International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Energy Optimization on Symmetric Key Encryption and Decryption Algorithm using Genetic Algorithm

Ratnesh Mishra, Ravi Shanker Shukla, Rajesh K. Shukla, R.R. Tewari

Abstract- In this paper we have proposed energy optimization on symmetric key encryption and decryption algorithm are using genetic algorithm where we have used symmetric key for encryption & decryption algorithm that optimize the energy in terms of power consumption related to the laptop battery. This method combines the concept of a genetic algorithms and cryptography in very different ways. The algorithm uses deterministic way to generate pseudo random number and applied crossover & mutation deterministically. The algorithm exploits the features of the GA deterministically because GA is fast. Finally we got the actual message of ASCII code by using decrypted algorithms minimises power consumption relatively.

Keywords: ASCII, GA, Encryption, Decryption, Cryptography, Crossover, Mutation.

I.INTRODUCTION

The stealing of set of connections tools may impersonate considerable hazard to a wireless set of connection, since arrangement of the set of connection can be recover from a lost access point or wireless interfaced card.

Thereby steadily increasing set of connection tools, such as router, in easy get to place jointly with physically powerful and physical security controls,

the risk of theft can be minimized by using the cryptography which is the skill of making announcement incomprehensible each one with the exception of the indeed beneficiary.A Cryptography algorithm is indexed by some key(s) for encrypting message as secret message and decipher of message as original message [1]. The representation for surreptitious enter system which was first projected by Shannon shown in fig.1. In this paper we give new algorithm developed by us for encryption and decryption. We are using symmetric key for encryption and decryption algorithm which is developed by us. After that optimize the energy and get the result of power consumption in percentage which is related to the laptop battery power [2]. The combine method is the concept of a genetic algorithms and cryptography is a very different way. The genetic algorithms are in deterministic way to generate pseudo random number.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
Ratnesh Mishra, Department of Computer Science & Engineering, Birla Institute of Technology Mesra, Ranchi, Patna Campus, Bihar, India
Ravi Shanker Shukla, Computer Science, Saudi Electronics University, Saudi Arabia,
Rajesh K. Shukla, Department of Computer Science & Engineering, Birla Institute of Technology Invertis University, Bareilly, UP,India.
R.R. Tewari, Department of Electronics & communication Engineering, J.k. Institute of Technology, University of Allahabad, UP,India.

The genetic algorithm operates crossover and mutation as applied deterministically then reason to use [3]. A genetic algorithms to exploits the features of the GA deterministically and also GA is fast.

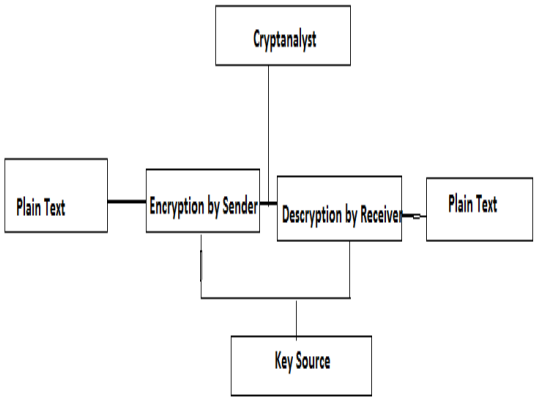

Fig.1. The representation for secret key system first proposed by Shannon [6].

2 Related Work [1] In this research paper author talked about the experimentation, here we employed the MS.NET Compact Framework as an up to date and accepted platform for secure improvement portable applications and protected information. However coding/decoding step by step processes were controlled with the algorithm, it is present by Framework. The power competence of crypto step by step process with changing input and slab ranges is highly different. Thus, the user of a cellular phone must opt the most suitable limitation of a crypto step by step process by taking into account the level of safety required and the functioning rate with the intention of the users are enthusiastic to recognize and depending on the security level. They choose power and it is essential to perform coding and decoding process with esteem towards the battery lifetime. Author got results; a best feasible value for power utilization of AES algorithms is achieved when slab range and input ranges are equal. In this paper author projected energy/security profiles on behalf of users of movable devices, this is based on 128, 192 and 256 bits slabs/inputs. The results of power utilization capacity, while performing data coding be able to be worn to consistently envisage power utilization of decoding process: decoding need 14% more power than coding process.

[2] In this paper authors said about the encryption which is done so that the data will be more secured and to optimize energy various compression techniques and LEACH protocol has been applied. Here both lossless and lossy compression is done. We can see that more number of nodes is alive when the data is compressed. By this method we can augment life time of sensor nodes in wireless sensor network. Nearby many more question to be resolved around energy management. Author said reduce the energy consumption of sensor nodes in wireless sensor networks.
[3] In this paper the authors proposed algorithm and the original blowfish algorithm have been developed using C# language. The main comparison factors which were used are avalanche effect and execution time; the results show that the avalanche effect in the proposed algorithm is better than the original blowfish algorithm in both changes when one bit has been changed in the key or in the plaintext. The avalanche effects in the proposed algorithm when one bit has been changed in the key and when one bit has been changed in the plaintext were 45.21 % and 46.44 % respectively. But the avalanche effects in the original blowfish algorithm when one bit has been changed in the key and when one bit has been changed in the plaintext are 38.63 % and 37.17 % respectively. That indicates that the proposed algorithm is stronger than the original one. According to the execution time factor which was used to compare the proposed algorithm with original blowfish algorithm the results show that the average execution time for the proposed algorithm is 55.1 milliseconds whereas in the original blowfish algorithm is 6.6 milliseconds, which better than the proposed algorithm. The proposed algorithm needs more time to be executed rather than original blowfish algorithm since it uses genetic algorithm processes which increases security. [4] In this paper author talked about the power competence of imitation which be a significant in favour of battery-powered implantable stimulators. Author has used a genetic algorithm (GA) to determine the power-best possible waveform outline intended for neural inspiration. In this paper GA be joined to a computational sculpt of extracellular inspiration of a mammalian myelinated axon. GA steps forward; waveforms turn out to be increasingly power capable and meet power-most favourable shape. The consequence of the GA was steady transversely quite a lot of trials, and ensuing waveforms be similar to curtailed Gaussian curves. Initiate sculpt of a population of mammalian axons and in vivo test on a cat sciatic nerve, the GA-optimized waveforms be more power capable. [5]In this research paper author talked about implementation of coding and decoding system. Input formation procedure with intermediary coding process to make available good protection to the broadcast data. Now single input replacement step by step process which be worn to make sure secrecy in set of connection, it is shared and execute through the assist of hereditary utility to make available further protection.

