Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

Application of Steganography and Cryptography for Secured Data Communication – A Review

Babangida Zachariah
School of Architecture, Computing & Engineering
FTMS Global Col., Malaysia

Patience Ndang Yabuwat
Computer Science Department
KSCOE Gidan Waya, Nigeria

Ephraim Bernard
School of Architecture, Computing & Engineering
FTMS Global Col., Malaysia

***Abstract* - The need for security in data communication is as long as mankind; since eavesdroppers often intercept such communication for malicious purposes. Several techniques such as steganography and cryptography have been employed to hide the existence of communication and scramble such communication making it difficult to interpret in cases where steganography fails. Combining Cryptography and steganography has proven to have taken data communication security to another level. In this work, a review of these techniques is presented with major focus on two journals titled "Dual Layer Security of Data Using LSB Image Steganography Method and AES Encryption Algorithm" [1] and "An Efficient Data Hiding Scheme Using Steganography and Cryptography Technique" [2]were considered for review. A brief description of the techniques is provided. It is found that these techniques could improve security of data communication beyond the present levels if properly combined with little or no performance degradation.**

Keywords: Data Security, Steganography, Cryptography, Least Significant Bit (LSB), Fourteen-Square Substitution

1.0 INTRODUCTION

Communication is as old as the universe itself and the need for security in such communication is as old as mankind. The need for security in data communication is even more with advances in technologies such as the computers and networks. The user of such technologies desires security/privacy of the messages sent over either wireless or wired transmissions. That is, the message is received only by the intended receiver [3]. Hackers on the other hand are interested in intercepting such communications to read the content and for malicious attacks such as spoofing, exploit password, phishing, and many more. According to [4], 7% of all adults in the USA are victims of identity theft and on the average $3,500 is lost in each incidence. In [5], it was reported that there are at least 2,418 cases of National Health Services Data Breaches every year. In another report of February, 2014, titled "Third Report on Card Fraud", European Central Bank showed that of the 0.02% increase over the 2011 cases, One-Point-Thirty-Three billion Euros (€1.33 billion) was lost due to total fraudulent transactions in 2012, 60% was due to internet/telephone payments, 23% due to Point-of-Sale (POS) terminals, and 17% due to Automated Teller Machines (ATMs) [6]. These imply that the security of data communication should be everyone's concern since most of these frauds are as a result of some eavesdropper intercepting communication and making meaning out it thereby able to attack. These rising concern has led to the development of several security measures and techniques such as cryptography [7] and steganography [8].

1.1 CRYPTOGRAPHY

Cryptography, also called cryptology is a word from Ancient Greek words: Kryptos (hidden secret), Graphein (writing), and Logy (study) [9]. It describes the techniques of scrambling data from the third party called eavesdropper. That is, it is essentially the encryption of data such that it is difficult to make meaning of it if not the intended recipient. It is the science of mathematics that uses algorithms such as Hash Functions, Public, or Private Keys to encrypt and decrypt data.

Those days when printed documents were means of communication, mechanical encryption was used [10]; in this era of digital data, digital cryptography is used to secure communication of such information. In digital cryptography, keys are used in the encryption and decryption processes. If the same key is used at encryption and decryption, it is called Symmetric Encryption; if different keys are used at encryption and decryption, it is called Asymmetric Encryption. The distribution and management of these keys is usually the challenge of modern cryptography. Symmetric cryptography may be categorized as Block Cipher or Stream Cipher and use such key schemes as Data Encryption Standard (DES), Triple-DES, Advanced Encryption Standard (AES), Rivest Cipher (RC4, RC5), Blowfish, KASUMI; Asymmetric cryptography key scheme includes Rivest Shamir Adleman (RSA), Diffie-Hellman (D-H) Encryption, Digital Signature Algorithms (DSA), Elliptic Curve Cryptography (ECC) [11]. For the purpose of this, RSA and AES are explained.

