Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6189-6194, 2017
ISSN: 1816-949X

An Amended RSA Algorithm for Secure Communication

Nisha P. Shetty
Department of Information and Communication Technology,
Manipal Institute of Technology, 576104 Manipal, Karnataka, India

Abstract: One of the foremost challenges faced while communicating in this digitized world is security. The need for legitimate and accredited information exchange is so great that it has become one among the major research areas today. This study presents a three layer security model which expedites a safe and sound information exchange between the end users. The message from the sender is first scrambled using RSA algorithm and the cipher text is cloaked within an image. The correct stego-image is shared with the receiver only if he answers the previously shared (only between sender and receiver; undisclosed to others) question correctly. The receiver first gleans the cipher text from the stego-image and thenceforth proceeds to crack the extracted cipher text to obtain the original message.

Key words: Steganography, RSA, encryption, cipher, stego-image, Shared

INTRODUCTION

In this era of internet where many people rely on online sector for their day to day deeds, ranging from banking to simple e-Mail communication, major setbacks suffered by the communication zones is the breach of genuineness, authorization and solitude of information. To thwart this misuse and interception of essential data by illegal entities techniques like cryptography, steganography (Kaur *et al*., 2014), digital signatures, etc., have been introduced.

"Cryptography" originates from the amalgamation of two greek words "Krypto" meaning "hidden" and "graphene" meaning "writing" (Ahmad *et al*., 2015). It has ranged over a period of 4000 years tracing back to Egyptian 'hieroglyph' as its source (Al-Vahed and Sahhavi, 2011). There are 3 types of cryptosystems (Mane, 2015):

- Secret key cryptosystem: encryption and decryption is done via one key
- Public key cryptosystem: 2 keys, i.e., 1 for encryption and other for decryption is used
- Hash function: makes use of a hash value having fixed length calculated on the plain text to warrant that the file has not been altered by an imposter or a virus

Benefits:

- Protects from unlicensed revelation, spoofing and forgeries
- Promotes data veracity and non-repudiation

Drawbacks:

- Huge time and money costs
- Even if the cipher text can't be deciphered, an attacker can destroy or remove the text from the system making it inaccessible to all, owing to poor design of the system. This introduces the need to conceal from public eye

"Steganography" (Kaur *et al*., 2014) arising from Greek words "steganos" or "covered" and "graphie" or "writing" takes cryptography a step beyond by hiding the coded message within any other normal message in such a way that its presence can't be suspected. Many legends over the time has shown some or the other type steganography. One such fascinating legends is that of the Pirates who tattooed a secret maps on the heads, so that it is cloaked by human hair. Most common digital steganography technique is "Watermarking" (Podilchuk and Delp, 2001) which administers the copyright of content conveyed across internet by enclosing a concealed message (invisible watermark) in images, moving pictures, sound files, texts, etc.

Pros: Vital information masked from human eye useful in preventing hacking.

Limitations: Care should be taken to ensure that the hidden message does not compromise the quality of the original message.

Literature review: Among various cryptographic algorithms such as RSA, AES, DES or hash functions such as MD5, SHA, etc. RSA is the most popular algorithm till date. This study briefly expounds on some research done in the field of cryptography and steganography. Below research of some of the prominent people in the field are listed.

Boneh and Shacham (2002) researched on four variants of RSA designed with the intention of speeding up the decryption process in RSA. Their research concluded that while batch RSA was fully backward compatible with the existing RSA techniques, multi-factor RSA and rebalanced RSA offered better rapidity while decrypting.

Rawat and Walfish (2003) divided the message into small parts and hash code generated for each block is concatenate with the message blocks. Subsequently, the integrated string is encoded. At the receiver each block is processed parallel to obtain the speedup. Even though, this method increases the security it is not suitable for applications offering low bandwidth where short messages must be exchanged.

Chang *et al*. (2005) tried to solve the utmost intricate part of RSA algorithm is the factoring the product of two large prime numbers by developing three new DNA-based procedures which are parallel subtractor, parallel comparator and parallel modular arithmetic.

Chandra *et al*. (2014) examined various symmetric and asymmetric key cryptographic algorithms emphasizing on their importance, pros, cons and future scope.

