IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

A Survey on Various Algorithmic Methods for Encryption and Decryption

K. Kamalam

Asst. Professor, KG College of Arts & Science, Coimbatore

Abstract: A computer network is a group of computer systems which are connected together through various communication channels which make easy use of resource-sharing between the wide ranges of users. Security was not an important and essential issue in early days. But now as billions of ordinary citizens are using networks for banking, shopping, Air Ticket Reservation, Online Examinations, Filling their Income Tax, Business, Marketing, Stock Exchange, hospitals, government organizations, and industries and so on.Computer securityis also known as cyber securityand IT security because it protects the computer system from theft or damage to the hardware, software or the information stored in it.Securityis a techniquewhich is used tomake certain data stored in a computersystem which cannot be read or translated by any persons or individuals without any authorization because it involves data encryption and password.Computer hackingis one of the technique used for modifying or altering computer software and hardware with unauthorized access to the computer system. In short term it can be called as "hackers."This paper provides a review and survey of some of the symmetric and asymmetric techniques used in computer networks. Feature of achieving the effectiveness, flexibility, security, and efficiency.

Keywords: AES, Blowfish, Cryptography, Decryption, Symmetric Encryption, IDEA, RC4, RSA.

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form. Cryptography is a processofcodinganddecodingmessagesin secured form bythesenderandrecipientofthemessage. Cryptography is used to overcome the various aspects in information security such as data confidentiality, data integrity, privacy, authentication, reliability, verification, validation and non-repudiation of data.
Cryptography includes the following process secret writing, the enciphering and deciphering of messages in secret code or cipher, the computerized encoding and decoding of information, cryptanalysis. Cryptography is a plaintext or ordinary text orcleartext intocipher textand this process is called encryption and then back againknown as decryption.

Figure:1 Structure of Cryptography

A. ENCRYPTION

Encryption is a process of converting the electronic data into another form which is called ciphertext. Cipher text cannot be easily understood by anyone except authorized parties. In cryptography, encryption is the process of encoding the messages or information only the authorized parties can access it.. The translation and converting of fdata into a secret code is called as Encryption and it is the most effective and successful way to achieve data security. To read an encrypted file, user must have process the secret key or password which enables in to decryptform. Unencrypted data is called plain text; encrypted data calledcipher text.There are two main types of encryption listed below

1. Asymmetric Encryption (it also called Public-Key Encryption) and
2. Symmetric Encryption

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

B. DECRYPTION

The process of decoding the data which is in encrypted form into a secret format is called Decryption. Decryption requires a secret key or password. Decryption is the process of converting encrypted data back into its original form which can be understood by the user.

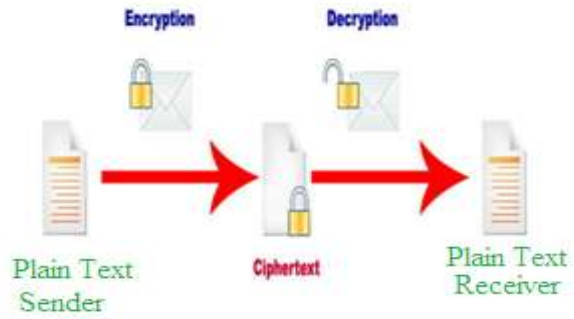

Figure: 2 Process of Encryption and Decryption

II. ENVIRONMENT OF CRYPTOGRAPHY

Cryptography is the art and science of keeping messages in secure manner. The required basic definitions and concepts [23] in Cryptography are reviewed here.

Plaintext: Plaintext is ordinary readable and original text before being encrypted into ciphertext or after being decrypted.Plain textis in portable format on every machine.

Ciphertext: Ciphertextcan also be called as encrypted text. Before the process of encryption it is called plaintext. In cryptography, cipher is an algorithm that is applied on the plain text to get the ciphertext and it is also called as encrypted data. Theinformation whichis encoded and it is unreadable by a human or computer without the suitable algorithm. The reverse of encryption is decryption. It is the process of converting ciphertextinto readable plaintext.

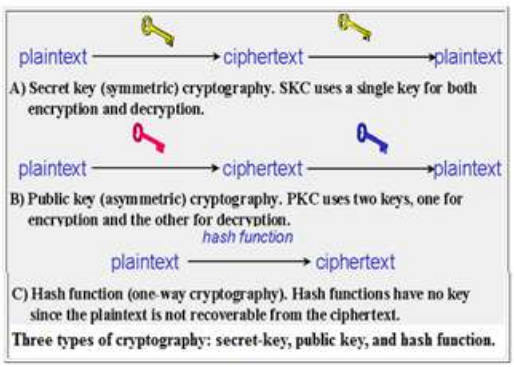

Figure: 3 Types of Cryptography

III. OVERVIEW OF EXISTING ALGORITHMS IN CRYPTOGRAPHY

A.DATA ENCRYPTION STANDARD (DES)

DES is a symmetric-key algorithm which is used for the encryption of electronic data. The Data Encryption Standard (DES) is used for data encryption and it uses Secret Key Cryptography (SKC), which is the only one key for encryption and decryption. Public Key Cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key [12].

