ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

The Blowfish Algorithm Simplified

Avinash M Ghorpade[1], Harshavardhan Talwar[2]

Associate Professor, Dept. of Electronics and Communication, Maratha Mandal Engineering College, Belgaum, Karnataka, India[1]

PG Student [DECS], Dept. of Electronics and Communication, Maratha Mandal Engineering College, Belgaum, Karnataka, India [2]

ABSTRACT: The development rate of the web surpasses than some other innovation which is measured by clients and data transmission. Web has been developing at a quick rate since its origination, on a bend geometric and at times exponential. These days, the Internet is moving rapidly in three unique headings, for example, size, preparing force, and programming complexity making it the quickest developing innovation mankind has ever made. With the quick development of web, we have to ensure the touchy information from unapproved access. Cryptography assumes a key part in the field of system security. Right now numerous encryption calculations are accessible to secure the information however these calculations devour parcel of figuring assets, for example, battery and CPU time. This paper mostly concentrates on ordinarily utilized symmetric encryption calculation (algorithm) which is Blowfish calculation (algorithm). Test results are given to illustrate the execution of this calculation.

KEYWORDS: Blowfish, Cryptography, Encryption, Decryption

I.INTRODUCTION

The idea of cell automata gives the unmistakable comprehension about its mark, which is "Session of life". Cell mechanization is really a discrete scientific model speaking to the cell grid which works on the states and the guidelines are pertinent to cells after change. The Information security conveys much significance in exceptionally field of life. Particularly the Military undertakings and private business are extremely touchy in such manner. To keep information far from the entrance of unapproved clients or to make it safe from being tainted is called information security. Encryption is a vital security component. The standard of its working is to scramble the data into incomprehensible data and afterwards unscramble it for perusing utilizing a key. Encryption of the content (text) is not quite the same as that of a picture. Because of the natural characters of pictures, for example, mass information limit and high excess, encryption on picture or video objects has its own prerequisites. Numerous calculations give diverse levels of security and it depends on that they are so difficult to break, for example, we utilize Blowfish encryption calculation. On the off chance that the cost required to break a calculation is more prominent than the estimation of the encoded information, then the calculation most likely is viewed as sheltered. Be that as it may, present day top notch picture encryption techniques have a few provisos and are subjected to broad assaults by master cryptanalyst. Exhaustive study and examination between these systems are expected to quantify the execution and to pick the better one for the proposed application. For a few applications pace of encryption might be the essential purpose of concern and for some different cases the security will be critical.

Because of the quick increment in the computerized correspondence and trade of electronic information, the security of data has turned into a critical issue in business, industry, and organization. In cutting edge period security is the significant issue for each correspondence amongst sender and collector. On the off chance that there are any security ruptures in the middle of correspondence then there will be real misfortune to them two, sender and recipient. The cryptography utilized today gives numerous key systems for ensuring information and securing data.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

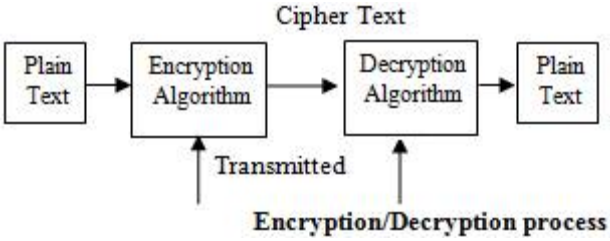

Fig 1- Text encryption and decryption

Cryptography is a crucial part for the Data Security Framework. It assumes an essential part in the security of information amongst sender and beneficiary. Cryptography gives us classification, exactness, decency, alongside information uprightness. Presently the cryptography is used routinely to secure information, which must be imparted and/or spared over long stretches, to ensure electronic asset exchanges and grouped interchanges.

