INTERNATIONAL JOURNAL OF ADVANCED STUDIES IN COMPUTER SCIENCE AND ENGINEERING
IJASCSE VOLUME 5, ISSUE 2, 2016
02/29/2016

Randomized passcode generation for Scan based hybrid symmetric cryptosystem

Shivanand S. Gornale
P G Department of Computer. Science, Rani Chennamma University,Belagavi, Karnataka,India.

Nuthan A.C
Department of ECE, GMIT, Bharathinagara, Karnataka, India.
Research Scholar,Jain University,Bangalore.

***Abstract*—**Securing sensitive information has huge prominence and its of greatest challenge for any organization. This work proposes one such attempt of network security. In this proposed technique sensitive data is encrypted using multiple data encryption techniques. Here data in text form is handled as an image and hence exclusive image encryption techniques are also applied to strengthen the architecture. So there is an hybridization of data and image enciphering techniques. Data encryption techniques like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are used to convert plaintext into ciphertext. This ciphertext is scrambled with respect to position using scan based image encryption techniques. In order to have greater security, a randomization is included effectively.

***Index Terms* -** Hybrid crypto-system**,** AES, DES, Random Number Generator (RNG), LFSR.

I. INTRODUCTION

Primary function of the information security is to provide confidentiality for data being stored or transmitted [1]. Information security is of two types namely computer security (Concerns about the data stored in computer) and network security (Concerns about the data being transmitted). Cryptography, Steganography etc is some of the techniques to handle information security.

In cryptography understandable text called plaintext (text, image, audio, and video) is converted to non understandable text called ciphertext using encryption algorithm and a key [2]. The revert conversion of ciphertext into plaintext is called decryption.

Encryption may be Symmetric Key or A Symmetric Key encryption. Symmetric Key Cryptography uses same key for both encryption and decryption but asymmetric Key Cryptography uses a key for encryption and different key for decryption. Thus there is no sharing of private information between sender and receiver in asymmetric key encryption.

Symmetric-key ciphers are of two types, Block ciphers and Stream ciphers. Block ciphers take as input a block of plaintext and a key, and the output is a block of cipher text of the same size. The stream cipher encrypts stream of data.

The crypto systems which are in use are static i.e. only one of the standard algorithms is used at a time making the system easy to hack. To make the architecture more robust multiple algorithms are used [3, 4 and 5].

II. PROBLEM FORMULATION

Paper [3] presents an implementation of three standard cryptography algorithms. But Paper [4,5] implements multiple algorithms on universal architecture and there is switching among the algorithms at random times. This architure proved more secured due to use of random switching among the standard algorithms.

The advantage of asymmetric Key cryptography over symmetric key cryptography is the sender is avoided to share secret key with the receiver. In Paper [5] there is a hybridisation of Symmetric and asymmetric key encryption. In paper [4,5] the secret text was handled directly as data. As an enhancement to the previous work here the text is handled as an image so that encryption techniques which are exclusive for image encryption can be used for the data encryption. Since the data is arranged as frame (image like) the image encryption techniques [8, 9, and 10] like scan based transposition image techniques is used to encrypt the data.

Further multiple data encryption standards are used to encrypt the data thereby making the architecture much more robust. In paper [4, 5] the LFSR based random number generator was used to bring the randomness in choosing the multiple algorithms alternatively. But as an enhancement to this paper [6] recommends integration of LFSR based

Passcode generation block [6] block in the architecture to generates 16-bit passcode which makes the architecture flexible in choosing type of wave filters, level of decomposition, order of detailed regions for embedding using triple stegging.

In order to enhance the randomness further, 4 types of random generators are used in this paper instead of single LFSR technique [6]. A 2-bit seed is used to select one of the random number generators at time of data transaction. Hence there is randomness in choosing the random number generator [7].This paper uses the same passcode generation block as in [7], but here the purpose of using the random number is to select between the encryption standard, type of scan type to be performed for scrambled transposition of data elements. Figure 1 shows the schematic diagram of the work.

