Dr. Mamta Sood, Manohar Wagh, Monika Cheema / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.883-890

A Review on Various Data Security Techniques in Wireless Communication System

Dr. Mamta Sood[1], Manohar Wagh[2], Monika Cheema[3]
[1]*Head, Electronics & Communication Engg. Dept., TIT College, Bhopal*
[2]*M.Tech Scholar (Digital Communications), TIT College, Bhopal*
[3]*Asst. Prof., Electronics & Communication Engg. Dept., SF IT*, Mumbai

ABSTRACT

The data transfer, either through wired media or wireless media, needs privacy or a security. In case of wireless means of communication when the data is in the route, in order to protect the data from going into the hands of an unauthorized person, the two main techniques are used i.e. Steganography and Cryptography. Steganography hides the messages inside other harmless digital media without altering it such that no one can detect the presence of secret message whereas cryptography is the science of writing the secret message and the science of encryption and decryption. Basically Cryptography may be public key cryptography also called asymmetric where different keys are used for encryption and decryption or the private key processes or it may be the private key cryptography also called symmetric which uses the same key for both the encryption and decryption processes. Symmetric cryptographic algorithms operating on single bit at a time are said to be stream ciphers and those operating on data in groups or blocks are said to be symmetric block ciphers.

This paper aims at the study of various symmetric block ciphers like Data Encryption Standards (DES), Triple-Data Encryption Standards (T-DES) And Advanced Encryption Standards (AES). Also this paper compares the various encryption and decryption algorithms used in Data Encryption Standards (DES) and Advanced Encryption Standards (AES) which may be implemented in various hardwares like ASICs and FPGA. Field Programmable Gate Arrays are the digital Integrated Circuits which can be reconfigured are widely used to provide the high performance and the low cost application for the purpose of performing cryptographic applications.

Keywords - Advanced Encryption Standard(AES), Cryptography, Data Encryption Standards (DES), Field Programmable Gate Arrays (FPGA)

1. INTRODUCTION

1.1 Wireless Communication Techniques

In earlier few decades, the data transfer was done mainly by two media- Guided media and Unguided media. Guided media can also be termed as wired media where medium is very important issue. Few examples of wired media are twisted pair cable(s), co-axial cable(s), fiber optic cable(s) etc. Drawbacks of such wired communication are interference, attenuation and limitations to number of receivers which ultimately causes the more attenuation. The solution to this is the Unguided communication where wired media is replaced by wireless means of communication Unguided media can also be termed as wireless media where bandwidth produced by an antenna is an important issue. The communication can be achieved by using the antennas at the transmitter and receiver sections in wireless communication.

Wireless communication technologies which are in use nowadays are as follows [1] –

1. The Wi-Fi Technology(Wireless Fidelity)
2. The Bluetooth Technology.
3. The Zigbee Technology.
4. Dash7 (Wireless Sensor Network) Technology.

All the above techniques have their unique features and certain advantages or limitations. Each has its own constraints, so one can use any of the above techniques.

1.2 Security aspects of Wireless Communication Techniques.

For the purpose of providing security to the data which is transmitted from transmitter to receiver, various secured data transmission techniques are used. These techniques are protecting the data from going into the hands of the unauthorized person. Main techniques are – Steganography and Cryptography.

Steganography technique aims to transmit a message on a channel, where some other kind of information is already being transmitted. The goal of steganography is to hide messages inside other "harmless" digital media in a way that does not allow any person to even detect the presence of secret message. Steganography does not alter the structure of the secret message, but hides it inside a medium so that the change is not visible. In other words, steganography prevents an unintended recipient from suspecting that the data exists and the security of the steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

Cryptography is the science of writing the secret message and the science of encryption and decryption [2]. It hides the contents of a secret message from an unauthorized person but the content of the message is visible. In cryptography, the structure of a message is scrambled in such a way as to make it meaningless and unintelligible.

Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography is the very much important technique which provides very accurate, confidential and accountable data transfer through the wireless media. Usually the data is more secured when it is harder to discover the key.

Cryptography uses different key based ciphering and deciphering algorithms [3]:-

a. Asymmetric algorithm :

Also called as a public key algorithm.

