Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Implementation of Data Security by using Both Cryptography and Steganography Algorithms on FPGA

Shaik Mahammad Rasheed*
M. Tech, PG Scholor, Department of Computer Science & Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India

Abstract*— *In today's world, security is done through networks which are used to transmit confidential information. Security is demanding in a wide range of applications. Cryptographic algorithms play an important role for providing security to the data against malicious attacks. RSA algorithm is widely used in the popular implementations of the Public Key Infrastructure. In asymmetric key cryptography, which is also known as Public Key cryptography, two different keys (key pairs are formed with these two keys) are used. One key is used for encryption & only that corresponding key must be used for decryption. No other key can decrypt the message –not even the original (i.e. the first) key which is used for encryption. The main use of this scheme is, every communicating party needs only a key pair for communicating with any number of other communicating parties. If someone can obtain a key pair, then he/she can communicate with anyone else. In this paper, we have done implementation of RSA algorithm by using two public key pairs and by using some mathematical logic rather than sending the value directly as a public key. If an attacker has an opportunity of getting the value, then he/she can directly find the value and can decrypt the message.

Keywords*— *Cryptography, Encryption, Decryption, Public Key, Private Key, FPGA, RSA Algorithm, LSB, Steganography.

I. INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. In traditional (symmetric-key) cryptography, the sender and receiver of a message know and use the same secret key. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key.

Because all keys in a secret-key (symmetric-key) cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management. To solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integer factorization and discrete logarithm problems).Although it is easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one (or more) secret keys between the sender and receiver. In practice, only a hash of the message is typically encrypted for signature verification purposes. Public-key cryptography is a fundamental, important, and widely used technology. It is an approach used by many cryptographic algorithms and cryptosystems.

II. CRYPTOGRAPHY AND TYPES

The process of transposition and substitution of the characters to hide and retrieve the data is done by Cryptography. We call Encryption at the sender side which is shown in Figure.1 and Decryption at the receiver side which is shown in Figure.2. We can encrypt and decrypt the data by using various keys. Keys are special digital functions or methods which converts plain text into inscribe format (cipher text) and it's vice versa. Every element of the network has two keys namely personal or private key that is known only to a particular person and public key is known by all persons in the network. Cryptography is of two types.

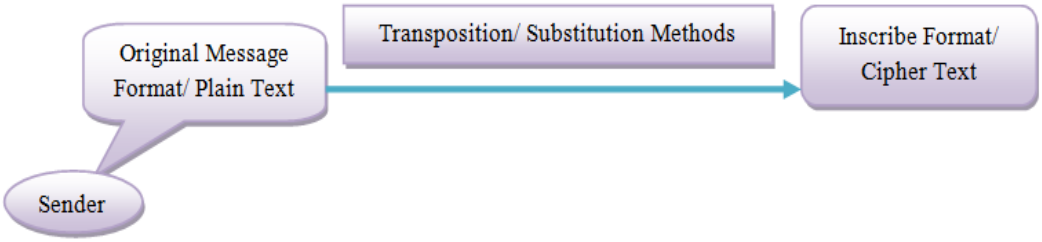


Figure 1: Encryption Process

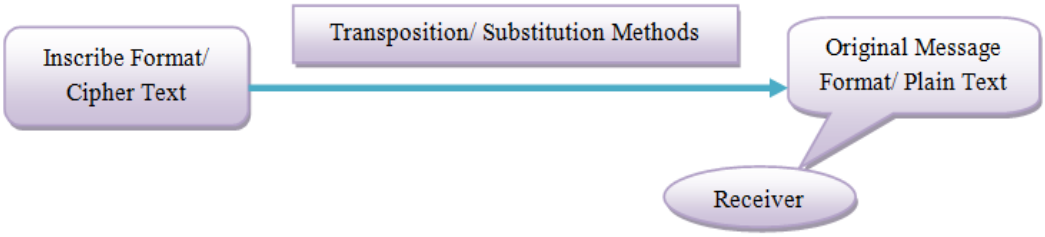


Figure 2: Decryption Process

A. Same key cryptography or Private Key cryptography

In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recover the plaintext from cipher text and vice versa, so this type of cryptography is also known as symmetric encryption and decryption. Figure.3 is showing the whole process of encryption and decryption which is carried out through receiver's private key. Through this cryptography form, it is obvious that the secret key must be known to both the sender and the receiver that is why it is known as private key cryptography. Transmitting the secret key on insecure network can also destroy the security.

