International Journal of Engineering & Technology, 7 (2.16) (2018) 94-97

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

VLSI Design flow for Secure Integrated Circuits based on DES, TDES, AES and Blowfish Algorithms and their performance

Kumara Swamy Varkuti[1*], Prabhu Benakop[2]

[1]Associate Professor & Associate Head, Dept of ECE,
Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana, India-501301
[2]Professor, Dept of ECE,
Indur Institute of Engineering and Technology, Siddipet Dist, Telangana, India-502103
**Corresponding author Email: ksvarkuti@gmail.com*

Abstract

Information Communication Technology (ICT) and Information Security (IS) are playing vital role in the present day communications. Information is prone to side channel attacks at software level where as it is very difficult to hack the information at hardware level. Security is the major concern in the paperless communication and cashless online transactions. This paper aims to implement the most secured Improved Modified Blowfish Algorithm (IMBFA) by incorporating cell substitution using Wave Dynamic Differential Logic (WDDL) and interconnect decomposition in the VLSI Design flow to not to allow the hacker to estimate or predict the key. Proposed IMBFA which can result in high speed, high throughput and effective memory utilization compared to Data Encryption Standard (DES), Triple Data Encryption Standard (TDES), Advanced Encryption Standard (AES) and Blowfish (BF). In this research paper, IMBFA yielded minimum delay as 71.067 ns, frequency of the design as 14.07 MHz, memory utilization as 62.481MB and throughput is 900Mbps compared to AES, TDES and DES algorithms. It is simulated using ModelSim, Synthesized using Leonardo Spectrum and implemented using Verilog HDL.

Keywords: ICT, IS, WDDL, DES, TDES, AES, BF, IMBFA, HDL.

1. Introduction

Cryptography is playing important role not only in securing the data but also securing the software and hardware from hackers. To overcome the brute force attack in DES, Triple DES algorithm is implemented, which is theoretically seems good, but practically requires more hardware. Advanced Encryption Standard (AES) is the mainstream cryptographic algorithm used to encrypt and decrypt the data. Even through AES is good for security; it is prone to Side channel attacks. Hence, Blowfish algorithm is used as industry standard cryptographic algorithm, which is not yet hacked and highly secured algorithm [1][2].

1.1. Data Encryption Standard (DES)

It takes 64-bit plain text and encrypts into 64-bit cipher text with the help of 56- bit key. It has 16- rounds of operations. It was the basic encryption algorithm before Triple DES (TDES). It is prone to brute force attack which means that hacker tries to break the key by applying 2n combinations of inputs, where n is the number of input bits. It's a popular and most widely used algorithm before TDES. It is most insecure algorithm compared to other algorithms [3].

1.2. Triple Data Encryption Standard (TDES)

It is triplication of Data Encryption Standard (DES). It has plaintext of 64- bit data blocks. It overcomes the Brute Force attack suffered by DES algorithm. TDES method is having three keying options:

- Option-1: Independent three keys k1, k2 and k3 as shown in below in fig.1 for encryption and fig.2 for decryption processes.

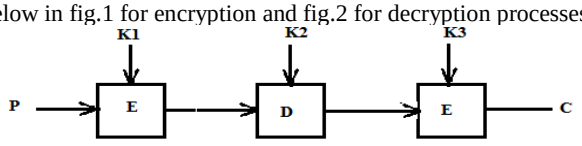

Fig.1: TDES Encryption Process

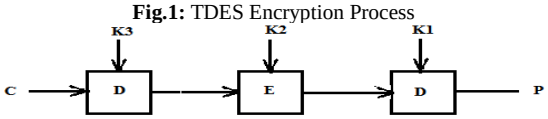

Fig.2: TDES Decryption Process

- Option-2: First two keys are independent and k1 = k3.
- Option-3: Three keys k1, k2 and k3 are equal.

Thus option-1 has three keys independent of each other (k1, k2 and k3) as shown in fig.1 for encryption and fig.2 for decryption which is the strongest among all. It has 168 bits key length where as option-2 has 112 key bits where the first two keys are independent (K1 and K2) and first key (K1) and third key (K3) are equal. It is less secured compared to option-1. The option-3 is having 56 key bits as same as DES but used thrice in the algorithm because of all three keys are equal and prediction can be done easily. It is a symmetric key block cipher. Secured than DES but takes more time to encrypt/decrypt than DES [3].