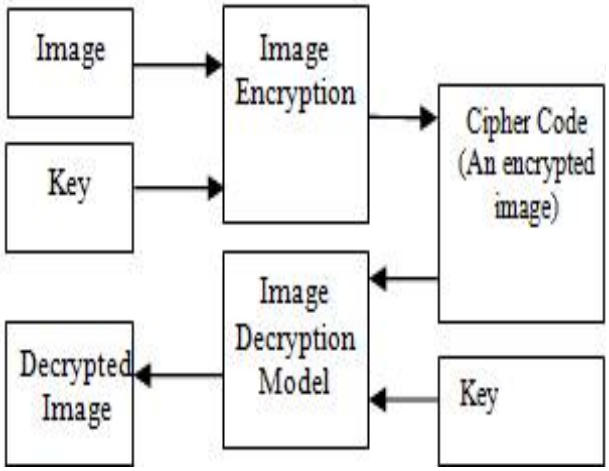

Fig 2- Image encryption and decryption

Cutting edge cryptographic strategies depend on number hypothetical or mathematical ideas. Before going on our fundamental theme we have to know in any event brief data about security patterns in cryptography, what are the different security assaults could be conceivable, what are the different security administrations and what are security instruments ought to be connected to accomplish those administrations.

A. Types of cryptography

1. Asymmetric Key Cryptography

In this kind of cryptography, there are two keys utilized: open key and private key, one for encryption and one for unscrambling reason. Well known cases are: RSA, ElGamal, Merkle's Riddles, and Elliptic Curve Cryptography (ECC). Asymmetric key cryptography is otherwise called open key cryptography. This calculation needn't bother with a secured starting trade of one or more keys between the sender and beneficiary. The calculation utilized for encryption and decoding was composed in a manner that, it makes simple for the collector to deliver the general population and private keys and to unscramble the message by private key. It is additionally simple for the sender to encode the message by using open key, and it is exceptionally troublesome for anybody to discover the private key in light of the learning of the general population key.

2. Symmetric Key Cryptography

In this sort of cryptography, same key is utilized for both encryption and decoding reason. Symmetric calculations can be partitioned into two sort stream cipher and block cipher. Stream cipher encode one piece (one bit) of plaintext at once when contrasted with block cipher which takes various bits (ordinarily 64 bits), and encrypt them as one unit in entirety. Symmetric ciphers are liable to be hurt by the known plaintext and picked content assaults, and in addition differential and direct. A few cases of well-known symmetric calculations are: Serpent, AES (Rijndael), Blowfish, RC4, RC6, DES, 3DES. Symmetric key calculations are less computationally escalated when contrasted with asymmetric key calculations. In any case, practically speaking, asymmetric key calculations are much slower when

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

contrasted with the symmetric key calculations. Asymmetric algorithm (also known as open key calculations) requires no less than a 3,000-piece key to attain at the same range of security as that of a 128-bit symmetric calculation.

B. Various Goals

1. Confidentiality- Data in PC is transmitted and must be a gotten to just by the approved party and not by any other person.
2. Authentication- Confirmation of the data got by any framework needs to check the character of the sender that whether the data is touching base from an approved individual or a false personality.
3. Integrity- Just the approved party is permitted to alter the transmitted data. Nobody in the middle of the sender and collector are permitted to adjust the given message.
4. Non Repudiation- Guarantee that neither the sender, nor the beneficiary of message ought to have the capacity to deny the transmission.
5. Access control- Just the approved gatherings can get to the given data.

C. Basic Terms

1. Plain Text- The first message that the individual wishes to speak with the other is characterized as Plain Text. For instance, Alice is a girl wishes to send "Hello Friend how you doing" message to the individual Bob. Here "Hellow Friend how you doing" is a plain instant (text) message.
2. Cipher Text- The message that can't be comprehended by any one or a good for nothing message is the thing that we call as Cipher content (text). For Example, "Ajd672#@91ukl8*^5%" is a Cipher Text created for "Hello Friend how you doing".
3. Encryption- Encryption A procedure of changing over plain content (text) into cipher content (text) is called as Encryption. The procedure of encryption requires two things-an encryption calculation (algorithm) and a key. An encryption calculation (algorithm) implies the procedure that has been utilized as a part of encryption. Encryption happens at the sender side.
4. Decryption- A converse procedure of encryption is known as Decryption. It is a procedure of changing over Cipher content (text) into Plain content (text). The procedure of decryption needs two things-a decryption calculation (algorithm) and a key. A decryption calculation (algorithm) implies the procedure that has been utilized as a part of Decryption. For the most part the encryption and decoding (decryption) calculation (algorithm) are similar.
5. Key- A key is generally a numeric or alpha numeric content or might be an uncommon symbol. The key is utilized at the season of encryption happens on the plain content (text) and at the season of decryption happens on the cipher content (text). For instance, if the Alice utilizes a key of 3 to encode the plain content (text) "President" then cipher content (text) delivered will be "Suhylghqw".