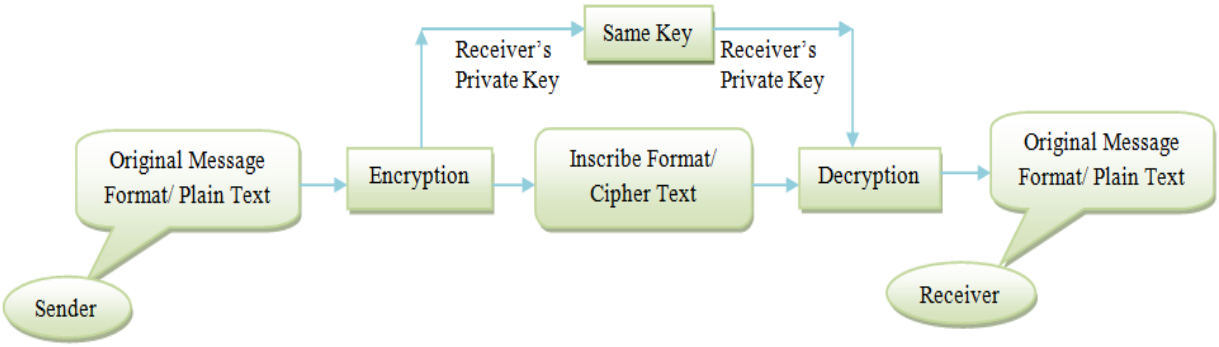


Figure 3: Same Key Cryptography

B. Different key cryptography or Public Key cryptography

In this type of cryptography, the receiver and sender apply different keys to encrypt and decrypt the message or recover the plaintext from cipher text and it's vice versa. This type of cryptography is also known as asymmetric encryption and decryption. Figure.4 is showing the whole process where receiver's public key is used for encryption and receiver's private key is used for decryption. In public key cryptography, each user or the workstation take part in the communication, has a pair of keys, a public key and a private key and a set of operations associated with the keys to do the cryptographic operations. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online.

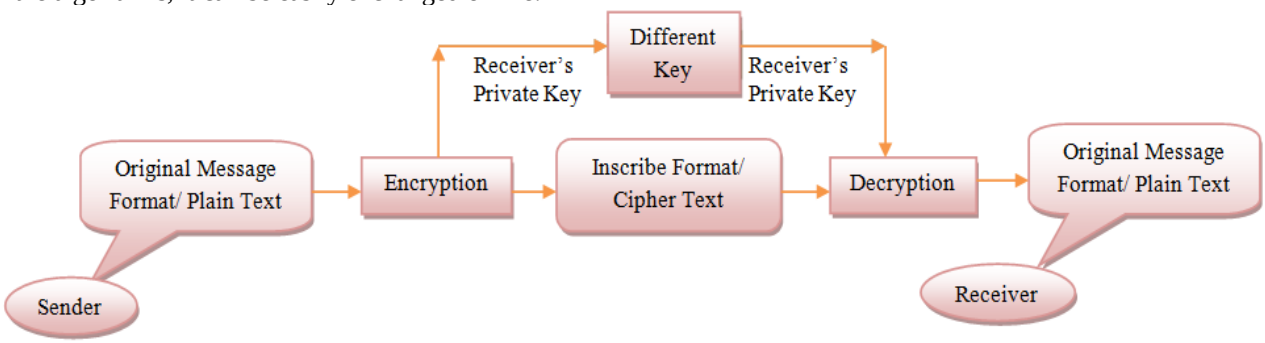


Figure 4: Different Key Cryptography

III. THE RSA ALGORITHM AND ITS MATHEMATICAL FOUNDATION

A. The Mathematical Foundation for RSA Algorithm

The RSA digital signature has precise mathematical foundations, which are as follows [1]:

***Theorem* 1:** (Fundamental theorem of mathematics) any positive integer *a* can be denoted as ai=P1.....Pn, where *P*1 > *P*2 > *P*3 … > *PT* are all prime numbers, *ai* > 0.

Theorem 2: (Euclid theorem) any two integers a and b have the greatest common factor d, in which d can be expressed as the linear combination of a and b with integer coefficient, namely *s, t* ∈ *Z*, which satisfies *d = sa + tb*.

Theorem 3: (Fermat theorem) If *p* is a prime number, then for any positive integer a that prime to *p*, *a (p-1)* ≡1 (mod *p*).

