ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

RFID Based Attendance Monitoring & Power Saving System

N Ramesh[1], R.Prakash[2], P.Sivapriyan[3], V.Gowsick[4], K.B.Praveen Chand[5]

Assistant Professor, Department of Mechanical and Automation Engineering, Mahendra Engineering College, Namakkal, Tamil Nadu, India[1]

U.G. Student, Department of Mechanical and Automation Engineering, Mahendra Engineering College, Namakkal, Tamil Nadu, India[2]

U.G. Student, Department of Mechanical and Automation Engineering, Mahendra Engineering College, Namakkal, Tamil Nadu, India[3]

U.G. Student, Department of Mechanical and Automation Engineering, Mahendra Engineering College, Namakkal, Tamil Nadu, India[4]

U.G. Student, Department of Mechanical and Automation Engineering, Mahendra Engineering College, Namakkal, Tamil Nadu, India[5]

ABSTRACT: In numerous sensor network devices, security is one of the critical issues. A number of symmetric-key encryption algorithms are employed in sensor network hardware and based on standard cryptography, many security algorithms are enhanced for wireless sensor network devices. However, many of these cryptographic algorithms contain own weakness, such as susceptible to selected plaintext attack, password attacks and computational complexity. In WSN, the security of Radio Frequency Identification (RFID) tags contain drawn wide attention from both academia and industry due to the possible wide RFID exploitation and lightweight cryptography in RFID is a significant mechanism in the security information of RFID devices. Therefore, a lightweight cryptographic Multilanguage Two Dimensional Array Substitution Technique (MTDAS) algorithm is presented for RFID tags in this paper to reduce the computational complexity and increase the security during the deployment. This MTDAS algorithm and its low power computational, size optimized accomplishment goals at very embarrassed devices such as passive RFID tags. Our proposed algorithm MTDAS gives cryptographic primitives at very low cost is of dominant significance for protecting applications of RFID. This MTDAS cryptographic algorithm was implemented by using multilingual characters set table. This table is dynamic in nature, and this type of encryption doesn't have any relationship between ciphertext and plaintext, so it is difficult for an intruder to get back the plaintext.

KEYWORDS: Wireless Sensor Networks, Security, Multilanguage Two Dimensional Array Substitution Technique (MTDAS), Lightweight cryptography, Radio Frequency Identification (RFID).

I.INTRODUCTION

Wireless sensor networks (WSNs) have base station and have battery-powered and low-cost devices known as sensor nodes. A Sink node is a powerful base station which gathers sensing data from sensor node and also progresses the data for transmits instructions to all sensor nodes. In WSN, the battery-powered sensor nodes collects data which senses the surrounding environment broadcast them through network [12]. Conversely, there is security impendence due to nature of the wireless sensor network and the constrained resource nature in WSNs. Specially, in an environment

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

where the protection and composed data privacy is significant, channel of secure communication must be recognized for between the sensor nodes. Therefore, in WSN, numerous cryptographic algorithms are enhanced. Nevertheless, many of the cryptographic algorithms are not sustained to lightweight process; therefore computation complexity is enhanced during the process of encryption and decryption to present secure communication in sensor nodes in WSN. Hence, the lightweight cryptographic process is necessary to decrease the computational complexity and energy consumption in WSN hardware devices [8][9].

Lightweight cryptography is generally described as cryptography for resource- constrained devices such as WSN hardware devices. It aims at a very wide variety of WSN devices. This system is implemented on a wide range of hardware and software and their communication is either wired or wireless devices. Hence for a number of applications, either energy or power consumption is essential, as for other applications a low latency is much more significant. The hardware area or size of software code is a limiting factor or that only a small amount of RAM is obtainable [5][6][7]. Further frequently than not, a combination of the aforesaid criteria needs to be satisfied. Therefore, we implement a lightweight cryptographic MTDAS algorithm for wireless sensor devices, especially in RFID devices.

RFID systems, specified the advantages of low cost and expediency in recognizing an object with non line of sight reading, containing numerous applications and numerous possible applications, such as in developed, provide access control, inventory control, chain management, e-passports, pharmacies/hospital management, etc. Conversely, there are a many malicious attacks against RFID methods, which are classified to active and passive attacks [2][3]. The attacks are modifying too by enhancing RFID methodology day by day. Depending on the huge number of using applications of RFID and by considering that RFID tags may have responsive private data like biomedical data or health, the security significance in RFID has risen. By considering the nature of RFID tags, to decrease the security effect and privacy issues, it is desirable to execute various encryption algorithms; these smart devices contain extremely constrained resorts in terms of memory, computational capabilities and power supply. In RFID tags, these limitations can create planning a secure tag further complicated because in order to progress a security, strong encryption algorithm is executed but there is no longer sufficient processing capacity [10][11]. To individuals and corporations, the risks consist of disclosing sensitive information considering labeled products to adversaries, allowing incorrect information from counterfeit tags/spoof tags, discovering one's individuality or location by tracking exact tags, and losing business due to denial of service attacks [3][5]. Hence, the preferred security necessities for RFID systems should contain contented privacy, availability, anonymity, authentication, and un-traceability. Consequently, current encryption algorithms that were considered for standard computer is not suitable for RFID tags because in order to realize these kinds of encryption, adequate computational ability, sufficient memory and power should be provided.

In this paper, MTDAS algorithm is presented in RFID devices to provide more security and low computational cost and low energy consumption of deployment. MTDAS is a cryptographic algorithm using Multilanguage with two dimensional array substitutions. MTDAS attains sufficient protection against recognized attacks and flexibility for competent execution in both hardware and software. It is notified that MTDAS is extremely proficient mainly in implementations of hardware in WSN.