II.EXISTING SYSTEMS

A. Triple DES (TDES):

The triple DES (3DES) calculation (algorithm) was required as a substitution for DES because of advances in key seeking. TDES utilizes three round message This gives TDES as a most grounded encryption calculation(algorithm) since it is to a great degree difficult to break 2^168 conceivable mixes. Another choice is to utilize two distinctive keys for the encryption calculation (algorithm). This decreases the memory necessity of keys in TDES. The burden of this calculation is that it is excessively tedious.

B. Data encryption standard (DES):

DES was developed around 1974 and embraced as a national standard in 1997. DES is a 64-bit piece (block) cipher with 56-bit key. The calculation (algorithm) forms with an underlying change, sixteen rounds block cipher with the last stage. DES application is extremely well known in business, military, and different spaces in the most recent decades. In spite of the fact that the DES standard is open, the outline criteria utilized are arranged. There has been extensive contention over the configuration, especially in the decision of a 56-bit key.Data Encryption Standard) was the principal encryption standard to be prescribed by NIST (National Institute of Standards and Technology). It was produced by an IBM group

C. Advanced encryption standard (AES):

AES was produced by two researchers Joan and Vincent Rijmen in 2000. AES utilizes the Rijndael block cipher. Block length and the Rijndael key can be 128, 192 or 256-bits. On the off chance that both the key-length and block length are

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

128-piece (bit), Rijndael will perform 9 handling rounds. In the event that the block or key is 192-piece (bit), it performs 11 handling rounds. On the off chance that either is 256-piece (bit), Rijndael performs 13 handling rounds.

D. Blowfish:

Bruce Schneier planned blowfish in 1993 as a quick, free other option to existing encryption calculations (algorithms). From that point forward it has been broke down significantly, and it is gradually picking up acknowledgment as a solid encryption calculation (algorithms). The Blowfish calculation has numerous points of interest. It is reasonable and productive for equipment execution and no permit is required. The rudimentary administrators of Blowfish calculation incorporate addition, table lookup and XOR. The table incorporates four S-boxes and also a P-array. Blowfish is a cipher which takes into account Feistel rounds, and the configuration of the F-function utilized sums to an improvement of the standards utilized as a part of DES to furnish the same security with more prominent rate and effectiveness in programming. It is indeed a 64-bit block cipher and also is proposed as a swap for DES. Blowfish is a quick calculation (algorithm) and can encrypt information on 32-bit microchips.

III.PROPOSED WORK

Blowfish algorithm generally categorised as a symmetric block cipher, planned by Bruce Schneier in 1993, that can be viably utilized for encryption and shielding of information. It utilizes a variable-length key, which varies from 32 bits to 448 bits, making it perfect for securing information. Blowfish Algorithm is a Feistel Network, emphasizing a basic encryption capacity 16 times.

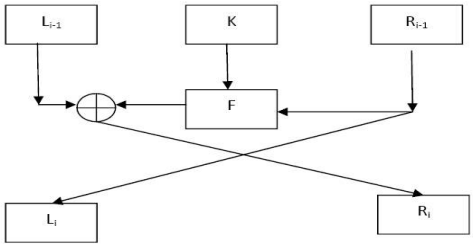

Fig 3- Feistal Network

The standard block size is 64 bits, where in the key can vary up to 448 bits. Despite the fact that there is an intricate introduction stage required before any encryption can occur, the genuine encryption of information is extremely effective on vast microchips. The remarkable components of Blowfish algorithm with impressive features and helps in my work are as per the following:

A. It controls information in extensive pieces

B. It comprises of a 64-bit block size.

C. It has an adaptable key, from 32 bits to no less than 256bits.

D. It utilizes exceptionally straightforward operations like expansion and XOR expansion.

E. It utilizes an outline that is easy to get it. This encourages examination and expansion the trust in the calculation.

