Universal Intelligent Data Encryption Standards: A Review

[1]RENJITH V RAVI, [2]DR.MAHALAKSHMI R
renjith_v_ravi@yahoo.co.in
Research Scholar[1], Karpagam University, Coimbatore, Tamil Nadu
Professor & HOD [2], Department of EEE, Sri Krishna College of Technology
Coimbatore 641 042, Tamil Nadu
INDIA

Abstract-*The most challenging aspects in the word of electronic communication is nothing but the data security. The significance of the exchanged data over the internet and other media types are increasing. One of the most interesting subjects in the security related communities is the hunt for the best solution to offer an essential protection against the data intruders' attacks together with providing these services in time. Cryptography is the one of the main category of data security which converts information from its original form into an unreadable form. There are two main uniqueness to distinguish an encryption system from another are its ability to secure the protected data against cryptanalytic attacks and its speed and efficiency in the process.Cryptographic research has a common objective to design protocols that offer a confidential and authenticated transmission channel for messages over an insecure network. If a cryptographic algorithm is said to be computationally secured, it cannot be broken with typical resources, either present or future and apart from the algorithm, key distribution is also more important to make an proficient cryptographic system.*

Keywords - Cryptography, Encryption, Cipher, latency, throughput

I. INTRODUCTION

The term cryptography is defined as the science of secret writing means, to prevent the disclosure of contents; the data in the communication are encoded before the transmission and decoded after reception. so that only the real person can see the real message. The main requirement of security is to keep safe the data from unauthorized access. And physical security is the best barricade (The machine to be protected is placed behind physical walls). However, this is not always an option, because of considering efficiency and/or cost. Instead of this, most of the computers are interconnected with each other openly, in that way exposing them and their communication channels that they use. In view of privacy, cryptography is used to encrypt or encipher the data residing on the storage devices or transmitting or receiving through th communication channels to make sure that any illegitimate access is unsuccessful. Also cryptography is used to provide authentication to different parties attempting the access of the same system. Suppose a party wants to grant one certain functionality of the system, he must provide something to prove his authentication. We can call these something as credential and additional care must be taken that these credentials are used by the original user. The most common credential is password. To protect against illegal usage, the Passwords were encrypted.

II. HISTORY OF CRYPTOGRAPHY

The development of cryptography fundamentally started from the improvement of DES (Data Encryption Standard). In 1977, IBM's tameness of a cipher named LUCIFER (embraced as DES by NBS (National Bureau of Standards) now NIST (National Institute of Standards and Technology). After the development of it, numerous cryptanalysts have endeavoured to break this calculation and at last DES encrypted message was cracked in just 22 hours in 1998. Of course there was a need of another encryption standard [1].

In 1997, the National Institute of Standards and Technology (NIST) advertised a system to create and pick an Advanced Encryption Standard (AES) to supplant the maturing Data Encryption Standard (Des).in 1998, NIST declared the acknowledgement of fifteen candidate algorithms and asked for the aid of the cryptographic research group in breaking down the candidates. This dissection incorporated an introductory examination of the security and productivity aspects for every calculation. NIST inspected the after effects of this preparatory research and chose MARS, Rc6, Rijndael, Serpent and Twofish as finalists. On October 2000 and having audited further open examination of the finalists, Rijndael won the opposition and get to be AES (Advanced Encryption Standard) in 2001. NIST chose to propose Rijndael as the Advanced Encryption Standard (AES). [1]

Rijndael, outlined by Joan Daemen (Proton World International Inc.) and Vincent Rijmen (Katholieke Universities Leuven) of Belgium, is a block cipher with a basic and rich structure. It is a symmetric block cipher that can scramble information blocks of 128 bits utilizing symmetric keys of 128, 192 or 256 bits. AES really was acquainted with supplant the Triple DES (3des) calculation utilized for a great measure of time generally. However, in the event that security was the main thought, then 3des would be a proper decision for a standardized encryption calculation for quite some time to come. The fundamental impairment was its abate software usage. For reasons of both effectiveness and security, a bigger block size is alluring. Because of its elevated amount security, rate, simplicity of execution and adaptability, Rijndael was picked for AES standard in the year 2001 [1],[5-7].

