International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Encryption and Decryption Using Bit Operations

Gurubasava[1], Rajesh Budihal[2]

[1]Assistant Professor, Dept. Of Computer Science & Enggineering, Sreyas Institute of Engineering and Technology Bandlaguda, Hyderabad-500068

[2]Assistant Professor, Dept. Of Computer Science & Enggineering, Sreenidhi Institute of Science & Technology Ghatkesar, Hyderabad-501301

Abstract: ***Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Only one particular element underlies many of the security mechanisms in use Cryptographic techniques hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication. A day to day use of cryptography in our life is increasing tremendously; this is because of necessity of our protecting data from unauthorized access. As the days are passing the old algorithms are not remaining so strong as cryptanalyst are familiar with them. The proposed encryption algorithm, in which for every eight bytes of plain text it will produce seven bytes of cipher text and in decryption for every seven bytes of cipher text it will reproduce eight bytes of plain text to illustrates about the comparison of various data samples during encryption and decryption process which results in terms of better performance metrics such as data size, memory, and throughput value.***

Keywords: Cryptography, cipher- text, encryption, decryption

1. Introduction

In today's world cryptography is very important and plays key role in electronic data transactions. Enormous amount of information is exchanged in between sender and receiver, through the internet, ecommerce, and telephone conversation. This can be done by various types of techniques such as password, cryptography and biometrics. Cryptographic algorithms are so much useful for secured communication. Various transactions in defense, file transfers in an organization internally requires network security. With the availability of internet, many intruders across the world can access our data. In order to secure our data from intruders we need cryptographic techniques Cryptography is the science of using mathematics to encrypt and decrypt the data. It enables us to store information and transmit it across insecure network so that it cannot be read by anyone except recipient.

The field of cryptography deals with the techniques for conveying information securely, and the goal of cryptography are to allow the intended recipients of a message to receive the message securely. Cryptography tries to prevent the attackers from understanding the message. The message in its original form is called plaintext. The transmitter of a secure system will encrypt the plaintext in order to hide its meaning. This meaning will be revealed only after the correct recipient tries to access it. This reversible mathematical process produces an encrypted output called cipher-text. The algorithm used to encrypt the message is a cipher. As the older algorithms are weak in providing security, so a new encryption and decryption algorithms are very much essential at present scenario. Today's the computers are faster and in feature its speeds will increase more and more. Brute force attacks are made to break the encryption and they are growing so faster. These attacks are the main drawbacks of older algorithm. But with feature this algorithms will be replaced by new techniques that will provide better protection. The project is focuses on implementation of new encryption algorithm Which is more faster, better immune to attacks, more complex, easy to encrypt and Many more advanced security feature included.

This paper focuses on a new encryption algorithm, in which for every eight bytes of plain text it will produce seven bytes of cipher text and in decryption for every seven bytes of cipher text it will reproduce eight bytes of plain text. The project also illustrates about the comparison of various data samples during encryption and decryption process which results in terms of better performance metrics such as data size, memory, and throughput value.

2. Literature Survey

The Paper [1] explains that cryptography means secret writing (Crypto-secret graphy-writing). It includes basic terminology, history of cryptography and cryptanalysis various types of crypto graphic Algorithms. Paper [2] deals with study of definitions of cipher, various types of cipher various types of cryptographic algorithms, such as DES, TDES, Various goals of cryptography. Paper [3] illustrates that In Wireless LAN hacking can be prevented by using encryption and decryption algorithms like DES, TDES and AES. To prevent outside attack more effectively a new algorithm is proposed ,the text and voice messages are successfully applied on a new algorithm. The results of new algorithm are compared with AES, DES, and TDES. since it operates at high data rate ,the key exchange between the users can be avoided and also it reduces encryption and decryption time by using new algorithm .