1.1.1 Rivest Shamir Adleman (RSA) Algorithm

RSA, developed by Clifford Cocks in 1973 and later by Rivest Ron, Shamir Adi, and Len Adleman in 1977. It is one the mostly used asymmetric encryption algorithm for digital signatures and for public key cryptography. It generates the public key used for the encryption and the private key used for decryption. The algorithm [12]:

1. Generate any two random prime values p and q such that $n = pq$ is equivalent to key bit length. For example, $p=3$ and $q=11$ thus, $n=(3*11)=33\approx1024$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

2. Set $n=pq$ and $\varphi(phi)=(p-1)(q-1)$. That is, $\varphi(phi)=(3-1)(11-1)=20$, and $n=(3*11)=33$.
3. Let e be an integer such that $1<e<\varphi(phi)$ and e and n are coprime. Say $e=7$
4. Set private/secret exponent/key d such that $(d*e) \bmod (\varphi(phi))=1$ That is, $d=3$ since $(3*7) \bmod (20)=1$
5. Public key is (n,e) and private key is (d,p,q). Thus, d,p,q and $\varphi(phi)$ must be kept secret.

Note that n is called modulus, e is called public/encryption exponent, d is called secret/decryption exponent. The larger the key length, the more the security

To encrypt a plaintext message m, the sender obtains the receiver's public key (n,e), represent m such that $1<m<n$, computes the cipher text $c=(m^e) \bmod (n)$, and sends the cipher text c to receiver. When the receiver gets the cipher text c, use the private key (n,d), to decrypt/extract the message $m=(c^d) \bmod (n)$.

1.1.2 Advanced Encryption Standard (AES) Algorithm

AES is a symmetric encryption algorithm established by National Institute of Standards and Technology (NIST) in 2001; based on three Rijndael ciphers of block size 128, with key lengths of 128, 192, and 256-bits. It uses the principle of Substitution-Permutation Networks, and is efficient both in hardware and software. The key size determines the number of repetitive transformations required to convert a plaintext to a cipher text. For 128-bits, 10 repetitions; 192-bits, 12 repetitions; and 256-bits, 14 repetitions are required. In converting plaintext to cipher text, each repetition has four similar but different stages of processing are done, with one stage depending on the key. The reverse of these is used to get back plaintext from cipher text. The high level description of the AES is provided [13] as:

1. *KeyExpansion*: using Rijndael's key schedule, derive cipher key. AES requires for each round, a separate 128-bit round key block and one more.
2. *InitialRound*
   - *AddRoundKey*: combine each byte of the state with a block of the round key using bitwise XOR.
3. *Rounds*
   - *SubBytes*: a non-linear substitution step that replaces each byte with another using a lookup table.
   - *ShiftRows*: a transposition step that shifts rows of the state cyclically in a number of steps.
   - *MixColumns*: a mixing operation which combines the four bytes in each column.
   - *AddRoundKey*
4. *Final Round (no MixColumns*)
   - *SubBytes*
   - *ShiftRows*
   - *AddRoundKey*.

Modern cryptography techniques have also evolved over time to what we presently have. It started as early as the days of electronic mails where digital signature and public-key crypto-systems were used **Invalid source specified.**. Several techniques of encryption have been used to ensure security of digital data, such techniques among several others includes

- Caesar: Affine Ciphers that use MODULUS operation [14], ROT-X that rotates plaintext by X places [15].
- Null Encryption that hides messages within messages using null confuses cryptanalysis [16].
- Polybius Square: ADFGVX which is a fractionating transposition cipher used during World War I [17], Bifid which uses fractionation by combining Polybius and transposition to achieve diffusion [18].
- Polygraphic (Square) Substitution: Two-Square, four-square, five-square [18], fourteen-square substitution [2].

1.1.3 Fourteen-Square Substitution Technique

Any N-square substitution technique uses N-tables containing alphabets, digits, and/or special characters of the keyboard. However, the completeness depends on N. The twelve-square being the most advanced before the fourteen-square proposed in this work uses twelve squares of six 5X5 matrices for alphabets and six 6X7 matrices for digits and special characters. The twelve-square technique has such limitations as "Q" is omitted, not all special characters are contained, does not differentiate between upper and lower cases of alphabets, only one mechanism for key generation, and one level encryption.