Here the process of encryption is performed using one key whereas the different key is used for the decryption process. Means it uses the different keys, one public key and another private key [3]. Both the keys are used to encrypt and decrypt the data.

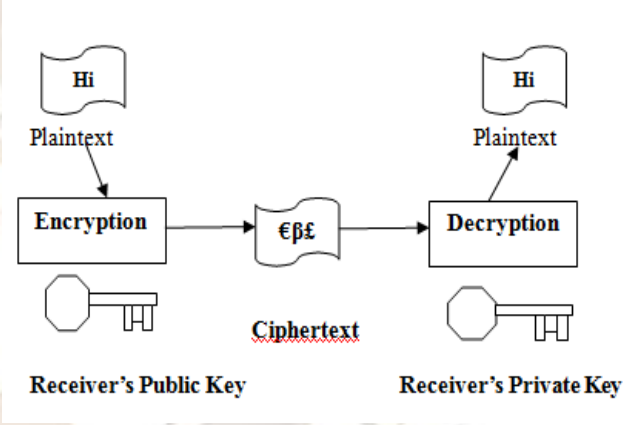

Fig.1. Public Key Cryptographic Algorithm[3].

b. Symmetric Algorithm :

Also called as a private key algorithm or the secret key cryptographic algorithm.

As its name suggests, it makes the use of same key for both encryption and decryption processes [3].

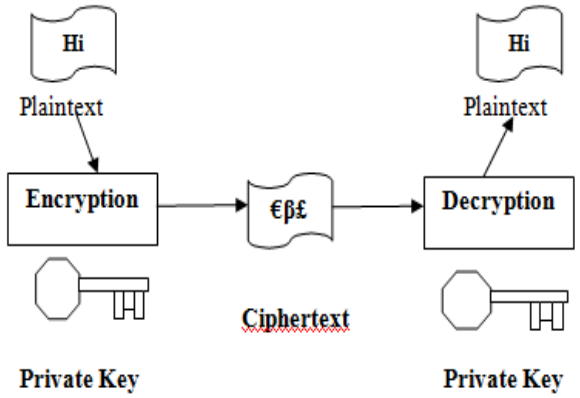

Fig.2. Private Key Cryptographic Algorithm[3].

Again the Symmetric Algorithms are further classified into two main categories [3]:

b.1. Block Ciphers :

In block ciphers, the whole data is divided or organized into the groups or blocks, so it is called as the block ciphers [4].

b.2. Stream Ciphers :

In stream ciphers, instead of grouping the data, only single bit data is sent at a time and so it is operated in real-time manner [5].

So the Symmetric block ciphers are most widely used in order to protect the data against the intrusion, or theft and to provide security and confidentiality to the data which is on the way of medium.

The most widely used Symmetric block ciphers to solve the problem of communication over unsecure channel nowadays are DES (Data Encryption Standard), T-DES (Triple Data Encryption Standard), and AES (Advanced Encryption Standards).

2. VARIOUS ENCRYPTION STANDARDS AND THEIR IMPLEMENTATIONS ON FPGA.

To solve the problem of communication over unsecure channel large number of symmetric block ciphers is used. Out of them, the following are the most widely used:

2.1 DES (Data Encryption Standard),

2.2 T-DES (Triple Data Encryption Standard),

2.3 AES (Advanced Encryption Standards).

Such encryption standards can be implemented various hardware like ARMs, ASICs or FPGAs.

2.1 DATA ENCRYPTION STANDARDS (DES)

2.1.1 An Overview of Data Encryption Standards (DES)

The United States National Institute of Standards And Technology (NIST) initially recommended the first standard i.e. Data Encryption Standard in order to protect the most sensitive, and valuable data and to keep the particular data more secured and confidential.

Basically the DES is the encryption method which is best applicable for non-military and the non-classified use, and it was designed by IBM in 1977[6].

The input to Encryption algorithm is 64-bit plaintext whereas it uses 56-bit cipher key and finally it provides the 64-bit cipher text. Our original text information is passed through various 19 processes which are very complex, each step using previous stage output in the form of an input to the next stage. Finally the 64-bit cipher text is available to us in the form of output of encryption

process. The same method is used for decryption purpose in reverse manner giving the 64-bit plaintext in the form of an output [7].

