Global Journal of Computer Science and Technology: F
Graphics & Vision
Volume 14 Issue 2 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Recent Advancements on Symmetric Cryptography Techniques - A Comprehensive Case Study

By Sangapu Venkata Appaji & Dr. Gomatam V S Acharyulu
*JNTUH, India*

*Abstract-* Now a day's Cryptography is one of the broad areas for researchers; because of the conventional block cipher has lost its potency due to the sophistication of modern systems that can break it by brute force. Due to its importance, several cryptography techniques and algorithms are adopted by many authors to secure the data, but still there is a scope to improve the previous approaches. For this necessity, we provide the comprehensive survey which will help the researchers to provide better techniques.

*Keywords: cryptography, plaintext, cipher text, encry-ption, decryption, cryptanalysis.*

*GJCST-F Classification: D.4.6*

# Recent Advancements on Symmetric Cryptography Techniques -A Comprehensive Case Study

Sangapu Venkata Appaji α & Dr. Gomatam V S Acharyulu σ

*Abstract-* Now a day's Cryptography is one of the broad areas for researchers; because of the conventional block cipher has lost its potency due to the sophistication of modern systems that can break it by brute force. Due to its importance, several cryptography techniques and algorithms are adopted by many authors to secure the data, but still there is a scope to improve the previous approaches. For this necessity, we provide the comprehensive survey which will help the researchers to provide better techniques.

*Keywords: cryptography, plaintext, cipher text, encry-ption, decryption, cryptanalysis.*

## I. Introduction

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords [1-8].

One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication [1-8]. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key[1-8]. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. "Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key" and, unfortunately, "private key") encryption, the same key (or another key fairly easily computed from the first) is used for both encryption and decryption. In asymmetric (also called "publickey") encryption, one key is used for encryption and another for decryption. A new Symmetric Key cryptographic algorithm has been proposed in this paper with its advantages and disadvantages[1-8].

### a) *Types of Cryptography*

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or cleartext) into ciphertext (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are i) Secret Key Cryptography which is also known as Symmetric Key Cryptography and ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography[1-8]. In other words, if the same key is used for encryption and decryption, we call the mechanism as Symmetric Key Cryptography. However, if two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different key is used for decryption; we call the mechanism as Asymmetric Key Cryptography.

i. *Secret key cryptography:* In secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the

*Author α: Assistant Professor, Department of Computer Science and Engineering, GokaRaju Rangaraju Institute of Engineering and Technology, Hyderabad, India. e-mail: appaji_sv@yahoo.co.in*
*Author σ: Retired Professor & HOD Department of Computer Applications, Sreenidhi Institute of Science and Technology, Hyderabad, India. e-mail: darsangvs@yahoo.co.in*

receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key [1-8]

ii. *Public key cryptography:* Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 3 describes the Public Key Cryptography [1-8]

*b) Terminology[1-8]:*

*Plaintext:* The original data is known as plaintext

*Cipher text:* The Encryption data or un understandable data is called cipher text

*Encryption:* The process of converting plaintext to ciphertext

*Decryption:* The Process of Converting Cipher text to plaintext.

*Block cipher:* The data is in the form of Blocks.

*Stream Cipher:* The data is in the form of streams.

*Key:* In cryptography keys are two types on Conventional key or Symmetric key or private key and Asymmetric key or public key.

*Symmetric key:* Both sides of Sender and receiver use the same key.

*Asymmetric key:* Two keys one is public key and private key.

*Cryptanalysis:* The study of ciphertext in an attempt to restore the message to plain text.

In cryptography there will Conventional encryption algorithms, public key cryptography algorithms were proposed by authors. In the next section we are going to survey on recent encryption algorithms by several authors.

## II. Process

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher [1-8].Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the key stream as a function of the previous n bits in the key stream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key stream it is. Synchronous stream ciphers generate the key stream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat. Block ciphers can operate in one of several modes; the following four are the most important: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB) [1-8]. The most common secret-key cryptography scheme used today is the Data Encryption Standard (DES), designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES has been adopted as Federal Information Processing Standard 46 (FIPS 46- 3) and by the American National Standards Institute as X3.92). DES is a blockcipher employing a 56-bit key that operates on 64-bit blocks [1-8] and they are shown in Fig 1 and 2.