The fourteen-square technique which is a modified twelve-square technique uses eight 9X6 matrices for both uppercase and lowercase characters and six 6X7 matrices for special characters. The tables for alphabets are formed with the first containing both upper and lowercase characters and two special characters, and all other follow from the preceding one having either row and/or column manipulations or switches. The tables for digit and special characters also follow the same pattern. To convert a plaintext, if it is an alphabet, the alphabet table k is lookup for the character $loc_k(i, j)$ and the corresponding character at $loc_{k+4}(i, j)$ of table $k+4$ is used to substitute such a character with $k<6$. The same goes for digits and special characters with $k<4$.

Cryptographic techniques used to cipher/encrypt plaintext, also have cryptanalysis techniques used to decipher/decrypt encrypted, these include

- Differential cryptanalysis [19].
- Integral cryptanalysis [20].
- Mod-n Cryptanalysis [21].
- Linear cryptanalysis [22].

Several other cryptanalysis tools are employed to circumvent the security of cryptographic systems. This makes cryptography by itself to be less reliant. Therefore, how can we improve the security of digital communication? Steganography is used in combination with cryptography to improve the security of digital communication since cryptography only scrambles the plaintext and not hides the existence of the data [23, 24, 25].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

1.2 Steganography

Steganography gotten from Greek word, Steganos which means "Covered" and Graphia which means "Writing" Thus, steganography is covered writing. It is the science and art of embedding data in some carrier such that its transmission is not suspected [8]. It may use such techniques as Watermarking to secure copyright/patent information in copies of confidential documents; or Channel Cover to establish secret protocol for secret communication. Steganography does not aim to make the content of communication to be difficult to read but it rather hides the very existence of the communication by using another medium (data/cover object) with redundancy as carrier [26]. Based on cover object, steganography may be classed as follows in [27]:

- Text steganography hides a secret message at n^{th} location of every word of the cover text.
- Image steganography hides a secret message at some bits locations of the cover image such that it is not distorted to attract the Human Visual System (HVS).
- Audio steganography hides secret messages at some bits locations of the audio files such that it is not distorted to attract the Human Auditory System (HAS). Thus, it is more difficult to achieve.
- Video steganography hides secrets messages in the bits locations of either images and/or audio parts of a video file.

And based on keys, steganography may be:

- Pure Steganography uses no key when embedding secret message in cover object.
- Public Key Steganography like public key cryptography uses a public-key for the embedding and private-key used extraction of the secret message.
- Private Key Steganography uses a single key for embedding and extracting secret messages.

In order to perform steganography, the redundant parts of the carrier object used. To achieve this, such methods as

- Moderate Significant Bit replacement which quickly degrades quality of the stego image.
- Transformation Domain Techniques. For example, Discrete Cosine Transform (DCT) similar to Discrete Fourier Transform; and Discrete Wavelet Transform performs the discrete sampling of wavelets.
- Least Significant Bit replacement.

1.2.1 Least Significant Bit (LSB) Image Steganography

LSB, simplest method of steganography relies on the fact that images can be described in terms of pixels; and every pixel is made of either 8-bits or 24-bits, depending on the color intensities. This approach simply replaces the last or last-bits of each byte. Thus, 8-bits pixel is able to store a 1-bit of secret data, and 24-bits pixel is able to store 3-bits in each pixel.

There are several researches on combining cryptography and steganography for a more secured data communication. However, in this paper, two of such researches titled "Dual Layer Security of Data Using LSB Image Steganography Method and AES Encryption Algorithm" [1] and "An Efficient Data Hiding Scheme Using Steganography and Cryptography Technique" [2]were considered for review.

2.0 DESCRIPTION OF SOLUTION

This section provides the description of the proposed solutions to security of data communication as presented in the two papers chosen.

The solution proposed by [2] uses a dual ciphering technique of cryptography that uses fourteen-square substitution of the plaintext, applies RSA encryption algorithm; and then the steganography technique that uses Least Significant Bit planes of the cover image embed the message.