2.1.2 Implementation of Data Encryption Standards (DES) on FPGA:

Various hardwares can be used to implement the DES algorithms on board. It may be ASICs, ARM, or FPGAs.

The single chip implementation can be done with the help of Xilinx XC4000 series Field Programmable Gate Arrays (FPGA) [8].

General DES Algorithm.

The process of DES uses a key of length 56-bits, and the data in the form of plaintext of 64-bits.

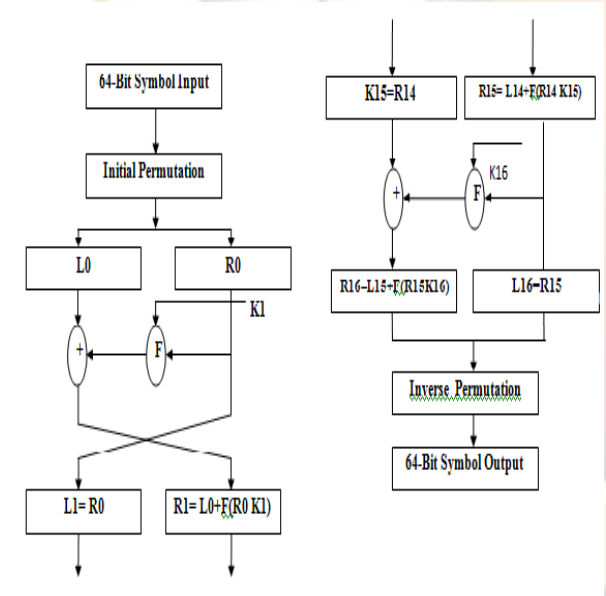

Fig.3. Block Diagram of DES Algorithm Iteration[8].

Fig.3. shows the block diagram of DES algorithm. Here 64 bit block of data is taken as an input. It is applied for the Initial permutation process so as to give the 64-bit output data. The 56-bit key generates sixteen 48-bit sub keys. It uses rounding algorithm concept. In each round, 64-bit output of 1st round is given to the 2nd round in the form of an input and the process is carried forward through the next consecutive rounds. Finally, 64-bit cipher text output is produced.

Whereas at the receiver section, after 16th round, 64-bit output is given to the inverse of initial permutation. In this way, the DES algorithm operates.

Actual FPGA implementation:

The Xilinx XC4000 series DES implementation can be best described in the following manner. It includes various processes as follows:

Scheduling key design process,
Round function Iteration,
S-Box implementation,
Initial Permutation and
Inverse Initial Permutation.

All the processes are executed one after another. The input symbol is given to the system. Simultaneously Key registers executes the process of designing the key required for the purpose of encryption. It performs such operation by providing the keys through multiplexer block. Once the key is designed, then round function iterations are performed. By making the use of Fig.3, the initial permutations and inverse initial permutations are executed.

However as the technology progresses, the code generated by the DES was easily detected. That means, the encrypted cipher text was easy to break [7].

This was one of the main drawbacks of Data Encryption Standard (DES) algorithm.

Whole DES operation is performed with the help of various blocks, each performing the specific functions can be shown as follows -

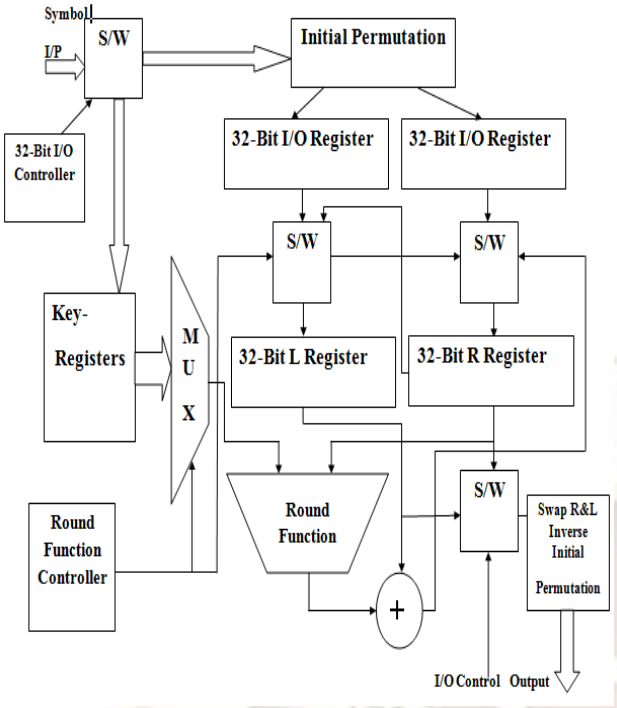

Fig.4. Block Diagram of DES Implementation[8].

