ijar
ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/3596
DOI URL: http://dx.doi.org/10.21474/IJAR01/3596

RESEARCH ARTICLE

TRIPLE LAYER SECURE ENCRYPTION: BY COMBINED RSA, IMAGE STEGANOGRAPHY&DIGITAL SIGNATURE.

Pooja Ahlawat.
M.Tech Scholar, Dept. of Computer Sc.& Applications, M.D. University, Rohtak, India.

……………………………………………………………………………………………....

Manuscript Info

Manuscript History

Received: 05 January 2017
Final Accepted: 08 February 2017
Published: March 2017

Key words:-
Cryptography, Steganography, RSA encryption, Digital Signature.

Abstract

With increase in use of Internet among public and availability of digital data sharing has taken industry professionals and researchers to giveindependent focus on information security. With growing internet users frequently required digital media store space toreceive and sendprivate information and this information requires protected against unauthorized attacks &access.In this paper I have presented a new technique for providing secure encryption to the user data. New proposed secure encryption will consists of a combination of RSA Encryption,Steganography along with digital signature.

……………………………………………………………………………………………....

Introduction:-

Cryptography offers us the ability to transmit critical data between resources in a way that protect form third party reading it. Cryptographyalso provide authentication of someone and data. Following types of algorithms are used to specify cryptographic algorithms:

1. Secret key: Encryption and decryption done by single key.
2. Public Key: Two separate key are used for both process.
3. Hash Functions: A mathematical transformation to irreversibly encrypt information[1, 2].

Steganographytechnique overlaps the existence of the secret datafrom an observer into a cover media. Three primary accessories are needed before performing steganography.First isinformation or data, Secondly Cover data medium and most important hidingtechnique. The cover medium can be a text file, an image, an audio file or video file but the most popular is the Image steganography. Primary objective of this technique is to avoid attention from the transmission of hidden information. If intruder detected any changes in the content or material, then the objective that has been processed to achieve the security level of the secret datais at risk, intruder will anyhow try to get the hidden data inside the message.

Background:-

RSA Algorithm is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978is represented in figure 1. It uses two big prime numbers randomly generated to define the public and private keys. The two different keys are used for encryption and decryption purpose. Sender, when the message gets transmit to receiver, encrypts the message using Receiver public key and then receiver can decrypt it using his own private key[3,4]. RSA operations can be divided into three broad steps; key generation, encryption and decryption.

Key Generation[5]:-

1. Select two distinct large random prime numbers p & q such that $p \neq q$.

Corresponding Author:-PoojaAhlawat.
Address:-M.Tech Scholar, Dept. of Computer Sc.& Applications, M.D. University, Rohtak, India.

2. Calculate: $n= p \times q$.
3. Calculate: $\phi (n) = (p-1) (q-1)$.
4. Select an integer e such that $1<e<\phi (n)$
5. Calculate d to satisfy the congruence relation
   $d \times e = 1 \bmod \phi (n)$; d is kept as private key exponent.
6. Public key is (n, e) and private key is (n, d).