III. BASIC TERMS USED IN CRYPTOGRAPHY

A. Plain Text and Cipher Text

In cryptography it is the genuine message that must be send to the next end simply before the encryption procedure is known as plain content. The encrypted manifestation of plain text is known as Cipher text. It is the message that can't be seen by anybody or pointless message. In Cryptography the plain quick message is converted into non clear message before the transmission of real message

B. Encryption and Decryption

A procedure of changing over Plain Text into Cipher Text is called as Encryption or Enciphering. In Cryptography, the utilization of encryption strategy is to send secret messages through an insecure channel. The two paramount things for encryption methodology are- an encryption algorithm and a key. An encryption algorithm implies the method utilized for encryption. Encryption happens at the sender side before the data transmission.

It is the opposite methodology of encryption. It is a procedure of changing over Cipher Text into Plain Text. In Cryptography deciphering method is utilized at the beneficiary side to get the genuine message from the non meaningful Cipher Text. This procedure obliges two things- a Decryption algorithm and a key. A Decryption algorithm implies the strategy utilized for Decryption. By and large the encryption and decoding algorithm are inverse to one another.

C. Secret Key

A Key is only a numeric or alpha numeric content or may be an exceptional image. The Key is utilized at the time of encryption happens on the Plain Text and at the time of unscrambling happens on the Cipher Text. In cryptography, the choice of key is exceptionally paramount since the security of encryption algorithm depends specifically on it.

D. Motivation behind Cryptography

There are essentially five objectives of cryptography. A heap of security capacities must be given by every security system to guarantee its mystery. These capacities are known as the objectives of the security system. These objectives could be recorded under the accompanying five fundamental classes

1. *Confidentiality*. The transmitted information from a computer must be gotten to by the authorized receiver and not by anyone
2. *Authentication.* The information received by any system need to check the identity of the sender that whether the information is landing from an authorized individual or a false identity. It implies that just the authenticated individuals can decipher the message substance and nobody else. The methodology of demonstrating one's identity. This implies that before sending and getting data utilizing the system, the receiver and sender identity ought to be confirmed.
3. *Integrity.* Date uprightness guarantees that the received information is not altered by any outsider, after the transmission. Then again overall guarantees just the authorized individual can alter the Information.
4. *Non Repudiation.* Guarantees that not, one or the other the sender, nor the receiver of message ought to have the capacity to deny the transmission. A system to demonstrate that the sender truly sent this message. Implies that not the sender or the receiver can dishonestly deny that they have sent a certain message.
5. *Access Control.* Just the authorized gatherings can get to the given information. Since secure systems normally get struck by intruders, which may influence their accessibility and sort of administration to their clients. Such systems give an approach to allow their clients the nature of administration they anticipate.

E. Block Cipher and Stream Cipher

One of the primary classification strategies for encryption procedure usually utilized is focused around the manifestation of data they work on. The two types are Stream and Block Cipher [1].

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

In a block cipher, data is encrypted and decrypted if data is in types of blocks. In its least complex mode, the plain text is isolated into blocks which are then nourished to cipher system to generate blocks of cipher text. Symmetric key block ciphers are the most noticeable and critical components in numerous cryptographic systems. Separately, they give confidentiality. The illustrations of block ciphers are DES, 3-DES, FEAL, SAFER, Rc5 and AES. The execution of any essential block cipher is for the most part known as Electronic Code Book (ECB) mode. Keeping in mind the end goal to build the security further extra modes are additionally characterized. They are (1) Cipher Feed Back (CFB) mode (2) Output Feed Back (OFB) mode (3) Counter mode (CTR). The counter mode has gotten well known in IPSec and IPv6 provisions [5-7].

Stream Cipher works on a stream of data by working on it by bits. It comprises of two major Segments: a key stream generator and blending capacity. Blending capacity is normally simply a XOR capacity, while key stream generator is the fundamental unit in stream cipher encryption method. Stream ciphers are by and large quicker than block ciphers in fittings, and have less intricate equipment hardware. Stream ciphers are more suitable for circumstances where transmission slips are exceedingly feasible.

F. Symmetric and Asymmetric Encryptions:

There are two primary classes of cryptography relying upon the sort of security keys used to encrypt/decrypt the data. These two classifications are: Asymmetric and Symmetric encryption procedures.

1). Symmetric Encryption

It is also called as single key cryptography or as public key cryptography. It utilizes a solitary key. In this encryption prepare the receiver and the sender needs to concur upon a solitary secret (shared) key. Given a message (called plaintext) and the key, encryption produces indiscernible data, which is about the same length as the plaintext seemed to be. Decryption is the opposite of encryption, and utilization the same key as encryption [8].