1.3. Advanced Encryption Standard (AES)

AES is a block cipher with 128 bit plaintext as input. It has variable key length. The block length and key length may be 128 with 9 rounds, 192 bits with 11 rounds, 256 bits with 13 rounds operations. Every round has four steps, i.e., sub bytes, shift rows, mix columns and add round key. AES encryption is most secured and fast compared to DES and TDES algorithms [2].

1.4. Blow-Fish (BF)

Blowfish is a symmetric key algorithm with variable key length. It is a block cipher with 64-bit blocks. The key length varies from 32 to 448 bits. The data encryption occurs through 16-round fiestel network. At the end the Left Encryption (LE) and Right Encryption (RE) are XORed with P-array P18 and P17 respectively. Each round has XOR, ADD, SUBSTITUTE and swap operations. It is a complex, fast, high throughput and more secure algorithm compared to DES, TDES and AES [4][5][6]. Theoretical comparison of DES, TDES, AES and BF algorithms [14] for block size, key length and number of rounds are given in the table 1.

Table 1: Comparison Of Blowfish, Aes, Triple Des And Des Algorithms For Block Size, Key length And Number of Rounds

SNO	ALGORITHM	BLOCK SIZE (BITS)	KEY LENGTH (BITS)	NUMBER OF ROUNDS
1	DES	64	56	16
2	TDES	64	168	48
3	AES	128	256	13
4	BF	64	448	16

1.5. Literature Review

PBFTDES paper described about various implementations of Blowfish with and without modulo adder and WDDL logic, Blowfish with constant delay n-bit adder and WDDL logic in comparison with TDES. The throughput of Blowfish with constant delay n-bit adder and WDDL logic implementation yielded good results compared to other implementations considered [1].

HWCSAES paper presented comparison of DES, 3DES, AES and 3AES algorithms. It is clearly states that proposed AES is more secured, taking less time and giving out more throughput compared to DES and 3DES [2].

PADCA paper presents different cryptography algorithms in which key size, file size, average encryption/decryption time is considered. It reveals that DES is taking less time than AES and Blowfish algorithms. Blowfish is more secured than other symmetric algorithms [3].

HTHSBFA presents blowfish algorithm implemented in four methods with and without Wave Dynamic Differential Logic (WDDL). Modified Blowfish Algorithm yielded minimum delay and maximum throughput compared to other implementations [9].

SBFAWN paper presents superiority of Blowfish over DES, TDES and AES algorithms in terms of encryption/decryption time and Throughput. It also states that blowfish is more secured algorithm compared to other algorithms considered in the paper [15].

BFAESA research work presents the efficiency of Blowfish and AES algorithms with respect to average encryption/decryption time and throughput for different block/key sizes. It shows that Blowfish algorithm is the best one compared to AES algorithm for security, delay and throughput [17].

PADEA research paper compared DES, 3DES, AES and Blowfish Algorithms for key/ block size, encryption/decryption time and throughput. It reveals that Blowfish algorithm is much better than AES, 3DES and DES algorithms in the performance parameters considered for the design [19].

2. Theoretical Analysis

2.1. Improved Modified Blow-Fish Algorithm

Blowfish algorithm is a symmetric key algorithm uses plaintext in the block sizes of 64-bits. It has 16-rounds of operations. Plain text of 64-bits separated as two halves, 32 bit each (LE and RE). We perform 16-rounds of operations during encryption and decryption processes which involve XOR, Fiestel function (F), XOR and SWAP the LE and RE operations in each round as shown in fig3. After 16-rounds of operations, it generates RE and LE by XOR operation with P17 and P18 respectively. Last step in encryption process is concatenation of LE and RE to generate 64-bit Cipher text. In IMBFA algorithm [1][7][12], if string (i) = "0" and Flag = "0" then it goes through function block else it goes without function block in every round of operation.

The flowchart gives clear explanation about IMBFA encryption process of converting plaintext in to a cipher text as shown in fig.3.