II.PROPOSED SYMMETRIC ENCRYPTION & DECRYPTION ALGORITHM

The proposed symmetric encryption & decryption (SED) algorithm is implemented. It be straightforward to put into operation in coding and decoding method. [4] [5].We are using symmetric key for encryption and decryption algorithm which is developed by us. After that optimize the energy & got the result of power consumption in percentage which is concerned to the laptop battery power. [6] The methods are combined for the concept of a genetic algorithm (GA) & cryptography is a very different way. The genetic algorithms are deterministic way to generate pseudo random number. The genetic algorithm operates crossover & mutation as applied deterministically then reason to use. A genetic algorithm is to exploits the features of the GA deterministically and also GA is fast. In fig.-2 shown about the block diagram of symmetric encryption and decryption, when sender sent the original message, that message encrypted by using ASCII code and substitution array sequential number and get reminder and quotient. Receiver side received encrypted message then decrypt of this message with using substitution array sequential number and reminder and quotient are using key generation process and get the ASCII value which is converted into original message. After that optimize the energy and got the result of power consumption in duration of communication process. The Single input replacement step by step process, which be worn to make sure secrecy in set of connection, it is shared and put into operation with the help of inherited purpose to provide added protection purpose [7][8][9].

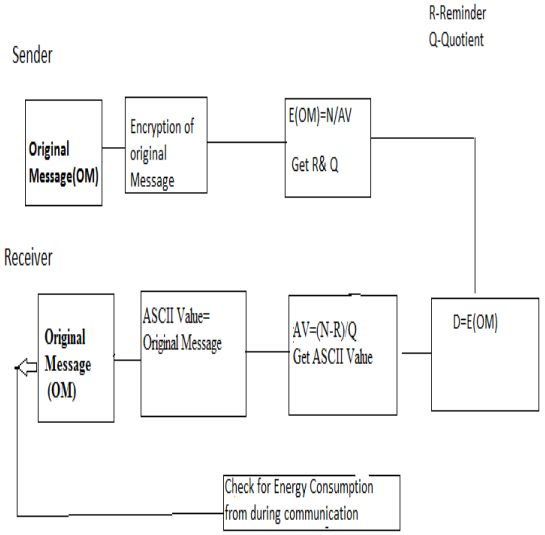

Fig.2. Block diagram of symmetric encryption and decryption algorithm.

3.1 Symmetric Key Encryption

We have given substitution array sequential number N and modulus M and reminder R. Then any substitution array sequential N modulus 35 reminder should be 2, this is satisfy by-2627 mod 35=2 means that 2627 mod 35 result should be 2 where 2 is reminder value. We can say that every substitution array sequential number N mod 35 results is 2.Now encrypt the simple message convert into the ASCII code, then substitution array sequential number N divide by ASCII value of the message.

After division we get two results one is quotient and second is reminder which is shown in table- 2 [10][11].

Encryption of the original message-

OM (Encryption) = N/AV=R&Q

3.2 Symmetric key Decryption

In decryption first we have received the cipher text which is not in original message. Then decrypt the cipher text after that we get the original message [12][13].

om = av-(n-r)/q

Where-

n- Substitution array sequential number

r- Reminder Number

q- Quotient number

om- original message

av- ascii value

Now finally received original message after the decryption of the message"SECURITY OF THE SYTEM"

Original Message-**"Security of the System"**

III.IMPLEMENTATION

The algorithms processed with sender and receiver knows the values of the parameter of the key.

{*a,q,n*, array size, starting number, ending number, modulus, reminder}

1. Given parameters are ***A,q*** of linear congenital method where values are known to the sender and receiver.
2. Find out Array size which is the size of array until which the random numbers are produced.
3. Starting number to start with the final array size number.
4. Ending number is the number to end with the final_ array size number.
5. Modulus is the number used to extract only those numbers to be used for substitution which give the reminder.
6. When the numbers between starting number and ending numbers are dived by modulus.
7. PRNG using GA and linear congenital method First we will consider about the assumption of Genetic Algorithm-

Genetic Algorithm-

(i) Array size is 6000(can be varied to higher value also).

(ii) Length of the chromosome is 13(can be varied).

(iii) Representation of chromosome is in binary.

(iv) Population size is fixed to 100(could be varied)

(v) 60 generators are requiring generating 60000.

By far the most widely used technique for PRNG is an algorithm first proposed by Lehmer, which is known as linear congruential method [12].

The algorithm is parameterised with four number as follows-

m- Modulus *m>0*

mpr- Multiplier *0<=mpr<m*

inc- Increment *0<inc,m*

The sequence random number is obtained by following iterative equation

$$Xn+1=mpr\ (Xn+C\ )MOD\ m$$

Where *Xn* is the initial value which is the value of the first chromosome of the first generation

Generation1-

$$X0=Xn$$

$$Xn+1=(mprXn+inc)MOD\ m$$

-

-

-

-

-X149

Note- There are using population size =150

In this research paper we consider about the first generation which is created the next generation numbers are using the GA Operators, Crossover and Mutation.

4.1 Genetic operator

The Hereditary operator is used for the purpose of solving GA algorithm so as to reach the solution to a given problem [14]. For the algorithm to be successful we require three types of operators (mutation, crossover and selection).Hereditary operator is created and maintained for diversity in hereditary mutation which brings together a new type of existing solution and their by select solution from the available one . To understand clearly John Koza has identified inversion and permutation operator, but the effectiveness of this operator has been conclusively demonstration and there is no discussion about the operator. Mutation operators are basically known as unary operator as they only operator on a single chromosome at a time. In contrast crossover operator are known to binary operators are on two chromosome at a given point of time by combing two chromosome that are already existing into a single new chromosome.