The Data Encryption Standard (DES) is a symmetric-key block secrete codeavailable by the National Institute of Standards and Technology (NIST) and it is an implementation of a Feistel Cipher. It uses 16 round Feistel structure and its block size is 64-bitkey.DES use the same key to encrypt and decrypt a message, i.e., both the sender and the receiver must know and use the same private key. It usesAdvanced Encryption Standard (AES) algorithm. DES is used in embedded systems such as smart cards, SIM cards and network deviceslikemodems, boxes, routers and so on.DES is a block cipher, which usescryptographic key. To encrypt a plaintext message, DES has 64-bit blocks. Each block is enciphered using the secret key into a 64-bit. Once a plain-text message is established to be encrypted, it is arranged and given in the form of 64 bit blocks with necessary inputs. If the number of bits in the message is not evenly divisible

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

by 64, then the last block will be padded [10][14].The DES satisfies the block cipher property. They are listed below

- Effect - A small change in plaintext will results in the very big change in the ciphertext.
- Completeness - Each bit of ciphertext depends up on the plaintext. NIST choose Rijndael, due to its simplicity and high performance. It is fast, compact, and has a very simple mathematical structure [4].

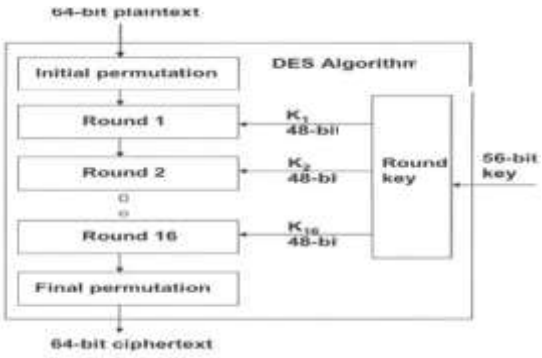

Figure: 4 DES

B. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher which is used by the U.S. government to protect the information and it is implemented in software and hardware throughout the world to encrypt sensitive data.AES is a symmetric-key algorithm, which means that the same key is used for both encrypting and decrypting the data. AES is found that it is at least six times faster than triple DES.A replacement for DES was needed as its key size was too small so Triple DES was designed to overcome this drawback but it was found slow. AES is an iterative rather than Feistelcipher.AES is based on 'substitution–permutation of network'. Unlike DES, the number of rounds in AES is also variable and it depends on the measurement lengthwise of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys where each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. AES is inflexible to all attacks, with the brute force, to decipher messages using all combinations in the 128, 192, or 256-bit cipher.

The features of AES are listed below

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

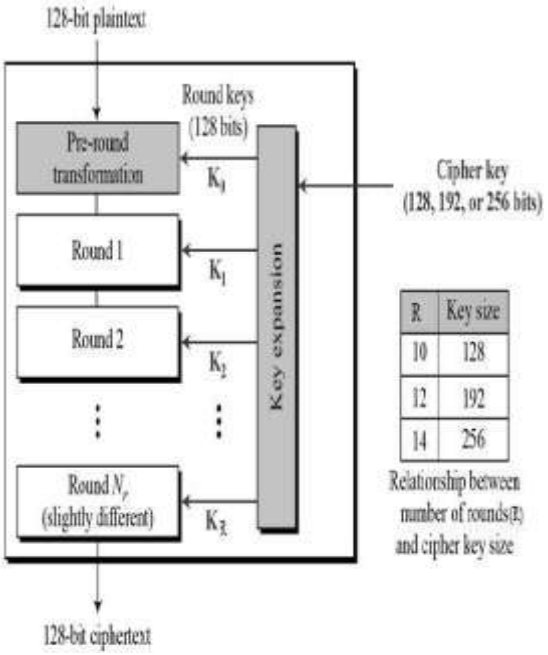

Figure:5 AES Structure with Example

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

The main loop process of AES performs the following functions: 1. SubBytes () 2. ShiftRows () 3. MixColumns () 4. AddRoundKey ().

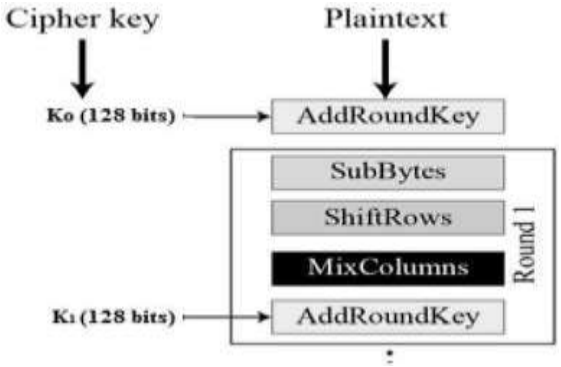

Figure:6 Loop Process of AES

C. Triple Data Encryption Standard (3DES)

Triple DESis a new standard algorithm which was designed to replace the original Data Encryption Standard (DES) algorithm, which makes the hackers ultimatelywell-read to crush with virtual ease. Triple DES is a standard and most widely used symmetric algorithm. Triple DES uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. The amount and size of the block for Triple-DES is 8 bytes. The total key length is up to 168 bits. Triple DES avoids vulnerability and it is also very slow.