III. RELATED WORK

Hung-Yu Chien, et.al, presented a novel RFID authentication protocol based on Error Correction Codes (ECC). This presented method has efficient performance in terms of efficiency, security, maintenance of server, robustness and cost. The tag only executes effortless tasks, such as simple bitwise computations and generation of random number. This lightweight process made it desirable to those low-cost RFIDs that sustain only simple tasks.

Woo Kwon Koo et.al, implemented a novel lightweight cryptographic algorithm HIGHT on Mica2 and the performance between HIGHT and realized cryptographic algorithms on TinySec is analyzed. Finally the performance appraisal of implementation has been showed. Hence, HIGHT is suggested for TinySec is concluded as like established cryptographic algorithms on TinySec.

Shweta Gaba et.al., analyzed and estimated the improvement of a contemptible and moderately implementation of fast hardware of the extended tiny encryption algorithm (XTEA). Initially the research was divided into detach units of encipher/decipher, but these has been united into a single unit. The plan can start by employing

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

finite state machine (FSMs) and it can utilize Verilog hardware description language to explain the plan. Reducing the area of chip and data transmission security was their major objective. The targeted hardware systems are the Xilinx Virtex IV modern field programmable gate arrays (FPGAs) and reconfigurable Spartan III.

Jacob John et.al, described an implementations of hardware of several effective light weight cryptographic algorithms and Security features. It is discovered that contrasted to stream ciphers and block ciphers are further appropriate for resource inhibited environments. The block ciphers AES, DESL, HIGHT, PRESENT gives efficient security to the data during the transmission. The HIGHT throughput is high compared to other block ciphers, which displays its progressing speed is more rapidly. The necessity of hardware resource of PRESENT is moderately less, which is only 1570 GEs. The humming bird-2 is including the stream cipher and block cipher properties. One more advantage of Humming bird-2 is that its energy utilization is low and speed of processing is more rapidly.

Diana Maimut et.al, focused on solutions of explaining lightweight-cryptography for RFID tags. It analyzed potential risks and the estimates researchers have taken to develop their privacy and security level.

Jehan-Francois Paris, et.al, presented enhancing the data of survivability stored in two-dimensional RAID arrays by allowing these arrays rearrange themselves when they identify a failure of disk. This rearrange can rebalance as much as probable the level of redundancy of every stored data, therefore minimizing the possible impact of further disk failures. It remains in consequence until the failed disk obtains mended. In this process, showed how this method is employed to two-dimensional RAID arrays containing 2n parity disks and n2 data disks and showed how it is enhance the mean time to array data loss by at least 200 percent as long as the rearrange process gets less than semi the time it obtains to restore a failed disk.

III. PROPOSED METHODOLOGY

A. MTDAS: Multilanguage Two Dimensional Array Substitution Technique

In this paper, we propose a MTDAS algorithm for RFID tags to reduce the computational complexity and provide the more security during the communication. MTDAS is presented to adopt novel advancing methodology, Lightweight Cryptography, in the RFID tags. We use our proposed algorithm MTDAS for following two reasons.

1. Effectiveness of end-to-end secure communication

In order to attain end-to-end security, WSN nodes have MTDAS cryptographic algorithm implementation. The cryptographic tasks with a limited amount of energy consumption are significant for the low resource devices, example battery-powered devices. Therefore, our proposed algorithm allows lower energy consumption for WSN devices.

2. Applicability to lower resource devices

This lightweight cryptographic primitive is smaller than the conventional cryptographic ones. Lightweight cryptographic primitives of our proposed algorithm can open probabilities of further network connections with lower WSN resource devices.

In this MTDAS technique, the Unicode value is obtained for each Multilanguage plaintext character. The constant value is assigned for mapping (M). Then the Unicode value is divided by mapping constant (M) which gives the quotient (Q) and reminder (R) value. The reminder values are grouped as two values in each group. The serial numbering is given to the grouped values and it is separated according to the odd and even numbers. The group named Odd is noted as (Row, Column) and the group named Even is noted as (Column, Row). The character for (Row, Column) and (Column, Row) is written from MTDAS 3 x 3 matrix. This is the cipher which we get from this method.

As an example consider the below given TABLE 1, 2 and 3 of encryption, 2D mapping array and decryption of MTDAS where the value for M=3 is assigned. The Unicode value for G is 71 so by dividing 71 by 3 we get Q=23 and R=2 similarly if we consider for the letter O the Unicode is 79 and is divided by 3 we get Q=26 and R=1. Then the reminder values (2, 1) are grouped. This assigns a serial value of 1 so it is consider as an odd parity. In the mapping array table if it is an odd then (row, column) is considered. For even numbers (column, row) are considered. But in this encryption technique only 3*3=9 characters are available so there is a possibility for frequency analysis since only 9 characters get repeated in the cipher text. The encryption and Decryption for the proposed methods are shown in TABLE 1 and 3.

Steps in MTDAS Encryption Algorithm

Step 1: Getting the plain text character by character.
Step 2: Getting Unicode for character (U).
Step 3: Getting the Mapping Constant (M).
Step 4: Calculating Quotient for each character Q = U/M.
Step 5: Getting Remainder value for each character R=U%M.
Step 6: Group every two Reminder value, At last if you are not getting pair choose any M value (0,1,2…etc) and then group it.
Step 7: Assign serial numbering for every group.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Step 8: Split serial Numbering as odd and even for each group.
Step 9: For odd value serial number, First value in the group states Row and second value states the Column.
Step 10: For even-value serial number, First value in the group states column and second value states the row.
Step 11: Using Step 9 and Step 10, Refer the two dimensional array to get a Block cipher value.