Khan researched on how genetic algorithm can be applied to the process of cryptanalysis by highlighting the work done by various researchers in that field.

Saxena and Kapoor (2014) divided the data into smaller chunks and distributed these chunks among various available cores of processors to imbibe simultaneous processing. Finally, these pieces were unified together to get the entire data set.

Jindal and Singh (2015) presented the horometrical survey of the RC4 algorithm back from its inception. Being simple and robust, this algorithm is enticing many researchers now a days. The study expounds on various research opportunities in the field.

Bahadori *et al*. (2010) employed a smartcard furnished with a crypto-coprocessor and a true random number generator to achieve 50% reduction in key pair bearing time. Their technique produces large prime numbers in a lesser time effectively reducing the time requisite for spawning key pair. During key generation process an apt public key is chosen from a lot of pre-demarcated public keys and Euclid's extended algorithm is used to create private keys. Johri *et al*. (2016) have done a detail study of steganography in all possible domains in.

Various works are done in the field of steganography such as video steganography built on genetic algorithm (Dasgupta *et al*., 2013) and using the vertical and horizontal reflection symmetry properties of the characters in individual sentences of the document to camouflage the messages (Majumder and Changder, 2013).

Singh *et al*. (2012) made use of null spaces (2 spaces for 1 and 1 space for 0) to embed the secret message in the cover text (Singh *et al*., 2012). A great deal of spaces were needed to encode a small message as each character, i.e., 8 bits required 8 spaces.

Bhattacharyya (2011) researcher modified the alphabets in the cover text to hold bits of the secret memo in such a way that the structural alteration of the letters is not easily discernable.

Yang *et al*. (2008) used edge areas of images for hiding data rather than using smooth areas in. Pixel value differentiation was used to find the edge areas of the images and LSB method was used for embedding the secret value.

P and B frames in video were used for secret text transmission and frame I contained control information by Ping and Zhang (2006). Researchers at the decryption end, extracted control information first, based on which implanted message was extracted.

The various advancements made in the field of steganography using digital audio as the carter are illustrated by Bilal *et al*. (2014).

MATERIALS AND METHODS

Steps followed during encryption and decryption are shown in Fig. 1 and 2, respecticvely. During encryption process the cipher text generated after applying RSA is hidden in an image and is sent to the reciever. Also to certify the sacredness of the stego-image a classified question is decided among the sender and reciever. Reciever gets the correct stego-image only after answering the secret question correctly and then he applies the proposed steganalysis algorithm to it to generate the cipher text. Decryption of cipher text then yields the plain text.

Stegnography algorithm: The algorithm used for hiding cipher text in the cover image is given and also is illuatrated in Fig. 3 (Ibrahim and Kee, 2012).

Encoding (Ibrahim and Kuan, 2011):

- Choose a cover Image from the database of available images
- Select a secret key
- Select a secret question (which is communicated prior between sender and receiver to retrieve the stego-image from the database). Transfer and zip the secret text (cipher text) obtained from RSA into a zip file
- Convert zipped text file to binary codes
- Transform secret key into binary codes
- Initialize bitsperunit to zero
- Hide two binary codes from the series within a pixel of the chosen image
- Echo viii. until all codes are enciphered
- Output: stego-image