The Paper [4] presents the main drawbacks of older algorithms are as they are not strong, as it is already known to cryptanalyst so protect the data from unauthorized access it needs further enhancement in cryptographic algorithms, Brute force attacks are so faster to break the encryption because today's computer are faster in its speed by using new cryptographic algorithm better

protection can be provided for multimedia documents. The comparison is made between the PSZ and RSA algorithm both these algorithm are used to convert the plain text into cipher text. PSZ algorithm includes a phases of substitution ,position and zigzag encryption, because of its complexity the algorithm becomes quite difficult to attack. The RSA algorithm is completely based on mathematics. The comparison is made based on constraints such as time requirements, confidentiality, integrity, usability and key length. PSZ algorithm provides better performance.

The paper [5] deals with the comparison between AES and Blowfish algorithm. The comparison is based on parameters like memory size, encryption cycle, and decryption cycle for both algorithms on ARM7 etc. AES key size is fixed, where as BLOWFISH uses the key of variable size .from the results it is observed that compared to Blowfish, AES requires more cycles for encryption and decryption process. Also it requires more memory size Hence BLOWFISH algorithm is suitable for embedded system like smartcard, mobiles for security purpose. Paper [6] deals with a rapid increasing in internet and network application , a huge amount of information is transferred over the internet, so there is need of encryption algorithms in ordered to protect the information from unauthorized access. The comparison of symmetric algorithms like DES, AES, and BLOWFISH takes place on the basis of time as parameter. The various symmetric algorithms are evaluated on different video files. From the result it is observed that different video files are having different processing speed. AES algorithm provides better performance than other algorithms in terms of time and throughput level.

Paper [7] discuses that Encryption process is of converting a message into an unreadable form by using encryption key and encryption algorithm with help of decryption key decryption algorithm only the authorized person can read it. So the information can be secured by means of encryption process. In any network of computers the information transferred is more there is a chances snooping. Development in digital data is exchanged in an electronic way. So does need the technology like information security to secure the data. Information security can provide confidentiality. As the generation goes on, much number cryptographic algorithms have developed to secure the information. In this paper most commonly used encryption algorithms like RSA, DES, TDES, AES, have been discussed .among these AES is the most efficient algorithm by considering parameters like time, speed, and throughput. In paper [8] explains that in information security systems encryption algorithms are used in order to protect the information stored and transferred over the wireless network. The comparison of Encryption algorithms like AES, DES, TDES, RC2, RC6 and BLOWFISH based on power consumption for wireless devices. Like (802.11 WEP and 802.11i WPA,WPA2) .the comparison of the algorithm shows that different results , for parameters like encryption and decryption speed, data trans mission, battery power, data locks, data types. In case of changing packet size with and without transmission of data using different architectures and different WLAN protocols. Blowfish has better performance than other encryption algorithms used.

The paper [9] states that, in multicasting data security can be provided by using encryption algorithms. As In case of multicasting the data can be shared by multiple no of users. There is need of the data encryption algorithms in ordered to share the information confidentially and also to protect the data from unauthorized access. With help the of encryption algorithms, the data can be shared between multiple users .encryption key is used at the sender side to convert the data to an unreadable format, which can be decrypted by using decryption key at the receiver side. In this paper a new encryption algorithm is used with strong key in order to transfer the data among these multiple users with high speed as compared to other encryption algorithm. The paper [10] deals with Information security have become an important issue in data communication. Any loss to the information can prove a great loss to the organization. Encryption techniques play a vital role in information security systems. The paper provides com the algorithms like two fish & blowfish, IBM RSA, RSA. Are compared based on the parameters like, round encryption time, description, block size, key size and throughput. Among these algorithms IBM RSA is having more processing time; more through put hence it is more suitable than other algorithms.

Paper [11] explains that security plays a vital role in the field of network communication and internet. The older cryptographic algorithms like DES become weak against the brute force attack. There is a lot of advancement in computational power in new generation algorithms. To improve the security of DES algorithm, the new transposition technique is added before the DES algorithm. So that it becomes difficult to attack by the intruder. Paper [12] explains that AES (Advanced encryption standard) is an approved cryptographic algorithm which is used to protect the data. The AES can be programmed in software or built with hardware. The paper presents a hardware implementation of the AES algorithm on FPGA. The AES algorithm was implemented in FPGA. The purpose of this attempt is to test the efficiency and optimization of the algorithm structure for the embedded implementation in the application.