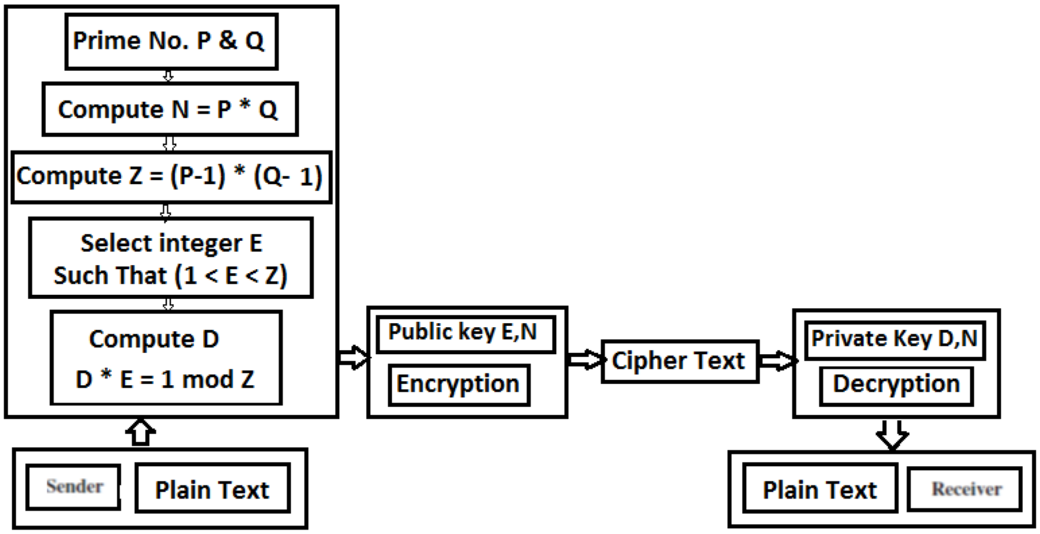


Figure 1:- Block Diagram for RSA

Encryption:
Plain text: $P < n$
Cipher text: $C= P^{e} \bmod n$.

Decryption:
Cipher text: C
Plaintext: $P=C^{d} \bmod n$.

Proposed Methodology:-

Required robustness and security can beachieved;steganography &cryptography is combined along with additional digital signature that provide third layer of security. For cover media I will take Imagefor steganography and RSA algorithm will be used for encryptionand is represented in figure 2. By combining, the data encryption will be done by RSA and then the cipher text will be used as input withImage media with the help of digital signature. The combination of these two methods along with digital signature will enhance the security of the data embedded.

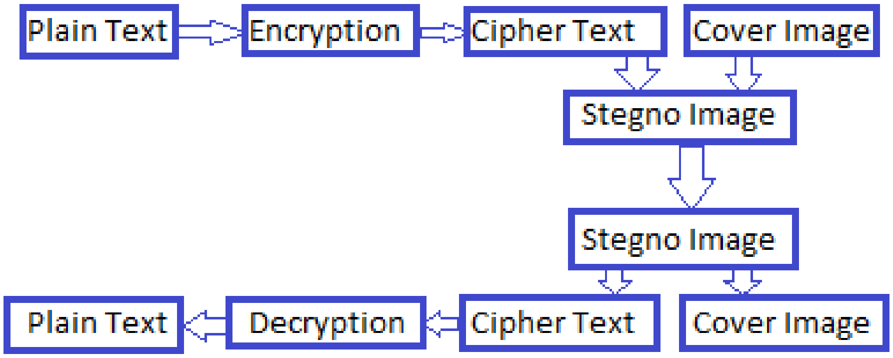


Figure 2:- Combination of Steganography and Cryptography

Working Architecture:-

A development of the complete proposed model is completed and the implementation of Encryption Process is also completed. As encryption is lifelong work to secure data. Day after day new and advanced techniques will be required to secure our data from hacker.