4.2 Crossover

In this research paper, the number of crossover to happen is taken to the pop size. If the generation is even numbered then the crossover take place from top to bottom in sequential way by passing chromosome like (1,2) (3,4) (5,6) (7,8) (9,10) (11,12) (13,14) (15,16) (17,18) (19,20)----------.If the generation is odd numbered the crossover occurs from bottom to top in sequential way by pairing chromosome like-(11,99) (98,97) (96,95) (94,93)-------.But assumption which is regarding the crossover site is also done in the algorithm which helps to avoid repletion of numbers generated.

4.3 Mutation

Mutation is an alteration in the genetic material of a cell which keeps on changing in a sequential manner. Due to this transformation can check the appropriate implementation of the hereditary .

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

They can also occur through monogenic areas, one of the finding on genetic variation between different species of Drosophila states that if a mutation causes a change in a protein produces by a gene, the results are expected to be harmful with an estimation 70% of amino acid polymorphism which have a damaging effect and the remainder being either neutral and marginally useful. The destructive effect in mutation it can help on genes organism. This mechanism helps in DNA [15] repair or in preventing correct mutation by reverting the mutated sequence back to its original states [16].A mutation keeps on involving the duplication of large sections of DNA, through a process of hereditary recombination. This duplication is great source of raw material for evolving new hereditary, where tens to hundreds of hereditary duplicated in animal genomes every million years. Most genes belong to larger gene families of shared ancestry, known as homology. Novel genes are produced by different methods, basically through the duplication and mutation of an ancestral gene, or by recombining different parts of genes, so as to form of new combinations having functions. Since the representation of the chromosome in binary just invert bit values at particular gene locus. As power utilization alertness is highly important in wireless devices as like mobile and laptop, we must make sure that necessary action, regarding information security altitude and sensible use of power take place at the same time. Thus the prediction that can be following is that cryptography with a longer symmetric key shall ensure higher degree of security at the cost of higher power utilization.We consider slab sizes moderately large that have need of more coding rounds. The Power utilization is depends on the application development. To note if the user encrypts data and decrypts on a laptop or other device, power cipher potency process resolve. Differences from the existing scenario where a user code/decode of data on a laptop mechanism only.[17] We use crypto (symmetric encryption and decryption algorithms) power-resourcefully requirement to understand the interaction between power utilization and encryption and decryption constraint shown in table no-1 which shows the original message convert into ASCII code .We use the formula for encrypting original message and got the quotient and reminder . After decrypting received the message by using formula and get the ASCII value and then convert into the original message. Experiments show about the optimize energy consumption with comparison of AES encryption and decryption algorithm and SED algorithm. Finally after the compression of these algorithms find the SED algorithm very fast process and optimize the power consumption.

IV.METHOD

The experiment objective is to come out with enslavement existing among secret input span and slab sizes taking place of single supply, and power utilization scheme, power-secret message potency the diagnose dependencies have been express below in fig.3.

Retrieval Number: I7722078919/19©BEIESP
DOI: 10.35940/ijitee.I7722.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

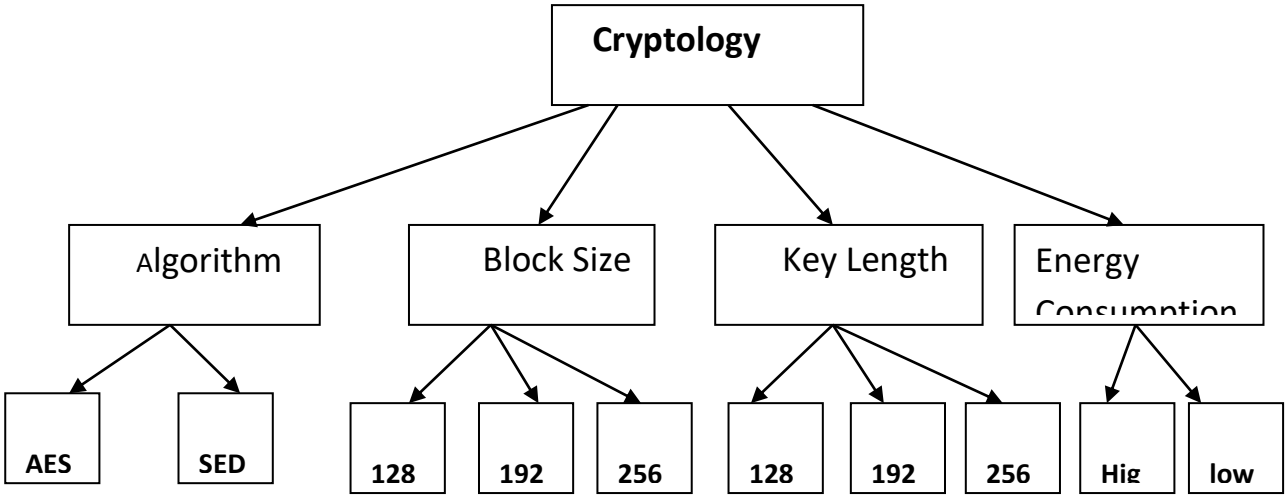

Fig.3. Cryptology Model with AES and DES Algorithm.