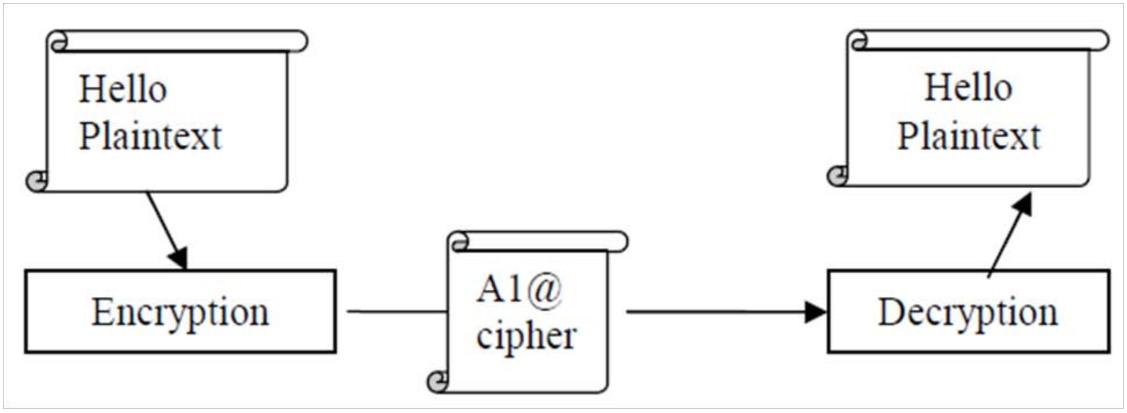

*Figure 1 :* Secret key cryptography

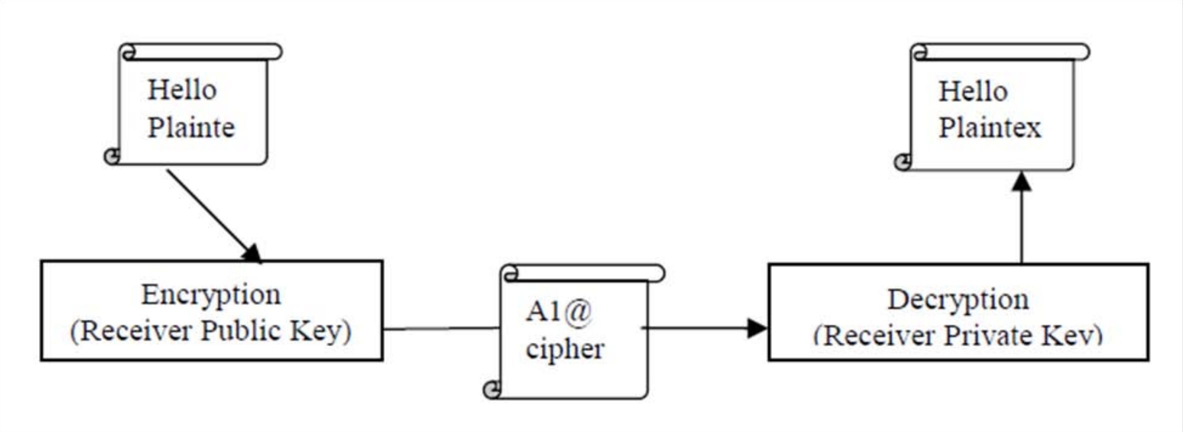

*Figure 2 :* Public key cryptography

## III. Our Contribution

This work categorizes the algorithms into different categories to emphasize the structure that drives the cryptography. We will give in this section some characteristics of standard methods in relation to cryptography. Algorithms Designed After 2000: In this section we survey the most recent algorithms that have been designed after year 2000. In particular the algorithms based on symmetric approach, in the following we briefly review the state-of-the-art until 2014 and the main ideas and the algorithms to which the new solutions refer.

### a) *During 2000 To 2007*

Adams, C et.al [9] examines the cryptographic security of the CAST-256 symmetric block encryption algorithm. The CAST-256 cipher has been proposed as a candidate for the Advanced Encryption Standard currently under consideration by the U.S. National Institute of Standards and Technology (NTST). It has been designed for a 128-bit block size and variable key sizes of up to 256 bits to suit AES requirements. Specifically consider the cryptographic security of the cipher in relation to the cryptanalytic property of diffusion and the cryptanalysis techniques of linear and differential cryptanalysis.

Weidong Shi et.al [10] present a novel technique to hide the latency overhead of decrypting counter mode encrypted memory by predicting the sequence number and pre-computing the encryption pad that we call one-time-pad or OTP. In contrast to the prior techniques of sequence number caching, our mechanism solves the latency issue by using idle decryption engine cycles to speculatively predict and pre-compute OTPs before the corresponding sequence number is loaded. This technique incurs very little area overhead. In addition, a novel adaptive OTP prediction technique is also presented to further improve our regular OTP prediction and pre-computation mechanism. This adaptive scheme is not only able to predict encryption pads associated with static and infrequently updated cache lines but also those frequently updated ones as well. Experimental results using SPEC2000 benchmark show an 82% prediction rate. Moreover, we also explore several optimization techniques for improving the prediction accuracy. Two specific techniques, two-level prediction and context-based prediction are presented and evaluated.

AlKalbany, A et.al [11] presents a hardware implementation of the algorithm, using field programmable gate arrays (FPGA). In this work, the authors discussed the algorithm, the implemented micro-architecture, and the simulation and implementation results. Moreover, a detailed comparison with other implemented standard algorithms was presented. In addition, the floor plan as well as the circuit diagrams of the various micro-architecture modules was presented.

Shiguo Lian et.al [12] proposed a block cipher based on the chaotic standard map, which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator. The parameter sensitivity of the standard map is analyzed, and the confusion process based on it is proposed. A diffusion function with high diffusion speed is designed, and a key generator based on the chaotic skew tent map is derived. Some cryptanalysis on the security of the designed cipher is carried out, and its computational complexity is analyzed. Experimental results show that the new cipher has satisfactory security with a low cost, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos.

Guerreiro, Ana Maria G et.al [13] explores the applicability of using an artificial Spiking Neural Network with a symmetric blockcipher. The goal is to develop a novel neural block cipher where the keys are generated by a spiking neural network and can have any desired block length. With the new algorithm the private keys do not have to be exchanged and present a stronger process of key scheduling. The system allows a rapid change in encryption keys and a network level encryption to be done at very high speed without the problem of factorization of other systems. The block cipher will be transformed in a public cryptosystem, less vulnerable to brute force attacks, and it is hoped to be also resistant to linear attacks since the spiking neuron network architecture brings non-linearity to the encryption/decryption process.

Iain Devlin, Alan Purvis [14] introduces Deluge, a second generation FPGA based key search system that specifically targets stream ciphers. The economically feasible implementation described is in dramatic contrast to other attack techniques and lends weight to the argument that brute-force attacks are underestimated in the security evaluation of cipher designs. Moreover with exhaustive search substantially cheaper than state guessing it is suggested that the practice of designing the state to be twice key length is excessive.

### b) *During 2010 & 11*

Ayushi [15] proposes a new method for security with symmetric key. Here the encryption, first it generates the ASCII value of the letter, Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000] .Reverse the 8 digit's binary number. Take a 4 digits divisor (>=1000) as the Key: Divide the reversed number with the divisor: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipher text i.e. encrypted text. Now store the remainder in first 3 digits & quotient in next 5 digits. In the decryption process, Multiply last 5 digits of the cipher text by the Key: Add first 3 digits of the cipher text with the result produced in the previous step: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number: Reverse the number to get the original text i.e. the plain text. Experimental results show it will provide somehow better complexity.