Steps for processing the 'Q' values

Step 1: The obtained quotient (Q) values form the MTDAS method in the encryption process has to be separated as an odd and even parity.
Step 2: If the resultant is an odd parity then single right side rotation of the corresponding quotient bits is done and the rotated bits is NOTed using NOT gate.
Step 3: The NOTed output bits and the cipher text from TABLE 1 are given to 21 bit permutation block. The permuted output is obtained.
Step 4: The 21 bit permutation output and the 21 bit key values are added (XOR operation).
Step 5: This is the final cipher text obtained by encrypting both quotient and reminder values.
Step 6: In other hand if the resultant bits are even then double right side rotation is done.
Step 7: The rotated output and the cipher text from TABLE 1 are given to another 21 bit permutation block.

Table 1 MTDAS Encryption

Plain Text (Multi Language)	**G**	**O**	**D**	**B**	**L**	**E**	**S**	**S**	**Y**	**O**	**U**
Unicode (U)	71	79	68	66	76	69	83	83	89	79	85
Two Dimensional Mapping Constant (M) (Multi Language)	3	3	3	3	3	3	3	3	3	3	3
Quotient Q= U / M	23	26	22	22	25	23	27	27	29	26	25
Reminder R=U mod M	2	1	2	0	1	0	2	2	2	1	0
Reminder Grouping	2,1		2,0		1,0		2,2		2,1		1,0
Serial Numbering	1		2		3		4		5		6
Parity Assignment	Odd		Even		Odd		Even		Odd		Even
Row and Column	Row, Column		Column, Row		Row, Column		Column, Row		Row, Column		Column, Row
Block Cipher	**ஆ**		**ய**		**ந**		**அ**		**ஆ**		**அ**

Table 2 Two dimensional mapping array table with M=3

Block Cipher (Multilanguage)	**ஆ**		**ய**		**ந**		**அ**		**ஆ**		**அ**
Row and Column	Row, Column		Column, Row		Row, Column		Column, Row		Row, Column		Column, Row
Parity Assignment	Odd		Even		Odd		Even		Odd		Even
Serial Numbering	1		2		3		4		5		6
Reminder Grouping	2,1		2,0		1,0		2,2		2,1		1,0
Reminder R=U mod M	2	1	2	0	1	0	2	2	2	1	0
Quotient Q=U/M	**23**	**26**	**22**	**22**	**25**	**23**	**27**	**27**	**29**	**26**	**25**
Two Dimensional Mapping Array Constant (M) (Multilanguage)	3	3	3	3	3	3	3	3	3	3	3
Unicode (U)	71	79	68	66	76	69	83	83	89	79	85
Plain Text	**G**	**O**	**D**	**B**	**L**	**E**	**S**	**S**	**Y**	**O**	**U**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Table 3 MTDAS Decryption algorithm