The paper [13] explains that Network Security is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use, Cryptographic techniques, hence the main objective is to focus on this area Cryptography. Cryptography is an emerging technology, which is important for network security. The network administrator is responsible for to protect the network from unauthorized access. And also continuous monitoring is required. The paper [14] deal with the increasing popularity of digital devices, computers and networks, Today's world depends

on more and more digital data. In many cases storing data is very big concern. These data can be protected from un authorized access. Encryption is a process of converting a file or message into unreadable form with a decoding key only the intended recipient can read it. Decryption is exactly the reverse process of converting the message which is in unreadable format to original message. In this some of algorithms like RC4, AES, Chao based algorithms have been compared. Among these algorithms, RC4 algorithm is easy to break comparatively, AES is the modified version of DES.

The paper [15] presents secure RSA for secure file transmission, this is a modified version of RSA algorithm which is a asymmetric cryptography, the two keys are used here to transfer the message or information one for encryption(public key)and another decryption(private key)process which is used at the receiver side. If someone obtains both the keys he can communicate with anyone else. Brute force attack is one of the most problems in RSA. Many improvements are done to improve RSA, like MultiPower RSA, BATCH RSA, MultiPrime; Secure RSA eliminates some drawback of RSA that might prevent a hacker from stealing and misuse of data. The paper also presents comparison between RSA file transfer and Secure RSA file transfer. Modified RSA algorithm can be used where high security file transmission required in public forums. The paper [16] presents a block cipher based encryption algorithm generating mechanism is proposed to analyze encryption time and decryption time of the selected cryptographic algorithms. In this algorithm for evaluation, results calculation using different plaintexts in the same key (DPSK) mode. In the evaluating process of the plaintext the corresponding key are both generated by randomly? The expected results showing that, under the same key size and for the same size of the data, proposed algorithm will be about several times faster than existing algorithm, and there are other runtime characteristics which further highlight the difference between these cryptographic algorithms.

In Paper [17] presents the increasing popularity of internet, Many times it is necessary to send important and secure information to the receiver. Main objective of paper is exploring way of encryption done; improve some aspects of the algorithm which is already existed and create way for the excellent security. Implementation of encryption of the information is done in such a way that it will be impossible for the attackers to read the resources sent on the web. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are the methods used for the encryption. In this encryption, conversion of file containing text is done using AES algorithm and key will be encrypted using ECC algorithm. Result will be text (cipher) which is decrypted on the receiver's side. AES and hybrid cryptography provides better security data transfer in wireless network. The paper [18] deal with Encryption is a process of converting plain text to a cipher text the input text (plaintext) using a secret key and an encryption algorithm. Input text is referred to as plain text and the secret text generated is known as cipher text. Encryption algorithms are mainly categorized into two types which are symmetric key encryption algorithm and asymmetric key encryption algorithm. Same key is used In Symmetric key encryption algorithm the same key is used by both sender and receiver but in asymmetric key algorithm sender and receiver both uses the different keys. Paper also presents a technique based on symmetric key encryption algorithm which uses ASCII vales of input text to encrypt the data. Text data encryption techniques are very useful in data communication where one user want to send some secret messages to other users.