F. It is quick as this algorithm rate on a 32-bit microchip is 26 clock cycles for every byte.

G. It is minimized as it can be executed below 5kb memory.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

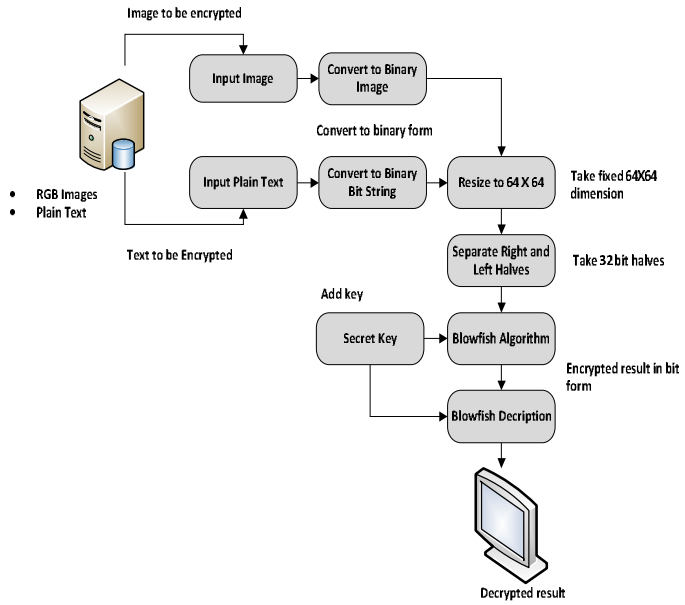

Fig 4- Block diagram of the encryption and decryption process

Blowfish algorithm comprises of a 64-bit block size with a variable key length between 32 bits up till 448 bits. It has 16-round Feistel cipher and uses substantial key-subordinate S-boxes. In structure it looks like CAST-128, which utilizes settled S-boxes.

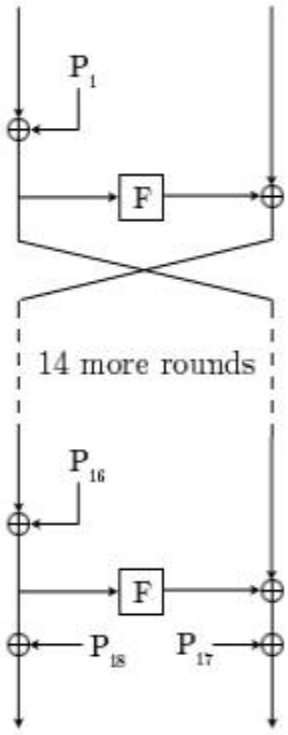

Fig 5- Feistel Structure of Blowfish Algorithm

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

The chart above demonstrates Blowfish's encryption schedule. Every line speaks to 32 bits. There exist five sub key arrays: generally one 18- entry P-array (signified as K in the outline, to stay away from perplexity with the Plaintext) and four 256-entry S-boxes (S0, S1, S2 and S3).