Fig.4 shows the DES-Implementation block schematic.

2.2. TRIPLE DATA ENCRYPTION STANDARDS (T-DES)

The main drawback in Data Encryption Standards (DES) was that, the cipher text generated by this technique was detected very easily.

Due to such limitations, the United States government discovered the new Encryption Standard known as 'Triple Data Encryption Standard', shortly abbreviated as T-DES [7].

The T-DES applies the DES algorithm three times to the plaintext in order to get the cipher text. So when we use key K and apply it to the DES algorithm we get the E_K (I) as the encryption of I and D_K(I) as the decryption of I. Then we apply such DES algorithm three times and finally the available output was the actual output of T-DES process [7].

The encrypted T-DES output of I was $E_{K3}(D_{K2}(E_{K1}(I)))$ where K_1, K_2 and K_3 are the three keys.

The decrypted T-DES output of I was $D_{K1}(E_{K2}(D_{K3}(I)))$ where K_1, K_2 and K_3 are the three keys[7].

2.3 ADVANCED ENCRYPTION STANDARDS (AES)

2.3.1 An Overview of Advanced Encryption Standards (AES)

The National Institute of Standards and Technology (NIST) got this standard in the form of protecting standard after making the call for security standards in 1997. There was the need of standard which could fulfil the requirements like the algorithm should be royalty free and publically disclosed algorithm based on symmetric key cryptography as a block cipher. And the block size to be taken was 128-bits, 192-bits and 256-bits.After the call for submitting the security standards and after performing the various selection procedures of scrutiny, the AES was finally selected as the widely accepted security standard out of the 15 candidate standards. AES is simple, secured and can be suited to both hardware and software implementation [1]. All the factors were fulfilled by the well known Rijndael algorithm. This algorithm was developed by two persons Vindert Rijmen and Daemen [9].

So depending upon the size of the block the various algorithms were developed. The block sizes used were 128-bits, 192-bits and 256-bits. The operation of AES 128-bits, 192-bits and 256-bits was performed by using 10, 12,14 number of rounds. Following Fig.5 shows the AES-128 algorithmic structure utilising 10 round transformations.

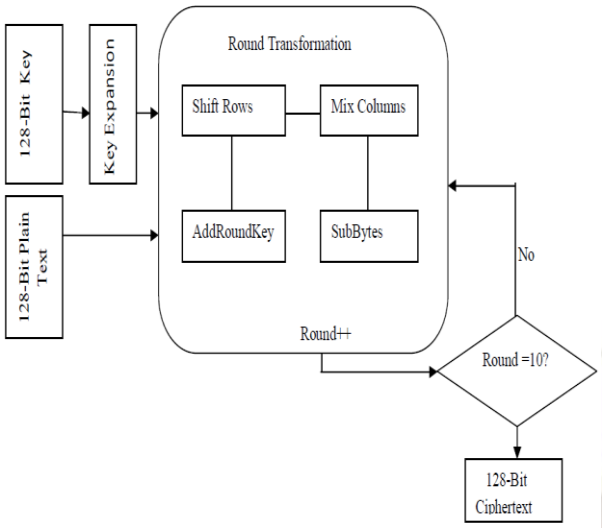

Fig 5: AES 128 Algorithmic Structure[10].

Fig.5 [10] shows the structure of an Advanced Encryption Standards (AES-128E). Such algorithm is performed on RC-10 prototyping board having Spartan III FPGA chip [10].

