{ mod}(N)$.
- v. Finally, calculate $dr = d \text{ mod}(r-1)$, $ds = d \text{ mod}(s-1)$ and $dw = d \text{ mod}(w-1)$.
- vi. The public key would be (e, N) and the private key would be (dr, ds, dw, r, s, w)[20].

Encryption Operation

For a given plain text m which belongs to Z_n the encryption algorithm is the same as that of the original RSA: $c = m^e \text{ mod} N$

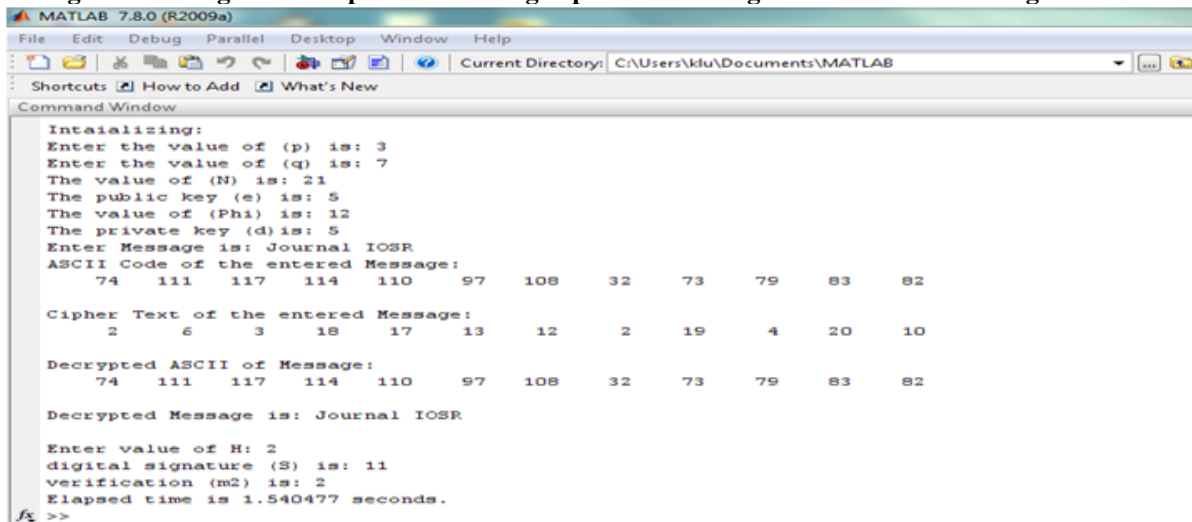
Decryption Operation

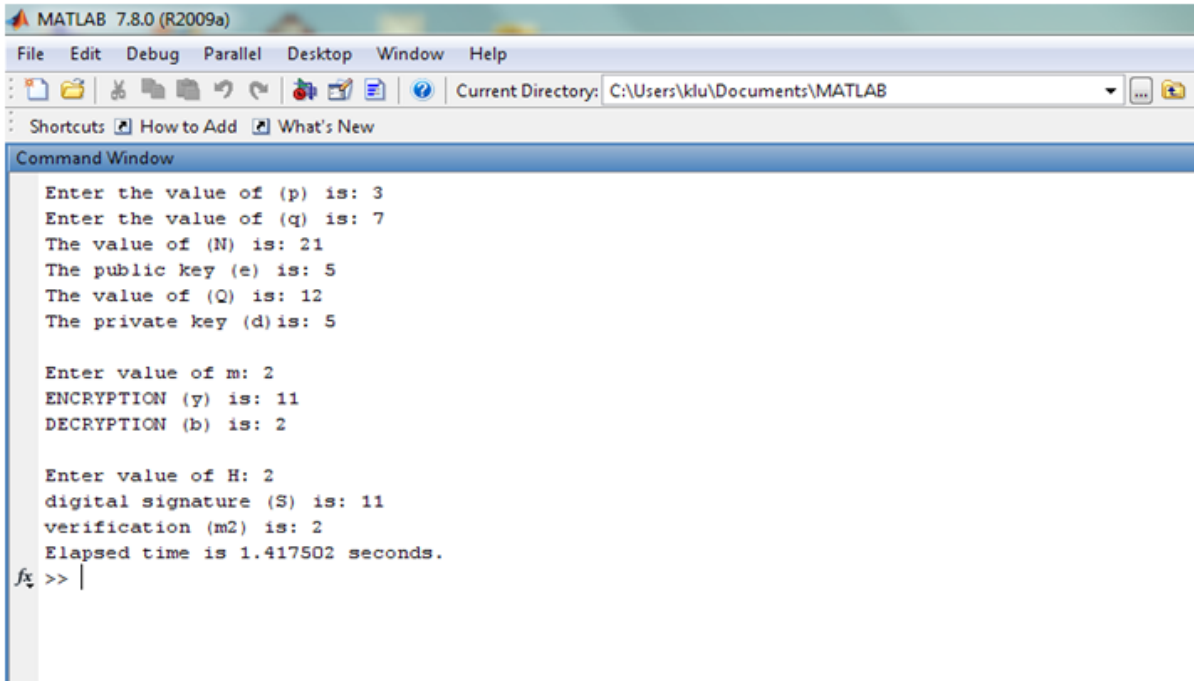
In order to decrypt a cipher-text c:

- i. The decipher first computes $m1 = cr^{dr} \text{ mod} r$, $m2 = cs^{ds} \text{ mod} s$, and $m3 = cw^{dw} \text{ mod} w$ where $cr = c \text{ mod} r$, $cs = c \text{ mod} s$ and $cw = c \text{ mod} w$
- ii. Next, using CRT m can be obtained as $m = c^d \text{ mod} N$, in order to increase its efficiency.

III. Implementation And Results

3.1 Original RSA Algorithm Implemented Using Alphabetic Message and Numerical Message



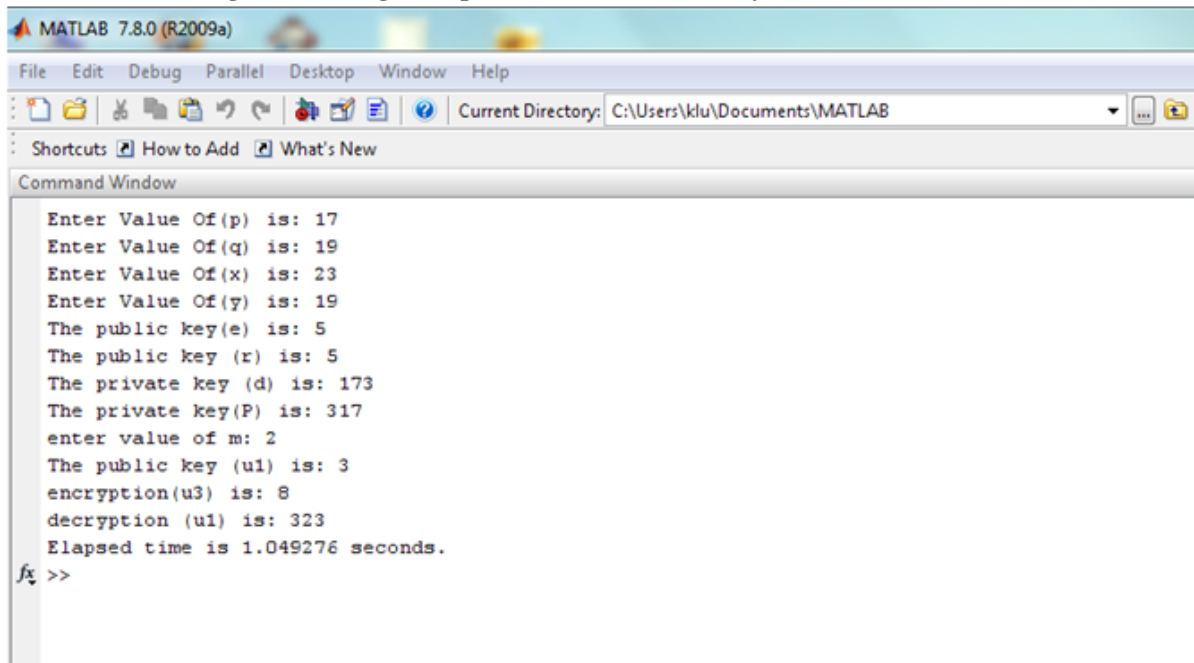


```
MATLAB 7.8.0 (R2009a)
File Edit Debug Parallel Desktop Window Help
Current Directory: C:\Users\klu\Documents\MATLAB
Shortcuts How to Add What's New
Command Window
Enter the value of (p) is: 3
Enter the value of (q) is: 7
The value of (N) is: 21
The public key (e) is: 5
The value of (Q) is: 12
The private key (d) is: 5

Enter value of m: 2
ENCRYPTION (y) is: 11
DECRYPTION (b) is: 2

Enter value of H: 2
digital signature (S) is: 11
verification (m2) is: 2
Elapsed time is 1.417502 seconds.
fx >> |
```