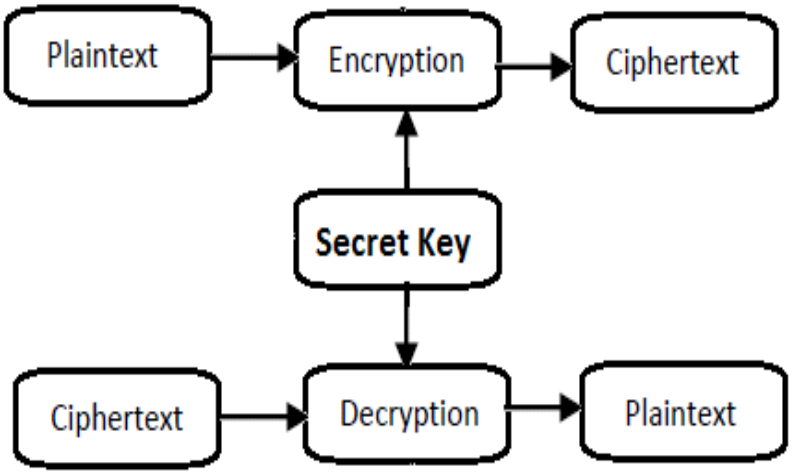

Figure 1: Symmetric Key Cryptography Process

2). Asymmetric Encryption

It is likewise called as public key cryptography. It utilizes two keys: public key, which is known to the public, utilized for encryption and private key, which is known just to the client of that key, utilized for decryption. The public and the private keys are identified with one another by any numerical means. As such, data encrypted by one private key might be encrypted just by its comparing public key [8]. Encryption and decryption technique as indicated underneath in Figure 2.

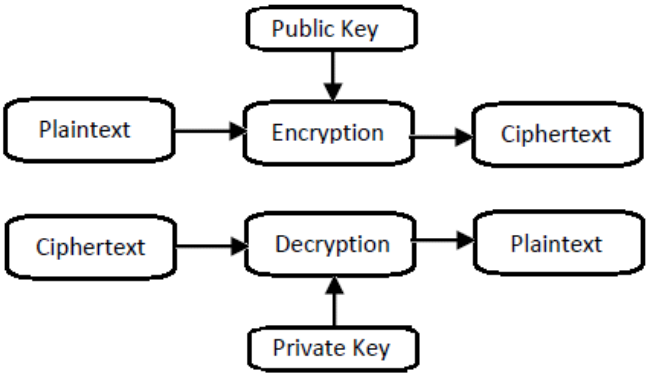

Figure 2: Asymmetric Key Cryptography Process

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

G. Mode of Operation

There are many variance of cipher, where different techniques are used to strengthen the security of the system. The most common methods are ECB (Electronic Code Book), CBC (Chain Block Chaining Mode) and OFB (Output Feedback Mode). There are many other modes like CTR (Counter Mode), CFB (Cipher Feedback Mode).[6]

H. Cryptanalysis

There are two general methodologies for attacking a routine encryption system [5]:

1. *Cryptanalysis.* This is used for deciphering a message without any knowledge of the enciphering details. Cryptanalysis is the science of recovering the plaintext of a message without the access to the key. Successful cryptanalysis may recover the plaintext or the key. It also finds weakness in the cryptosystem.
2. *Brute – Force attack.* The attack tries every possible key on a piece of cipher text until an intelligible translation into plain text is obtained. This is tedious and may not be feasible if key length is relatively long.

I. Strength of the encryption algorithms

The quality of the encryption algorithms is focused around how it is powerless against the attacks made on it. The real attacks on the encryption strategies are, for example, the chosen plain text attacks, known plaintext attacks, brute force attacks, linear cryptanalysis and so forth. To stay away from these attacks required efforts to establish safety ought to be upgraded with the encryption.

1) Confusion and Diffusion. These [5] are the two essential techniques for building any cryptographic framework. Claude Shannon presented the terms Confusion and Diffusion. As per Shannon, in an ideal cipher, "all statistics of the cipher text are independent of the particular key used". Confusion is a technique of guaranteeing that a cipher text gives no sign about the first plain text. This is to attempt and upset the endeavors of a cryptanalyst to search for examples in the cipher text, in order to reason the comparing plain text. In Diffusion, each one plain text digit influences numerous cipher text digits, which is equal to stating that each one cipher text digit is influenced by a lot of people plain text digits [5].