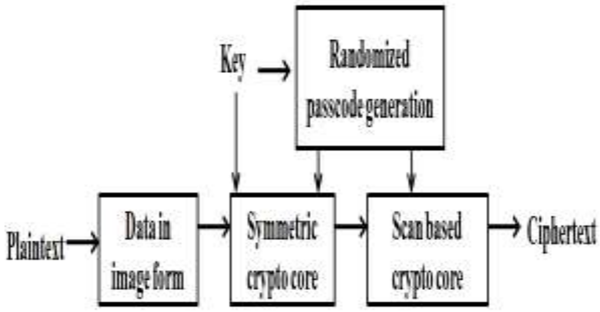


Figure 1 :Schematic diagram of the work

III. DATA ENCRYPTION ALGORITHM [4]

DES encrypts a block of 64-bit plaintext into 64-bit cipher text using 64-bit secret key. Block diagram of the DES algorithm is shown in the Figure 2.

DES was adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46)[11].

DES Encryption process has two functions

1. Processing the plaintext
   The processing of plaintext proceeds in three phases.
   a. Conversion of Plain text into permuted input
   b. Production of preoutput using Feistel cipher structure
   c. Conversion of preoutput to cipher text

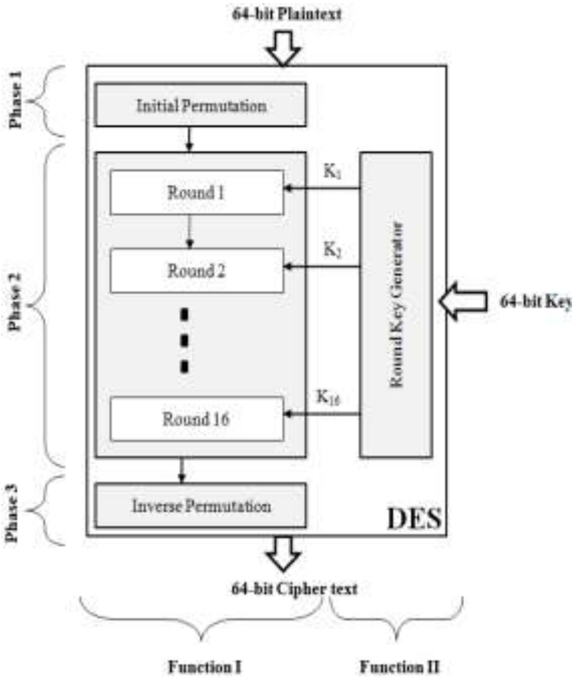


Figure 2 :DES encryption

2. Round-Key generation

DES takes 64-bit key as input. Among 64-bit key only 56 bits are effective and used directly by the algorithm. The other 8 bits may be used for error detection or set arbitrarily or can be ignored [12].

The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each byte [11]. The round-key generator creates sixteen 48-bit round/sub keys out of a 56-bit cipher key.

The operation is summarized in the figure 3. This has two stages:
1. Parity drop
2. Key expansion

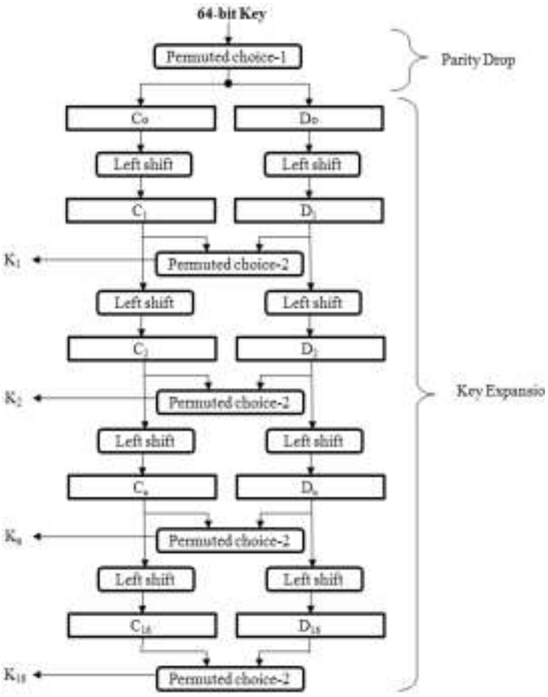


Figure 3: Round-key generator

IV. ADVANCED ENCRYPTION ALGORITHM

National Institute of Standards and Technology (NIST) selected Rijndael (Developed by Dr. Vincent Rijmen and Dr. Joan Daemen) as the proposed AES algorithm and published a final standard FIPS PUB 197 in November of 2001[13]. Figure 4 shows the block diagram of the AES algorithm.