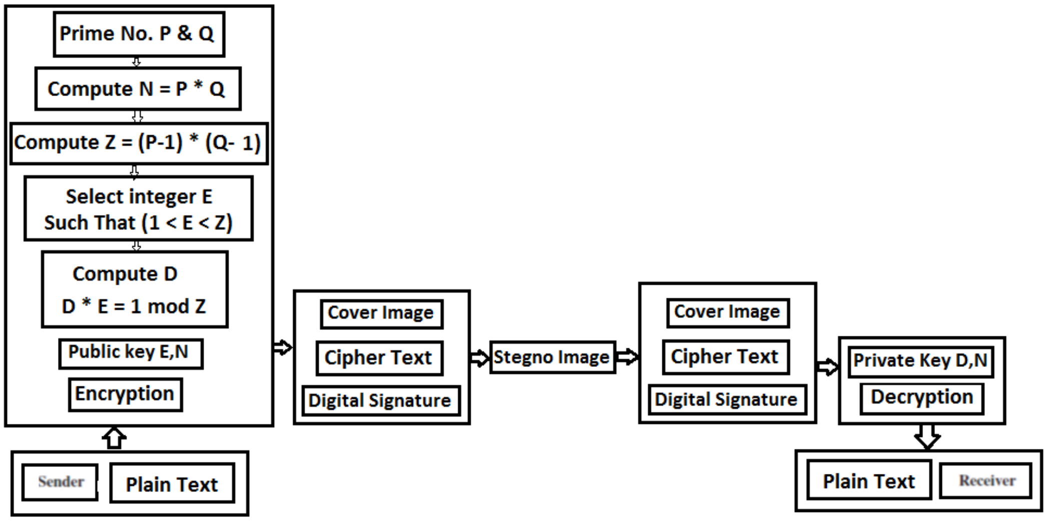


Figure 3:- Detailed Architecture for Proposed Technique

As details architecture is represented by in the figure 3. The Process is stated by converting plain text of uses into the cipher text by using RSA encryption process, Cipher text as plain text for Steganography, Cover Image required is input by user, Digital Signature that is of user choice. Here in implementation I have considered four – digit numeric value for digital signature and that is entered by user. Encryption Process is completed as per the detailed Architecture.