Paper [19] explains that Cryptography is the study of hiding information. The conversion of information takes place from a readable state to unreadable form. In order to avoid unauthorized access, senders retain the ability to decrypt the information. The three type of Cryptographic algorithm are Asymmetric key cryptography, symmetric key cryptography and hashing. Encryption processes in which both the sender and receiver share the same key are known as symmetric key cryptography. The comparison between most commonly used symmetric key cryptography algorithms is made such as AES, Two fish, CAST-256 and Blowfish. The different data load are comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used, as. The comparison is made on the basis of the parameters like speed, block size, and key size. Paper [20] explains that in the today's world, security is a one of the very important thing which is required to transmit confidential information over the network .Security is also demanding in wide range of applications. Cryptographic algorithms play an important role in providing the data security against malicious attacks. As they are consuming significant amount of computing resources like CPU time, memory, encryption time etc. Symmetric key algorithms are used over asymmetric key algorithms as they are very fast in nature. Symmetric algorithms are classified as block cipher and stream ciphers algorithms. The comparison of AES algorithm takes place with RC4 algorithm in terms of CPU time, encryption time, memory utilization and throughput at different settings like variable key size and variable data packet size. Results show that RC4 is better than AES.

The paper [21] states that as popularity of wireless networks increases any wireless communication security is crucial during data transmission. The encryption and decryption of data is the main challenge faced in the wireless communication for security of the data transmission source to destination. It also includes the study of cryptography security AES algorithm and its present application in communication, data communication and wireless communication. Advanced Encryption Standard (AES) works on a 128 bit data encrypting it with 128 bits of keys for ensuring security. The paper [22] explains that now a day's sharing the information over internet is becoming a critical issue due to security problems. Hence more techniques are needed to protect the shared data in an unsecured channel. The present work focus on combination of cryptography First point is data which is to be transmitted from source to destination in the network must be encrypted using the encrypted algorithm in cryptography .Second point is encrypted data must be hidden in an image or video or an audio file with help of algorithm. Third point is by using decryption technique the receiver can view the original data from the hidden image or video or audio file.

Transmitting data or document can be done through these ways will be secured. Three encryption techniques like DES, AES and RSA algorithm along with steganographic algorithm like LSB substitution technique and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption process and also its buffer size experimentally.

The paper [23] focuses on different kinds of encryption techniques that are exist. It is a literature survey of some modern cryptography. The advantages and disadvantages of the methods are also discussed in brief. It also aims image encryption techniques, double encryption, information encryption techniques and Chaos-based encryption techniques.

Some of the most common issue which we have identified as from the literature survey is as follows.

- Encryption time: - time taken by encryption algorithm to convert plain text cipher text.
- Memory: - the memory deals with amount of memory space it takes for the whole process of encryption and decryption.
- Throughput value: - throughput can be calculated total plaintext in bytes divided by the encryption time.
- Key length: - is an important issue to design any algorithm. The larger key length will results in slow execution which gives the poor performance. If the key length is small then it will results in poor security.

Some of performance parameters like memory; data size can be improved by using the proposed algorithm called "Encryption and Decryption Using Bit Operations". In most of the cryptographic algorithms as we have studied from the literature survey, There are some parameters where improvement is necessary. These parameters are efficiency, execution time, throughput value, space complexity and many more. It is already known that due to unstructured design of the algorithm these parameters cannot fulfill for betterment of the algorithm. All most all algorithms used key for encryption and decryption which can be reflect execution time, efficiency and other performance parameters. Key length is important issue to design any algorithm, because larger key length will be cause of slow execution and poor performance of the algorithm. And smaller key length can cause poor security. Our proposed algorithm is mainly based on data size and amount of memory required for execution an algorithm. In our proposed system after encrypting the input data for every eight bytes of plaintext it will generate seven bytes cipher text and in decryption, for every seven bytes of cipher text eight byte of plain text will be produced. So the size of the data will be going to reduced during encryption process. Hence a new algorithm is proposed known as "Encryption and Decryption Using Bit Operations".

3. Proposed Methodology

The In most of the encryption and decryption algorithms, the encryption and decryption process needs some of the characters are to be interchanged with key. But our proposed algorithm works on the basis of bit shifting and stuffing technique. This requires seven bits to represent a printable character as per its ASCII value. As we know that in computer system to represent a printable character it requires one byte , i.e. 8 bits so a printable character occupies 7 bits and last bit value is 0 which is not useful for the character. In our proposed technique we are stuffing a new bit in the place of unused bit which is shifting from another printable character. So in our proposed algorithm after encryption for every eight bytes of plain text it will generate seven bytes cipher text and in decryption for every seven bytes of cipher text it will reproduce eight bytes of plain text.