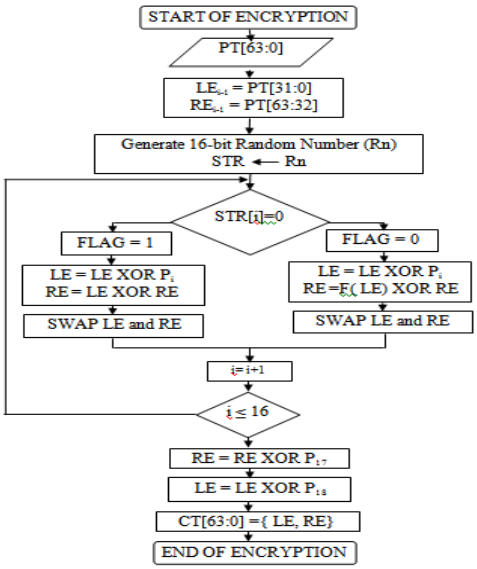

Fig.3: IMBFA Encryption Process Flowchart

The modified approach for blowfish algorithm [7][8] consists of the same specifications as that of Blowfish algorithm except that of a random number defined as Rn of 16-bit string, can be any integer from 0 to 65535 (i.e. within the range of 2^16). A variable called flag is considered, it can be either 0 or 1. Initially its value remains 0. The positions in which a '0' is encountered from LSB to MSB then set the flag to '1' otherwise '0' as shown in fig4. Treat the position of '0' in the string as a round number of an IMBFA algorithm. If the flag is equal to '0', then the encryption process is same as Blowfish algorithm else no F Function applied in that round i.e. LE is directly sent for calculation of RE as shown in fig.3.

In Fig4 shown below, the positions that are holding '0' entries are round numbers of blowfish encryption algorithm, in such rounds the F function will not work in the encryption and decryption statement. The function statements are given below in the form of equations (1) and (2) where LE is left encryption, RE is right encryption and F is function output generated by taking each succeeding 8-bits from LSB to MSB of LE as an address of particular location (w, x, y and z) of each S-Box:

$$RE = F(LE) \oplus RE; \text{ -- (1)}$$

$$F(LE) = ((S1(w) + S2(x)) \oplus S3(y)) + S4(z); \text{--(2)}$$

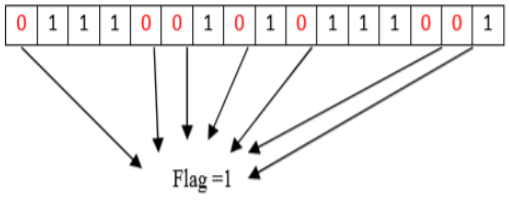

Fig.4: Working of Modified blowfish encryption algorithm.

The modified blowfish encryption algorithm runs on the input plain text. It consists of a function block with four Look Up Tables (LUTs) acting as S-Boxes shown below in fig.5.

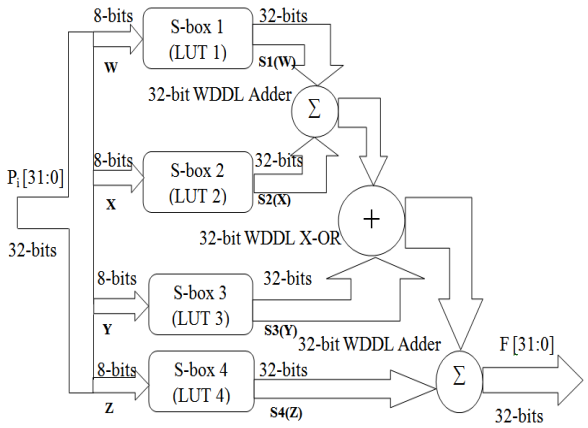

Fig.5: Fiestel Function Block of Blowfish Encryption Algorithm.

The Fiestel function (F) block internal process [9][10][11] is gives clarity in generating 32-bit output with Addition, XOR and Addition using WDDL logic on 32-bit input to the function block. Each s-box is applied with 8-bit input from LE as address of the location in s-box and outputs 32-bits of data stored in s-box.

2.2. Advanced Encryption Standard (AES)

It has block size of 128-bits and key size is 128, 192 or 256 bits with 9, 11 and 13 rounds of operations respectively. With block size of 128-bits and 128-bit key size, it has 9-round, each round involves four steps i.e., sub bytes, shift rows, mix columns and add round key. Last round has only three operations i.e. Sub bytes, Shift rows and Add round key [2]. Decryption is just reverse process of encryption as shown in Fig6, which describes about encryption and decryption of AES process in detail [13]. It takes more time to encrypt and decrypt because of matrix manipulations which requires more memory space to store the information. It is an industry standard algorithm.