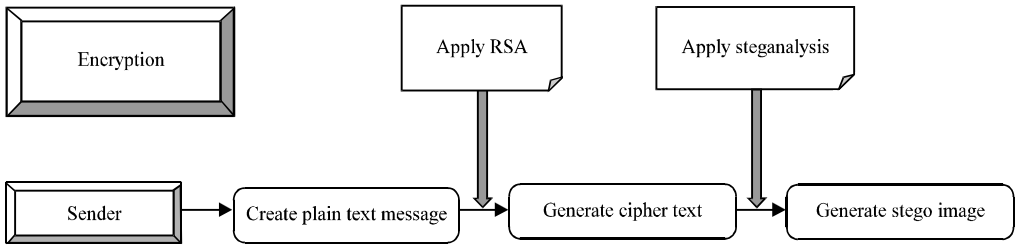

Fig. 1: Encryption process

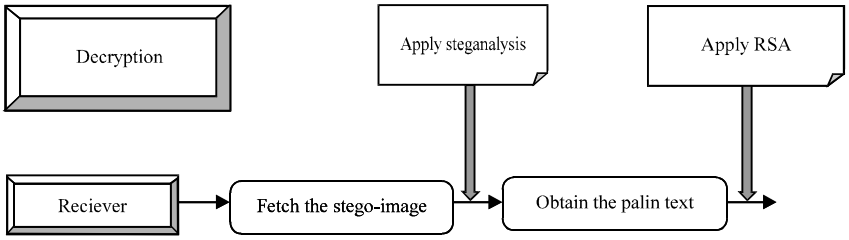

Fig. 2: Decryption process

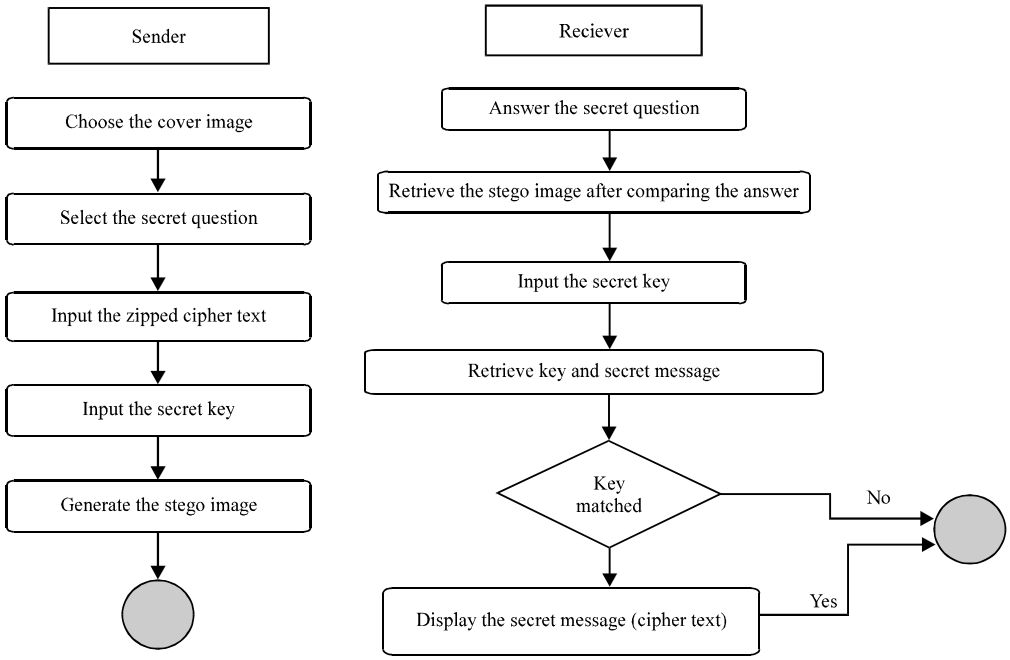

Fig. 3: Block diagram of stegnography process

Decoding (Ibrahim and Kuan, 2011):

- Answer the secret question to retrieve the correct stego-image:
- Enter the secret key
- Compute bits per unit
- Retrieve 2 binary codes from each pixel
- Decipher all the retrived binary codes and convert it into original format
- Compare the secret key entered by the receiver with the embedded secret key
- If match found, display the cipher text
- If no match found display error messges
- Output: secret text (cipher text)

RESULTS AND DISCUSSION

Simple embedding zip files into image commands on windows and unix platforms for embedding message in image: In windows platform:

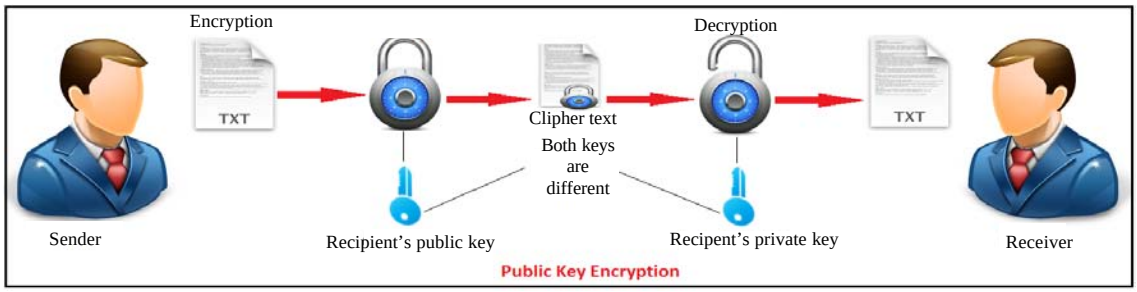

Fig. 4: Block diagram of RSA process

"copy/B picture.gif+YourMenu.zip newfile.gif"