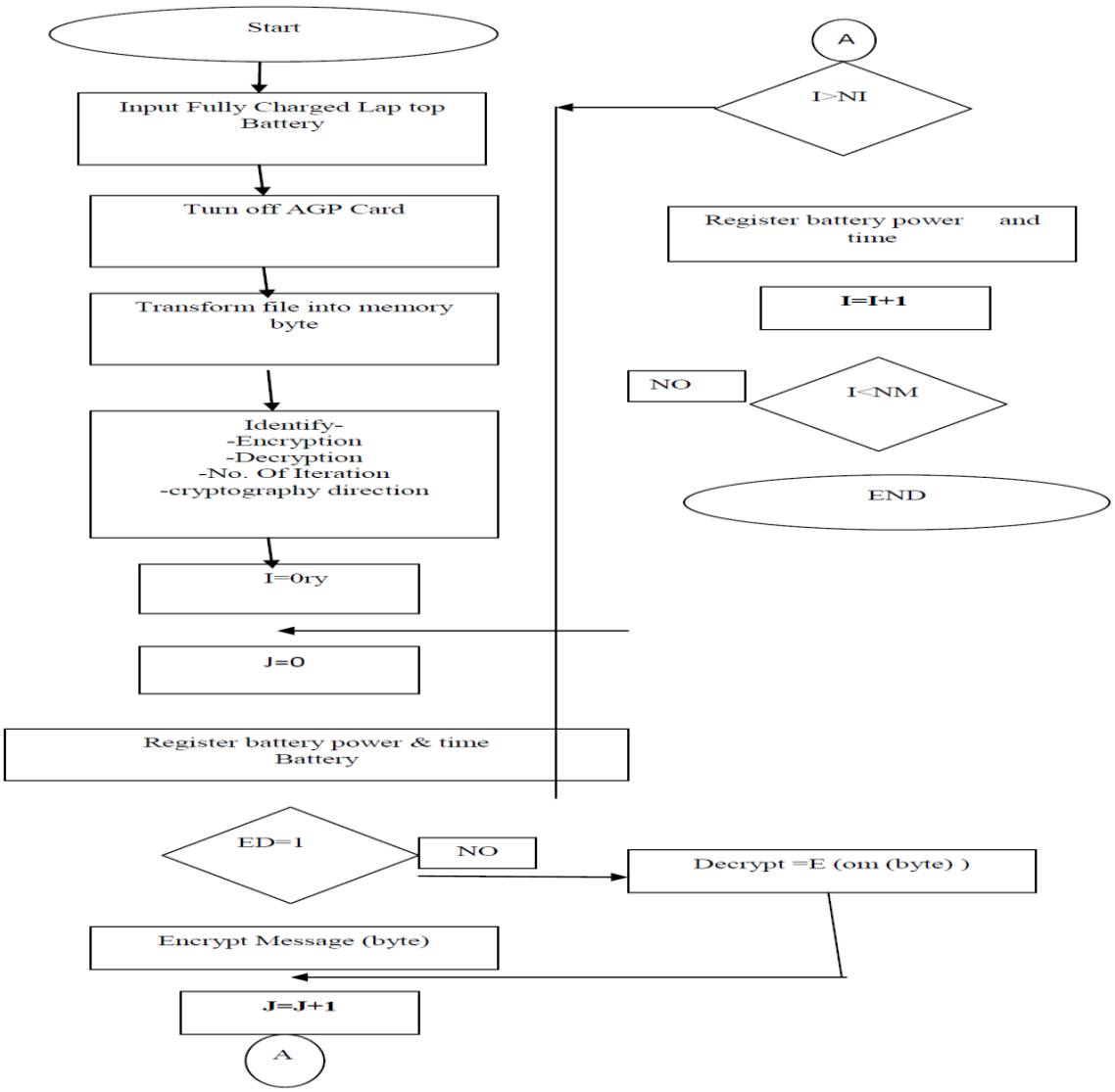

Fig.4. Flow Chart of Energy measurement algorithm for a crypto algorithm (AES & SED)

5.1 Conduct Experiment

We include urbanized program for implement the step by step process in C# language for the Dot NET Framework. The experiments were performed on the Laptop of the model is Dell Vostro processor-Intel Core(TM) i3 5005U CPU @ 2.0GHz,4GB RAM,64 bit operating system win10,AGP Card Intel graphics 5500. We are using Dot NET structure v3.5, moved throughout the part of information with the intention of the prevalent quantity of data. The users work on locally as well as on the internet are made by the text file, for encoding, we used a benchmark which size is 300KB. Surreptitious data necessitate employ of whichever 192 or 256 bit inputs [18]. Though, the new manuscripts [19] assert to facilitate the 10-round AES is hypothetically possible to be cracked by cryptanalysis [20]. The AES step by step process is a symmetric slab code, which supports input ranges of 128, 192 and 256 bits, through information in inconsistent-span slab. The slab span and the input span be able to be set separately (AES cannot do this) to 128, 192 or 256 bit. Rijndael step by step process to apply a span quantity of round, depending on the input/slab ranges, as follows:

9 rounds if both the key and block size is 128 bits;
11 rounds if either the key or block size is 192 bits;
13 rounds if either the key or block size is 256 bits;

The first order intended on behalf of each and every experiment be the same: battery of laptop completely stimulating at 100% level. The text folder is laden as of a storage space to an array and an coded step by step process which is applied with algorithm *E(OM)=N/AV* and get the remainder(R) and quotient (Q). In the direction of accomplish considerable series drain for more precise measurement, the encryption process is repeated 22 times. After each experiment, the series is stimulating yet over to 100%. The same procedure is also applied for measuring power utilization of a AES coding and decoding algorithm. We make available the summary of the test results in Table.4 (for AES Encryption Algorithm by set slab range of 16 bytes, 24 bytes and 32 bytes) and Table.5 (for AES description changeable slab sizes of 16 bytes, 24 bytes and 32 bytes).

6	I	73
7	T	84
8	Y	89
9	Space(Gap)	32
10	O	81
11	F	70
12	Space(Gap)	32
13	T	84
14	H	72
15	E	69
16	Space(Gap)	32
17	S	83
18	Y	89
19	S	83
20	T	84
21	E	69
22	M	77

Encryption of the original message

OM (Encryption) = *N/AV=R&Q*

Table 1.ASCII value of relevant data

Sr. No.	OM-Alphabet	ASCII Value
1	S	83
2	E	69
3	C	67
4	U	85
5	R	82

Table 2. Encrypted the original message

Sr. No.	*OM*(Alphabet)	ASCII Value	*N*(Array Sequential Number)	*N/AV*	*Q*(Quotient)	*R*(Reminder)

Retrieval Number: I7722078919/19©BEIESP
DOI: 10.35940/ijitee.I7722.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