Encryption process: - In this process let us consider I_1, I_2, I_3, I_4, I_5, I_6, I_7, and I_8 represents 8 printable characters of plain text and the values in the boxes represent the byte equivalent values of each character. i.e. a_1, a_2, a_3, a_4, a_5, a_6, a_7 represents 7 bits of Character I_1 and their values may be either 0 or 1.Similarly remaining character represented in boxes as shown in figure (1). In this process the last character I_8 bits h_1 ,h2,h3,h4,h5,h6,h7 are shifted and stuffed into the characters I_7 ,I_6, I_5, I_4, I_3, I_2, I_1 respectively and it is as shown in figure (2) . Consider the eight characters are a, b, c, d, e, f, g and h. i.e. I_1=A, I_2=B, I_3=C I_4=D, I_5=E, I_6=F, I_7=G and I_8=H
The equivalent byte values of these characters before encryption are as follows.

I_1 ASCII value 65 and its bits: 01000001 i.e. a_1=1, a_2=0, a_3=0, a_4=0, a_5=0, a_6=0, a_7=1
I_2 ASCII value 66 and its bits:01000010 i.e. b_1=1, b_2=0, b3=0, b_4=0, b_5=0, b_6=1, b_7=0.
I_3 ASCII value 67 and its bits:01000011 i.e. c_1=1, c_2=0, c_3=0, c_4=0, c_5=0, c_6=1, c_7=1.
I_4 ASCII value 68 and its bits:01000100 i.e. d_1=1, d_2=0, d_3=0, d_4=0, d_5=1, d_6=0, d_7=0.
I_5 ASCII value 69 and its bits:01000101 i.e. e_1=1, e_2=0, e_3=0, e_4=0, e_5=1, e_6=0, e_7=1.
I_6 ASCII value 70 and its bits:01000110 i.e. f_1=1, f_2=0, f_3=0, f_4=0, f_5=1, f_6=1, f_7=0.
I_7 ASCII value 71 and its bits: 01000111 i.e. g_1 =1, g_2 =0, g_3=0, g_4 =0, g_5 =1, g6 =1, g_7 =1.
I_8 ASCII value 72 and its bits:01001000 i.e. h_1=1, h_2=0, h_3=0, h_4=1, h_5=0, h_6=0, h_7=0.
After encryption by using our proposed method the equivalent byte values of these characters are as follows.
I_1 bits: 01000001, i.e. h_7=0, a_1=1, a_2=0, a_3=0, a_4=0, a_5=0, a_6=0, a_7=1
I_2 bits: 01000010, i.e. h_6=0, b_1=1, b_2=0, b_3=0, b_4=0, b_5=0, b_6=1, b_7=0
I_3 bits: 01000011, i.e. h_5=0, c_1=1, c_2=0, c_3=0, c_4=0, c_5=0, c_6=1, c_7=1
I_4 bits: 11000100, i.e. h_4=1, d_1=1, d_2=0, d_3=0, d_4=0, d_5=1, d_6=0, d_7=0
I_5 bits: 01000101, i.e. h_3=0, e_1=1, e_2=0, e_3=0, e_4=0, e_5=1, e_6=0, e_7=1
I_6 bits: 01000110, i.e. h_2=0, f_1=1, f_2=0, f_3=0, f_4=0, f_5=1, f_6=1, f_7=0
I_7 bits: 11000111, i.e. h_1=1, g_1=1, g_2=0, g_3=0, g_4=0, g_5=1, g_6=1, g_7=1

During encryption process eight bytes of Input data (plain text) is applied as the input to the encryption algorithm

where as we can get the seven bytes of cipher text at the output side.