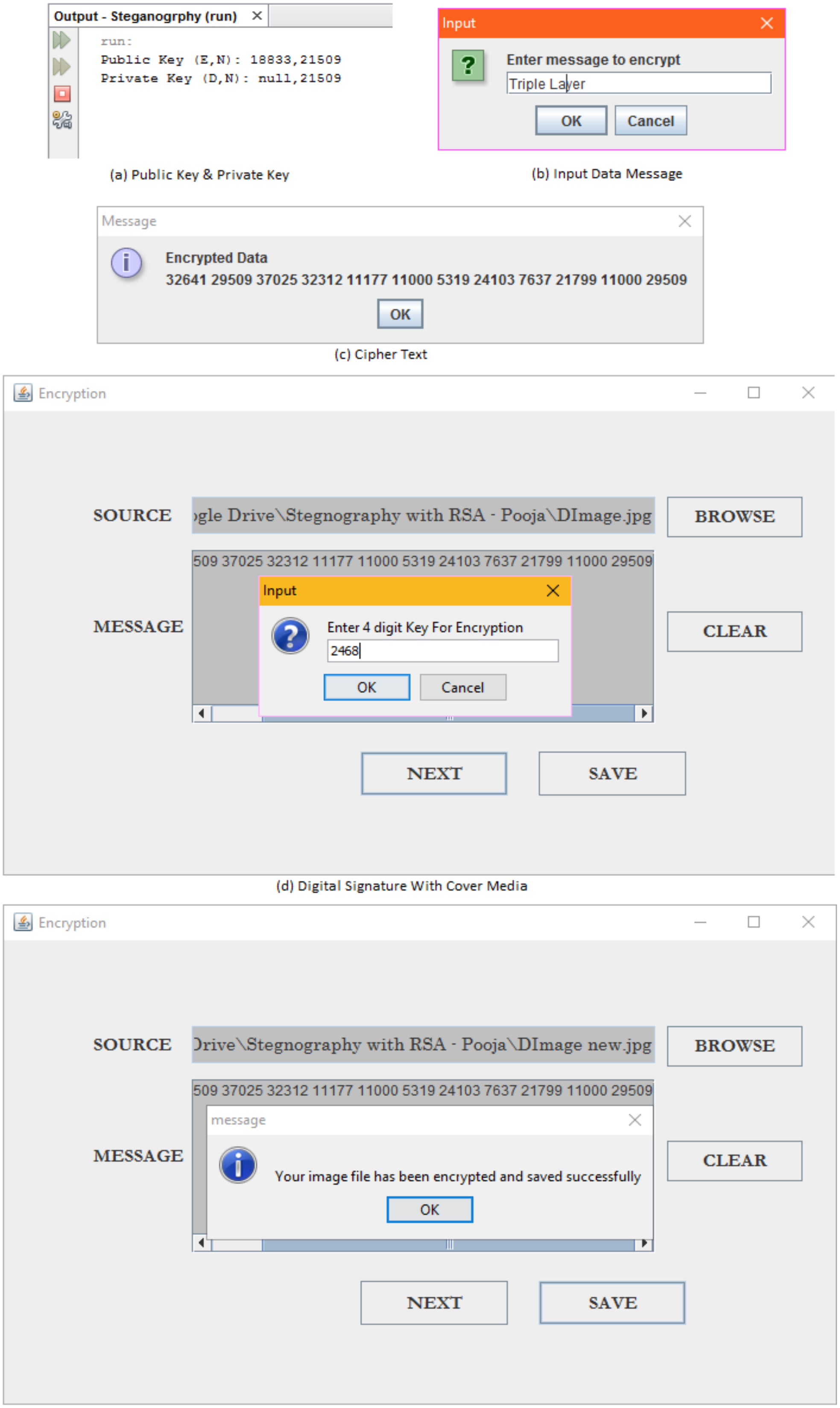
Results:-

According to the details architecture of the proposed new techniques shown in figure 3 I have developed new model. Figure 4 contains the complete encryption process. In Figure 4(a) contains the public & the private key randomly generated with the help of RSA encryption process and Figure 4(b) contains the data to be in secured. Figure 4(c) contains the cipher text that is obtains from RSA encryption process. Further Figure 4(d) contains the source of the cover media along with the last layer of security that is digital signature. And the final image Figure 4(e) contains the final message with the save new media that contains data to be hidden.

Decryption process is illustrated in figure 5. Figure 5(a) contains the source media that contains data along with the digital signature both value input by the user. Further figure 5(b) contains the cipher that is obtains from the step one of decryption process that separates cipher text from cover media with the help if digital signature.

Conclusion& Future Work:-

By this extra layers of security will be available to provide security to our document in today's words. If any how intruder is able to detect the text in the image. Then also that text is no more than cipher text and is also secured by digital signature. Thus triple Encryption is provided to the user data.Decryption process is not completed in the development of this model. My encryption process is working as per proposed model.



```
run:
Public Key (E,N): 18833,21509
Private Key (D,N): null,21509
```