3.2 Modified RSA Algorithm Using Multiple Public and Private Keys



```
MATLAB 7.8.0 (R2009a)
File Edit Debug Parallel Desktop Window Help
Current Directory: C:\Users\klu\Documents\MATLAB
Shortcuts How to Add What's New
Command Window
Enter Value Of(p) is: 17
Enter Value Of(q) is: 19
Enter Value Of(x) is: 23
Enter Value Of(y) is: 19
The public key(e) is: 5
The public key (r) is: 5
The private key (d) is: 173
The private key(P) is: 317
enter value of m: 2
The public key (u1) is: 3
encryption(u3) is: 8
decryption (u1) is: 323
Elapsed time is 1.049276 seconds.
fx >>
```

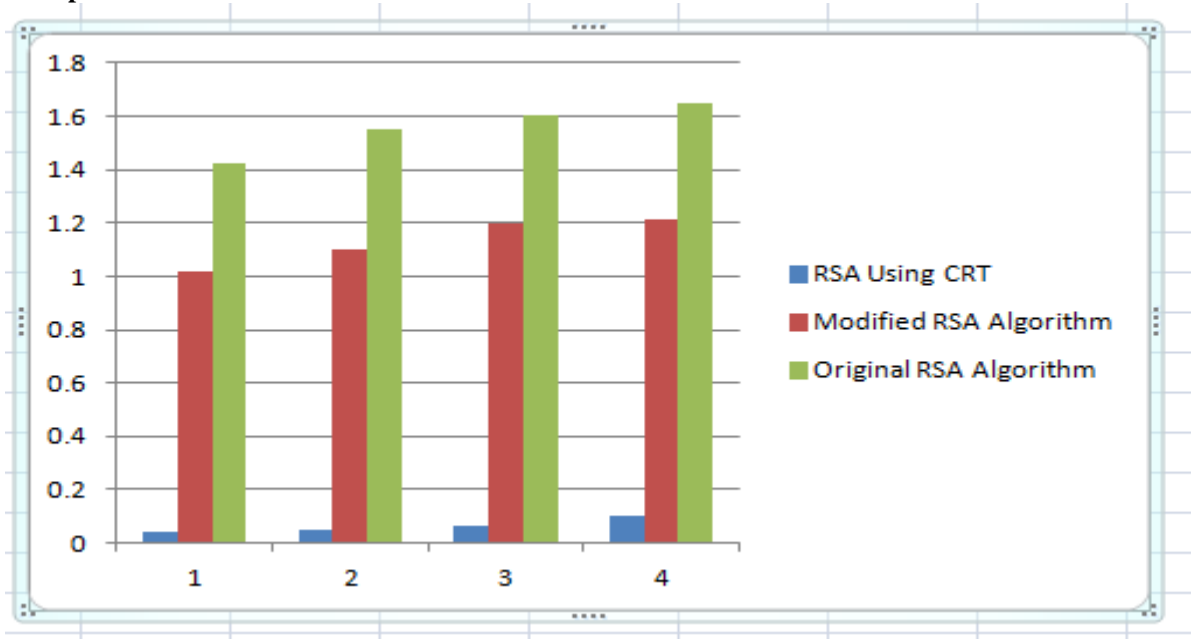
3.3 RSA Algorithm Using Chinese Remainder Theorem(CRT)

```

MATLAB 7.8.0 (R2009a)
File Edit Debug Parallel Desktop Window Help
Current Directory: C:\Users\klu\Documents\MATLAB
Shortcuts How to Add What's New
Command Window
Enter the value (p) is: 3
Enter the value (q) is: 3
Enter the value (r) is: 7
The value of (N) is : 63
The value of (Z) is : 24
Public key(e) is : 5
Private key(d) is : 5
input message value (m) is: 2
Encryption (C) is : 32
private key first (dp): 1
private key second(dq): 1
private key third(dr) : 5
Decryption(M) is : 2
Elapsed time is 0.041714 seconds.
fx >>
    
```

IV. Graphs

Computation Time V/s Prime numbers



V. Conclusion

The observed results from our work clearly mention that by using a single (public and private key) the computational time required is less but problem is less secure. To have more secured transmission of information we can use Chinese remainder theorem so that there will be reduction of time of evaluation. So to have both secure transmission and time bound application we can use two key methods.