2.3.2 AES implementation on FPGA:

Encryption Process:

The process of encryption implemented on FPGA is AES-128 implementation shown in Fig 6[11]. The data which is received at AES encryption block undergoes mainly four operations-

a. Sub-bytes Operation :-

Also called as bytes substitution. Here 128-bit block is taken. Its input is then divided into 16 bytes and they are arranged in the form of 4x4 matrix. Such matrix is called as state matrix.

A00	A01	A02	A03
A10	A11	A12	A13
A20	A21	A22	A23
A30	A31	A32	A33

Then S-box is taken and the transformations are performed such that the substitution process occurs. And its output is given by the another matrix given below-

B00	B01	B02	B03
B10	B11	B12	B13
B20	B21	B22	B23
B30	B31	B32	B33

b. Shift Rows Operation :-

It performs the diffusion process. Here the row 1 is shifted by one byte, row 2 is shifted by two bytes and row 3 is shifted by three bytes keeping row 0 unshifted. So the original matrix is,

B00	B01	B02	B03
B10	B11	B12	B13
B20	B21	B22	B23
B30	B31	B32	B33

After such transformations, the output available is given by another matrix as follows –

C00	C01	C02	C03
C10	C11	C12	C13
C20	C21	C22	C23
C30	C31	C32	C33

c. Mix Columns Operation :-

It is also called as multiply columns.

Here multiplication of the standard matrix which is in hexadecimal is done with the matrix which is obtained in shift rows operation. The output matrix thus produced is given as follows –

The standard matrix is as follows -

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

and output matrix is

D00	D01	D02	D03
D10	D11	D12	D13
D20	D21	D22	D23
D30	D31	D32	D33

d. Add Round Key Operation :-

Here, the output matrix of previous step is X-ORED with the round key. The original key is 128-bot in size. The expansion of the matrix done into 40 more columns. Various transformations are

performed to get the exactly required cipher text. One thing is very much important to be noted here is that, for r-1 rounds all of the above mentioned four steps are performed. Whereas for the last round, only Sub-byte operation, Shift Rows operation and Add Round Key operations are performed.