(a) Public Key & Private Key

Enter message to encrypt

Triple Layer

(b) Input Data Message

Encrypted Data

32641 29509 37025 32312 11177 11000 5319 24103 7637 21799 11000 29509

(c) Cipher Text

SOURCE: ›gle Drive\Stegnography with RSA - Pooja\DImage.jpg

MESSAGE: 509 37025 32312 11177 11000 5319 24103 7637 21799 11000 29509

Enter 4 digit Key For Encryption

2468

(d) Digital Signature With Cover Media

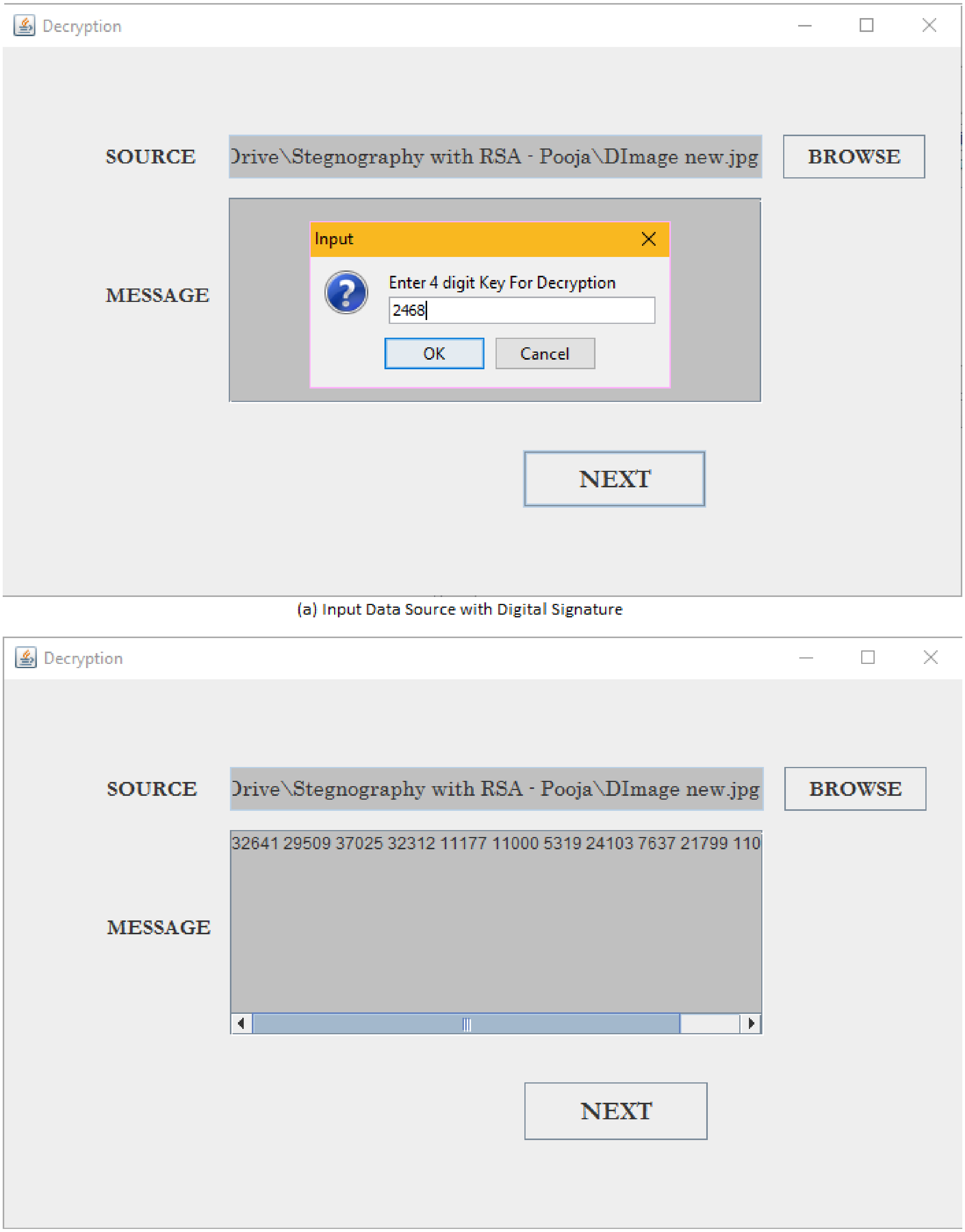
SOURCE: Drive\Stegnography with RSA - Pooja\DImage new.jpg

MESSAGE: 509 37025 32312 11177 11000 5319 24103 7637 21799 11000 29509

Your image file has been encrypted and saved successfully

(e) Triple Layer Security Applied

Figure 4:- Detailed description of encryption process of new proposed Technique


Decryption

SOURCE: Drive\Stegnography with RSA - Pooja\DImage new.jpg

MESSAGE:

Input

Enter 4 digit Key For Decryption

2468

(a) Input Data Source with Digital Signature

Decryption

SOURCE: Drive\Stegnography with RSA - Pooja\DImage new.jpg

MESSAGE: 32641 29509 37025 32312 11177 11000 5319 24103 7637 21799 110

(b) Cipher text

Figure 5:- Description of decryption process of new proposed Technique

References:-

1. Zin.w, soe. “Implementation and Analysis of three Steganographic Approaches”, University of Computer Studies, Mandalay, 2011,
2. Manoj.s,“Cryptography and Steganography”, International Journal of Computer Applications (0975-8887), 2010, vo1-no.12,
3. Aman Kumar, Dr. SudeshJakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm’s", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.
4. Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, 2011.
5. Uma Somani, KanikaLakhani and Manish Mundra, “Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 1st International Conference on PDGC, 2010.