1	S	83	2627	2627/83	31	54
2	E	69	3747	3747/69	54	21
3	C	67	4867	4867/67	72	43
4	U	85	1477	1477/85	17	32
5	R	82	4027	4027/82	49	09
6	I	73	2347	2347/73	32	11
7	T	84	1227	1227/84	14	51
8	Y	89	1227	1227/89	13	70
9	Space(Gap)	32	4867	4867/32	152	03
10	O	81	2347	2347/81	60	79
11	F	70	4277	4277/70	27	27
12	Space(Gap)	32	4867	4867/32	152	03
13	T	84	1227	1227/84	14	51
14	H	72	667	667/72	09	19
15	E	69	3747	3747/69	54	21
16	Space(Gap)	32	4867	486732	152	03
17	S	83	2627	2627/83	31	54
	Y	89	1227	1227/89	13	70
19	S	83	2627	2627/83	31	54
20	T	84	1227	1227/84	14	51
21	E	69	3747	3747/69	54	21
22	M	77	2067	2067/77	26	65

Table 3. Decryption of the encrypted message (Cipher message)

OM=AV= (N-R)/Q

Sr. No.	*Q*	*R*	*N*	*N-R*	*N-R/Q*	*AV*	*OM*
1	31	54	2627	2573	2573/31	83	S
2	54	21	3747	3726	3726/54	69	E
3	72	43	4867	4824	4824/17	67	C
4	17	32	1477	1445	1445/17	85	U
5	49	09	4027	4018	4018/09	82	R
6	32	11	2347	2336	2336/32	73	I
7	14	51	1227	1176	1176/14	84	T
8	13	70	1227	1157	1157/13	89	Y
9	152	03	4867	4864	4864/152	32	Space(Gap)
10	60	79	2347	2268	2268/79	81	O
11	27	27	4277	4250	4250/27	70	F
12	152	03	4867	4864	4864/152	32	Space(Gap)
13	14	51	1227	1176	1176/14	84	T
14	09	19	667	648	648/09	72	H
15	54	21	3747	3726	3726/54	69	E
16	152	03	4867	4864	4864/152	32	Space(Gap)
17	31	54	2627	2573	2573/31	83	S
18	13	70	1227	1157	1157/13	89	Y
19	31	54	2627	2573	2573/31	83	S
20	14	51	1227	1176	1176/14	84	T
21	54	21	3747	3726	3726/54	69	E
22	26	65	2067	2002	2002/26	77	M

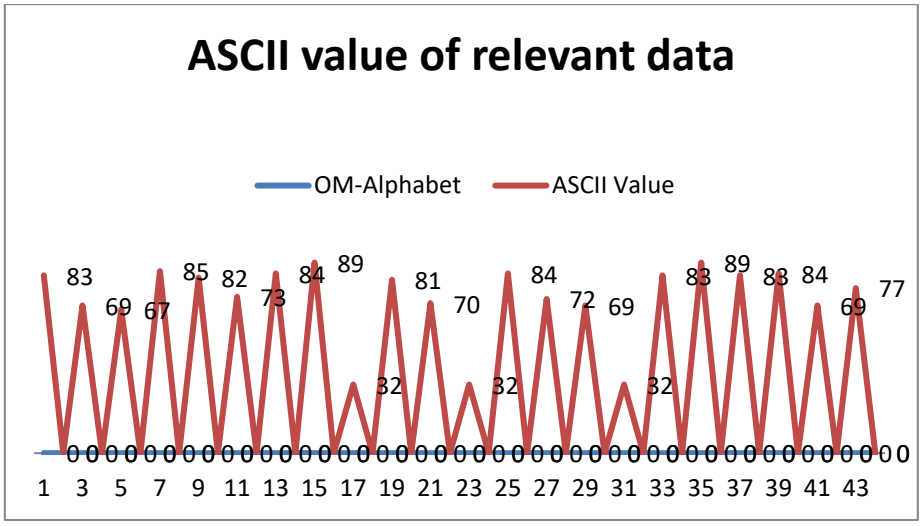

Fig.5 Graph Representation of ASCII value of relevant data

In fig.5 show about the graph representation of orignal message characters data of ASCII value means that orginal message character convert ninto ASCII value.

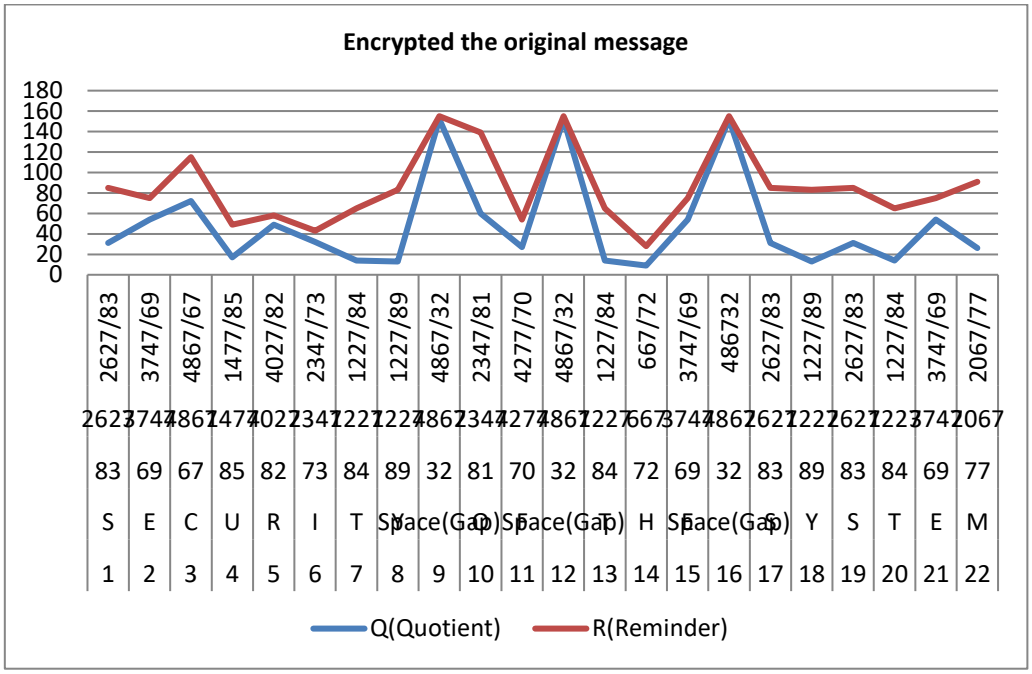

Fig.6. Encrypted the original message.