The following Fig. 6[11] represents the flowchart for whole encryption process –

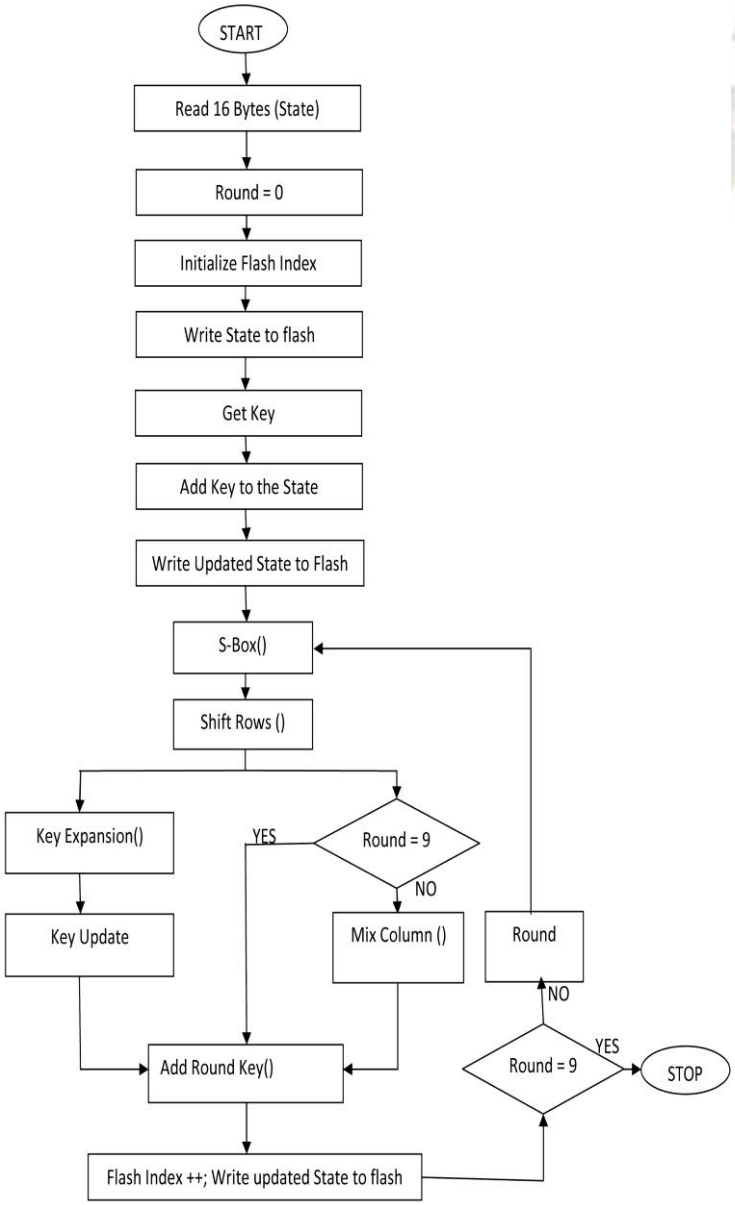

Fig 6: Encryption Design Flow [11].

Decryption Process:-

After performing the encryption process to get the cipher text at the transmitter section that cipher text needs to be converted into the plaintext again. So such cipher text again undergoes four main operations as follows -

a. Inverse Sub-Bytes Operation.

b. Inverse Shift Rows Operation.

c. Inverse Mix Columns Operation.

d. Inverse Add Round Key Operation

The entire decryption process is shown by a flowchart given above in Fig. 7[11].

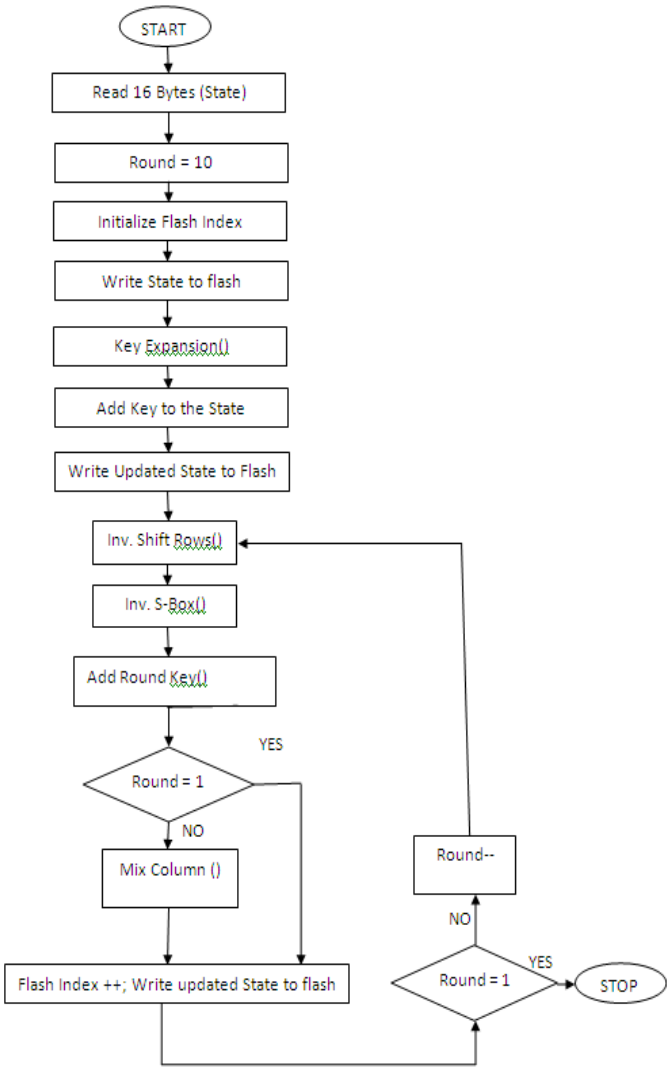

Fig 7: Decryption Design Flow [11].

All these operations are performed exactly reverse manner so as to recover the plaintext through cipher text with the help of decryption process.

3. SUMMARY AND COMPAROSION BETWEEN THE DES AND AES IMPLEMENTATION RESULTS

Initially, the single chip implementation of DES algorithm is performed taking single FPGA device i.e. a using Xilinx XC4013E series [8]. The resources used were 438 Combinational Logic Blocks (CLBs) and 54 Input/Output blocks (IOBs) keeping the average connection delay of 8.27211 nsec the speed of 26.7 Mbps [8], it achieved the throughput of 26.7 Mbits/sec (3.34 Mbytes/sec) [8]. The conclusion drawn is that, if the single chip ilmplementation is performed instead of using the three FPGA chips, more security can be provided o the data [8].