Decryption process: - In decryption process every seven bytes of cipher text produces eight characters of plain text. So after decryption process the decrypted data will automatically get its original size. The figure (3) shows the data before decryption and the figure (4) shows the data after decryption.

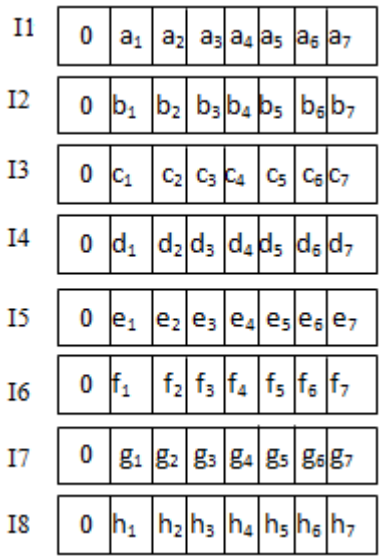

Figure 1: Before Encryption

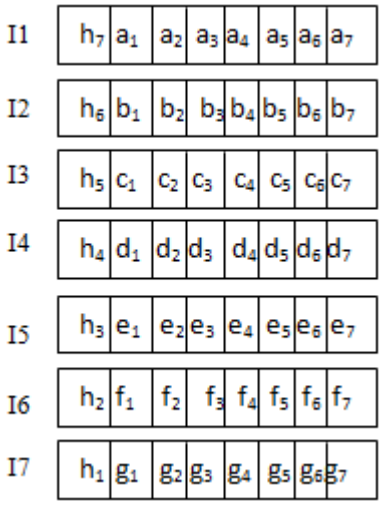

Figure 2: After Encryption

3.1 Proposed Algorithm

Algorithm1: Encryption of Data

Start

STEP 1: Read the 8 bytes of char from the input file
STEP 2: Repeat the steps (3) eight times
STEP 3: Shift all the bits of 8th byte one by one to the 1st position and copy to the 1st bit of all the remaining seven bytes.
STEP4: Repeat the steps (1), (2), (3) for remaining bytes in the input file

End

Algorithm2: Decryption of Data

Start

STEP 1: Read the seven bytes of char from input.
STEP 2: Repeat the step no (3) seven times.
STEP 3: Extract the 1st bit of each byte and extract the remaining bits to the decrypted characters
STEP 4: Shift the extracted 1st bit to the respective location of the eight byte characters.
STEP 5: Repeat steps (3) and (4) for all the 7 bits and OR with all the shifted bit to obtain the 8th byte
STEP 6: Repeat the steps (1) to (5) for remaining bytes in the decrypted file.

End

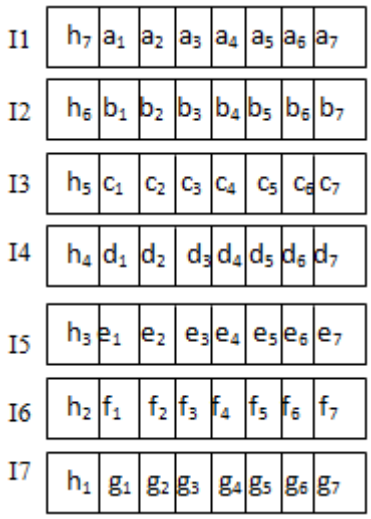

Figure 3: Before Encryption

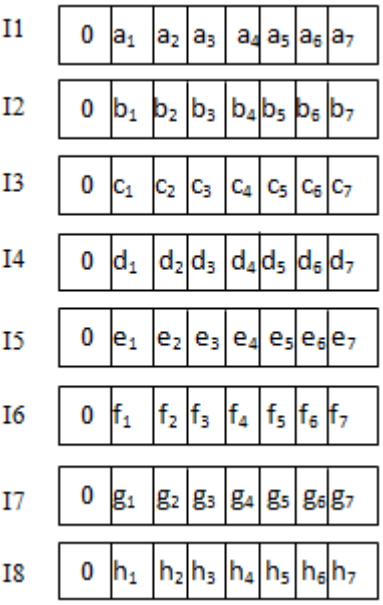

Figure 4: After Encryption

4. Performance Analyses

The experiment is carried out, by applying different sizes of data samples as input to the encryption and decryption process, after encryption the size of data is reduced and after decryption the size of decrypted data is

increased . The below table represents the variation of size of different data samples sets after encryption and decryption. The performance metrics are data size, encryption time, decryption time, through put value.