Definition 1 (Euler function (*n*)) When *n* = 1, ϕ (1) = 1, when *n* > 1, the value of ϕ (*n*) is the amount of positive integer that less than *n* and prime to *n*.

Theorem 4: If *p* and *q* are all prime numbers and *p*≠ *q*, then ϕ (*pq*) =ϕ (*p*)ϕ (*q*) = (*p* −1)(*q* −1).

Theorem 5: **(**Euler theorem) If integer *a* is co prime to integer n, then aᵠ(n) ≡ (mod *m*). entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

Above theorem have the following 3 deductions:

1. If p is prime number and *n = p*, then *a(p-1)* ≡ 1(mod *p*), namely the Fermat theorem.
2. *a* ϕ *(n+1)* ≡ a (mod *p*).
3. If n = *pq*, *p* and *q* are prime numbers and p≠ *q*, for 0<*m*<*n*, if (*m, n*) = 1, then (n) 1 *m m* ϕ + ≡ (mod *n*), namely m (p-1)(q-1)+1 ≡ (mod *n*).

Above five theorems will be used in the feasibility proof of RSA digital signature algorithm in the following section.

***Theorem 6*:** If *p* and *q* are prime numbers and *p*≠ *q*, *rm* ≡ 1 (mod (*p* − 1)(*q* − 1)) , *a* is any positive integer, *b* ≡ *am* mod *pq*, *c* ≡ *br* mod *pq*, then *c* ≡ *a* mod *pq*.

B. RSA Key Generation Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1)(q-1) [Theorem 4].
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1. [Theorem 2].
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi). [Theorem 6].
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.
   - n is known as the *modulus*.
   - e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
   - d is known as the *secret exponent* or *decryption exponent*.

C. Encryption Algorithm

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m
3. Computes the cipher text c = me mod n.
4. Sends the cipher text c to B.

D. Decryption Algorithm

Recipient B does the following:-

1. Uses this private key (n, d) to compute m= cd mod n.
2. Extracts the plaintext from the message representative m.

One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The RSA scheme has become the most widely accepted and implemented approach to public key encryption. RSA is named after its inventors Rivest, Shamir, and Adleman.RSA is a block cipher in which the plaintext and cipher text are integers between 0 and n- 1 for some n. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

C = Memod n

M = Cdmod n = (Me)dmod n = Medmod nBoth sender and receiver must know the values of n and e, and only the receiver knows the value of d. This is a public key encryption algorithm with a public key of KU = {e,n} and a private key of KR = {d,n}.For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of *e, d, n* such that *Med*= M mod *n* for all M<*n.*
2. It is relatively easy to calculate *Me* and *Cd* for all values of M <*n.*

Steps:

- Begin by selecting two prime numbers, *p* and *q*, and calculating their product *n*, which is the modulus for encryption and decryption.
- Next, we need the quantity φ*(n) re*ferred to as the Euler quotient of *n*, which is the number of positive integers less than *n* and relatively prime to *n.*

- Then select an integer *e* that is relatively prime to φ*(n) (i.*e., the greatest common divisor of *e* and φ*(n)* is 1).
- Select two numbers a and b such that b=ae
- Using this numbers formulate two public key {b,n},{a}
- Finally, calculate d as the multiplicative inverse of e(which is public key in normal RSA), modulo φ(n). But to calculate it let the receiver choose any positive natural number and multiply it with a then add b, divide the result by a and finally subtract the chosen value then the receiver has e. then calculate d as usual.
- It can be shown that d and e have the desired properties.
- Suppose that user A has published its public key and that user B wishes to send the message M to A.
- Then B calculates C = Mb/a(mod n) and transmits C.
- On receipt of this cipher text, user A decrypts by calculating M = Cd(mod n).