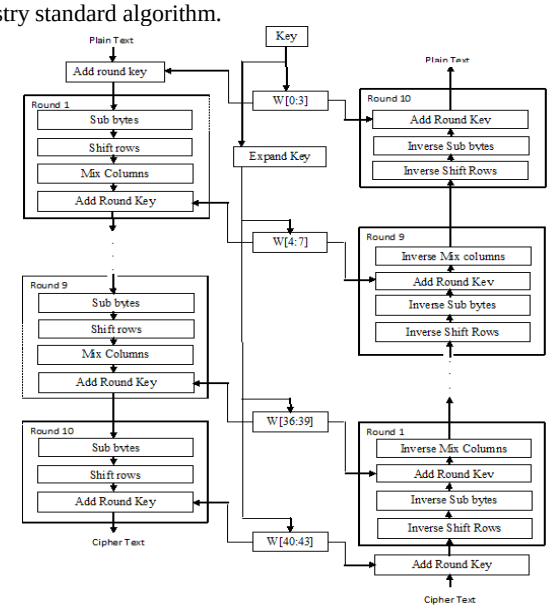

Fig.6: Flowchart for AES Algorithm for Encryption and Decryption.

3. Design of Blowfish Algorithm

As shown in fig.7 below, IMBFA algorithm architecture [7] is designed with three major blocks, i.e. Encryption unit, Decryption unit and Sub key generation unit. Encryption unit receives inputs from 64-bit plain text, P-array of p1 to p18 partial keys, clock and Enc/Dec and generates an output of 64-bit Cyphertext as per the algorithm. Whereas decryption is reverse process to the encryption in which decryption unit receives inputs as 64-bit Cyphertext, p-array of p18 to p1 partial keys, clock and Enc/Dec and generates an output of 64-bit plain text. Sub key generation unit has 448-bit key as input and 18 partial keys (i.e. p1 to p18) as outputs which are helpful in generating LE and RE in encryption and LD and RD in decryption in each round of operation.

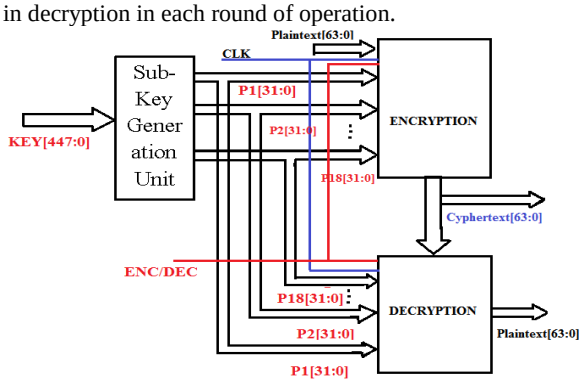

Fig.7: Top level Design module of Blowfish Algorithm

It has sub-key generation unit for generation of sub-keys to be used in each round of operation. The plain text is of 64-bit block and it is divided in to two halves as Left Encryption (LE) and Right Encryption (RE) each of 32-bits. In each round of operation, the algorithm will perform RE and LE operations as shown in fig3 for encryption. The Fiestel function (F) in each round to generate RE from LE with substitution, addition, XOR and addition operations as shown in fig.5.

Thus, the IMBFA algorithm follows the normal procedure for 16-rounds. RE16 and LE16 are XORed with P17 and P18 respectively to generate RE17 and LE17. Then LE17 and RE17 are concatenated to generate Cyphertext i.e. CT [63:0]. Reverse operation is performed for the decryption operation.

The sub-key generation unit is to generate 18- sub-keys (P-Array) from 448-bit input key, i.e., K-array has 14 input sub-keys of 32-bit each, can be used in generating P-Array of P1 to P18 initial sub-keys, each one is 32-bit width [1] which is updated as per the following equations (3):

P1 = P1^K1, P2 = P2^K2…
P14 = P14^K14,
P15=P15^K1, P16=P16^K2, P17=P17^K3, P18=P18^K4; (3)

Where K1 to K14 (32-bits each) are generated from 448-bit input key. Initially we load P-Array of P1 to P18 with known values of each 32-bit width. Sub key generation unit is updating the p-array for every encryption operation of 64-bit plain text.

4. Results and Discussion

The implementation of Improved Modified Blowfish algorithm is compared with AES, Triple DES and DES Algorithms is given below in the table 2. This research paper aims at minimizing the propagation delay, increasing throughput effective memory and area utilization.