The algorithm processes data block of size 128 bits using a cipher key of length 128, 192 and 256 bits. Each data block is a 4×4 matrix called the state on which the basic operations of AES algorithm are performed. AES does not use a Feistel network but process the entire data block in parallel during each round using substitutions and permutation.

AES encryption/decryption process has two functions

1. Round-Key generation
2. Processing the plaintext/cipher text

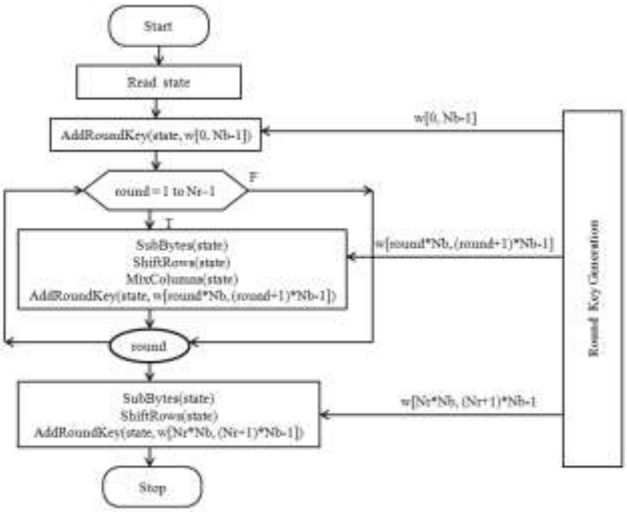


Figure 4 :AES encryption

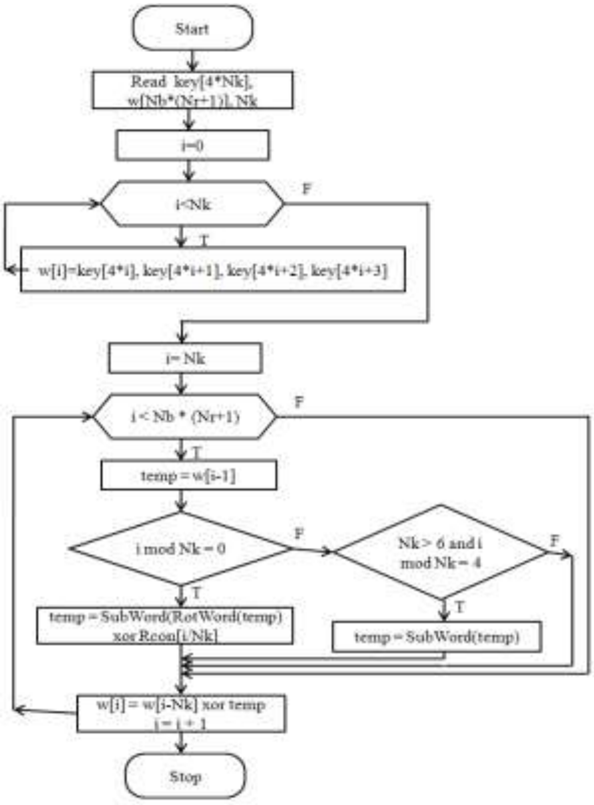


Figure 5 : Generation of subkeys for AES

Figure 5 shows the steps to be done to generate round keys. After commencing the first round of key addition, a round function consisting of four distinctive byte oriented transformation are performed.

They are:

- Substitute bytes: Byte by byte substitution of the block using S-box (table)
- Shift rows: Circular shift or a simple permutation operation is performed.
- Mix columns: Each column of the block multiplied with a constant matrix, the result obtained is substituted back to the block which makes use of arithmetic over GF (Galois field).
- Add round key: Simple bitwise XOR operation between the current block and expanded key.

These transformations are applied to the data block (i.e. state).The decryption process of AES is the converse of each transmutation explained above except for the Mix column iteration. The structural resemblance for both encryption and decryption makes hardware implementations easier [14].