Debasis Das and Abhishek Ray [16] deals with the Cellular Automata (CA) in cryptography for a class of Block Ciphers through a new block encryption algorithm based on Reversible Programmable Cellular Automata Theory. The proposed algorithm belongs to the class of symmetric key systems. The encryption algorithm present in this paper is constructed using programmable CA based on rules. The rules specify the evolution of the CA from the neighbourhood configuration to the next state. In Cellular Automata, rules are being selected to reduce the circuit complexity. This work ensures to generate 2256 potential keys which means that a brute force attack impossible. This algorithm also uses 128 bit block size which, implies an increase in security but may slow down the encryption/decryption process.

Wuling Ren et.al [17] proposes a hybrid encryption algorithm based on DES and RSA. The currently used encryption algorithm employed by the Bluetooth to protect the confidentiality of data during transport between two or more devices is a 128-bit symmetric stream cipher called E0. It may be broken under certain conditions with the time complexity O(264). In the proposed hybrid encryption algorithm, instead of the E0 encryption, DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission in the Bluetooth system will be more secure. Meanwhile, it is clear that the procedure of the entire encryption is still simple and efficient as ever. In addition, the confidentiality of the hybrid encryption algorithm is also discussed.

Manikandan g et.al [18] propose a Software tool which involves Cryptographic enciphering and deciphering using two algorithms of different dimensions and also they are well assisted with File Splitting and Merging mechanisms. In this authors used modified Blowfish algorithm and RC4 algorithm for Encryption and Decryption of data. This Software tool involves Cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. In this approach a file which has secret data is sliced into two halves and then the cryptographic encryption phase is carried out. In order to achieve more security and can adopt more than one cryptographic scheme which definitely ensures nil suspicion and more security Results clearly justifies that our tool serves as a better solution both in terms of performance as well as security in the author's perspective.

Manikandan et.al [19] propose a method of combining  block and stream cipher for increasing the key strength so that it will be very hard for the intruder to break  the key and intruder will have no idea about the key formation from the combination of block and stream cipher. It integrates the Block and the Stream cipher for generating a fresh key using blowfish algorithm from the actual key provided by the user. The original key is supplied as a plaintext to the blowfish algorithm and it produces a cipher text will be taken as fresh and it is supplied as the key for RC4 algorithm. Thus obtained is hard to crack because it involves addition of the complexity from the block cipher to the key for a stream cipher.

Sairam Natarajan et.al [20] proposed a multi level of multiple encryption schemes which enhances the security of the algorithm This System is developed in such a way that it is platform independent. Where the existing systems are limited to platform dependent design. It is developed through multiple encryption algorithms whereas the existing systems are always focused as encryption at single level. Here use a Random function generator which generates a n-digit random number based upon the n-number of Encryption algorithms used. Thus generated n-digit number determines the order of selecting Encryption algorithms. Since the number determining the order is completely random it is infeasible to crack the order of execution.

Rasmi P S et.al [21] present a hybrid cryptographic system that combines both the symmetric key algorithm, which uses the properties of a circle and asymmetric-key algorithm of RSA with CRT. The circle symmetric key algorithm is based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages all cases. The asymmetric algorithm is RSA with CRT which improves the performance of the basic RSA algorithm by four.

Khanna, N et.al [22] introduced a new advanced symmetric key cryptographic method called NJJSAA. The authors introduced new bit manipulation method for data encryption and decryption of any file. Nath et al already developed some symmetric key methods where they have used some randomized key matrix for encryption and decryption methods. In the present work the authors have used a bit manipulation method which include bit exchange, right shift and XOR operation on the incoming bits. To exchange bits the authors used a randomized key matrix of size (16×16) using the method developed by Nath et al. The present method allows the multiple encryptions and multiple decryptions. To initiate the encryption process a user has to enter a text-key which may be maximum of 16 characters long. From the text-key the authors have calculated randomization number and the encryption number. The method used was developed by Nath et al. A slight change in the text-key will change the randomization number and the encryption number quite a lot. Multiple encryption using bit exchange, bit right shift and XOR operations makes the system very secured. The present method is a block cipher method and it can be applied to encrypt data in sensor network or in mobile network. The advantage of the present method is that one can apply this method on top of any other standard algorithm such as DES, AES or RSA. The method is suitable to encrypt any large or small file. There is a scope to further enhance the present method of encryption.

Ganesh, A.Ret.al [23] propose to use an improved version of the hybrid encryption scheme, which is a combination of Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) with cross encrypted keys for secure key exchange and node authentication and hybrid encryption for enhanced cipher-text security. In case of transmission in WSNs, Statistical Cooperative Diversity based on Alamouti code is the most commonly used transmission scheme. However, for an arbitrary number of sensors, Alamouti code limits the BER performance and energy is not distributed equally, thereby creating the energy-hole problem which leads to early dysfunction of the sensors and may eventually lead to dysfunction of the Wireless Sensor Network (WSN). Extended Cooperative Space-time Block Codes (ECBSTBCs), which are obtained from Alamouti code, have the same characteristics of Alamouti code with the energy being distributed equally among the active sensors. With these factors in mind, we propose to use ECBSTBC as the transmission scheme. The improved hybrid scheme is ideal for ECBSTBC based WSN due to the speed of operation and higher degree of security that it offers.