J. Overview of Cryptography

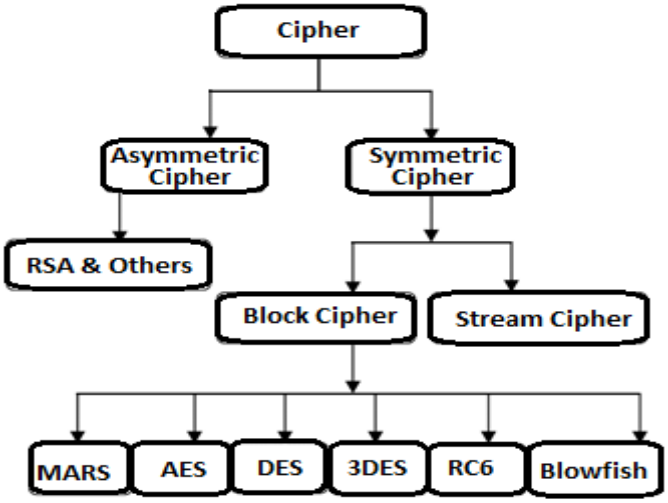

Figure 3: Overview of cryptography

IV.A STUDY ON SOME BLOCK CIPHERS

1) Data Encryption Standard (DES). DES [9] was the first encryption standards to be distributed by NIST [2] (National Institute of Standards and Technology).it was composed by IBM focused around their Lucifer Cipher. Initially,56 bits of the key are chosen from the introductory 64 by permuted choice(1).the staying eight bits are either tossed or used as equality check bits. The 56 bits are then partitioned into two 28-bit parts; every half is thereafter treated independently. In progressive rounds, both parts are turned left by one or two bits and then 48 sub key bits are chosen by permuted choice(2),24 bits from the left half and 24 from the right. The key timetable for decoding is comparable, the sub keys are in converse request compared to encryption.[9]

2) Advanced Encryption Standard (AES). AES [9] is a symmetric-key block cipher distributed by National Institute of Standards and Technology (NIST) in December 2001.aes is a non-Feistel cipher that encrypts and decrypts an information block of 128 bits. It utilizes 10, 12, or 14 rounds. The key size which could be 128,192, or 256 bits, relies on upon the amount of rounds. In the event that both block length and key length are 128 bits, AES will perform 9 handling rounds. In the event that the block and key are 192 bits, AES will perform 11 handling rounds. In the event that the block and key are 256 bits, then it performs 13 preparing rounds. Each one transforming rounds includes four steps: [9]

• Substitute bytes: Uses a S-box to perform a byte by byte substitution of the block.

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

• Shift rows: A basic permutation.

• Mix column: A substitution system where information in every column from the shift row is multiplied by the algorithm's grid.

• Add round key: The key for the handling round is Xored with the data

3) *Triple DES.* In cryptography, TRIPLE DES is the regular name for Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard cipher calculation three times to every information block. The first DES cipher's key size of 56 bits was by and large sufficient when that calculation was outlined, yet the accessibility of expanding computational force made brute force attacks possible. Triple DES gives a generally straightforward strategy for expanding the key size of DES to ensure against such attacks. It takes three 64- bit keys, for a general key length of 192 bits. In Triple DES,the information is encrypted using the first key, decrypted using the second key, lastly encrypted with the third key. Triple DES runs three times slower than normal DES, yet it significantly more secure. The technique for decrypting is the same as the strategy for encryption, with the exception of it is executed in opposite [9].

4) *Blowfish.* Blowfish is a symmetric block cipher that might be viably utilized for encryption and shielding of data. It takes a variable-length key, from 32 bits to 448 bits, making it perfect for securing data. Blowfish was outlined in 1993 by Bruce Schneier as a quick, free option to existing encryption algorithms. Blowfish calculation is a Feistel Network, emphasizing a basic encryption work 16 times. The block size is 64 bits, and key might be any length up to 448 bits. It is essentially quicker than most encryption algorithms when actualized on 32- bit microprocessors with expansive data caches. The calculation comprises of two parts: a key expansion part and a data-encryption part. Key expansion changes over a key of at most 448 bits into a few sub keys shows totalling 4168 bytes [9].