In Linux Platform:

"cat image.png secret.zip>image2.png"

Here:

- The original image is picture.gif/image.png
- Your Menu.zip/secret.zip is the zip file to be hidden in the image
- Newfile.gif/image2.png is the stego-image

For extracting the hidden message from the image: "unzip image2.png/newfile.gif"

RSA algorithm: This algorithm, proposed by Babu *et al*. (2015) is one of the most widely used algorithms till date. It involves 3 steps as shown in Fig. 4.

Key generation:

- Choose any two prime numbers p and q
- Compute n = p×q
- Compute φ(n) = (p-1)×(q-1)
- Choose e such that 1<e<φ(n) and e and φ(n) are coprime
- Compute a value for d such that (d×e) % φ(n) = 1

Pubic key generation:

- Public key is (e, n)

Private key generation:

- Private key is (d, n)

Encryption: ABC wants to send DEF an encrypted message M so she obtains his RSA public key (e, n) and generates cipher text using $C = M^e \bmod n$.

Decryption: DEF uses his private key (d, n) to decrypt the message $M = C^d \bmod n$.

Table 1: Encryption

Symbol	Original No.	M = (No+1)	M^3 mod 33 = C
S	19	20	14
U	21	22	22
N	14	15	9

Table 2: Decryption

Symbol	Original no (No. -1)	C^7 mod 33 = M	Cipher
S	19	20	14
U	21	22	22
N	14	15	9

Example:

let, e = 3, d = 7, n = 33

To encrypt the message "SUN" numeric value of the character is incremented by one and is used as plain text message. While decrypting the plain text number obtained from cipher text is decremented by one and its corresponding character is fetched. The process is depicted in Table 1 and 2 shown.

CONCLUSION

Steganography is the art of concealing data within other data and is used to transfer the messages stealthily avoiding a "hack". The proposed technique presents a three tier security model where RSA based encryption, secret question and steganography techniques together shields the crucial data. As the stego-images does not suffer from any noticeable changes that could be discerned by a human eye at a glance, it provides a vital protection for imperative information s uch as credit card information so that they can be protected from eavesdroppers (man in the middle attack). The presented method addresses the losses suffered by RSA on account of brute force attack and chosen cipher text attacks (Babu *et al*., 2015) by avoiding the capture of cipher texts by unauthorized entities. Future work in this area would be improving the efficiency of the presented methodology by using some advanced algorithms such as elliptic curve cryptography or AES for encryption without

compromising on the quality of the stego-image (having higher PSNR (Peak signal to noise ratio)) or incorporating signatures using hashing or digital signatures to endorse authenticity. Extending the work to develop stego-videos can also be a future step in this direction.

REFERENCES

Ahmad, S., K.M.R. Alam, H. Rahman and S. Tamura, 2015. A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. Proceedings of the International IEEE Conference on Networking Systems and Security (NSYSS), January 5-7, 2015, IEEE, Dhaka, Bangladesh, ISBN:978-1-4799-8127-4, pp: 1-5.

Al-Vahed, A. and H. Sahhavi, 2011. An overview of modern cryptography. World Applied Program., 1: 55-61.

Babu, E.S., C. Nagaraju and M.H.M.K. Prasad, 2015. A secure routing protocol against heterogeneous attacks in wireless adhoc networks. Proceedings of the 6th ACM International Conference on Computer and Communication Technology (ICCCT '15), September 25-27, 2015, ACM, Allahabad, India, ISBN:978-1-4503-3552-2, pp: 339-344.

Bahadori, M., M.R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani, 2010. A novel approach for secure and fast generation of RSA public and private keys on smartcard. Proceedings of the 8th IEEE International Conference on NEWCAS, June 20-23, 2010, IEEE, Montreal, Quebec, ISBN:978-1-4244-6806-5, pp: 265-268.

