

An Updated RSA Algorithm Based Cryptosystem for Data Encryption & Data Decryption

Pachore Abhijit A¹, Prof. Arpit Solanki²

^{1,2}RKDFS School of Engineering, Indore

Abstract:

The main objective of cryptography is to send information or message in hidden manner from one side to another in such a way that the intruder or attacker cannot crack the content and even unable to feel the presence of secret message. Although many new techniques have been proposed by many researchers to transmit data in encoded form from one side to another. But still it is possible to identify the original message. This paper proposed a new hybrid security model based on cryptography. A critical review of modern methods have been done. On the basis of the research gap we proposed and implemented a novel technique.

Keywords: *Cryptography, RSA, Security Attacks, Decryption, Encryption*

1. INTRODUCTION:

In today's world, security is a major problem especially when it comes to hiding secret information from total strangers. So, converting a message into a form that cannot be easily cracked is an ultimate option for all. Due to the new and improved techniques used by hackers, sharing information on the internet is less secure now a days. To overcome such problems have evolved techniques like steganography and cryptography.

If we uncover the pages of history we find that in those times too, secret information was passed from one party to another via various means like invisible ink, tattoos and much more and that has become the brain child for the present techniques like cryptography where the online secret information sharing has become more secure for parties who have a sensitive information that cannot fall in wrong hands.

2. CRYPTOGRAPHY SECURITY SERVICES:

The security services include [4]:

- **Data Confidentiality**
- **Data Integrity**
- **Authentication**
- **Non repudiation**
- **Access Control**

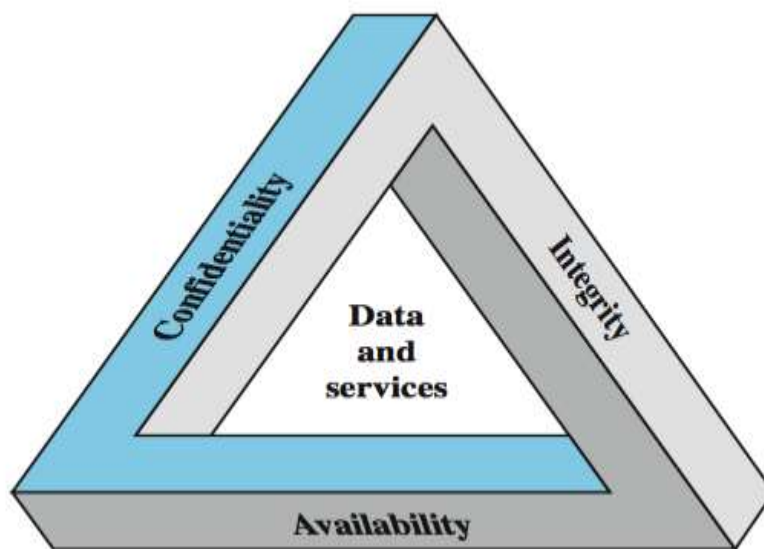


Figure 1.1: Security Services

3. RELATED WORK:

Yang Ren-er, ZhengZhiwei, Tao Shun, Ding Shilei[4] , have presented DES algorithm for encryption along with LBS algorithm so that the hidden information is given a dual protection and the information is compressible and invisible to anyone else. Problem of the research was DES algorithm. Now days it is easily breakable.

Mr. Madhusudhan Mishra, Mr. Gangadhar, Tiwari, Mr.Arun Kumar Yadav,.[5] the authors has used a new technique. The author has used RSA algorithm for encryption along with F5 algorithm. To hide the encrypted message in the lower image, the author has also used a two tier security layers- first using cryptography key and second using stego key.

Manu Devi, Nidhi Sharma, [6] the proposed system the author has used LBS steganography for image embedding. The author has calculated the PSNR for the better quality of the image and how it is calculated has also been

mentioned. The higher the PSNR value, the better is the quality of the stego image. The main aim of the research was developing a new and enhanced technique of hiding the data. The main motive was to make the encrypted message totally unbreakable from the inside.

Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R.[1] has proposed model gives two tier security to secret data. Further our proposed method gives high embedding capacity and high quality stego images using advanced encryption standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with least-significant-bit (LSB) substitution is used to hide encrypted message into true color RGB image.

Its two main keys are used i.e. in encryption and decryption. RSA is an algorithm based in the theorem of factoring two large prime numbers. [3, 5]

4. PROPOSED WORK:

RSA Algorithm has following steps.

1. Select two large prime numbers P , Q and R.
2. Calculate $N=P*Q*R$
3. Select the public key (encryption key) E such that it is not a factor of (P-1) and (Q-1) (R-1).
4. Select private key (decryption key) D such that the following equation is true:

$$(D * E) \bmod (P-1) * (Q-1) * (R-1) = 1$$

5. For encryption, calculate the cipher text CT from the plain text PT as follows:

$$CT = PT^E \bmod N$$

6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:

$$PT = CT.\text{MODINVERSE}(PHIN)$$

$$DP = D.\text{REMAINDER}(PM1)$$

$$DQ = D.\text{REMAINDER}(PHIN1)$$

$$C2 = P.\text{MODINVERSE}(Q)$$



5. CONCLUSION:

In this paper, we have elaborated the basic concept of cryptography and the key management schemes. A critical review of modern methods have been done. On the basis of the research gap we proposed and implemented a novel hybrid technique. Which is a fusion of all popular security mechanisms. From the experimental result of the proposed method. It is proved that the decryption time of the proposed cryptosystem is better than that of the existing system.

REFERENCES:

- [1]. Vitthal S., BhosaleRajkumar S., PanhalkarArchana R “A Novel Security Scheme for Secret Data using Cryptography and Steganography” DOI: 10.5815/ijcnis.2012.02.06
- [2]. Manjunath N, S.G.Hiremath “Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique” ISSN : 2347-2820, Volume -3, Issue-5 2015
- [3]. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena “Security Improvisation in Image Steganography using DES” 978-1-4673-4529-3/12/_c 2012 IEEE
- [4]. Yang Ren-er, ZhengZhiwei, Tao Shun, Ding Shilei Image “Steganography Combined with DES Encryption Pre-processing” 978-1-4799-3434-8/14 ©2014 IEEE DOI 10.1109/ICMTMA.2014.80
- [5]. Mr. Madhusudhan Mishra, Mr. Gangadhar Tiwari, Mr. Arun Kumar Yadav “Secret Communication using Public key Steganography” [978-1-4799-4040-0/14/\$31.00 ©2014 IEEE
- [6]. Manu Devi Nidhi Sharma “Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images” 978-1-4799-2291-8/14/\$31.00 ©2014 IEEE

BIOGRAPHIES

	<p>Abhijit A Pachore, Pursuing Master Degree in Computer Science & Engineering from RKDFS School of Engineering, Indore. He Completed B.E. from University of Pune with First class. His area of research is Information Security.</p>
	<p>Prof. Arpit Solanki, Working as Professor in Computer Science & Engineering at RKDFS School of Engineering, Indore.</p>