	2	1	0
2	अ	आ	इ
1	ई	ट	ठ
0	ਘ	அ	ஆ

B. Hardware MTDAS Encryption

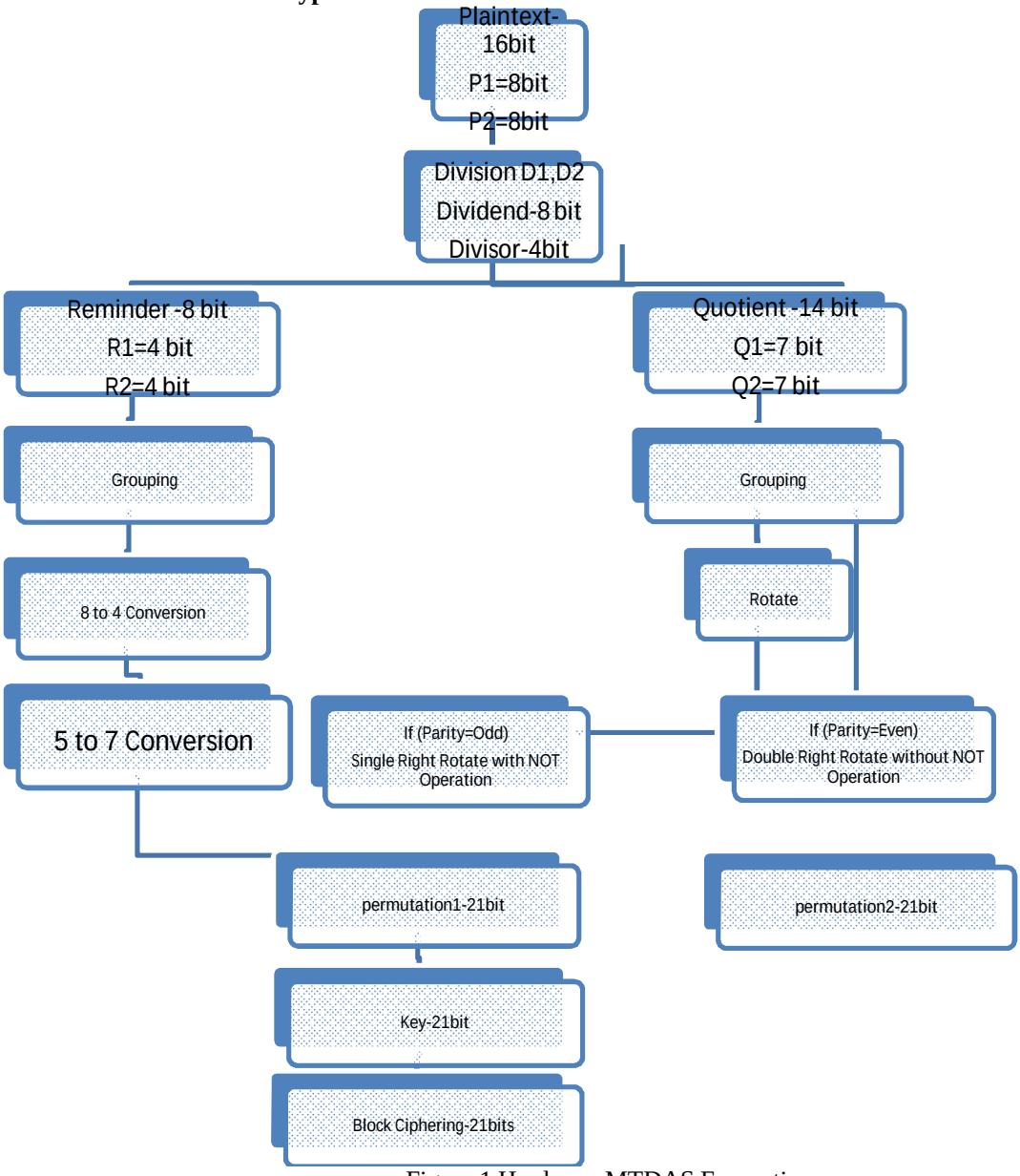


Figure 1 Hardware MTDAS Encryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

The hardware MTDAS algorithm has been shown in Figure 1. In this process, first we assign the Unicode value to each letter of plain text, after that the Unicode value of plaintext is converted into binary value. The binary division is performed based on dividend 8 bit and divisor 4 bit. The binary value of each plaintext value divided by the 'M=3' value which gives the quotient (Q) value and reminder (R) value. In binary division, the quotient value is represented in 7 bit since maximum hexadecimal value used here is FF which when divided by 3 and the reminder value is represented in 4 bit since the reminder values lies between 0, 1, 2. Since here the M value is 3. From the obtained values of reminder by the binary division process, the grouping of the reminder values is done. Each of the 4 bit values of reminder 1 & 2 (R1, R2) is grouped. These grouped values get reduced from 8 bit to 4 bit. This four bit value is added along with the parity bit. For an odd parity binary value '0' is added. For even parity binary value '1' is added. Then five to seven conversions are executed. The obtained quotient values (Q) from the division process are grouped (Q1,Q2). This grouped 14 bit values are now given to the binary right rotation block. The permutation method is applied after 5 to 7 bit conversions. In permutation process, the rotated 14 bits are now given to the permutation block along with the 7 bit obtained from the output of Five to Seven conversions. The initial permutation of this 21 bit is done. The separate permutation is done for odd and even parity. If parity is odd, single right rotate with NOT operation can be executed, otherwise the single right rotation is performed without NOT operation. The key 21 bit is applied after permutation, after that XOR operation is added. Finally, the plaintext is encrypted.

C. Hardware MTDAS Decryption

Figure 2 shows the hardware MTDAS decryption, it is inverse operation of hardware MTDAS encryption. In this process, the block ciphering 21 bit is converted into plain text. Inverse permutation is executed using the key 21 bit. The reverse process of permutation gives the inverse permutation. The inverse rotation is employed after reverse permutation. The reverse process of rotation that is doing left side rotation gives the inverse rotation. Seven to five and four to eight bit conversions are executed after inverse rotation. After inverse rotation, inverse binary is applied. In binary division, the obtained quotient value (Q) and divisor value (D) are multiplied and its output is added with the reminder value (R). finally the plain text is obtained from cipher text.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