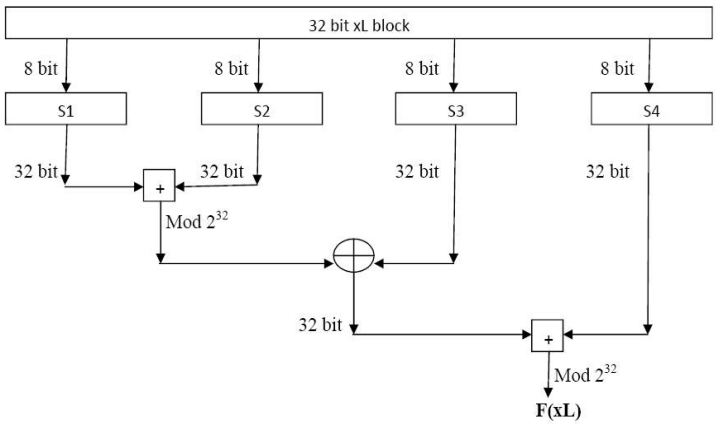

Fig 6- S-Box operation (F function) of Blowfish algorithm

Each round r comprises of 4 activities: Initially, XOR the left half (L) of the information with the r th P-array passage, second, utilize the XORed information as contribution for Blowfish's F-function, third, XOR the F-function's yield with the right half (R) of the information, and keep going, swap L and R.
The F-function parts the 32-bit information to four parts of eight-bit quarters, and uses the quarters as contribution to the S-boxes. The S-boxes acknowledge 8-bit info and produce 32-bit yield (output). The yields are summed modulo 232 and XORed to deliver the last 32-bit yield (see picture in the upper right corner).
After the sixteenth round, fix the keep going swap, and XOR L along with the K18 and R along with the K17 (output whitening).

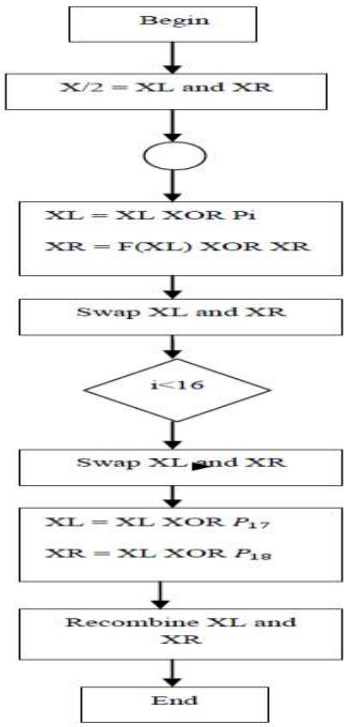

Fig 7- Flowchart for blowfish algorithm

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Decoding is precisely the same as encryption, aside from that P1, P2… P18 are utilized as a part of the opposite request. This is not all that conspicuous in light of the fact that xor is commutative and acquainted. A typical misguided judgment is to utilize backwards request of encryption as decryption calculation (algorithm) (i.e. to begin with XORing P17 and P18 to the ciphertext, then utilizing the P-sections as a part of converse request).
Blowfish's key timetable begins by introducing the P-array and S-boxes with qualities got from the hexadecimal values of pi, which contain no undeniable example. The mystery key is then, byte by byte, cycling the mystery key if important, XORed with all the P-passages all together. A 64-bit each of the zero blocks is then encrypted with the calculation the way things are. The resultant ciphertext exchanges P1 and P2. The same ciphertext is now encrypted all over again with the resultant new subkeys, and the new ciphertext changes P3 and P4. This keeps going, supplanting the whole P-array and the whole S-box sections. On the whole, the Blowfish encryption calculation will run 521 times to create all the subkeys - around 4KB of information is prepared.
Since the P-array is 576 bits in length, and generally the key bytes are XORed along through all the particular 576 bits amid the introduction, numerous usage bolster key sizes up to 576 bits. While this is positively conceivable, the 448 bits point of confinement is here to guarantee that all of each subkey relies on upon the entire key, as the last four estimations of the P-array don't influence all of the ciphertext. This point ought to be taken in thought for usage with an alternate number of rounds, as despite the fact that it expands security against a thorough assault, it debilitates the security ensured by the calculation. What's more, given the moderate instatement of the figure with every change of key, it is allowed a characteristic assurance against animal power assaults, which doesn't generally legitimize key sizes longer than 448 bits.

IV.EXPERIMENTAL RESULTS

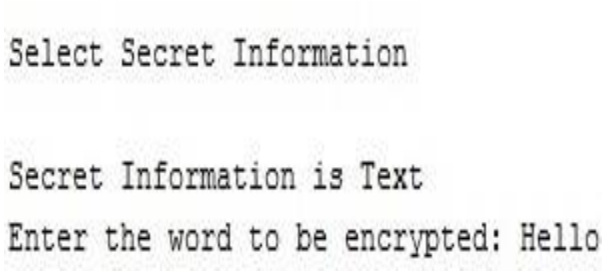

Fig 8- Dialogue box asking for the text to enter for encryption.