IV. STEGANOGRAPHY

Steganography is the method of concealing a secret message at intervals in such a way that somebody cannot understand the presence or contents of the hidden message. Steganography can hide the message thus there's no data of the existence of the message within the place. The term Steganography is forked from the Greek words "stegos" that means "Cover" and "grafia" that means "writing" process it as "covered writing". Generally, there are two forms of information concealing techniques mistreatment images: abstraction and frequency domain. The abstraction domain is predicated on embedding message within the least significant bit (LSB) of image picture element. The fundamental LSB methodology is straightforward for implementation. However it's weak against some attacks like low-pass filtering and compression. The frequency domain embeds the messages within the frequency coefficients of pictures. These concealing ways overcome the issues found within the abstraction domain. Steganalysis is nothing however the method of police works hidden information which is crested mistreatment Steganography. Steganalysis detects Stego-images by analyzing varied image options between Stego-images and cover-images. In recent researches, various Steganography techniques supported genetic algorithms. Currently the Steganography techniques are developed on varied FPGA hardware. Field Programmable Gate Array i.e. FPGA, provides the reconfigurability similarly because the hardiness for the image process. Due to the utilization of FPGA we will develop another approach supported AN embedded FPGA system for image processing. Field Programmable Gate Array (FPGA) is wide utilized in embedded applications like automotive, communications, industrial automation, control, medical imaging etc. And while not requiring hardware change out, the uses of FPGA kind devices will expand the merchandise life by change information stream files. FPGAs have capability to hold a complete system on one chip additionally it permits in-platform testing and debugging of the system. Moreover, it offers the chance of utilizing hardware/software co-design to develop a high performance system for various applications by incorporating processors.

A. Proposed Steganography Method

Message coding on a picture may be divided into 2 components, one portion is knowledge activity and the other one is reversible knowledge activity. In knowledge activity half there's a digital image within which we have a tendency to write secret message by removing LSB of image pel and add our secret message on corresponding LSB position, then the output image is termed Stego image. For retrieving the key message program splits the image into its channels and applies the inverse lifting theme to every channel to the extent such as by the user. Once the transformation is completed, the program retrieves the message out of the pixels of the duvet image. Different streams of digital media may be used as a canopy stream for a secret message. Steganography is that art of writing secret message in order that solely the sender and therefore the supposed recipient are responsive to the hidden message. A prospering info activity ought to end in the extraction of the hide knowledge from the image with high degree of knowledge integrity. Current trends favour exploitation digital image files because the cowl files to cover another digital file that contains the key message or info.

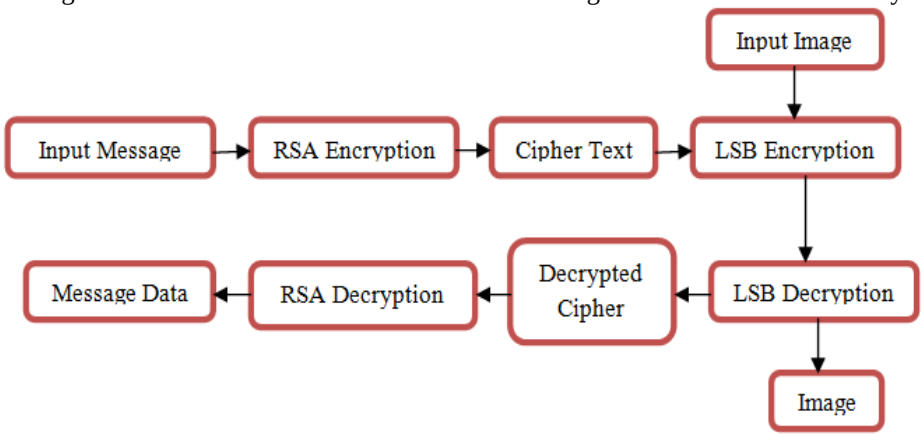


Figure 5: Block Diagram of Invisible Stenography

B. Header File Creation

To create the header file for Cover image and secret Message by using GUI in Matlab software.

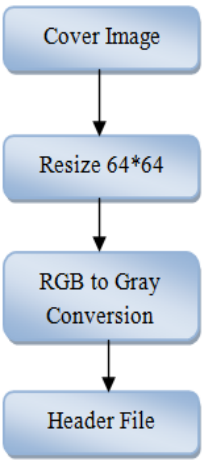


Figure 6: Header File conversion by using Matlab software

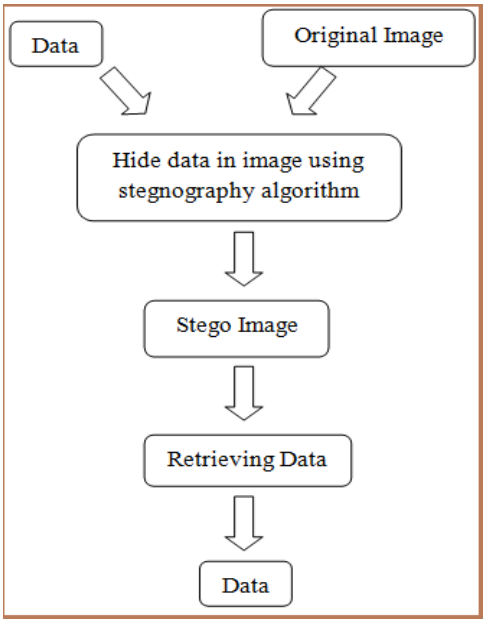
C. Least Significant Bit (LSB) Technique