Zhang Yunpeng et.al [24] proposed a new index-based symmetric DNA encryption algorithm. Adopting the methods of Block-Cipher and Index of string, the algorithm encrypts the DNA-sequence-based plaintext. First, the algorithm encodes each character into ASCII codes. And then, according to the nucleotide sequence, the researcher should convert it to the DNA coding. Besides, the researcher selects the special DNA sequence as the encryption index, and likewise, the pretreated plaintext will be divided into different groups. Next, the key created by the Chaos Key Generator based on the Logistic Mapping and initialized by the number x0 and μ, will take XOR operation with the block-plaintext. The type of number x0 and μ, which is selected by the researcher, is double. Then, the result of these processes will be translated on the DNA sequence. In addition, compared to special DNA sequence, the algorithm finds the sequence which has no difference with it. Then, the algorithm will store the position as the Cipher-text. The researcher proves the validity of the algorithm through simulation and the theoretical analysis, including bio-security and math-security. The algorithm has a huge key space, high sensitivity to plaintext, and an extremely great effect on encryption. Also, it has been proved that the algorithm has achieved the computing-security level in the encryption security estimating system.

Sashank, K.et.al [25] presents a new method of symmetric block encryption using indices called Index-Based Symmetric Block Encryption. Instead of going through a number of tedious rounds while encrypting the data, the data can be encrypted in just two rounds. Also, no two identical data blocks have the same ciphers. i.e. if a single block has been encrypted twice we don't get identical ciphers. There by avoiding linear cryptanalysis and chosen cipher text attack. Encrypting the same document twice doesn't yield the same set of ciphers.

Gaspar, L. et.al [26] presents three ways of extending soft general purpose processors for cryptographic applications. The proposed extension is aimed at symmetric key cryptography and it guarantees secure key management. Three security zones are created and physically separated in each of three configurations: processor, cipher and key storage zones. In the three zones, the secret keys are manipulated in a different manner - in clear or enciphered, as common data or keys. The security zones are separated on the protocol, system, architectural and physical levels. The proposed principle is validated on Altera NIOS II, Xilinx Micro Blaze and Actel Cortex M1 soft core processor extensions. The NIOS II processor needs fewer clock cycles per data block encryption, because the security module is included in the processor's data path. The data path of the Micro Blaze is unchanged and thus shorter, but additional clock cycles are necessary for data transfers between the processor and the security module. The Cortex M1 processor is connected via AHB bus and the cryptographic extension is accessed as an ordinary peripheral - a coprocessor. Although the interfacing is different, the three processors with their extensions attain the required high security level.

Matalgah, Mustafa M et.al [27] present two methods to tackle this effect while at the same time not tolerating security. We first present a modification to the way the traditional Data Encryption Standard (DES) itself is performed to make it prone to errors caused by the wireless channel. Secondly, we present a modification to the way encrypted data is transmitted over the channel. The two proposed methods are shown to achieve less SAC effect and hence improved error performance, higher data rates, and at at least as secure as traditional encryption algorithms. We assume the additive white Gaussian noise (AWGN) channel model in our analysis.

*c) During 2012*

Vishwa gupta et.al [28] developed a new cryptography algorithm which is based on block cipher concept. In this algorithm authors used logical operation like XOR and shifting operation. This algorithm Initially select plane text of 16 bytes (or we can vary from 16 to 64 depend on requirement). Initially insert key of size 16 bytes (depend on plane text value) Apply XOR operation between key (Key_Block4213) and plane text block (Text_Block). Result will store in Cipher Block1. Apply right circular shift with 3 values. Result will store in new Cipher_Block2. Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3. Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4. Cipher_Block4 is the input of the next round as a plane text block. Experimental results show that proposed algorithm is very efficient and secured by authors perspective.

Ravindu Madanayake et.al [29] proposed algorithm, which supports for user desired security level and processing level. It is a block cipher which is a derivation on the fiestle network architecture. The algorithm provides security levels and their corresponding processing levels by using various keys for the encryption/decryption process. This facility is achieved by using fuzzy logic. The results of the proposed encryption algorithm will be analyzed by comparing with other existing encryption algorithms. Finally the aim of the research is to come up with an encryption algorithm which can provide either low processing or high security according to user's requirement which will be more advanced than the existing encryption algorithms.

Parvez khan Pathan and Basant Verma [30] showing a new encryption key model and there decryption part, this encryption algorithm model which will improve avalanche effect as well as execution time as compared with various encryption algorithms. Here Input 128 bit plain text and 128 biit key convert in to binary form. Divide plain text in to two block of 64 bit each. LPT & RPT Divide key to two block of 64 bit each. LK & RK. Perform 4 bit RCC to Left plain text block. XOR result of step 4 with LK. XOR RPT and RK. Perform 3 bit RCC to result of step 5 Perform 5 Bit LCC to Right key.

Break 128 bit key to 16 sub key of 8 bit from K0……K15. XOR result of step 5 with K0. XOR result of step 6 with K3. Perform XOR result of step 6 with result of step 7 Perform XOR result of step10 with step 8. Perform XOR result of step 8 with K7->fourth block Perform XOR result of step 13 with k15first block Perform XOR result of step 12 with k11-> third block Perform XOR result of step 11 with result of step 14 Divide the result of step 11 in to two part of 32 bit each perform 2 bit LCC to first and 2 Bit RCC to second Block.-->second block Performing XOR to all the block we get cipher text. The proposed models will secures information from all the anomalies which is constantly follow-up over public network. It significantly simplifies model written as security purpose while improving the efficiency of cryptography algorithm.