5) *MARS Algorithm.* MARS [7] is a shared key block cipher, with a block size of 128 bits and a key size of 128 bits. It was intended to meet and surpass the prerequisites for a standard for shared key encryption. It takes four 32-bit words plain text as input and produces four 32-bit words cipher text as output. The cipher itself is word arranged, in that all the interior operations are performed on 32-bit words, and thus the inner structure is endian neutral (i.e., the same code deals with both little endian and big endian machines). At the point when the input (or output) of the cipher is a byte stream, we utilize little endian byte requesting to translate every four bytes as one 32-bit word.

The cipher comprises of a "cryptographic core" of keyed transformation, which is wrapped with two layers of cryptographic core giving fast key avalanche.

The main stage gives quick mixing and key avalanche, to baffle chosen plain text attacks, and to make it harder to "strip out" rounds of the cryptographic core in straight and differential attacks. It comprises of expansion of key words to the data words, emulated by eight rounds of S-box based, unkeyed sort 3 Feistel mixing (in "forward mode")[7].

The second stage is the "cryptographic center" of the cipher, comprising of sixteen rounds of keyed sort 3 Feistel transformation. To guarantee that encryption and unscrambling have the same quality, we perform the initial eight rounds in "forward mode" while the last eight rounds are performed in "backwards mode"[7].

The last stage again gives quick mixing and key avalanche, to ensure against chosen cipher text attacks. This stage is basically the converse of the first stage, comprising of eight rounds of the same sort 3 Feistel mixing as in the first stage (aside from in "backward mode"), emulated by subtraction of key words from the data words[7].

6) *RC6.* Rc6[10] is fundamentally the same to Rc5 in structure, utilizing data-subordinate pivots , expansion modulo 2w and XOR operations; actually, Rc6 could be seen as joining two parallel Rc5 encryption forms. Then again, Rc6 does utilize an additional duplication operation not exhibit in Rc5 so as to make the pivot subject to each bit in a word and not only the minimum noteworthy few bits. Number increase is utilized to build the diffusion accomplished for every adjust so fewer rounds are required and the speed of the cipher could be expanded.

Like Rc5, Rc6 is a completely parameterized group of encryption algorithms. A rendition of Rc6 is all the more correctly pointed out as Rc6-w/r/b where the word size is w bits, encryption comprises of a nonnegative number of rounds r and b signifies the length of the encryption key in bytes. Since the AES submission is focused at w = 32 and r = 20, we might utilize Rc6 as shorthand to allude to such forms. At the point when whatever available

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

estimation of w or r is planned in the text, the parameter qualities will be detailed as Rc6-w/r. Of specific importance to the AES exertion will be the forms of Rc6 with 16-, 24- and 32-byte keys. For all variants, Rc6-w/r/b works on units of four w-bit words utilizing the accompanying essential operations [10].

7) *TWOFISH.* It utilizes a 16 round Feistel like structure with extra whitening of the input and output. The main non-Feistel components are the 1-bit pivots. The pivots could be moved into the F capacity to make an immaculate Feistel structure, however this requires an extra pivot of the words simply before the output whitening step [10].

The plain text is part into four 32-bit words, these are Xored with four key words in input whitening step. This is trailed by sixteen rounds. In each one adjust, the two words on the left are utilized as input to the g capacities. (One of them is pivoted by 8 bits first.) The g capacity comprises of four vast key-subordinate S-boxes, took after by a straight mixing step focused around a MDS network. The after effects of the two g capacities are consolidated utilizing a Pseudo Hadamard Transform (PHT) and two keywords are included. These two results are then Xored into the words on the right (one of which is turned left by 1 bit first and other one is pivoted right a short time later). The left and right parts are then swapped for the following round with the exception of the last adjust and the four words are Xored with four more key words to process the cipher text [10].

8) *CAST.* CAST [11] is the first adjust finalist of AES rivalry. It is created via Carlisle Adams and Stafford Taveres in canada, it utilizes 64-bit block for 64-bit and 128-bit key size variants and 128-bit block sizes for the 256-bit key form. The complete determination of CAST calculation is given in.it utilizes a f - function that processes a 32-bit output from a 32-bit input, and each one round comprises of modifying one 32-bit quarter of the block by XOR ing it with the f-function of an alternate 32-bit quarter of the block. There are 48 rounds in aggregate, which are sorted out in gatherings of four, called quad rounds. Encryption begins with six forwards quad rounds, and then continues with six switched quad rounds, which are turned around precisely as would be fundamental for decryption. Implies, for decrypting information, it is just important to change the request in which the sub keys are utilized. CAST cipher might be split up to just 5-round.however, if the level of the round function is bring down, the CAST cipher could be split up to more number of rounds. CAST encryption technique has been under thorough dissection among crypt analysts throughout the previous 10 years. Minor shortcomings have been found like non-subjective assault, HOD strike however nothing extendable past 5-6 rounds [11].