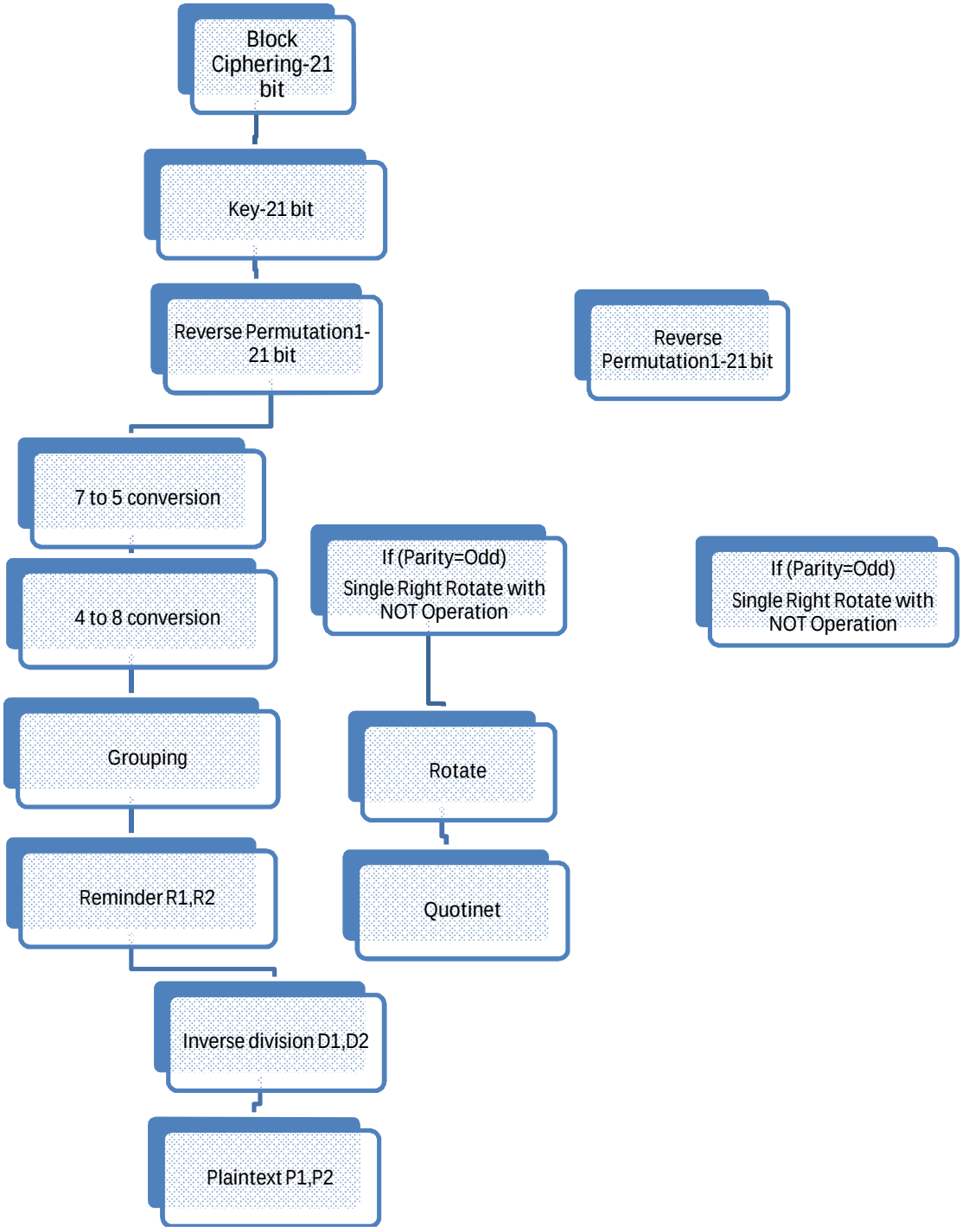


Figure 2 Hardware MTDAS Decryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