Manikandan et.al [31] propose a new hybrid techniqueof combining "the twins" cryptography, Steganography along with the compression techniques which results in a new extreme of providing informational security. The importance of information not only depends upon its contents but also upon its safety arrival to the receiver. In the encryption, Getting Plaintext which is to be sent to the recipient from the user. C Plaintext is compressed by encoding it in LZW Compression algorithm which produces a new plaintext. C Transformation of plaintext in to cipher text by undergoing an encryption process using the modified cryptographic algorithm. C The third step will be embedding process and thus obtained cipher text is hided inside any cover image using a Steganographic algorithm. C Thus the resulted Steg image is communicated through any communication channel to the receiver. In the decryption Extraction Process will be carried out first which separates the embedded message from the Steg image. C Thus obtained message will be in the scrambled form, so decryption process should be carried out by following the modified cryptographic Decryption process. C Finally, the receiver can able to read the actual secret message sent at the sender's end by decompressing it. Experimental results shows that our system is unique in its design and as well as in its performance when compared to a specific steganographic or a cryptographic technique.

Sunita Bhati et.al [32] proposed a new encryption algorithm "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme. The BREA is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system. In the encryption process The letters of alphabet are assigned numerical values from 1 to 26 in sequence i.e. A, B, C, ......., X, Y, Z assigned numerical values 1, 2, 3, ........., 24, 25, 26 respectively, the digits from 1 to 9 assigned numerical values from 27 to 35 respectively and the zero (0) remains as it is. The plaintext is partitioned into fixed-length blocks of size 16 bytes (or 128 bits) each. These blocks are represented by a matrix Mp. The values of Key matrix (K) are randomly selected from the range 1 to 26. The size of Key matrix is equivalent to the block size of plaintext i.e. 16 bytes. K = [ k1, k2, ......................, k16 ] K = Random (1, 26, 16) Calculate the Transpose matrix of plaintext block matrix (Mp), which is denoted by MpT. Calculate encrypted Key matrix Ke using the following formula: Ke = K mod 2 Add both the matrices MpT and Ke and the resultant matrix is denoted by Cpk. Cpk = MpT + Ke . Rotate first three rows horizontally of Cpk matrix such that rotate one byte from first row, rotate two bytes from second row, rotate three bytes from third row and fourth row remains untouched. The resultant matrix is denoted by Chr . Rotate first three columns vertically of Chr matrix such that rotate one byte from first column, rotate two bytes from second column, rotate three bytes from third column and fourth column remains untouched. The resultant matrix is denoted by Cvr. Replace numeric values of Cvr matrix by their corresponding letters and if 36 exist in Cvr matrix, it is replaced by the special character #. The resultant matrix is denoted by Ce. This paper is an attempt to invent a new encryption model which is secure and very fast.

Suyash Verma et.al [33] proposed new encryption algorithm based on block cipher generating mechanism herewith to analyze the time-consumed by the complete process (process starting from sender encryption to receiver decryption) of the selected cryptographic algorithms with proposed algorithm. In this algorithm for evaluation, results calculation using different plaintexts in the same key (DPSK) mode. As the basis of the evaluating process, the plaintext and the corresponding key are both generated by randomly. The proposed encryption algorithm has been designed in a beneficial approach but of-course not sacrificing the security issues. It will be successfully implement on the various type of data. The expected results showing that, under the same key size and for the same size of the data, proposed algorithm will be about several times faster than existing algorithm, and there are other runtime characteristics which further highlight the difference between these cryptographic algorithm and provides a reference value for people's rational using.

Manisha Madhwani et.al [34] proposes an efficient algorithm for cryptography which is based on static Look Up table and Dynamic Key. Symmetric encryption and decryption is used in this algorithm. The proposed algorithm is more secure and simple to implement. This application makes use of built in android Intents and SMS Manager to send and receive messages. This application makes use of built in android Intents and SMS manager to send and receive messages. The decrypted message is received on our application at the receivers end. Hence, this application is cost effective, simple and easy to use.

M. B. Abdelhalim et.al [35] proposed a hardware implementation of the Modified TEA algorithm (MTEA) , which uses the Linear Feedback Shift Register (LFSR) to overcome the security weakness of the standard TEA algorithm against attacks. The implementation of MTEA algorithm is benchmarked with the standard TEA algorithm considering the area, throughput and power consumption. The pre-layout synthesis results show that there is no significant degradation in the considered metrics due to using MTEA over standard TEA; hence MTEA is a good security candidate to be implemented in RFID systems.

Hossain, M. J et.al [36] presents a reconfigurable system that can encrypt digital data. The system provides the option of choosing one of familiar encryption methods DES, 3 DES and AES to the user. All these methods are symmetric type block cipher cryptography. DES takes 64 bit key to encrypt each 64 bits block of the entire message. AES on the contrary takes 128 bit key to encrypt each 128 bitsblock. Providing reconfigurability, the architecture enables the user to choose one of the existing techniques according to the level of security required. So the designed architecture is both flexible and reliable enough for the user to secure their privacy of conversation or e-commerce transaction. The architecture is designed using Verilog hardware description language, synthesized in Xilinx Synthesis Tool (XST) and Simulated by Verilogger Pro 6.5. It may be implemented in commercially available FPGAs.

Khiabani, Y.Set.al [37] considers the problem of end-to-end security enhancement by resorting to deliberate noise injected in ciphertexts. The main goal is to generate a degraded wiretap channel in the application layer over which Wyner-type secrecy encoding is invoked to deliver additional secure information. More specifically, we study secrecy enhancement of the Data Encryption Standard (DES) block cipher working in cipher feedback model (CFB) when adjustable noise is introduced into the encrypted data in an application layer. A verification strategy in the exhaustive search step of the linear attack is designed to allow Eve to mount a successful attack in the noisy environment. Thus, a controllable wiretap channel is created over multiple frames by taking advantage of errors in Eve's cryptanalysis, whose secrecy capacity is found for the case of known channel states at receivers. As a result, additional secure information can be delivered by performing Wyner type secrecy encoding over superframes ahead of encryption. These secrecy bits could be taken assymmetric keys for upcoming frames. Numerical results indicate that a sufficiently large secrecy rate can be achieved by selective noise addition.