Acknowledgements

Authors like to express their deep gratitude to K Sony, Assistant Professor Department of ECE K L University for her great support and encouragement during the implementation of this work and also we would also like to thank our communications research members and also our friends for their help in completion of this paper.

References

- [1]. William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition
- [2]. R.L.Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public key cryptosystem",
- [3]. comm..ACM feb1978, 21(2):120-126
- [4]. W.Diffie and M.E.Hellman, "New directions in cryptography", IEEE Trans. Inform. Theory, Nov.1976,22: 644-654.

- [5]. Chung-Hsien Wu; Jin-Hua Hong; Cheng-Wen Wu, "RSA cryptosystem design based on the Chinese remainder theorem," Design Automation Conference, 2001. Proceedings of the ASP-DAC 2001. Asia and South Pacific , vol., no., pp.391,395, 2001
- [6]. H. Ren-Junn, S. Feng-Fu, Y. Yi-Shiung and C. Chia-Yao "An efficient decryption method for RSA cryptosystem" Advanced Information Networking and Applications, 2005 (AINA 2005). 19th International Conference on, 2005, pp. 585-590 vol.1.
- [7]. Z. Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 82(10):1215-1219,2005.
- [8]. D. Poulakis. A variant of Digital Signature Algorithm. Designs, Codes and Cryptography, 51(1):99-104, 2009
- [9]. C. Kaufman, R. Perlman, M. Speciner, "Network security," Prentice Hall 1995
- [10]. Ronald L. Rivest, Adi Shamir, Len Adelman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science Technical Memorandum82 (April 1977).
- [11]. Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Publishing Company Ltd, New Delhi, ISBN-13: 978-0-07-066046-5, 2010.
- [12]. <http://www.rsa.com/rsalabs/node.asp?id=2167>
- [13]. Niven, I., and Zuckerman, H.S. An Introduction to the Theory of Numbers. Wile , New York, 1972.
- [14]. <http://www.scribd.com/doc/55154238/31/DISADVANTAGES-OF-RSA>
- [15]. Atul Kahate —Cryptography and Network Security| 3rd edition.
- [16]. Gagandeep shahi Charanjit Singh "Cryptography and its Implementation Approaches" International Journal of Innovative Research in Computer and communication Engineering, Vol.1,Issue 3,May 2013,PP 668-672
- [17]. M. Bellare and P. Rogaway. "Optimal Asymmetric Encryption." In A. De Santis, ed., Proceedings of Eurocrypt 1994, vol. 950 of LNCS, pp.92-111. Spinger-Verlag, May 1994
- [18]. <http://en.wikipedia.org/wiki/RSA>
- [19]. M. Wiener. "Cryptanalysis of Short RSA Secret Exponents." IEEE Transactions on Information Theory, Vol. 36, No. 3, pp,553-558, 1990
- [20]. M.J.Hinek, M.K.Low, and E.Teske. On some attacks on multi prime RSA. In K.Nyberg and H.M.Heys, editors, Selected areas in Cryptography, volume 2595 of Lecture Notes in Computer Science ,pages 385-404. Springer, 2002.
- [21]. N. Ojha and S. Padhye," Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key", International Journal of Network Security, Vol.16, No.1, PP.53-57, Jan, 2014

Authors Profile

K.SONY is Assistant Professor in KL University. She Completed M.Tech Electronics and Communication Engineering from ANNA University. He is getting his specialization in Signal processing applications.. He is member of IETE. Her interest in research areas includes Optical Communication and Image processing applications



DESOWJA SHAIK was born in India, A.P, in 1994. He is pursuing her B.Tech in Electronics and Communication Engineering from K L University. He is getting his specialization in communication. He presented 3 papers in International technical fests at reputed engineering colleges. He is member of IETE. His interest in research areas includes Networking and Cryptography and Communication.



B.DIVYA SRI was born in India, A.P, in 1994. She is pursuing her B.Tech in Electronics and Communication Engineering from K L University. She is getting her specialization in communication. She is member of IETE. Her interest in research includes VLSI and Image processing.



G.ANITHA was born in India, A.P, in 1994. She is pursuing her B.Tech in Electronics and Communication Engineering from K L University. She is getting her specialization in communication. She is member of IETE. Her interest in research includes Antennas and Networking.