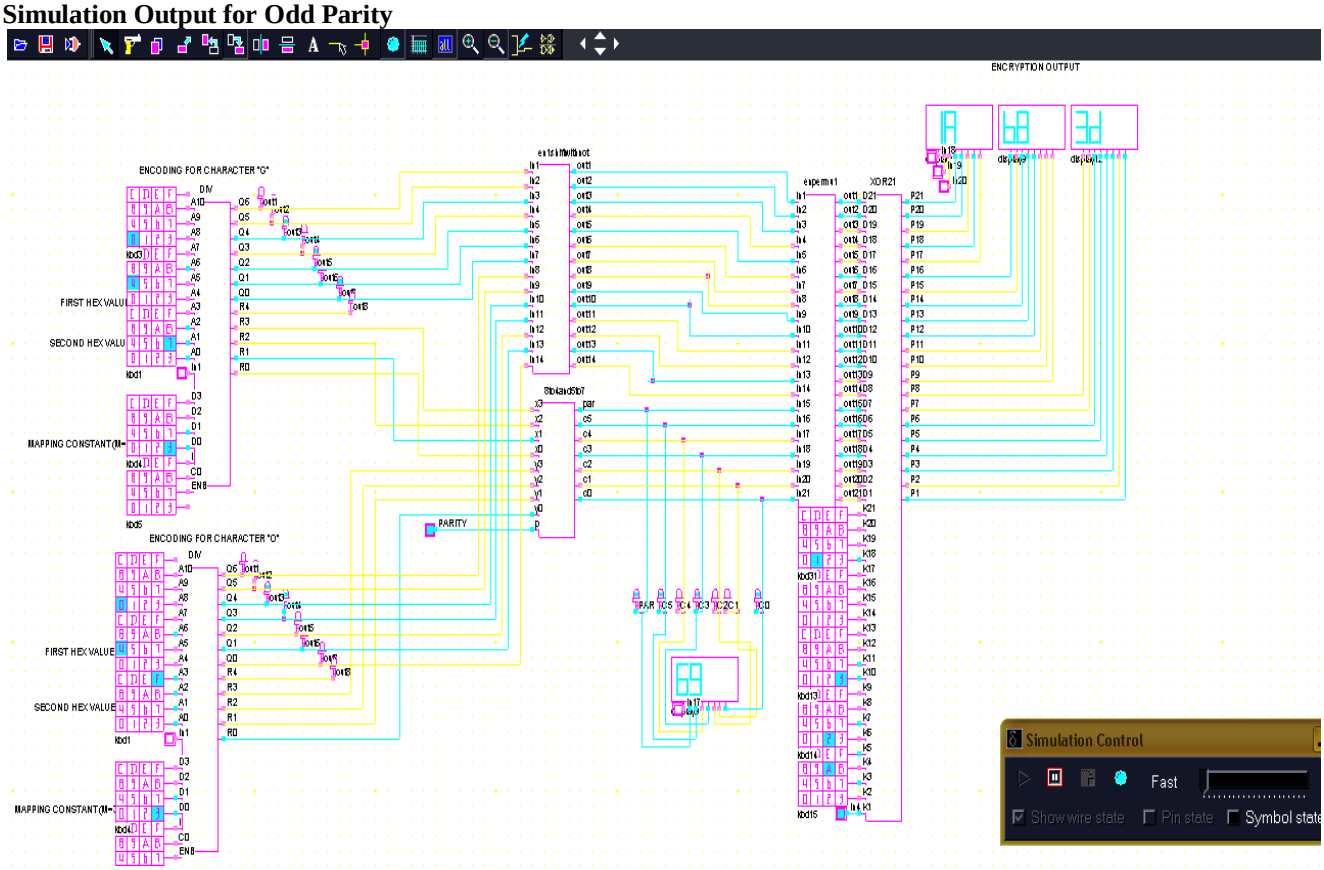
IV. RESULTS AND DISCUSSIONS

A. TOTAL ENCRYPTION BLOCK

For Odd Parity

The below shown is the simulation output for the whole Encryption block for odd parity. The first block is the Division block. The Unicode value of input in binary form is given to Division block. It gives the quotient (Q) and reminder (R). The grouped 'Q' values are given to the Rotation block and its output is given to INVERTER and the grouped 'R' values are given to 8 to 4 conversions and 5 to 7 conversions block and for the parity value '1' is given. The output of both 'Q' and 'R' values are given to the Permutation block. The permuted output and the key values are finally given to XOR block and the final encrypted output is displayed in the Hexadecimal display.

Simulation Output for Odd Parity



For Even Parity

The below shown is the simulation output for the whole Encryption block for odd parity. The first block is the Division block. The Unicode value of input in binary form is given to Division block. It gives the quotient (Q) and reminder (R). The grouped 'Q' values are given to the Rotation block and the grouped 'R' values are given to 8 to 4 conversions and 5 to 7 conversions block and for the parity value '0' is given. The output of both 'Q' and 'R' values are given to the Permutation block. The permuted output and the key values are finally given to XOR block and the final encrypted output is displayed in the Hexadecimal display.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

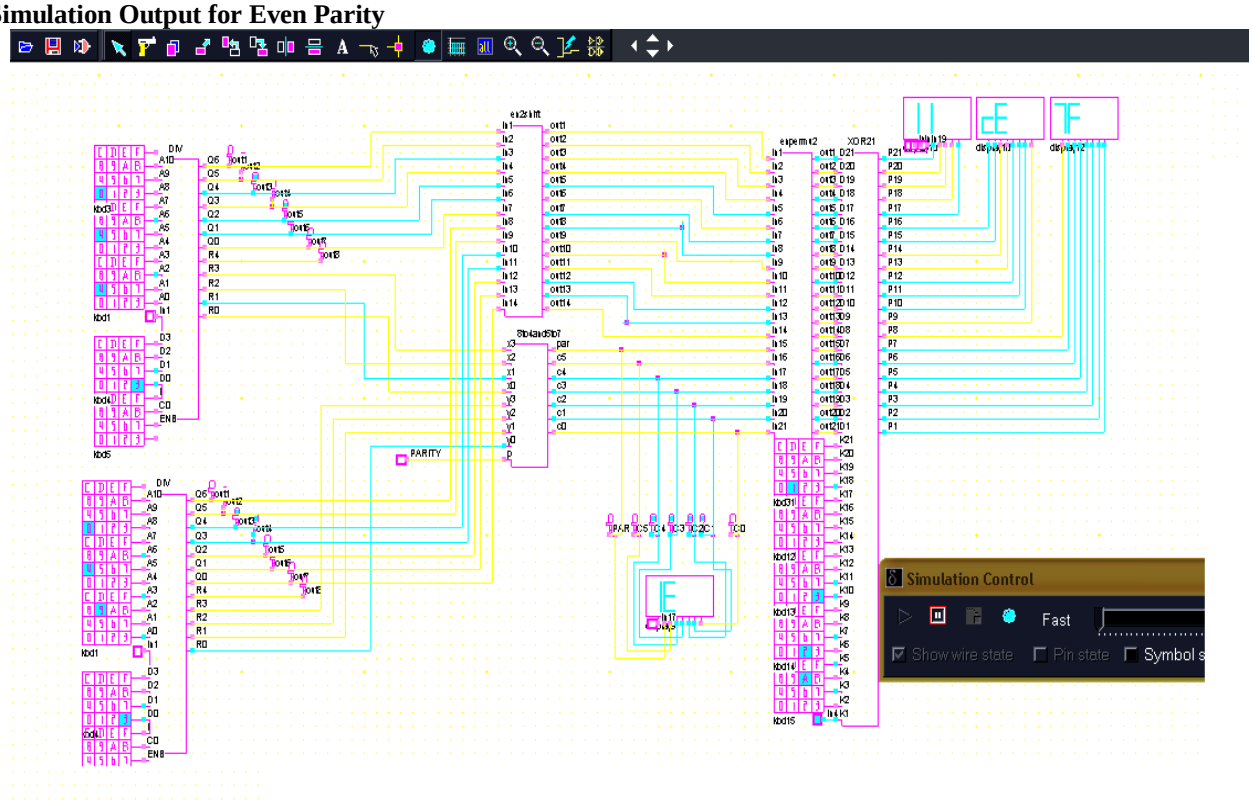
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Simulation Output for Even Parity



B. TOTAL DECRYPTION BLOCK

For Odd Parity

The reverse process of the encryption gives the decryption. The encrypted output and the 21-bit key values are first given to the XOR block. Its output is then given to the Inverse Permutation block. The first 14 bit values are given to Inverse Rotation block and the remaining 7 bit are given to 7 to 5 and 8 to 4 conversion block. The output of the Rotation block yields the 'Q' value and the output of 7 to 5 and 8 to 4 conversion block is the reminder 'r' value. The 'Q' and the 'R ' value are given to the Inverse Division block. Then the divisor value 3 is given to that block finally we get an input Plain Text.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