In Fig.6. show about the encrypted the original message and we get the quotient and reminder valuewhich value is very important in duration of decryption and again get the ASCII value and after that we get again original message.

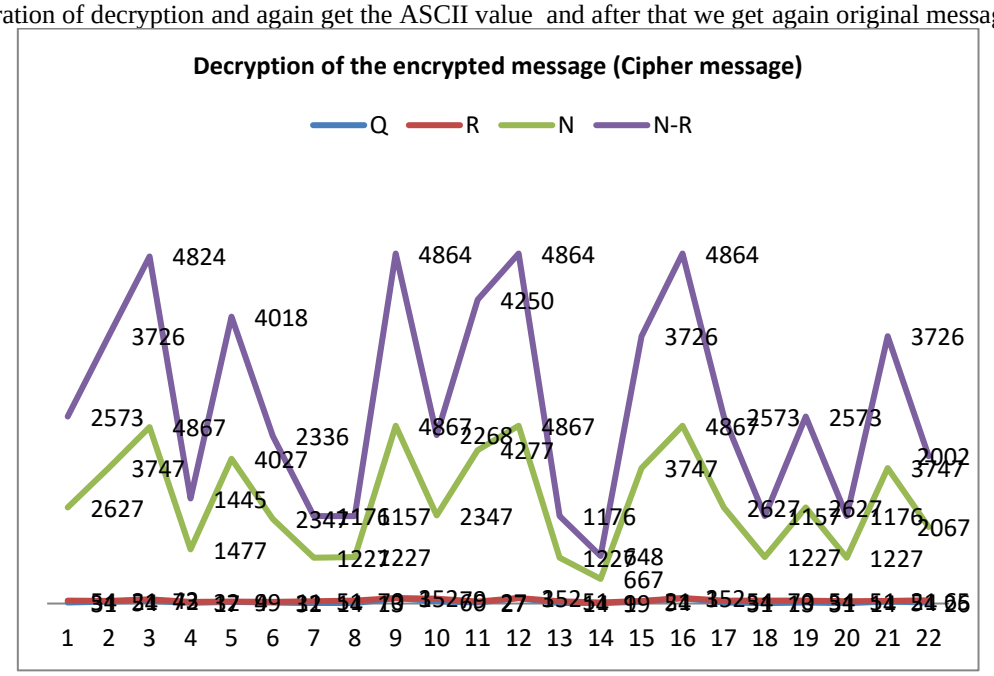

Fig.6a . Graph Representation of Decryption of the encrypted message (Cipher Message).

Retrieval Number: I7722078919/19©BEIESP
DOI: 10.35940/ijitee.I7722.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

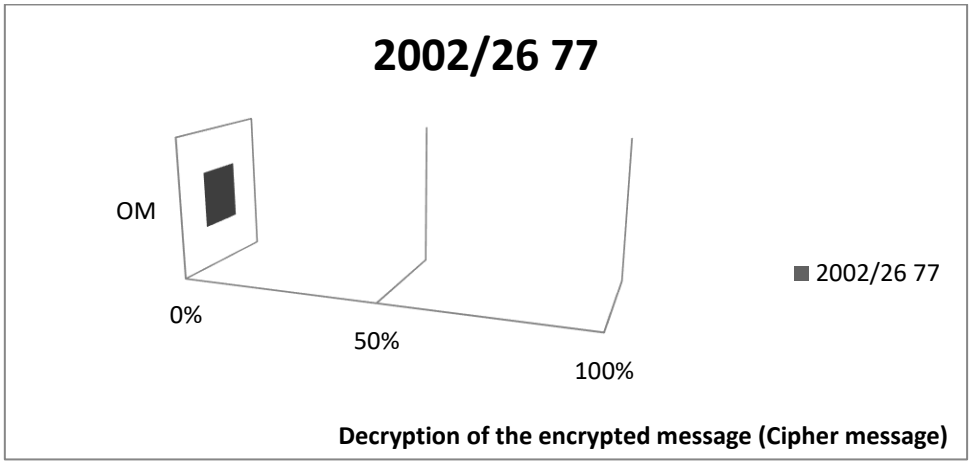

Fig.6b. Graph Representation of Decryption of the cipher message get the original message.

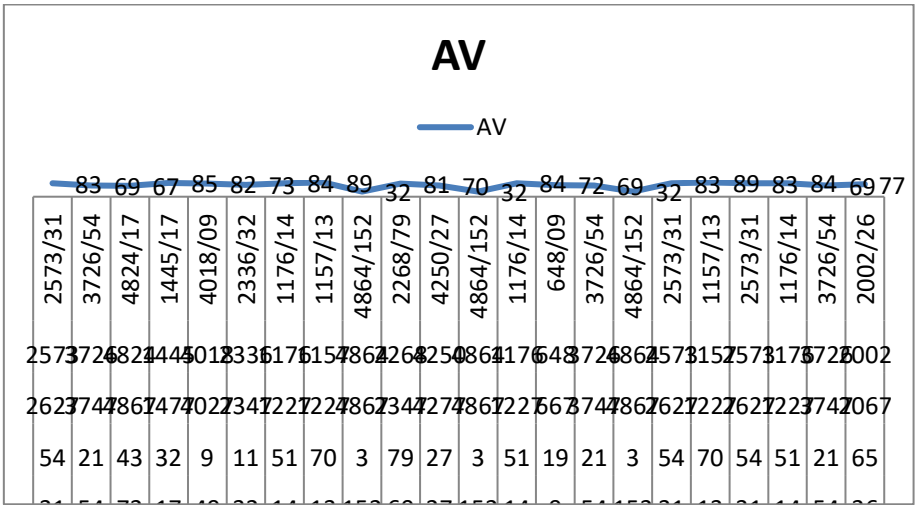

Fig.6c. Graph Representation of Cipher text again convert into ASCII Value(AV).