Monika Agrawal and Pradeep Mishra [38] present a new approach for data encryption based on Blowfish algorithm. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. With this new approach we are implementing a technique to enhance the security level of blowfish algorithm and to further reduce the time for encryption and decryption. The striking feature of modified blowfish encryption algorithm is that for the same input plaintext the cipher text generated at each time will be different. This is because every time a new random number gets generated and this as a result gives difference in the application of F function over each round. The advantage of different cipher text generated for the same input is it will greatly enhance the security aspect of blowfish algorithm.

### d) *During 2013*

Anju et.al [39] proposes proposed new algorithm in symmetric key cryptography. The proposed algorithm contains two levels of Exclusive OR (XOR) operation. In the encryption it takes input the key randomly. Convert the key to 16-bit binary format. Construct the list for the prime no. then convert each number to the 16-bit binary format. XOR the binary values of key and prime number. Pick the characters one by one from the whole Data(Plain Text). Convert the characters one by one to 16-bit binary format. XOR the step4 resultant and Step5 resultant. Result produced in step7 is divided in two parts including each of 8-bit value. Put the decimal values for each 8-bit value and convert each value to Text format. Finally, cipher text is generated. In the decryption Convert the decimal values of cipher text into binary format selecting one by one. Convert the cipher text to 16-bit binary format. Construct the list for the prime no. then convert each number to the 16-bit binary format. XOR the binary values of Cipher Text and prime number. Enter the Key randomly. Convert it to the 16-bit binary format. XOR the step4 resultant and Step5 resultant. Result produced in step6 is converted into decimal value. Convert the decimal values to Text format. Finally, Plain text is achieved. This algorithm is useful in transmission of messages and data between one user and another.

Ibukun Eweoya and Olawande Daramola [40] proposes an improved playfair encryption and decryption that will be hard to break by brute force procedure. It uses a 16 X 16 arrays of ASCII characters ensuring relevance in all computing fields instead of the conventional 26 upper case alphabets substitution. This work has discussed playfair cipher as a powerful tool during World War II but nearing extinction, modern computers rendered it insecure for their strength to easily break it, though its rudiments have been used to birth other algorithms of relevance today. However, further researches can make it secure and reliable for modern applications thereby revolutionizing speed and security in software. This work turns the traditional playfair of 26 characters substitution into 256 ASCII codes substitution, and introduces confusion, transposition and permutation into playfair encryption. In addition, the refined playfair was integrated with 128 bits AES in order to create an enhanced security module. It is envisioned that a hardware implementation that is based on our refined playfair plus AES security module would be a worthy investment for embedded systems security in form of FPGA,VDHL or ASIC.

Kamal Jyoti [41] propose a enhance amalgam encryption solution using AES and RC4 which can overcome overhead and security limitations. Hybrid algorithm will be proposed by combining the flexibility of rivest cipher and strong security of AES algorithm. Each block of AES will have different security keys to make it stronger. This research will improve the secure communication in large structure based grid computing systems. Moreover in case of breaching into network, encryption provided by our proposed hybrid algorithm is very difficult to decrypt

Janailin Warjri et.al [42] proposes a new Symmetric Key algorithm called as KED (Key Encryption Decryption) using modulo69. Here not only alphabets and numbers are used, but special characters have also been included. Two keys are used in which one is a natural number which is relatively prime to 69 and finding the inverse modulo69 of it and the other key is a random number generated by the proposed key generation method. In the encryption process. intially substitute or assign integer value for plain text. Multiply Synthetic value with first key i.e., k1. Now add the result with second key i.e., k2. Then calculate with modulo69. In the decryption process, assign integer value for cipher text. Subtract ‘k2’ from above integer value. Multiply above result with inverse modulo69 of ‘k1’ i.e., ‘n1’. Finally calculate with modulo69.

Krishna Kumar Pandey et.al [43] uses enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. In conventional encryption methods the key for encryption and decryption is same and remain secret. The algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. The algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender. This internal key will store in the sender end database and send to the receiver end by other path for preventing brute force attack and other harmful attacks on security. Proposed method is essentially block cipher method and it will take less time with providing security if the file size is large. Where existing algorithms efficiently works with 2 Mb file. The result comparison shows that “proposed technique” gives better result as compared “BP1” and “BP2”. When users are focusing on security then they can select proposed algorithm for better result with less time complexity.

Obaida Mohammad Awad and Al-Hazaimeh [44] presents a new algorithm for block data encryption that enhances the security level. In the encryption process, the letters of alphabet are assigned numerical values from 33 to 126 in sequence i.e. A, B, C, ..., X, Y, Z are assigned numerical values from 65, 66, 67, ...., 88, 89, 90, respectively, based on the ASCII code substation concepts. The plaintext is partitioned into fixed-length blocks of size 16 bytes (4*4) rows and columns. These blocks are represented by a matrix MO. The values of key matrix (KO) are randomly generated from the range 33 to 126. The size of key matrix is equivalent to the block size of plaintext 16 bytes (i.e. 4*4 matrix size). Calculate the transpose matrix of plain-text block matrix (MO), which is denoted by MOT. Convert the key matrix generated randomly to a binary key donated by KB using the following formula: KB = KO mod 2. Add both of MO with KB and the result matrix is denoted by MC. MC = MO + KB Capsulation process: Non-linear mixing between the MC and KO. In other words, insert the key inside the block cipher to generate 8*4 rows and columns matrix of data block and key. Linear mixing: using bits shuffling to create a diffusion effect, while substitution is used for confusion. Replace the numeric values after performing linear mixing by their corresponding characters based on ASCII code system to generate an encrypted block. In the decryption process, Capsulation process: involves extracting the key from the cipher-block data. Decryption process: involves calculating the binary key (KB) then subtracting the operation between the encrypted data and the binary key. The end result of such operation is the plain text data (original text). Based on security analysis, it can be concluded that the proposed algorithm is secure because it has satisfied correlation coefficient test. Thus, the proposed algorithm will be efficiently used or considered as a good alternative as compared to other existing algorithms.