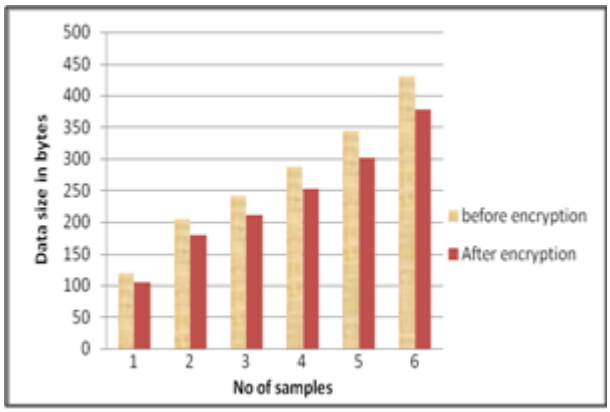

Figure 5: Data size before and after encryption

The different sizes of data samples are applied to the encryption. The above graph shows that the comparison between different sizes of the data samples before encryption and after encryption. And it is observed that the size of the data in bytes is reduced during encryption process i.e. the size of the data is more before the encryption process and size of data is gradually going to reduces after every encryption process.

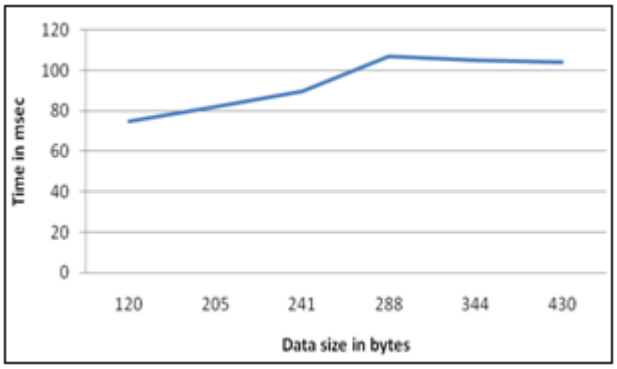

Figure 6: Encryption time versus data size

The above graph shows that the comparison of different size of data samples and the time taken for the whole encryption process.

Through put= Total plain text in bytes encrypted/ Encryption time

The throughput of an algorithm is calculated by dividing total no of bytes(plain text)encrypted by encryption time.

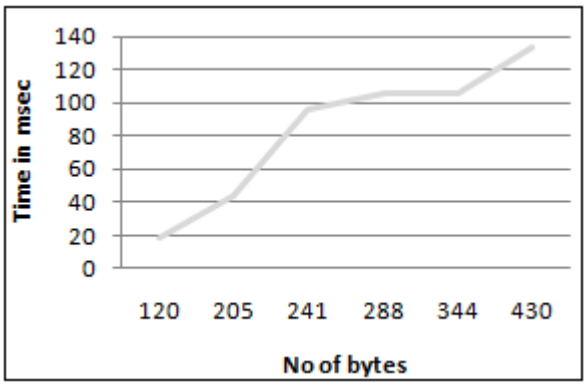

Figure 7: Decryption time versus data size

The graph shown in figure 7 shows that the comparison between the decrypted data and time taken for the whole decryption process (decryption time). And it is observed that decryption time is varies with data.

5. Conclusion And Future Scope

In this project we have made a new implementation of encryption and decryption using bit operations which was very effective in terms of complexity and security. The main objective was to evaluate the performance of our algorithm in terms of data size . Our proposed algorithm is very effective in terms of performance metrics such as encryption time, through put value, decryption time, and execution time. also our proposed algorithm performance is better than exiting algorithms . Hence finally we conclude that the encryption and decryption using bit operation is very effective in providing security.