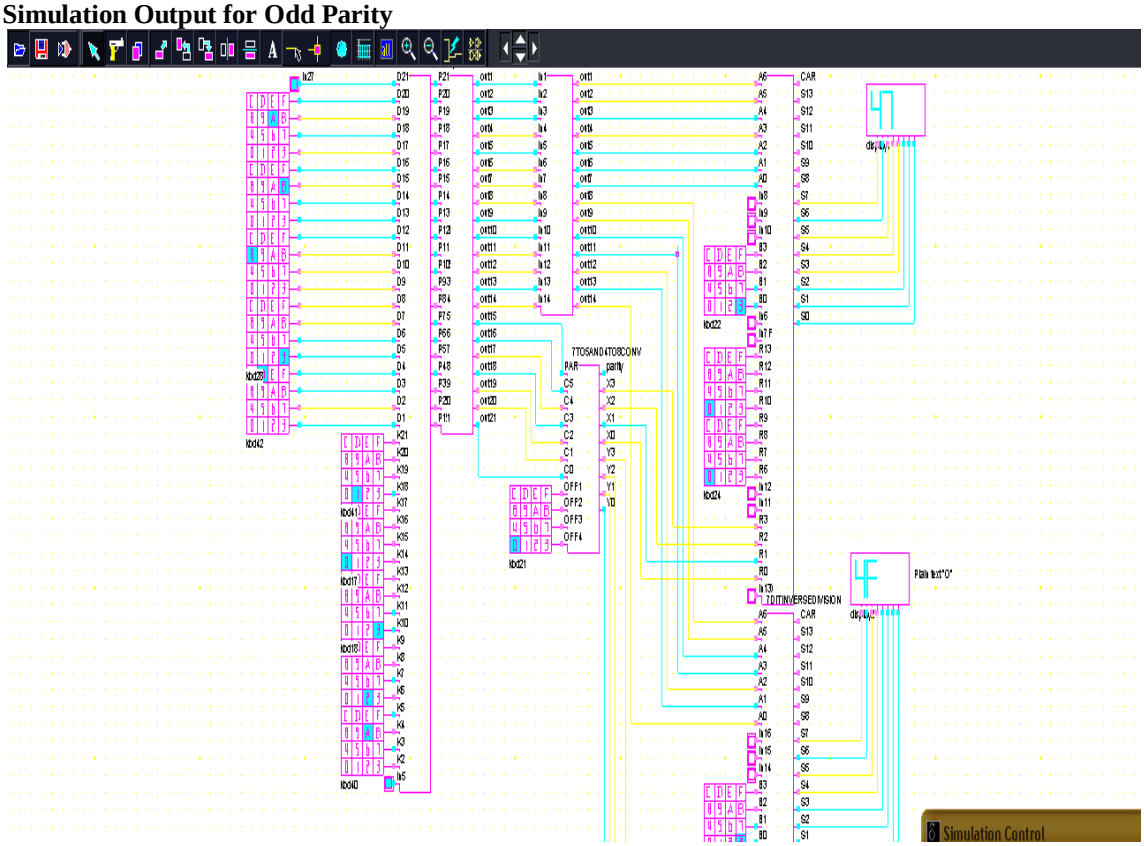
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Simulation Output for Odd Parity



For Even Parity

The reverse process of the encryption gives the decryption. The encrypted output and the 21-bit key values are first given to the XOR block. Its output is then given to the Inverse Permutation block. The first 14 bit values are given to Inverse Rotation block and the remaining 7 bit are given to 7 to 5 and 8 to 4 conversion block. The output of the Rotation block yields the 'Q' value and the output of 7 to 5 and 8 to 4 conversion block is the reminder 'r' value. The 'Q' and the 'R ' value are given to the Inverse Division block. Then the divisor value 3 is given to that block finally we get an input Plain Text.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