Propagation is the time taken by the algorithm to convert plain text to cyphertext. As the delay is less (71.067ns) compared to other implementations as shown below in fig.8.

Table 2: Comparisons of Improved Modified Blowfish, AES, Triple DES and DES Algorithms for Delay, Throughput, MU and AU

No	Crypto-algorithm /parameter	Delay (ns)	TP (Mbps)	MU (MB)	% of AU (Slices &LUTs)
1	Improved modified Blowfish Algorithm (IMBFA)	71.067	900	62.481	11
2	AES	158.93	800	68.719	14
3	Triple DES	197.241	320	36.843	72
4	DES	76.56	835	33.259	66

TP: Throughput MU: Memory Utilization, AU: Area Utilization

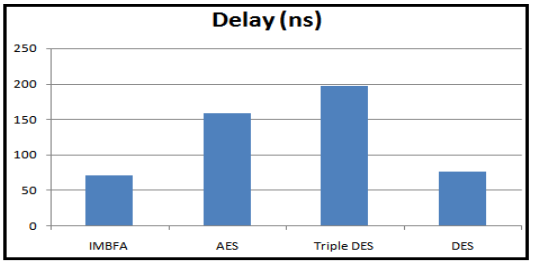

Fig.8: Delay comparisons of IMBFA, AES, Triple DES and DES implementations

Throughput is the ratio of number of bits Encrypted/Decrypted to the Time taken by the algorithm. As per the results obtained shown in fig.9, BF implementation yielded best throughput (112.5MBps) compared to other implementations considered because of its less time to encrypt and decrypt and efficient algorithm implementation.

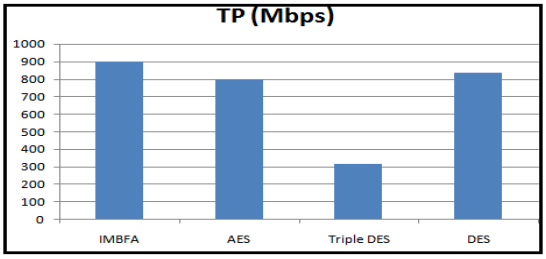

Fig.9: Throughput comparisons of IMBFA, AES, Triple DES and DES implementations

As shown in fig.10, AES algorithm is utilizing more memory (68.719MB) than IMBFA, Triple DES and DES algorithms because of more number of matrices to be stored in 9-rounds of operations to be performed such as sub bytes, shift rows, mix columns and Add round key operations in every round of both Encryption and Decryption processes.

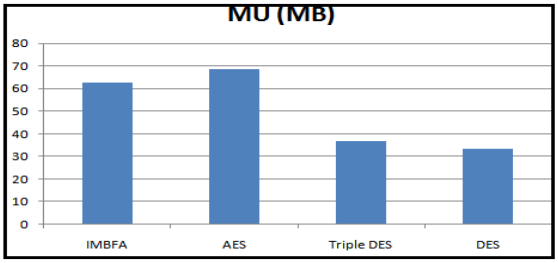

Fig.10: Memory Utilization comparison of IMBFA, AES, Triple DES and DES implementations

As shown in fig.11, area utilization in TDES is more because of TDES repeats DES process three times. Hardware over burden more in TDES and DES where as 1MBFA requires less AU and more secured

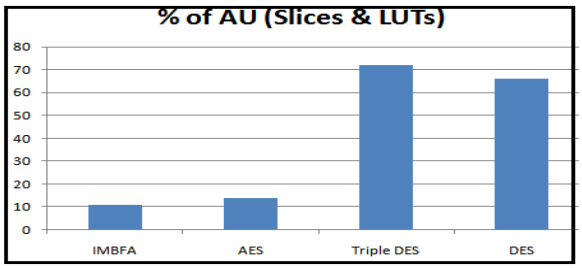

Fig.11: Area Utilization comparison of IMBFA, AES, Triple DES and DES implementations

5. Conclusions

As discussed in the results and discussion that Improved Modified Blowfish Algorithm implementation gave better results compared to other implementations. Blowfish Algorithm has 71.067ns delay, and thus increased throughput to 900Mbps compared to AES, TDES and DES implementations. It is providing more security because of 448 bit key length and incorporating WDDL logic in the Encryption and Decryption process of Crypto-processor digital design flow. However, the memory utilization is less for DES algorithm compared to other designs considered because of its less complexity and less security to the plaintext.