But for the same purpose if AES algorithm is used for the encryption and decryption purpose, then the results were different and gave better throughput.

If optimized sub-pipelined architecture is taken for implementation purpose with device XC4VLX85, using 40 Block RAMs, frequency 500 MHz and the number of slices 8901, then the throughput of 64 Gbps can be achieved. Per slice the throughput will be 7.19 Mbps [12].

4. CONCLUSION AND FUTURE SCOPE OF WORK

DES and T-DES algorithms were providing the secured data transmission. The cipher texts generated by them were easily broken and also the throughputs obtained were very low.

But AES overcomes all the drawbacks ok DES and T-DES algorithms. AES provides strong cryptographic features. To prove this, one simple example is taken. The key size used in DES is 56-bits, in decimals 7.2×10^{16} possible keys. Whereas in AES keys of different sizes i.e. 128-bits, 192-bits and 256-bits are used, in decimals there are 3.4×10^{38} possible keys, 6.2×10^{57} possible 192-bit keys and 1.1×10^{77} possible 256-bit keys.

Means there are 10^{21} more 128-bit keys than 56-bit keys. If any machine is assumed to be detecting the DES key in a second, such device will take 149 thousand years to crack the 128-bit AES key. This is the main reason behind using the the AES cryptographic algorithm nowadays.

Various wireless communication techniques like Bluetooth, Zigbee or WiFi can be implemented on FPGAs. Out of which the Bluetooth is already implemented on FPGAs in some papers which uses 128-bit keys. But to increase the flexibility by increasing the key sizes up to 192-bits or 256-bits, the more efficient algorithms can be developed in future.

REFERENCES

[1] Mamta Sood, Manohar Wagh and Monika Cheema, "Implementation of a Wireless Communication System – A Review", in International Journal of Computer Applications (0975 – 8887) Volume 63– No.15, February 2013.

[2] Mohammad Fakir Husain Starker and Md. Sheffield Pares, "A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount Of Data".

[3] Naïf A. Kofahil, Turkic Al-Somali and Khalid Ai-Zamia "Performance Evaluation Of Three Encryption/Decryption Algorithms", in 0-7803-8294-3/04/$ 20.00-2004 IEEE, Pages 790-793.

[4] M.J.B Robs haw, "Block Ciphers", Technical Report, RSA Laboratories, Number TR – 601, July 1994.

[5] M.J.B. Robs haw, "Stream Ciphers" Technical Report, RSA Data Security, Inc., Number TR-701, Pages 46, and July 1995.

[6] National Bureau of Standards (U.S.), "Data Encryption Standards (DES)", Federal Information Processing Standards Publication 46, National Technical Information National Technical Information Service, Springfield, VA, April 1977.

[7] Tariq Jamal, "IEEE POTENTIALS", 0278-6648/04/$20.00, IEEE 2004, April-May 2004. Pages 36-38.

[8] K. Wong, Mewari and E. Dawson, "A Single Chip FPGA Implementation of" The Data Encryption Standard (DES) Algorithm", In 0-7803-4984-9/98/$10.00,IEEE 1998.

[9] J. Daemen and V.Rijmen, "The Block Ciphers Rijndael", Lecturer Notes In Computer Science, Vol.1820/2000, pp. 277-284.

[10] Joseph Zambreno, David Nguyen and Amole Chaudhary. Exploring Area/ Delay Tradeoffs in an AES FPGA Implementation. In Proceedings of the 14th Annual International Conference on FPLA. Pages 575-585. Springer 2004).

[11] Anural Gupta, Afandi Ahmadd, Mhd Saeed Sharif And Abbes Amira, "Rapid Prototyping of AES Encryption For Wireless Communication System On FPGA".

[12] Dong Chen, Guochu Shou,Yihong Hu, Zhigang Guo," Efficient Architecture & Implementations of AES" In 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, Pgs V6-295 V6-298.