V. RANDOM NUMBER GENERATOR[7]

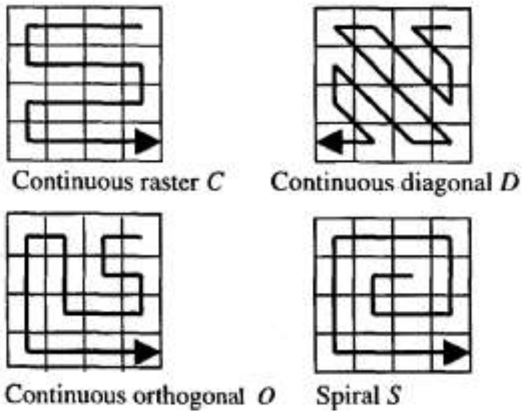
Random numbers are used in a data encryption, circuit testing, system simulation etc. The hardware-based RNGs are faster and robust than software-based methods. This paper uses 4 random number generators. All these are based on some mathematical equation. Table 1 summarizes the 4 RNGs used in this paper with corresponding mathematical equations

Table 1: RNGs with mathematical equations

RNG	Equation
Linear Feedback Shift Register (LFSR) [16]	$x_n = a_1 \bullet x_{n-1} \oplus a_2 \bullet x_{n-2} \oplus$------$\oplus a_m \bullet x_{n-m}$
Chaos-based random number generator [17, 18,19,20, 21]	x(i+ 1) =μx(i)(1-x(i)) Where μ=3.9.
BB (Brahmagupta-Bhaskara) equation based random number generator [23]	$n(x^2)_p \mid_{p+1} = (y^2)_p$ Where p is odd prime
Compound Sine and Cosine Chaotic Maps [24]	$x_{n+1} = \cos(ax_n) + \sin(bx_n)$

VI. SCAN BASED IMAGE ENCRYPTION

Paper [8] proposed a scan based image encryption. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are reverses of transformations 0, 2, 4, 6, respectively [8, 9].The basic scan patterns are shown in the figure 6.



Continuous raster *C* Continuous diagonal *D*

Continuous orthogonal *O* Spiral *S*

Figure 6: Basic scan patterns

VII. PROPOSED SYSTEM AND EXECUTION

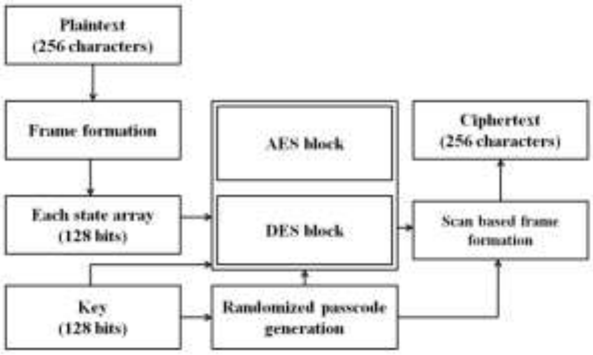


Figure 7: General Block diagram of proposed method

The bird view of the proposed method is shown in the Figure 7. The proposed method has done in four stages:

Stage 1: Generation of frame

In this technique a block of 2048 bits (256 ASCII characters) are encrypted at a time. 2048 bits are subdivided into 16 128-bits data stream. Each 128-bits are converted into a 'state' (4x4 matrix each element of 8 bits size). These 16 states are arranged into 4x4 matrixes to form a frame. Hence a frame is matrix of size 16x16 and each element is of size 8-bits.

Stage-2: Randomised Passcode generation

The first 2-bits of 128-bits AES key is used to select one of the 4 types of random number generators. Table 2 gives the selection of type of random number generation. The next 4-bits of 128-bits AES key is used as seed for the 4-bit random generator. This random number generator produces a 104-bits passcode. This 104-bits passcode is used to choose type of data encryption (AES/DES), type of scan, direction of scan performed in each 'state' and frame. Usage of 104-bits passcode is as follows:

- First 5-bits are used to place the 16 states in a frame based on scan pattern.
    - 1st-2nd bits: Used to select the type of scan. The mode of selection is summarized in Table 3.Example- if the 2 bits are '01' then 16 blocks ar e arranged diagonally scaned patter in a frame.
    - 3rd-4th bits: used to select the startpoint from the scan needs to be started. The Table 4 summarises the location of the startpoints. Example- If 2 bits are '11' then the scan starts from the south –east corner pixel.
    - 5th bit- if this bit is '1' ten the scan happens in clockwise fashion .if it is zero
- Next 96- bits of passcode:
    - 96 bits are grouped into 16 6-bit numbers. Each 6 bits is responsible in selecting the type of algorithm (AES/DES) and type of scan and direction of scan performed in each 'state'.
    - 1st bit: If this bit is '1' then AES is performed on 128-bit state along with 128 bit key. If this bit is '0' then DES is performed. Next 5 bits are used to select the type of scan, location of scan startpoint and direction of propagation of the scan in similarity with that of frame.
- This process is done to all 16 states.

Table 2: Mode of random number generation

First 2 bits of 128 bit AES key	Random Number generation type
00	Linear Feedback Shift Register (LFSR)
01	Chaos-based random number generator
10	BB equation based random number generator
11	Compound Sine and Cosine Chaotic Maps

Table 3: Mode of scan selection

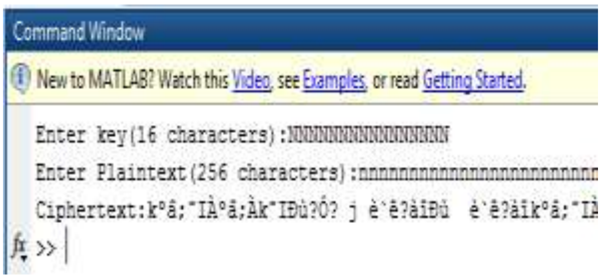
1st -2nd bit pascode	Scan Type
00	Continuous Raster
01	Continuous Diagonal
10	Continuous Orthogonal
11	Continuous Spiral

Table 4: Location of start points.

3rd-4th bit	Location of start points
00	North east corner
01	North west corner
10	South west corner
11	South east corner

Stage-3: Encryption block

In this stage, each 128 bits of state is encrypted using AES or DES block. Since DES operates on 64 bits of the data and state is of 128 bits, DES is operated twice taking 2 columns of state at a time. First 64 bits of AES key is used as the key for first columns of state and next 64-bits of AES key is used for 3rd and 4th columns of state.


Command Window
New to MATLAB? Watch this Video, see Examples, or read Getting Started.

```
Enter key(16 characters):NNNNNNNNNNNNNNNN
Enter Plaintext(256 characters):nnnnnnnnnnnnnnnnnnnnnnnnn
Ciphertext:k°â;¨IÀ°â;Àk¨IÐù?Ó? j è`ê?àiÐù  è`ê?àìk°â;¨IÀ
>>
```

Figure 8: Output of the proposed work

Stage-4: Reformation of frame

Each encrypted state is further scrambled using Scan pattern transposition in accordance with 16 6-bit passcode. And then all the 16 states are arranged using scan pattern in accordance with the first 5 bits passcode.

The output the present architecture is as shown in the Figure 8.

VIII. CONCLUSIONS

The concept of universal coding (use of multiple algorithms) with random switching is implemented. So instead of using single algorithm the usage of multiple algorithms helps in increasing the security. Any number of cryptographic standards can be implemented. Architecture inherits the statistical and other advantages of AES and DES. Passcode will be architecture based rather than the user based making the architecture more robust against the eavesdropping. The architecture is dynamic since there is option in choosing type of algorithm, scan pattern, and random number generator. The flexibility in architecture provides variety in implementation to attain desired robustness and fault tolerance. In this the passcode generation block is made dynamic by using multiple methods of random generation like chaotic based, logistic based etc.

The same architecture can be implemented on FPGA and ASIC in future to attain the advantages of hardware implementation.

REFERENCES

[1] Committee on National Security Systems: *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, 26 April 2010.

[2] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography", Sapienza University of Rome, Italy.2010.

[3] YadollahEslami, Member, IEEE, Ali Sheikholeslami, Senior Member, IEEE, P. Glenn Gulak, Senior Member, IEEE, Shoichi Masui, Member, IEEE, and Kenji Mukaida, "An Area-Efficient Universal Cryptography Processor for Smart Cards", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 14, PP. 43-56, January 2006.