As soon as you run the program the dialogue box pops up asking us whether we wish to choose text or image encryption. When we select text encryption, the code asks us to enter the desired text for encryption.

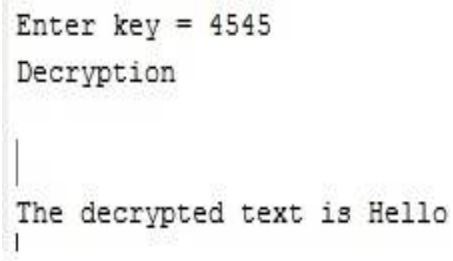

Fig 9-Dialogue box asking to enter the key and displaying the decryption result.

When you tap enter for the desired text to be encrypted the code asks for the secret key and if the key entered is correct, the program is executed and we obtain the decryption result.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Fig 10- Dialogue box asking for the image for encryption.

When you run the code a dialogue box pops us asking us to select either text or image encryption. If we choose image, the code asks us to upload a desired image to be encrypted.

Fig 11- Dialogue box displaying the original image converted to binary image.

When you further run the program, the original image is converted in 64X64 bits binary image.

Fig 12- Dialogue box displaying the encrypted image.

Further the binary image is encrypted using the blowfish algorithm which uses S-blocks and p-array and encrypts the selected image.

Fig 13- Dialogue box displaying the decrypted image.

Finally when you tap decryption, the further part of the code is executed and the blowfish algorithm is executed to obtain the decrypted image which is same as the original image.

V. CONCLUSION

In this paper the transition of encrypted text and image over the web we have utilized the blowfish algorithm. Already utilized algorithms like AES, DES thus more has been supplanted by the blowfish calculation, as a result of creating fruitful viability on security. Blowfish algorithm cannot be effectively broken by the programmers until they locate the right mixes. This is more complicated to shape the accurate mixes of the lock. To make the calculation more grounded number of rounds has been expanded. It requires less investment to encrypt and decrypt the required text and image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

than whatever other algorithms. For future upgrade propelled calculations can be design for better security and encrypt more convoluted text and image.

ACKNOWLEDGMENT

It gives me an immense pleasure to express my gratitude and respect to all those who guided me in the completion of my paper.
I am thankful to my guide Prof. A.M Ghorpade, Dept. of electronics and communication, Maratha Mandal Engineering College Belgaum, for helping me to complete this paper. I am also thankful to all the staff members who directly or indirectly contributed their efforts to complete this paper.
I also thank my entire classmate and friends for their kind help in bringing out this paper in stipulated time. The paper would be incomplete if I do not thank my parents and well-wishers for their moral support during the course of the paper.

REFERENCES

[1] Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2nd edition, 2008.
[2] Anand Kumar M and Dr. S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael Algorithms", International Journal of Computer Network and Information Security, pp. 22 28, 2012.
[3] Obaida Mohammad Awad and Al-Hazaimeh, "Design of a New Block Cipher Algorithm", Network and Complex Systems, Vol. 3, No. 8, pp. 1-5, 2013.
[4] Md Imran Alam, "A Comparative Analysis of Different Encryption Techniques of Cryptography", International Journal of Advanced and Innovative Research, Vol. 2, Issue 9, pp. 160 166, 2013.
[5] Ali M Alshahrani, "Different Data Block Size Using to Evaluate the Performance Between Different Symmetric Key Algorithms",
[6] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3
[7] KundankumarRameshwarSaraf, Vishal PrakashJagtap and Amit Kumar Mishra, Text and Image Encryption Decryption Using Advanced Encryption Standard,International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
[8] S.Dhanalakshmi, Dr.T.Ravichandran, A New Level Of Image Processing Technique Using Cryptography And Steganography, ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 3, March 2013 659
[9] Kaladharan N, Unique Key Using Encryption and Decryption of Image, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014
[10] Mayank Mishra, Prashant Singh, ChinmayGarg, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal of Information & Computation Technology. ISSN 0974- 2239 Volume 4, Number 7 (2014), pp. 741-746