Bhattacharyya, S., 2011. Hiding data in text through changing in alphabet letter patterns (CALP). J. Global Res. Comput. Sci., 2: 33-39.

Bilal, I., R. Kumar, M.S. Roj and P.K. Mishra, 2014. Recent advancement in audio steganography. Proceedings of the International Conference on Parallel, Distributed and Grid Computing, December 11-13, 2014, IEEE, Solan, India, ISBN:978-1-4799-7682-9, pp: 402-405.

Boneh, D. and H. Shacham, 2002. Fast variants of RSA. CryptoBytes, 1: 1-9.

Chandra, S., S. Paira, S.S. Alam and G. Sanyal, 2014. A comparative survey of symmetric and asymmetric key cryptography. Proceedings 2014 International Conference on Electronics, Communication and Computational Engineering, November 17-18, 2014, IEEE, Hosur, India, ISBN:978-1-4799-5748-4, pp: 83-93.

Chang, W.L., M. Guo and M.S.H. Ho, 2005. Fast parallel molecular algorithms for DNA-based computation: Factoring integers. IEEE Trans. NanoBiosci., 4: 149-163.

Dasgupta, K., J.K. Mondal and P. Dutta, 2013. Optimized video steganography using Genetic Algorithm (GA). Procedia Technol., 10: 131-137.

Ibrahim, R. and L.C. Kee, 2012. MoBiSiS: An android-based application for sending stego image through MMS. Proceedings of the 7th International Multi-Conference on Computing in the Global Information Technology ICCGI, June 24-29, 2012, IARIA, Venice, Italy, pp: 115-120.

Ibrahim, R. and T.S. Kuan, 2011. Steganography algorithm to hide secret message inside an image. Comput. Technol. Appl., 2: 102-108.

Jindal, P. and B. Singh, 2015. RC4 encryption: A literature survey. Procedia Comput. Sci., 46: 697-705.

Johri, P., A. Mishra, S. Das and A. Kumar, 2016. Survey on steganography methods (text, image, audio, video, protocol and network steganography). Proceedings of the 3rd International IEEE Conference on Computing for Sustainable Global Development (INDIACom), March 16-18, 2016, IEEE, New Delhi, India, ISBN:978-1-4673-9417-8, pp: 2906-2909.

Kaur, S., S. Bansal and R.K. Bansal, 2014. Steganography and classification of image steganography techniques. Proceedings of the International IEEE Conference on Computing for Sustainable Global Development (INDIACom), March 5-7, 2014, IEEE, New Delhi, India, ISBN:978-93-80544-10-6, pp: 870-875.

Majumder, A. and S. Changder, 2013. A novel approach for text steganography: Generating text summary using reflection symmetry. Procedia Technol., 10: 112-120.

Mane, R.R., 2015. A review on cryptography algorithms, attacks and encryption tools. Intl. J. Innovat. Res. Comput. Commun. Eng., 3: 8509-8514.

Ping, X.X. and T. Zhang, 2006. Steganography in compressed Video stream. Proceedings of the 1st IEEE International Conference on Innovative Computing, Information and Control, (ICICIC) Vol. 1, August 30-September 1, 2006, IEEE, Beijing, China, ISBN:0-7695-2616-0, pp: 269-272.

Podilchuk, C.I. and E.J. Delp, 2001. Digital watermarking: Algorithms and applications. IEEE. Signal Process. Mag., 18: 33-46.

Rawat, A. and S. Walfish, 2003. A parallel signcryption standard using RSA with PSEP. Project Rep., 1: 1-10.

Saxena, S. and B. Kapoor, 2014. An efficient parallel algorithm for secured data communications using RSA public key cryptography method. Proceedings of the IEEE International Conference on Advance Computing (IACC), February 21-22, 2014, IEEE, urgaon, India, ISBN:978-1-4799-2573-5, pp: 850-854.

Singh, P., R. Chaudhary and A. Agarwal, 2012. A novel approach of text steganography based on null spaces. IOSR. J. Comput. Eng., 3: 11-17.

Yang, C.H., C.Y. Weng, S.J. Wang and H.M. Sun, 2008. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inform. Forensics Secur., 3: 488-497.