Fig shows the 1-bit LSB. In Fig. 1, the picture element price of the quilt image is 141(10001101)2 and therefore the secret knowledge is zero. It applies to LSB-1 that the modified picture element price of the quilt is 140(10001100)2. LSB will store 1-bit in every picture element. If the quilt image size is 64 x 64 picture element image, it will therefore store a complete quantity of bytes of embedded knowledge.

1	0	0	0	1	1	0	1
						Pixel	Value
					0	0	1
						Secret	Data
1	0	0	0	1	1	0	0
					Change	Pixel	Value

Figure 7: Example of LSB.

Proposed methodology supported LSB technique; we have a tendency to propose a replacement watermarking algorithmic rule. Most of researchers have planned the primary LSB and therefore the third and forth LSB for activity the information however our planned watermarking algorithmic rule is victimization the third and fourth LSB for activity the information And victimization the RGB watermark image embedding in blue element of original image attributable to less sensitivity. This can be attributable to the protection reason. So, nobody can expect that the hidden information within the third and therefore the forth LSB. Fig. 2 shows the framework of the planned methodology. First, we have a tendency to choose the image that may be a colour image and that we can transfer the information to binary worth when writing it. Then, we have a tendency to hide the information within the image victimization the planned algorithmic rule. Fig. three shows the embedding algorithmic rule in VLSI.



V. CONCLUSION

In this paper an algorithm is proposed for RSA a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation. These two public keys are sent separately, this makes the attacker not to

get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security. This paper has also mentioned some Steganography techniques that space unit planned on field programmable gate array. Mainly the spatial domain and work domain techniques space unit taken into thought. Once inquiring the synthesis results for individual techniques, we've discovered that FPGA is that the simplest resolution for the economical image method. Also by correct hardware style development we tend to square measure ready to improve the results for spatial domain i.e. LSB technique. Also future work is going to be done on improvement of developed hardware architectures with connection power, timing, and area.

REFERENCES

[1] "An Enhanced Rsa Algorithm for Low Computational Devices" by Maheswari Losetti, Kanaka Raju Gariga in International Journal of Advanced Research and Innovations Vol.1, Issue .2, pp 114-118.

[2] "Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption" by Kuldeep Singh, Rajesh Verma, Ritika Chehal in International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012, pp 204-206.

[3] "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" by Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, pp 134-138.

[4] "Cryptanalysis of short RSA secret exponents", by MJ Wiener. (1990), IEEE Transactions on Information Theory, Vol 36, No 3, pp 553-558.

[5] "RSA-Based Undeniable Signatures", by R Gennaro. (2000), Journal of Cryptology, Vol 13, No. 4, pp 397-416.

[6] "Signature schemes based on the strong RSA assumption", by R Cramer, V Shoup. (2008), ACM Transactions on Information and System Security, Vol 3, No 3, pp 161-185.

[7] "Robust and Efficient Sharing of RSA Functions", Gennaro. (2008), Journal of Cryptology, Vol 13, No 2, pp 273-300.

[8] "Efficient generation of shared RSA keys", D Boneh, M Franklin. (2001), Journal of the ACM, Vol 48, No. 4, pp 702-722.

[9] Rivest, R.; A. Shamir; L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 (2): 120–126, doi: 10.1145/359340.359342, 1977.

[10] B. Schneier, Applied cryptography, second edition, NY: John Wiley & Sons, Inc., 1996. William Stallings, Cryptography and Network Security, Pearson Education, Fourth Edition.

[11] Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publishing Company Limited.

[12] "Comparative Analysis of AES and RC4 Algorithms for Better Utilization",by Nidhi Singhal, J.P.S.Raina, International Journal of Computer

[13] Trends and Technology- July to Aug Issue 2011.

[14] "Reverse Encryption Algorithm: A Technique for Encryption & Decryption" , Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 201 2013,pp 90-95.

[15] "Cryptography and its two Implementation Approaches" by Gagandeep shahi, Charanjit singh , International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013,PP 668-672.