In fig 6-a,-b and-c. show about the graphoical representation of decription of the ecrypted message using formulas and get the original message-first fall we consider about the qutoient and reminder value which is used in formula and get the ASCII value which is convert into original message character and we can say that this is orignal message after decryption of cipher message.

V.RESULT & ANALYSIS

We require a way to make decisions regarding power utilization and security to reduce the utilization of battery power-driven procedure. We examine a method for analyzing trade-offs between power and safety. The objective is to assist the design of power resourceful protected communication schemes for the wireless surroundings in the future. We will put forward three approaches to reduce the power utilization of security protocols: first, substitute of paradigm security protocol primitives that get through high power as maintaining the same protection level and Second adaption of standard security protocols. And new plan of security protocol where power competence is the main focus.

The subsequent responsibilities that will be performed are shown as follows:

1. An evaluation is carrying out between the results of the selected different encryption and decryption schemes in conditions of the encryption time, battery power and throughputs.
2. A find out the effect of changing data types
3. The effect of symmetric key for encryption and decryption algorithm on power consumption.

The power utilization standards for individual AES & SED algorithm be achieve by consecutively their .NET packed in structure. Crypto verifies starting place of implementations and measuring the recent series drain. For accomplishment precious consequence of the series drain when data is coding / decoding, process. Since encryption and decryption time may vary, we perform encryption and decryption separately which is shown in fig.3.We are giving three energy/security profiles for users of laptop device which is stand on 16, 24 and 32 byte slab/inputs. The results of power utilization capacity, when carry out the data encryption it can be used to reliably predict power utilization of decryption process from Table-6 and

Table-7: decryption requires .09% more energy than encryption. In this experiments result shows about the optimize energy consumption with comparison of AES encryption and decryption algorithm and SED algorithm. Finally after the comparison of these algorithms find the SED algorithm very fast process and optimize the power consumption w,r,t. Table-4.,Table-5,Table-6 and Table7.

Sr. No.	Block Size	Key size	Iteration(22 rounds) times- HH:MM:SS	Laptop Battery Consumption (%)
01.	128	128	00:00:44	.38%
02.	128	192	00:00:51	.34%
03.	128	256	00:00:58	.39%
04.	192	128	00:00:54	.37%
05.	192	192	00:00:54	.37%
06.	192	256	00:00:49	.34%
07.	256	128	00:00:48	.33%
08.	256	192	00:00:53	.36%
09.	256	256	00:00:54	.37%

Table 4. AES Encryption Algorithm.

Sr. No.	Block Size	Key size	Iteration(22 times) HH:MM:SS	Laptop Battery Consumption (%)
01.	128	128	00:00:55	.37%
02.	128	192	00:00:58	.39%
03.	128	256	00:00:57	.38%
04.	192	128	00:00:56	.38%
05.	192	192	00:00:57	.39%
06.	192	256	00:00:64	.43%
07.	256	128	00:00:62	.42%
08.	256	192	00:00:61	.41%
09.	256	256	00:00:62	.42%

Table 5. AES Decryption Algorithm.

Sr. No.	Block Size	Key size	Iteration(22 times) HH:MM:SS	Laptop Battery Consumption (%)
01.	128	128	00:00:34	.23%
02.	128	192	00:00:41	.28%
03.	128	256	00:00:48	.30%
04.	192	128	00:00:44	.30%
05.	192	192	00:00:44	.30%
06.	192	256	00:00:39	.27%
07.	256	128	00:00:38	.26%
08.	256	192	00:00:43	.29%
09.	256	256	00:00:44	.30%

Table 6. SED Encryption Algorithm.

Sr. No.	Block Size	Key size	Iteration(22 times) HH:MM:SS	Laptop Battery Consumption (%)
01.	128	128	00:00:50	.34%
02.	128	192	00:00:53	.36%
03.	128	256	00:00:52	.35%
04.	192	128	00:00:51	.34%
05.	192	192	00:00:52	.35%
06.	192	256	00:00:59	.40%
07.	256	128	00:00:57	.39%
08.	256	192	00:00:56	.38%
09.	256	256	00:00:57	.39%

Table 7. SED Decryption Algorithm

Retrieval Number: I7722078919/19©BEIESP
DOI: 10.35940/ijitee.I7722.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The same method is useful in favour of compute the power utilization of a symmetric coding and decoding step by step process. The review of the test results from Tables.6. (in support of SED encryption Algorithm through set slab range of 16 bytes,24 bytes and 32 bytes) and Tables.7 (for SED description through changeable slab ranges of 128 bits, 192 bits and 256 bits). Now we calculate power utilization level measured from Table.4, we can create three precautions profiles (Highest Profile, Medium Profile, Lowest Profile) for laptop users as follows-

From Table.4-

Highest energy with highest security-.39%..
Medium energy with medium security-.34%
Low energy with low security -.33%

From Table.5-

Highest energy with highest security-.43%..
Medium energy with medium security -.38%
Low energy low security - .37%

From Table.6-

Highest energy with highest security - .30%..
Medium energy with medium security- .26%
Low energy low security - .23%

From Table.7-

Highest energy with highest security- .39%
Medium energy with medium security- .36%
Low energy low security - .34%

Finally after the comparison of these algorithms find the SED algorithm very fast process and optimize the power consumption w,r,t. Table-4.,Table-5.,Table-6., & Table-7.

VI.CONCLUSION

In this paper, we found the conclusion about the Symmetric Encryption and Decryption (SED) Algorithm that optimizes the energy in terms of power consumption related to the laptop battery with Features of Genetic Algorithms. We have given a new algorithm which is developed by us for encryption and decryption. The concept of a genetic algorithms and cryptography is a very different way. The genetic algorithm operates crossover and mutation as applied deterministically then reason to use. A genetic algorithms to exploits the features of the GA deterministically and also GA is fast. The encryption and decryption algorithms are using ASCII code.Table-1- ASCII value of relevant data, Table-2.Encrypted the original message and Table-3. - Decryption of the encrypted message (Cipher message).