The contribution of this work stems on the fourteen-square substitution technique of ciphering which accommodates all characters of the keyboard. This is an advancement/modification of other techniques like twelve-square. Also, the uniqueness of this work lies in the steganography embedding approach. It used the number of bytes of the cover image to determine the location where to store the cipher text. These locations may be at 6^{th}, 7^{th}, and/or 8^{th} locations storing two bits at a time at two adjacent bits locations. This is called multiple least significant bits replacement.

The solution proposed by [1] is a dual layer security for data communication which employs an encryption/decryption layer which uses AES encryption algorithm with public key of 128 bits; and steganography layer that uses the LSB method. This work at the steganography performs the embedding process of plaintext in the cover image using a simple LSB method replacing the last LSB only if it does not match with the current plaintext bit to be replaced; and the stego image is then encrypted. Therefore, the image transmitted that carries the secret message is actually encrypted thereby, not allowing an eavesdropper to be able to make any meaning of the image nor the data.

The summary of the comparison is provided in table 1.

3.0 PERFORMANCE AND COMPARISON

In the today's world of prevalent technologies, what gives a system its proper place in terms of acceptance is its performance measure. This performance measurement, determined using certain performance metrics and techniques, is usually concerned with a particular aspect of the system under consideration. For this work, the performance of the two chosen proposed solutions of data communication security is based on the performance of the existing technologies used. That is, the performance is implied. It should also be noted that for steganography, in terms of security, its performance depends on the embedding technique used.

For works under consideration, both used LSB technique which has less distortion of the image used. However, [1] used a single bit of a pixel, [2] used two bits of a pixel, which implies more distortion though not too noticeably to the HVS. The former would require more pixels since it uses a single bit on every byte, while the later would require less pixels since it uses two bits.

RSA algorithm used by [2], is known to have timing attack, high power consumption, and hardware and software

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

inefficiency issues thereby considered to be less secured; to complement this, the fourteen-square substitution technique is used. AES algorithm on the other hand used by [1] is known to be efficient in terms of hardware, software and power consumption thereby considered to be highly secured [12].

In [2], it is the plaintext that is encrypted. However, in [1] it is the stego image that is encrypted.

Java and Netbeans Integrated Development Environment (IDE) was used to develop the system in [1] which implies cross platform independence. However, though the programming language or IDE used was not explicitly stated by [2], it was stated that the system has "no support for cross platforms" A comparison is provided in table 1.

Basis	[2]	[1]
Encryption Algorithm	Fourteen-Square and RSA	AES
Encryption Key Length	4000	128
Ratio of Encryption	High	High
Security Vulnerability	High	Low
Data Encrypted	Plaintext	Stego Image
Steganography Bits Locations	Multiple (2-bits per pixel)	Single Bit
Distortion tendency	More	Least
Cross Platform Support	No	Yes
Language and IDE	Not Stated	Java and Netbeans

Table 1: Comparing the Two Researches

4.0 RELATED WORKS

This section describe researches related to our work. It should however be noted that the area of steganography and cryptography has a huge body of literatures. Therefore, we do not claim to have covered all relevant literature.

In [28], the authors described some of the various techniques of steganography and cryptography with focus on AES algorithm, alteration component, random key generation, distortion process, key-based security and static parsing techniques. That is, either of the techniques or algorithm could be used or combined for the encryption purpose before embedding the data.

In [29], the authors described the use of Digital Signatures Algorithm (DSA) and Multiple Least Significant Bit (MLSB) Steganography. That is, having applied DSA for encryption purpose, the MLSB which may randomly replace some Least Significant Bits (LSB) of the selected sample – Typical or Independent MLSB – Which have proven to be more efficient. The benefits of DSA were also provided.

In [30], the authors exploit the basic concepts of steganography and cryptography, providing a comparison of the techniques as used for security of data communication. A description of Symmetric, Asymmetric Key Cryptography, and Hash functions was provided.

In [31], where a true review of few body of researches is provided in tabular form. A brief description of the various techniques used in the considered literatures was provided. The review which covered some of the researches done in the area of steganography and cryptography between year 2012 and 2014 with the aim of introducing the concepts.