Future scope of this research work is to decrease the delay, improve the frequency and yielding better throughput of Blowfish compared to other design approaches such as AES, TDES and DES algorithms. Further one can concentrate to how to reduce over memory utilization and minimize the area required in implementing the design.

References

[1]. V.Kumara Swamy, Dr Prabhu G Benakop, “Predominance of Blowfish over Triple Data Encryption Standard Symmetric Key Algorithm for Secure Integrated Circuits using Verilog HDL”, International Journal of Network Security & Its Applications(IJNSA), ISSN:09758307, DOI:10.5121/ ijnsa.2017.9603, Vol.9, No.6, November 2017

[2]. Prachi V. Bhalerao, Rahul D. Ghongade, Vishal B. Langote, “Hardware implementation of Cryptosystem by AES algorithm using FPGA”, International Journal of Computer Science and Mobile Computing, ISSN:2320-088X, Vol.6, Issue.5, Pg.84-89, May 2017.

[3] Md. Alam Hossain, Md.Biddut Hossain, d. hafin Uddin, Shariar Md. Imtiaz, “Performance analysis of different cryptography algorithms”, International Journal of Advanced Research in Computer Science and software Engineering, ISSN: 2277-128X, Vol.6, Issue.3, Pg.659-665, March 2016

[5] Nusrat Jahan Oishi, Arafin Mahamud, Asaduzzaman, "Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6",2016 International Conference on Networking Systems and Security (NSysS), 7-9 Jan, 2016..

[6] Viney Pal Bansal,Sandeep Singh, "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), 21-22 Dec. 2015

[7] Vaibhav Poonia, Dr.Narendra Singh Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters", International Journal of Engineering Research and General Science, ISSN: 2091-2730, Volume 3, Issue 1, January-February, 2015.

[8] Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M.Fouad, "Speech Encryption Applying a Modified Blowfish Algorithm", October 2014.

[9] V.Kumara Swamy, Dr Prabhu G Benakop, “High Throughput and High Speed Blowfish Algorithm for Secure Integrated Circuits”, Annals computer science series, ISSN: 1583-7165(Print), ISSN: 2065-7471(Online), Vol. 12, Issue. 1, Pg.24-29, July 2014, Romania.

[10] Kurniawan Nur Prasetyo, YudhaPurwanto, Denny Darlis, "An implementation of data encryption for internet of things using Blowfish algorithm based on FPGA", Vol 2, 2014.

[11] V .Kumara Swamy, Dr Prabhu G Benakop,Performance Analysis of

Secure Integrated Circuits using Blowfish Algorithm, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue 17, Version 1.0,Page no.10-15, December 2013, Global Journals Inc (USA), ISSN: 0975-4172 (Online), ISSN: 0975-4350 (Print).

[12] Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012.

[13]M.Chandra Mohan,V.Kumara Swamy, Dr. T.Srinivasulu,Design of High Speed AES Algorithm, International Conference on Electronics and Communication Engineering (ICECE-2012),GNIT, Hyderabad, Andhra Pradesh, India, 19-20,July 2012

[14] 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, pp.877, May 2012

[15] Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks", International Journal of Computer Applications, ISSN: 0975-8887, Vol.44, Issue.11, April 2012.

[16] Walied W. Souror, Ali E. Taki el-deen, Rasheed Mokhtar-awady Ahmed, Adel Zaghlul Mahmoud - An Implementation of High Security and High Throughput Triple Blowfish Cryptography Algorithm, International Journal of Research and Reviews in Signal Acquisition and Processing (IJRRSAP) Vol. 2, No. 1, March 2012, ISSN: 2046-617X.

[17] M. Anand Kumar, Dr. S. Karthikeyan, "Investigating the efficiency of Blowfish and Rejindael (AES) Algorithms", International Journal of Computer Network and Information Security, DOI:10.5815/ijcnis.2012.02.04, Pg.22-28, Feb.2012.

[18] Gurjeevan Singh, Ashwani Kumar Singla, K. S. Sandha - Through Put Analysis of Various Encryption Algorithms, IJCST Vol.2, Issue3, September 2011.

[19] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, "Performance Analysis of Data Encryption Algorithms", IEEE Xplore, 978-1-4244-8679-3/11, July 2011, DOI: 10.1109/ICECTECH.2011.5942029