9) *X-MODDES.* It [12] is a block cipher algorithm and one of a kind autonomous methodology which utilizes a few computational steps alongside series of administrators and randomized delimiter choices by utilizing some suitable mathematical rationale. It is extraordinarily intended to transform diverse cipher texts by applying same key on same plain text. It is one of the best performing fractional symmetric key algorithms especially for the text message with restricted size. It additionally ensures the cipher text from the attacks like Brute-force like ambush in light of the fact that it is completely subject to the key and code can't be deciphered by applying all conceivable mixes of keys [12].

10) *KASUMI.* It [14] is a block cipher with a 64-bit block size and a 128-bit key size. It is a close variant of Matsui's block cipher MISTY1, up to some strengthening of the data encryption part and some lightening of the key schedule part. KASUMI has an embedded structure. While the top level of its recursive construction is an 8-round Feistel scheme involving a 32-bit to 32-bit function, the two lower levels are using the variant of the Feistel scheme known as the Misty scheme to build a 32-bit to 32-bit function FO and a 16-bit to 16-bit function FI. KASUMI and two modes of operation allowing to derive a stream cipher and a MAC | known as UEA1 (UMTS Encryption Algorithm 1) and UIA1 (UMTS Integrity Algorithm 1) | were standardised by 3GPP for use in the third generation mobile system UMTS. A stream cipher also derived from KASUMI and almost identical to UEA1 was also adopted, under the name A5/3, as the third standard encryption algorithm of the second generation mobile system GSM [14].

11) *Tiny Encryption Algorithm.* It [13] is a Feistel type cipher (Feistel, 1973) that uses operations from mixed (orthogonal) algebraic gatherings. A dual shift causes all bits of the data and key to be mixed repeatedly. The key schedule algorithm is basic; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). TEA appears to be exceedingly resistant to differential cryptanalysis (Biham et al., 1992) and achieves complete diffusion (where an one bit difference in the plain

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

text will cause approximately 32 bit differences in the cipher text). Time performance on a workstation is exceptionally amazing.

TEA utilizes a Feistel network (a symmetric block cipher) that uses a combination of bit shifting, XOR, and add operations to create the necessary diffusion and confusion of data. It does these operations on 32 bit words rather than single bytes, an exceptionally important optimization that the authors note avoids "wasting the power of a computer." It utilizes a 128 bit (4 expression) key, blending in its individual word segments in a viable key schedule. The original implementation operates on 64 bits (two words) of data at a time, although variants, (for example, Block TEA) allow arbitrary-sized blocks [13].

12) *XTEA.* The block cipher XTEA, outlined by Needham and Wheeler, was distributed as a technical report in 1997. The cipher was an aftereffect of altering a few weaknesses in the cipher TEA (also composed by Wheeler and Needham), which was utilized within Microsoft's Xbox gaming support. XTEA has a 64-round Fiestal cipher with 64 bits block size and 128 bits key size. Both TEA and XTEA are actualized in the Linux kernel[13].

13) *CLEFIA.* It [14] was created together by Sony and the University of Nagoya and distributed at [15]. Clefia[29] is a 128-bit block cipher with its 128, 192 and 256 bits as key length, which is compatible to AES. CLEFIA comprises of two parts: a data processing part and a key scheduling part. CLEFIA utilizes a generalized Feistel structure having four data lines, and each data line is having width of 32 bits. Additionally, there are key whitening parts at the starting and the end of the cipher.in CLEFIA the amount of rounds that relies on upon the key size: 18 rounds for 128-bit keys, 22 rounds for 192-bit keys, and 26 rounds for 256-bit keys.

CLEFIA's data processing part takes after the four branch Generalized Feistel design and in each round half of the state (i.e. 64 bits or 8 bytes) is updated by two different round capacity F0; F1 which are byte-situated SP network: after the XOR of the round key, the S-layer with 4 S-boxes in parallel is applied, trailed by the P-layer which is a matrix multiplication.

In Key schedule part An intermediate key is generated from the master key with a Feistel-like transforms as in the state. Then the round keys are obtained from the intermediate key, with XOR and bit permutations [30].