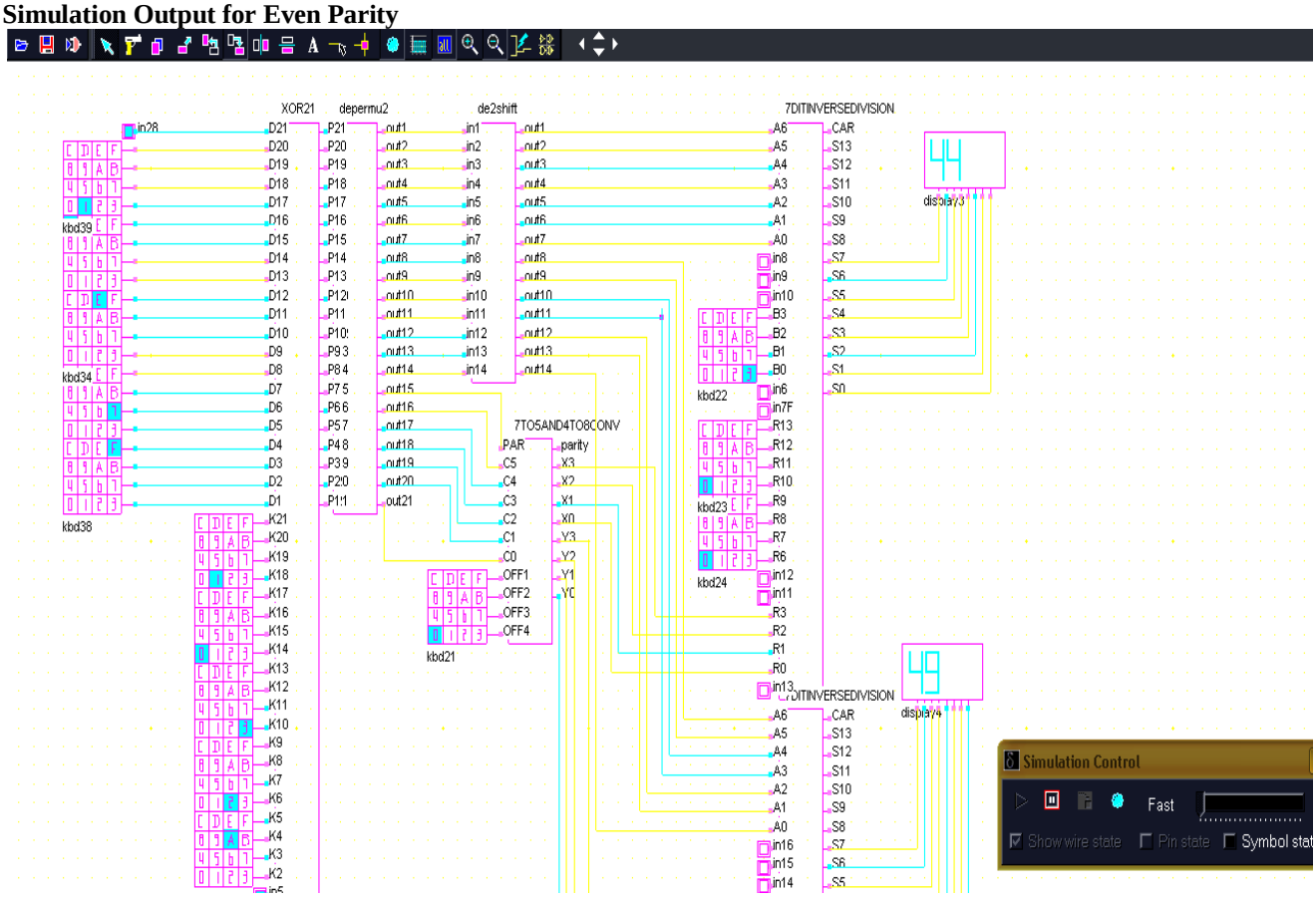
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Simulation Output for Even Parity



V.CONCLUSION

In this paper, MTDAS algorithm has been proposed for WSN devices with lightweight cryptography. Here using this algorithm various languages of world having Unicode can be used for encryption. Thus here the intruder finds a great difficulty in finding the plaintext language. Due to the low energy consumption and the small chip size needed for our MTDAS design for encryption and decryption, it is particularly suitable for resource limited applications for example RFID tags and also all wireless sensor devices. For the hardware implementations, we use this type of encryption in RFID tags. By using MTDAS cryptographic algorithm, energy consumption can be reduced. Finally, we can conclude that MTDAS algorithm has secure than the conventional cryptography algorithm and the brute force attacks, and it is more size-optimized, and low power consumption which creates it particularly suited for RFID applications.

REFERENCES

[1]. Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu and Dong-Geon Lee (2014), "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors", Volume 8267 of the series Lecture Notes in Computer Science, pp 3-27.
[2]. Diana Maimut and Khaled Ouafi (2012), "Lightweight Cryptography for RFID Tags", IEEE Security & Privacy, Vol.10, No.10, Pp. 76-79.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

[3]. Hung-Yu Chien and Chi-Sung Laih (2009), "ECC-Based Lightweight Authentication Protocol with Un-traceability for Low-Cost RFID", Journal of Parallel and Distributed Computing.
[4]. Jacob John (2012), "Cryptography for Resource Constrained Devices: A Survey", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 11,Pp. 1766- 1770.
[5] Jehan-Francois Paris, Thomas J. E. Schwarz and Darrell D. E. Long (2007), "Self-Adaptive Two-Dimensional RAID Arrays", IEEE International Performance, Computing, and Communications Conference, Pp. 246 – 253.
[6]. Matsuda S. and Moriai S. (2012), "Lightweight Cryptography for the Cloud: Exploit the Power of Bitslice Implementation,"CHES 2012, LNCS 7428, pp. 408–425, Springer.
[7]. Saied Hosseini-Khayat and Mohamad Sawan (2012), "Ultra-low Power Encryption Engine for Wireless Implantable Medical Devices", 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), Pp. 150 – 153, DOI:10.1109/MWSCAS.2012.6291979.
[8]. Sergey Panasenko and Sergey Smagin (2011), "Lightweight Cryptography: Underlying Principles and Approaches", International Journal of Computer Theory and Engineering, Vol. 3, No. 4, Pp.516-520.
[9]. Shibutani K., Isobe T., Hiwatari H., Mitsuda A., Akishita T., and Shirai T. (2011), "Piccolo: An Ultra-Lightweight Blockcipher," CHES, LNCS 6917, pp. 342–357, Springer.
[10].Shweta Gaba, Iti Aggarwal and Dr. Sujata Pandey (2012), "Design of Efficient XTEA Using Verilog", International Journal of Scientific and Research Publications, Vol.2, Issue 6, Pp.1-4.
[11].Suzaki T., Minematsu K., Morioka S., and Kobayasi E.(2011), "Twine: A lightweight, versatile block cipher," In Proceedings of ECRYPT Workshop on Lightweight Cryptography
[12].Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, Dong Hoon Lee (2008), "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", Information Security and Assurance, Pp. 73 – 76.