The SED algorithm successfully encrypts and decrypts all the 256 ASCII characters. The only drawback of this is its need twice the amount of storage space for a message (quotient + reminder) .The results of power utilization capacity is depend on the performing of data encryption which can be used to consistently and calculate energy utilization of decryption procedure from Table -6 & Table-7 which is related to the symmetric encryption and decryption algorithm (SED): decryption requires .09% more energy than encryption. In this experiments result shows about the optimize energy consumption with comparison of AES encryption and decryption algorithm and SED algorithm. Finally after the comparison of these algorithms find the SED algorithm very fast process and optimize the power consumption.

REFERENCES

1.]J. Toldinas, V. Stuikys, R. Damasevicius, G. Ziberkas, M. Banionis,2011, “Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices” ISSN 1392 – 1215, ELECTRONICS AND ELECTRICAL ENGINEERING, SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS, No. 2(108).
2. Rakesh V, Sarala S M, May-June, 2015,” Energy Optimization In Wireless Sensor Network
3. Using Different Compression And Encrytion Techniques” International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015 ISSN 2091-2730.
4. Yousef Bani Awwad and Mohammad Shkoukan, March 2017”.The Affect ofGenetic Algorithmson Blowfish Symmetric Algorithm” IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3.
5. Amorn Wongsarnpigoon and Warren M Grill, 23 June 2010,” Energy-efficient waveform shapes for neural stimulation revealed with a genetic algorithm” IOP Publishing Ltd,Journal of Neural Engineering, Volume 7, Number 4
6. Sindhuja K , Pramela Devi S, 2014, “A Symmetric Key Encryption Technique UsingGenetic Algorithm” Sindhuja K et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1),ISSN:0975-9646

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7. C.E. Shannon ,"Communication Theory of security system ",Bell system Technical Journal ,28 ,1949.
8. National Bureau Standards, "Data Encryption Standard (DES)," FIPS Publication 46; 1977.
9. [8]Spillman R, "Cryptanalysis of Knapsack Ciphers using Genetic Algorithms," Cryptologia, Vol.17, No.4, pp. 367-377, 1993.
10. Methew, R.A.J., "The use of genetic algorithms in cryptanalysis," Cryptologia, 7(4),187-201, April1993.
11. Garg Poonam "Genetic algorithm Attack on Simplified Data Encryption Standard algorithm," International journal Research in Computing Science, ISSN1870-4069, 2006
12. Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B, Jan 2006
13. A.J Paul, P.Varghese,P. Mythilli, "Matrix Array Symmetric Key Encryption", Journal of Computer Society of India, Vol.37,Issue No.1,Jan-March 2007,pp 48-53.
14. Garg Poonam, "Memetic Algorithm Attack on Simplified Data Encryption Standard Algorithm," proceeding of International Conference on Data Management, February 2008, pg 1097-1108.
15. Ankita Agarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, pp. (216 -218), April 2012.
16. M.Najaftorkaman, N. S Kazazi,"A method to encrypt information with DNA based cryptography", International Journal of Cyber-Security and Digital Forensics(IJCSDF),4(3):417-426,2015.
17. H.M Mousa, "DNA-Genetic Encryption Technique", International Journal of Computer Network and Information Security,2016,7,1-9.
18. W. Stallings, Cryptography and Network, Security, Principles and Practices, Fourth Edition,Prentice Hall,November 2005
19. Kelsey J., Lucks S., Schneier B., Stay M., Wagner D.,Whiting D. Improved Cryptanalysis of Rijndael // Fast Software Encryption, 2000. – P. 213–230.
20. Biryukov A., Keller N., Khovratovich D., Shamir A. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds // Advances in Cryptology – Eurocrypt 2010, 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science, 2010. – Vol. 6110. – P. 299–319.
21. Toemeh R., Arumugam S. Breaking Transposition Cipher with Genetic Algorithm // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 7(79). – P.75–78.

Compliance with Ethical Standards

The submitted manuscript follows all the compliance of ethical standard

Funding

This work has not been funded by any agency.

Conflict of Interest

There is no conflict of interest among the authors of this manuscript.

Authors Biography

Author-1

Ratnesh Mishra obtained a B.E. in Computer Technology From Nagpur University, M.Tech. Degree in Software Engineering from MNNIT Allahabad and Ph.D.Degree in Computer Science & Engineering Pursuing. Currently, he is working as an Assistant Professor in the Dept. of Computer Science & Engineering, BIT Mesra , Patna Campus, Patna. His research interest includes Computer Network, Computer Network Security, Web Technology, TCP/IP.

Author-2

Ravi S Shukla obtained aM.Tech. Degree in Software Engineering in 2002 and Ph.D.Degree in Computer Science & Engineering on 2015 from MNNIT, Allahabad, Deemed University. Currently, he is working as an Assistant Professor in the Dept. of Computer Science, College of Computing and Informatics, Saudi Electronic University, KSA. His research interest includes Computer Networking, TCP/IP, Mobile Computing and Adhoc networking

Author-3

Dr. R.K.Shukla is Professor and Dean Faculty of Engineering & Technology in Invertis University, Bareilly, UP, India. He is associated with teaching and research for past twenty five years. His research areas are ODEs & PDEs, Theory of Semigroup, Time Discretization Method and Factional Calculus. He has published more than thirty papers in national and international journals and authored of 11 books.

Author-4

Rajiv Ranjan Tewari obtained a M.Tech. Degree . Currently, he is working as Professor in the Dept. of Electronics & Communication, JK Institute of University of Allahabad, India.. His research interest includes Computer Networking, TCP/IP, Mobile Computing and Adhoc networking. Wireless Sensor Networks, Mobile Ad-hoc Networks and Robotics . Real time systems, Computer Networks and Advanced Computer Architecture. He has supervised several Ph.D. students. He has worked as Principal Investigator of several research projects funded by DRDO, AICTE and MHRD. He is serving as Coordinator, Centre of Computer Education, Institute of Professional Studies, University of Allahabad