In [32], the author described Secret and Public Key Cryptographic and Hash functions such as Hashed Message Authentication Code (HMAC), Message Digest (MD), Secure Hash Algorithm (SHA); and also Discrete Cosine Transform (DCT) and Discrete Wavelet Transform techniques of steganography.

5.0 SUMMARY, CONCLUSION AND RECOMMENDATION

In this review, techniques of steganography and cryptography have been described and a comparison of two relevant solutions employing these techniques have been presented. The solutions provided by the works under consideration have high impact in their unique ways since the goal is to provide security of data communication. For example, using RSA algorithm which is less secured but complimenting this with fourteen-square substitution technique provides the needed security; using AES algorithm which is more secured provides the needed security.

On the strength and weaknesses of the work under consideration, the writer finds [2] to have the tendency of distorting the cover image with large data or more cover images may be required to transmit large amount of data. For an eavesdropper with steganography knowledge observing more images transmitted would suspect such transmission and may intercept and try steganalyze and cryptanalyze the images. Also, considering [1] which encrypts the stego image instead of the plaintext, once an eavesdropper with steganography knowledge intercepts such, it would immediately be considered as having embedded information. Therefore, from this point of view, the writer is of the opinion that [2] provides a better steganography.

A possible future research direction could be to be combine compression technique – The Shannon Fano Algorithm known for its performance [33] - with Fourteen-Square Substitution, AES algorithm and Steganography to enhance security of data communication. This approach should then be compared with existing techniques in terms of size of messages that can be embedded in the cover image and the security provided.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

REFERENCES

[1] S. Satwinder and K. A. Varinder, "Dual Layer Security of Data Using LSB Image Steganography Method and AES Encryption Algorithm," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. Vol.8, no. No.5, pp. 259 - 266, 2015.

[2] K. Mangesh, J. Prasad and K. Ketan, "Efficient Data Hiding Scheme Using Steganography and Cryptography Technique," *International Journal of Scientific and Research Publication*, vol. Volume 5, no. Issue 4, 2015.

[3] M. Sood, W. Manohar and C. Monika, "A Review on Various Data Security Techniques in Wireless Communication System," *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com*, vol. Vol. 3, no. Issue. 2, pp. 883 - 890, 2013.

[4] R. Douglas, "Identity Theft Victim Statistics," Identity Theft and Scam Prevention Services, USA, 2010.

[5] T. B. B. Watch, "National Health Servivces (NHS) Data Breaches," The Big Brother Watch, UK, November, 2014.

[6] E. C. Bank, "Third Report on Card Fraud," ECB, Germany, 2014.

[7] D. Kahn, The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet., New York: The Macmillan Company, 1996.

[8] R. Kefa, "Steganography-The Art of Hiding Data," *Information Technology Journal* , vol. Vol.3, no. Issue.3, pp. 245-269, 2004.

[9] H. G. Liddell, R. Scott, H. S. Jones and R. McKenzie, A Greek–English Lexicon, Oxford University Press, 1843.

[10] S. I. I. R. Room, "History of Encryption," *SANS Institute InfoSec Reading Room*, 2001.

[11] J. Michael, "An Introduction to Symmetric, Asymmetric and Hash Functions," Cryptonomicon, 05 April 2010. [Online]. Available: https://michael555x.wordpress.com/2010/02/05/an-introduction-to-symmetric-asymmetric-and-hash-functions/. [Accessed 30 November 2015].

[12] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique," *International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Vol.2, Issue.4*, pp. 170 - 174, 2013.

[13] A. Biryukov and D. Khovratovich, "Related-key Cryptanalysis of the Full AES-192 and AES-256," 04 12 2009. [Online]. Available: http://eprint.iacr.org/2009/317.pdf. [Accessed 04 12 2015].

[14] M. Kozdron, "Affine Ciphers, Decimation Ciphers, and Modular Arithmetic," Cronell University, 2006. [Online]. Available: https://www.math.cornell.edu/~kozdron/Teaching/Cornell/135Summer06/Handouts/affine.pdf. [Accessed 30 11 2015].