14) *DESXL.* It [14] was proposed by Leander et al. in [16] and is focused around DESL, an adjusted variant of DES. DESL is like DES with the exception of the substitution layer, where the eight S-boxes are replaced with a solitary S-box that is rehashed eight times. Moreover the Initial Permutation and its reverse (IP; Ip^-1) are excluded in DESL. Additionally DESXL utilization key-whitening methods to build the key length [14]

15) *HIGHT.* It [14] was proposed by Hong et al. in 2006 [17]. HIGHT (high security and light weight) utilizes 64-bit block length and 128-bit key length, which is suitable for low-cost, low-power, and ultra-light implementation. HIGHT consists of a 32-rounds iterative structure which is a variant of generalized Feistel network. The conspicuous peculiarity of HIGHT is that it comprises of straightforward operations, for example, XOR, mod 28 additions, and bitwise rotation towards left. Along these lines, it is hardware-arranged as opposed to software-turned.

16) *MCrypton.* It was designed in 2005 by Lim and Korkishko [18] and is focused around Crypton [19]. It has a block size of 64-bit and offers three diverse key sizes: 64 bits, 96 bits and 128 bits. Each of the 12 rounds comprises of a substitution layer, a column-wise permutation layer, a column-to-row transposition layer and a key addition layer[14].

17) PRESENT. It [33] is a Substitution Permutation Network (SPN) block cipher pointed at compelled situations, for example, RFID tags and sensor networks. It was intended to be especially smaller and competitive in hardware. PRESENT works on 64-bit text blocks, repeats 31 rounds and utilizating keys of either 80 or 128 bits. This cipher was planned by Bogdanov et al. and announced at CHES 2007 [32]. Each one full round of PRESENT holds three layers in the accompanying order : a bitwise exclusive-or layer with the round subkey; a S-box layer, in which a fixed 4-bit S-box is connected sixteen times in parallel to the intermediate cipher state; a linear transformation, called player, comprising of a fixed bit permutation. Just the xor layer with round sub keys is an involution. Accordingly, the decryption operation requires the backwards of the S-box and of the player. After the 31st round there is an output transformation comprising of an exclusive-or with the last round subkey [33].

P-ISSN 2350-7756 | E-ISSN 2350-8442 | www.apjmr.com

V. CONCLUSION

In this wireless world nowadays, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption. Also from these study I can see that the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms.

REFERENCES

[1] J. Res. Natl. Inst. Stand. Techno." Report on the Development of the Advanced Encryption Standard (AES)" Journal of Research of the National Institute of Standards and Technology. Volume 106, Number 3, May–June 2001.

[2]Monika Agrawal, Pradeep Mishra"A Comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Vol. 4 No. 05 May 2012.

[3] Jawahar Thakur, Nagesh Kumar " DES,AES and blowfish: Symmetric key cryptography Algorithms: simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering" ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[4]Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", (2005). Available:http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html

[5]Mohan H. S. And A. Raji Reddy "Generating the New S-box and Analyzing the Diffusion Strength to Improve the Security of AES Algorithm" (IJCNS) International Journal of Computer and Network Security, 51Vol. 2, No. 9, September 2010.

[6] Mohan H.S, A. Raji Reddy and Manjunath T.N " Improving the Diffusion power of AES Rijndael with key multiplication" International Journal of Computer Applications (0975 – 8887), Volume 30– No.5, September 2011

[7] Mohan H. S and A Raji Reddy" Performance Analysis of AES and MARS Encryption Algorithms" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[8]Nagesh Kumar ,Jawahar Thakur and Arvind Kalia" Performance analysis of symmetric keycryptography algorithms: DES, AES and blowfish"2011 Journal Anu Books

[9] E. Surya,E. Surya" A Survey on Symmetric Key Encryption Algorithms" E Surya et al , International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477

[10] Harsh Kumar Verma, Ravindra Kumar Singh" Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms" International Journal of Computer Applications (0975 – 8887), Volume 42– No.16, March 2012

[11] Dr. S.A.M Rizvi,Dr. Syed Zeeshan Hussain and Neeta Wadhwa" A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms" available at cerc.wvu.edu/download/WORLDCOMP'11/.../SAM4138.pdf

[12]Manmeet Kaur, Manjit Kaur and, Gurmohan Singh" Comparison of TACIT Encryption Algorithm with Various Encryption Algorithms" International Journal of Electronics and Computer Science Engineering, Volume 2, Number 1, 2012.