Desai, A et.al [45] proposes an optimized parallel architecture of AES algorithm for disk encryption, suitable to be implemented in a multicore environment. CipherBlock Chaining (CBC) mode of encryption is used for implementing the disk encryption. As it does not support a parallel architecture, Interleaved Cipher Block Chaining (ICBC) mode (proposed by the cryptographic community that allows parallel implementation) has been implemented. The AES algorithm in CBC and ICBC modes has been implemented in C language and is parallelized using OpenMP API 3.1 standard. The performance analysis is done using Intel VTune™ Amplifier XE 2013. The parallel design (ICBC) exhibits improved performance over the sequential approach (CBC) and a speed up of approximately 1.7 is achieved.

Radha Aathithan, N et.al [46] propose a new symmetric block cipher encryption which provides confidentiality to the multimedia while transmitting through the network. The encryption relies on two typical operations, substitution and transposition. A complete binary tree performs substitution and a 2-d array performs non-linear diffusion in the 2 stage of the encryption/decryption process. The first stage spreads out the bits of a block into a complete binary tree and performs randomized substitution based on a pseudo random permutation key P. The second stage lays out the bits from first stage into a square matrix and performs random shifting row/column wise in a circular fashion based on the key P. The encryption process consists of n rounds of identical transformations applied to the plaintext yield the cipher text C. The proposed system is a novel non-conventional full encryption approach, which treats the entire multimedia bit stream as byte streams and uses the encryption scheme to encrypt the entire data stream. Thus the encrypted streamed data is transmitted by the sender and received and rendered in real-time by the receiver. The receiver can start playing back multimedia as soon as enough data has been received and stored in the receiver's buffer. The performance of the proposed algorithm is compared with two symmetric encryption techniques namely AES and RC6. The experimental results show that there is only a few seconds of startup delay, i.e., the delay between the sender streaming the data and the client receiving playback. Thus the proposed system enables the real time or on demand distribution of audio, video and multimedia over the Internet. Hence the proposed algorithm achieves multimedia data confidentiality at low encryptioneffort and suitable for real-time multimedia communication applications.

Verma, H.K et.al [47] presents an enhanced version of RC6 Block Cipher Algorithm (RC6e - RC6 enhanced version), which is a symmetric encryption algorithm [1] designed for 256-bit plain text block. RC6 uses four (w-bit) registers for storing plain text and for data-dependent rotations [2, 3], but this enhanced version (RC6e) uses eight (w-bit) register that helps to increase the performance as well as improve security. Its salient feature includes two-variable algebraic expression modulo 2w and 2 Box-Type operations, Box-Type I & Box-Type II. Each Box-Type operation uses two (w-bit) registers. Box-Type I works much like two registers (A & B or C & D) operation in RC6 but in Box-Type II bitwise exclusive-or is swapped by integer addition modulo 2w used in Box-Type I and vice-versa, it improves Diffusion in each round. This enhanced version needs 2r+4 additive round-keysand uses every round-key twice for encrypting the file. This enhanced version performs better withrespect to RC5 [4, 5] and RC6 [2, 3] when file size is larger.

## IV. Conclusions

Exchange of data over the internet is increasing day by day. Security is the main issue in communication over the internet called WWW. Protection must be given against intruders. Hence Cryptography plays a vital role in providing security. Due to this importance over internet security here we provide the detailed survey on block chypers, which will help the researchers to propose the better techniques.

## References Références Referencias

1. S. William, “Cryptography and Network Security: Principles and Practice”, 2nd edition, Prentice-Hall, Inc., 1999.
2. S. Hebert, “A Brief History of Cryptography”, an article available at http://cybercrimes.net /aindex.html.
3. ATUL KAHATE, “Computer and Network security”.
4. K. Gary, “An Overview of Cryptography”, an article available at www.garykessler.net/library/crypto.html.
5. E.Surya, C.Divya, “A Survey on Symmetric Key Encryption Algorithms”, International Journal of Computer Science & Communication Networks , Vol 2(4), 475-477.
6. Tony M.Damico, “A Brief History Of Cryptography”, an article available at http://www.studentpulse.com /articles/41/a-brief-history-of-cryptography.
7. Cryptography, http://www.newworldencyclopedia. org/entry/ Cryptography.
8. Oded Goldreich, “Foundations of cryptography: basic tools”, 2001.
9. Adams, C., et al. "An analysis of the CAST-256 cipher." Electrical and Computer Engineering, 1999 IEEE Canadian Conference on. Vol. 1. IEEE, 1999.
10. Shi, Weidong, et al. "High efficiency counter mode security architecture via prediction and precomputation."ACMSIGARCH Computer Architecture News33.2 (2005): 14-24.
11. AlKalbany, Abdullah, Hussein Ahmad Al Hassan, and Magdy Saeb. "FPGA implementation of the" pyramids" block cipher." SOC Conference, 2005. Proceedings. IEEE International. IEEE, 2005.
12. Lian, Shiguo, Jinsheng Sun, and Zhiquan Wang. "A block cipher based on a suitable use of the chaotic standard map." Chaos, Solitons & Fractals 26.1 (2005): 117-129.
13. Guerreiro, Ana Maria G., and Carlos Paz de Araujo. "A Neural Key Generator for a Public Block Cipher." Neural Networks, 2006. SBRN'06. Ninth Brazilian Symposium on. IEEE, 2006.
14. Devlin, Iain, and Alan Purvis. "Assessing the Security of Key Length." Trivium633.19 (2007): 26k.
15. Ayushi, A Symmetric Key Cryptographic Algorithm, IJCA, Volume 1 – No. 15,2010 ·