As this project is based on new encryption and decryption technique, to provide security these techniques are very essential, we will consider this technique for applying to different data samples like video files, audio and speech signals. In future we are going to provide a secret key for authentication to the encrypted data and decrypted data.

References

[1] www.wikipedia.com
[2] W.Stalling, “cryptography and network security: principles and practice” 5th edition p9-11
[3] G.Ramesh and R. Umarani, “data security in local area network based on fast encryption algorithm”, IEEE, Intact Journal on Communication Technology, June 2010, Issue: 02 p118-127
[4] Mr. Anil Hingmire “Data Encryption / Decryption process using PSZ methodology and performance Analysis with RSA.” (IJERA) ISSN: 2248-9622 (VNCET-30 Mar’12) 248-252
[5] Ms. Pallavi H.Dixit, Dr.Uttam L. “Comparative Implementation of Cryptographic Algorithms on ARM Platform” (IJIRSET) Vol. 2, Issue 10, October 2013p5505-5510.
[6] S. pavitra and Mrs. E. Ramadevi “Performance Evaluation of Symmetric algorithms” (JGRCS) ISSN2229-371X p43-45.

[7] Gurpreet Singh , Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security "International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013 p33-38.
[8] Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud "performance evaluation of symmetric Encryption Algorithms on Power Consumption for Wireless Devices", (IJCTE) Vol. 1, No. 4, October, 2009 1793-8201, p343-351
[9] M.Kiran Kumar, B.N.V.MadhuBabu, K.Nageswrarao "Providing Security for Data in Multicasting Using Encryption" International Journal of Engineering Inventions ISSN: 2278-7461, www.ijeijournal.com Volume 1, Issue 2(September 2012) PP: 62-65
[10] Lalit Singh Dr. R.K. Bharti " Comparative Performance Analysis of Cryptographic Algorithms "International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 11, November 2013 ISSN: 2277 128X p563-568
[11] Sombir Singh Dr.Sudesh Kumar " Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques " International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013 ISSN: 2277 128X P464-471.
[12] S. Venkateswarlu, Deepa G.M, G. Sriteja "Implementation of Cryptographic Algorithm on FPGA"International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 4, April 2013, pg.604 – 609
[13] Sumedha Kaushik Ankur Singhal " Network Security Using Cryptographic Techniques " International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012 ISSN: 2277 128X p105-107
[14] Kulkarni Laxmi G, N. A. Dawande "Encryption Algorithms Used for Secured Communication" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 p27-29
[15] Rajan.S.Jamgekar, Geeta Shantanu Joshi "File Encryption and Decryption Using Secure RSA"International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013 p11-14
[16] Suyash Verma, Rajnish Choubey, Roopali son "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, and July 2012) p18-21
[17] K.Brindha, G.Ramya Rajpal Amit Jayanti " Secured Data Transfer in Wireless Networks Using Hybrid Cryptography "International Journal of Advanced Research inComputer Science and Software Engineering Volume 3, Issue 10, October 2013 ISSN: 2277 128X ,p379-381
[18] Udepal Singh, Upasna Garg "An ASCII value based text data encryption systems" International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 1 ISSN 2250-3153 p1-5
[19] Apoorva1, Yogesh Kumar "Comparative Study of Different Symmetric Key Algorithms" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847 p204-206
[20] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC Algorithms for Better Utilization" International Journal of Computer Trends and Technology- July to Aug Issue 2011 p177-181
[21] Vedkiran Saini, Parvinder Bangar, "Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application "International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume2, Issue-6, April 2014p33-37
[22] B. Padmavathi, S. Ranjitha Kumari "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique "International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 4, April 2013 p170-174
[23] Mr. Gagendra Singh Chande Prabhat Kumar Singh "A Literature Review of Various Variants of RSA Cryptosystem" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014 ISSN: 2277 128X