[4]A.C.Nuthan, M.S.Naveen Kumar, Shivanand S Gornale and Ravikanth G Biradar, "Development of Randomized Hybrid cryptosytem", International Journal of ICT and Management, ISSN : 2026-6839, Vol.- I Issue- I November 2012

[5] A.C.Nuthan, M.S.Naveen Kumar, Shivanand S Gornale and Basavanna, "Development of Randomized Hybrid cryptosytem using Public and Private Keys", Lecture notes in electrical engineering 248, *Emerging Research in Electronics, Computer Science and Technology*, Springer India, 2014.

[6] Shivanand S Gornale and A.C.Nuthan, "Self generative passcode for Triple-Stegging using Discrete Wavelet Transform (DWT) and Elliptic Curve Cryptography (ECC)" , *Volume 2, Issue 4,ISSN 2278-6856, International Journal of Emerging Trends & Technology in Computer Science [IJETTCS]*, India, 2015.

[7]Shivanand S Gornale and A.C.Nuthan, "Randomized passcode for Triple-Stegging using DWT and ECC" , *Volume 12, Issue 6,ISSN 1694-0814, International Journal of Computer Science issues [IJCSI]*, India, 2015.

[8]Chao Shen Chen and Rong Jian Chen "Image encryption and decryption using SCAN methodology," *Proc. PDCAT*, 2006.

[9]S.S. Maniccam and N.G.Bourbakis, "Image and video encryption using SCAN patterns," *Pattern Recognition, vol.*37, pp.725-737, 2004.

[10]Panduranga H.T, Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", International Journal on Computer Science and Engineering, pages 297-300, Vol. 02, No. 02, 2010,.

[11] Federal Information Processing Standards Publication, FIPS PUB 46-3, Reaffirmed 1999 October 25

[12] William Stallings, *Cryptography and Network Security Principles and Practices*,Fourth Edition, Printice Hall, 2005.

[13]*Advanced Encryption Standard (AES)*,FIPS 197, November 26, 2001.

[14]AshwiniM.Deshpande,MangeshS.DeshpandeandDevendraN.Kayatanavar,"FPGA implementation of AES Encryption and Decryption",*International conference on "control, automation, communication and energy conservation"Proc.CACEC'09,2009, paper 1, p. 1-6.*

[15] P. H. Bardell, W. H. McAnney and J. Savir, "Build-in Test for VLSI: Pseudo-random Techniques", John Wiley and Sons, 1987.

[16] P. Alfke, "Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators", Xilinx Application Note, 1995.

[17] G. Chen, Y. Mao, CK Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol. 2 1, pp. 749-761,2004.

[18] K. Wong, B. Kwok, and W. Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Physics Letters A, Vol. 372, pp. 2645-2652, 2008.

[19] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, Vol. 89, pp. 480-491, 2009.

[20] X. Ma, C. Fu, W. Lei, S. Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", International Journal of Advancements in Computing Technology, Vol. 3, No. 5, 20 1 1.

[21] K. Gupta, S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Jour. of Information Security, pp. 139-150,2011.

[22] F . Huang, Y . Feng, "Security analysis o f image encryption based on two-dimensional chaotic maps and improved algorithm", Front. Electr. Electron. Eng. China, Vol. 4, No. 1, pp. 5-9,2009.

[23] N.Rama Murthy and .N.S.Swamy,"Cryptographic Applications of Brahmagupta Bhaskara Equation", IEEE Transactions on circuitS-I, Regular papers, voL53, July2006, pp.I565-I571.

[24] S. Maksuanpan, T. Veerawadtanapong, w. San-Urn, "Robust Digital Image Cryptosystem Based on Nonlinear Dynamics of Compound Sine and Cosine Chaotic Maps for Private Data Protection", ISBN 978-89-968650-1-8, ICACT2013, IEEE,2013.

[25] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", *IEEE International Symposium on Information Theory*, Ronneby, Sweden, 1976.

[26] Konheim, *A. Cryptography: A Primer*. New York: Wiley, 1981.