[15] "On the 2ROT13 Encryption Algorithm," 25 09 2004. [Online]. Available: http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf. [Accessed 30 11 2015].

[16] G. Kipper, "Investigator's guide to steganography," CRC Press LLC, 2004.

[17] J. R. Childs, General Solution of the ADFGVX Cipher System, Aegean Park Press, ISBN 0-89412-284-3, 2000.

[18] L. James, "practicalcryptography," 2009. [Online]. Available: http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-bifid-cipher/. [Accessed 30 11 2015].

[19] B. Eli and O. Dunkelman, "Differential Cryptanalysis in Stream Ciphers," in *International Association for Cryptologic Research EuroCrypt2007*, 2007.

[20] Gilles, Piret, Jean-Jacques and Quisquater, "Integral Cryptanalysis on reduced-round Safe++ - A Way Extend The Attack -," in *International Association for Cryptologic Research EuroCrypt2003*, 2003.

[21] K. John, S. Bruce and W. David, "Mod n Cryptanalysis, with Applications Against RC5P and M6," 18 May 2001. [Online]. Available: https://www.schneier.com/paper-mod3.pdf. [Accessed 30 November 2015].

[22] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," 13 July 2001. [Online]. Available: http://www.cs.bgu.ac.il/~beimel/Courses/crypto2001/Matsui.pdf. [Accessed 30 November 2015].

[23] K. B. Ravi and P. Murti, "Data Security and Authentication Using Steganography," *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. Vol. 2, no. Issue.4, pp. 1453 - 1456, 2011.

[24] K. B. Ravi, P. Murti and K. B. Hemanth, "AN AUTHENTICATED BSS METHODOLOGY FOR DATA SECURITY USING STEGANOGRAPHY –JPEG-BMP," *The International Journal of Multimedia & Its Applications (IJMA)* , vol. Vol.4, no. No.2, pp. 39 - 47, 2012.

[25] G. Rupali, S. Priyanka, B. Vaibhavi and P. N. Sawantdesai, "Data Hiding Using Steganography For Network Security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. Vol.3, no. Issue.2, pp. 5740 - 5743, 2014.

[26] B. Pria and S. Roopali, "A New Approach of Data Hiding in Images using Cryptography and Steganography," *International Journal of Computer Applications (0975 – 8887)*, vol. Vol.58, no. No.18, 2012.

[27] R. B. Abhilasha and A. B. Dhembhare, "An Efficient and Secure Data Hiding Technique - Steganography," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. Vol.3, no. Issue.2, pp. 941 - 949, 2015.

[28] M. V. Wajgade, G. Haryana and S. Kumar, "Stegocrypto - A Review Of Steganography Techniques Using Cryptography," *International Journal of Computer Science & Engineering Technology (IJCSET)*, pp. 423 - 426, 2013.

[29] S. Kaur and K. Harleen, "Data Hiding Using Cryptography: A Review," *International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6*, pp. 911 - 914, 2014.

[30] P. Kumar and V. K. Sharma, "Information Security Based on Steganography & Cryptography Techniques: A Review," *International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 10*, pp. 246 - 250, 2014.

[31] G. Latika and G. Yogita, "A Review of Steganography Research and Development," *International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 4*, pp. 871 - 874, 2015.

[32] M. Aarti, "Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation," *International Research Journal of Engineering and Technology (IRJET). Volume: 02 Issue: 01*, pp. 397 - 403, 2015.

[33] S. R. Kodituwakku and U. S. Amarasinghe, "COMPARISON OF LOSSLESS DATA COMPRESSION ALGORITHMS FOR TEXT DATA," *Indian Journal of Computer Science and Engineering, Vol.1, No.4*, pp. 416 - 425, 2010.

[34] R. L. Rivest, A. Shamir and L. Adleman, "A Method For Obtaining Digital SIgnatures and Public-Key Cryptosystems," *Communications of the ACM (Association for Computing Machinery)*, vol. 21, no. 2, p. 120–126, 1978.