[13]vikram reddy andem"a cryptanalysis of the tiny encryption algorithm "A thesis Submitted in partial fulfilment of the requirements for the degree of Master of Science in the Department of Computer Science in the Graduate School of The University of Alabama.

[14] Jorge Nakahara Jr (EPFL)," WG2 Lightweight Cryptographic Algorithms" available at www.ecrypt.eu.org/documents/D.SYM.5.pdf

[15] T. Shirai, K. J Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-Bit blockcipher CLEFIA. In A. Biryukov, editor, Proceedings of FSE 2007, volume 4593 of LNCS, pages 181-195. Springer, 2007.

[16] G. Leander, C. Paar, A. Poschmann, and K. Schramm. New lighweight DES variants.In

Proceedings of Fast Software Encryption 2007. FSE 2007, volume 4593 of LNCS, pages 196-210. Springer, 2007.

[17] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: a new block cipher suitable for Low-Resource device. In L. Goubin and M. Matsui, editors, Proceedings of CHES 2006, volume 4249 of LNCS, pages 46-59. Springer, 2006.

[18] Chae Hoon Lim,Tymur Korkishko " mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors " Information Security Applications , Lecture Notes in Computer Science Volume 3786, 2006, pp 243-258 .

[19] C. H. Lim. A Revised Version of CRYPTON - CRYPTON V1.0. In Fast Software Encryption - FSE'99, volume 1636 of LNCS, pages 31{45. Springer, 1999.

[20] F. X Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater. SEA: a scalable encryption algorithm for small embedded applications. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, Smart Card Research and Applications, Proceedings of CARDIS 2006, volume 3928 of LNCS, pages 222{236. Springer-Verlag, 2006.

[21] A. L. Jeeva, Dr. V. Palanisamy, K. Kanagaram" comparative analysis of performance efficiency and security measures of some encryption algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622,Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[22] W Stallings, CRYPTOGRAPHY AND NETWORK SECURITY, Printice Hall, 2003.

[23] [B.Schneier, Practical Cryptography,Wiley, 2003

[24]AES page available at NIST via http://www.nist.gov/CryptoToolkit.4

[25] Atul khate, Cryptography and Network Security, 2nd Ed, Tata Mcgraw hill, 2009, pp.87-2004.

[26]Buchanan, William J "*RC2 Encryption and Decryption in Microsoft .NET"*Technical Report 2010. Centre for Distributed Computing and Security, Edinburgh Napier University.

[27] Hamidreza Mahyar, "Reliable and High-Speed KASUMI Block Cipher by Residue Number System Code "World Applied Sciences Journal 17 (9): 1149-1158, 2012 ISSN 1818-4952

[28]3rd Generation Partnership Program. 3GPP Home Page, A Global Initiative. http://www.3gpp.org.

[29] The 128-bit Blockcipher CLEFIA Algorithm Speci_cation Revision 1.0 June1,2007. Available at http://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf.

[30] Alex Biryukov, Ivica Nikoli´c," Security Analysis of the Block Cipher CLEFIA. Available at http://www.cryptrec.go.jp/estimation/techrep_id2202-2.pdf.

[31]Jorge Nakahara, Pouyan Sepehrdad , Bingsheng Zhang , and Meiqin Wang "Linear Hull and Algebraic Cryptanalysis of the Block Cipher PRESENT ",CANS, volume 5888 of Lecture Notes in Computer Science, page 58-75. Springer, *(*2009*)*.

[32]Bogdanov,A.,Knudsen,L.R., Leander,G., Paar,C., Poschmann,A., Robshaw, M.J.B., Seurin,Y., Vikkelsoe,C.: PRESENT: an Ultra-Lightweight Block Cipher. CHES 2007, Springer, LNCS 4727, pp. 450–466 (2007).

[33] Stanislav Bulygin," More on linear hulls of PRESENT-like ciphers and a cryptanalysis of full-round EPCBC-96 " *IACR Cryptology ePrint Archive* (*2013*) .

[34] H. Yap, K. Khoo, A. Poschmann, M. Henricksen: \EPCBC { A Block Cipher Suitable for Electronic Product Code Encryption". In D. Lin, G. Tsudik, X.Wang (Eds.) CANS 2011, LNCS 7092, pp. 76-97.