16. Das, Debasis, and Abhishek Ray. "A parallel encryption algorithm for block ciphers based on reversible programmable cellular automata." arXiv preprint arXiv:1006.2822 (2010).
17. Ren, Wuling, and Zhiqian Miao. "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication." Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on. IEEE, 2010.
18. Manikandan, G., G. Krishnan, and N. Sairam. "A unified block and stream cipher based file encryption." Journal of Global Research in Computer Science2.7 (2011): 53-57.
19. Manikandan, G., et al. "An integrated block and stream cipher approach for key enhancement." Journal of Theoretical and applied information Technology 28.2 (2011): 83-87.
20. Natarajan, Sairam, An Ganesan, and Krishnan Ganesan. "A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme.", International Journal of Computer Science and Information Technologies, Vol. 2 (1) , 2011, 469-473.
21. A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetrickey Algorithm for E-commerce Applications, International Journal of Computer Applications, pp.14-18,2011.
22. Khanna, Neeraj, et al. "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm." Communication Systems and Network Technologies (CSNT), 2011 International Conference on. IEEE, 2011.
23. Ganesh, A. R., et al. "An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks. " Recent Trends in Information Tech nology (ICRTIT), 2011 International Conference on. IEEE, 2011.
24. Yunpeng, Zhang, et al. "Index-based symmetric DNA encryption algorithm."Image and Signal Processing (CISP), 2011 4th International Congress on. Vol. 5. IEEE, 2011.
25. Sashank, K., B. Dinesh Reddy, and S. Ratan Kumar. "Index based symmetric block encryption." Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on. IEEE, 2011.
26. Gaspar, Lubos, et al. "Secure extensions of FPGA soft core processors for symmetric key cryptography." Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2011 6th International Workshop on. IEEE, 2011.
27. Matalgah, Mustafa M., Walid Y. Zibideh, and Amer M. Magableh. "Alleviating the effect of the strict avalanche criterion (SAC) of symmetric-key encryption in wireless communication channels. " Communications and Information Tech - nology (ICCIT), 2011 International Conference on. IEEE, 2011.
28. Vishwa gupta, Advance cryptography algorithm for improving data security, International Journal of Advanced Research in Computer Science and Software Engineering, PP. 1-6, 2012.
29. Madanayake, Ravindu, et al. "Advanced Encryption Algorithm Using Fuzzy Logic." International Proceedings of Computer Science & Information Technology 27 (2012).
30. khan Pathan, Parvez, and Basant Verma. "Hyper Secure Cryptographic Algorithm to Improve Avalanche Effect for Data Security.", PP. 1420-145, 2012
31. Manikandan, G., N. Sairam, and M. Kamarasan. "A hybrid approach for security enhancement by compressed crypto-stegno scheme." Research Journal of Applied Sciences, Engineering and Technology 4.6 (2012): 608-614.
32. Bhati, Sunita, Anita Bhati, and S. K. Sharma. "A New Approach towards Encryption Schemes: Byte–Rotation Encryption Algorithm." Proceedings of the World Congress on Engineering and Computer Science. Vol. 2. 2012.
33. Suyash Verma, Rajnish Choubey, Roopali soni, An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 7, pp. 18-21, 2012.
34. Madhwani, Manisha, C. V. Kavyashree, and Jossy P. George. "Cryptography On Android Message Application Using Look Up Table And Dynamic Key (Cama)." IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661,pp. 54-59 ,2012.
35. Abdelhalim, M. B., et al. "Design & Implementation of an Encryption Algorithm for use in RFID System." delta 31.2 (2012): 15.
36. Hossain, Md, and Khaled Mahbub Morshed. "Reconfigurable encryption system: Encrypt digital data." Computer and Information Technology (ICCIT), 2012 15th International Conference on. IEEE, 2012.
37. Khiabani, Yahya S., et al. "Enhancement of secrecy of block ciphered systems by deliberate noise." Information Forensics and Security, IEEE Transactions on7.5 (2012): 1604-1613.
38. Agrawal, Monika, and Pradeep Mishra. "A Comparative Survey on Symmetric Key Encryption Techniques." International Journal on Computer Science & Engineering 4.5 (2012).
39. Anju, An Approach to Improve the Data Security using Encryption and Decryption Technique, International Journal of Information and

Computation Technology, Volume 3, Number 3, pp. 125-130, 2013.

40. Eweoya, Ibukun, Olawande Daramola, and Nicholas Omoregbe. "Improving Security Using Refined 16 X 16 Playfair Cipher for Enhanced Advanced Encryption Standard (AES).", Covenant Journal of Informatics and Communication Technology (CJICT) Vol. 1, No. 2, PP. 79-88, 2013.
41. Jyoti, Kamal. "Enhanced Amalgam Encryption Approach for Grid Security: A Review." International Journal 3.4 (2013).
42. Warjri, Janailin, and E. Raj. "KED-A Symmetric Key Algorithm for Secured Information Exchange Using Modulo 69." International Journal of Computer Network & Information Security 5.10 (2013).
43. Pandey, Krishna Kumar, Vikas Rangari, and Sitesh KumarSinha. "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security.", International Journal of Computer Applications, PP. 29-33, 2013.
44. Al-Hazaimeh, Obaida Mohammad Awad. "Design of a New Block Cipher Algorithm." Network and Complex Systems 3.8 (2013): 1-6.
45. Parallelization of AES algorithm for disk encryption using CBC and ICBC modes, Computing,2013 Fourth International Conference on Communications and Networking Technologies (ICCCNT), pp.1-7,2013
46. Radha Aathithan, N., and M. Venkatesulu. "A complete binary tree structure block cipher for real-time multimedia." Science and Information Conference (SAI), 2013. IEEE, 2013.
47. Verma, Harsh Kumar, and Ravindra Kumar Singh. "Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.