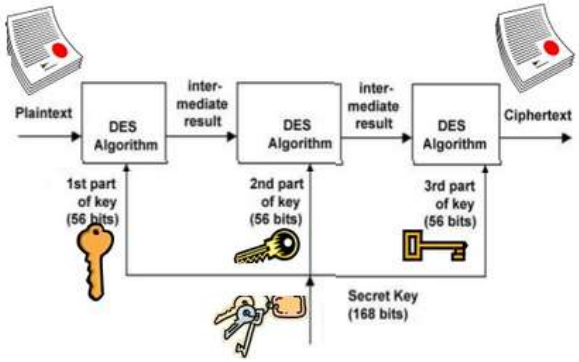

Figure: 7Triple DES

D. Blowfish

Blowfish is a secret symmetric-key or private key for block cipher which uses symmetric algorithm, it is designed in 1993 by Bruce Schneier. Blowfish is an encryptionalgorithm that can be used as a substitution and replacement algorithm for the DES or IDEA algorithms. Blowfish is a general-purpose algorithm and it uses a variable-length key, from 32 bits to 448 bits. Blowfish is faster than DES. Blowfish is unpatented, license-free, and available free for all type of uses. Blowfish has 16-round Feistel cipher and it is a key-dependent called S-boxes.

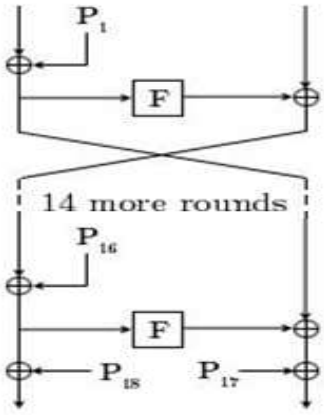

Figure: 8 Feistel Structure of Blowfish

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

Since Blowfish is a Feistel network, it uses XORingP17 and P18 to the ciphertext block, then using the P-entries in reverse order. Blowfish is one of the fastest block ciphers, except when changing keys. Each new key requires pre-processing which is equivalent to encrypting about 4 kilobytes of text. Blowfish is very slow compared to other block ciphers.
Serpent uses 128-bit block and 256-bit keys. As with Blowfish and Twofish, the Serpent algorithm is in the public domain. Serpent very highly used for "safety factor," or trustworthiness against attacks.

E. IDEA(International Data EncryptionAlgorithm)
IDEA is a symmetric encryption algorithm and developed by Dr. X. Lai and Prof. J. Masse. It replaces the DES standard. IDEA is a block cipher algorithm and it operates on 64-bit plaintext blocks. IDEA has key size of 128 bits long. This algorithms mix the different algebraic operations. Three algebraic operations are XOR, Addition modulo 216 and Multiplication modulo 216 + 1. All the three operations operate on 16-bit sub-blocks. IDEA algorithm is efficient on 16-bit processors. IDEA is symmetric key algorithm based on Substitution-Permutation Structure, using block cipher with 64 bit plain text with 8 rounds. The Key Length is 128-bit permuted into 52 sub-keys each of 128- bits. It does not contain S-boxes. The IDEA algorithm uses non-invertible hash function instead of a block cipher. IDEA is resistant to both linear and differential analysis..

F. Twofish
Twofish is a symmetric key algorithm based on the Feistel Structure. Twofish, uses block cipher along with 128-bit blocks and keys up to 256 bits long. Twofish is one of the fastest fixed-block algorithms which are currently available, and it has theoretical vulnerabilities. It uses 4 S-boxes. Twofish is an open to public sphere and not yet patented.
G. RSA
RSA is a public-key encryption algorithm and designed by Rivest, Shamir and Adleman. It is a standard for encrypting data which is sent over the internet. Unlike Triple DES, RSA is asymmetric algorithm. It can be used both for encryption and for signing with512 bits.

H. RC2
In cryptography, Ronald Rivest developed the RC2 algorithm which is the replacement for DES. RC2 encrypts data in 64-bit blocks along with variable key size of 128 bits in 8-bit increments. RC2 is easily compromised. It uses RSA Data Security.

I. RC4
In cryptography, RC4 (Rivest Cipher 4 is also known as ARC4 or ARCFOUR meaning Alleged RC4) is a stream cipher and it is a symmetric key algorithm. RC4 uses XOR to generate key sequence. RC4 is straightforwardness, simplicity and speed in software and multiple vulnerabilities. RC4 allows keys between 1 to 2048 bits. The length of the bits is limited to 40 bits.RC4used to generate pseudo-random bits withXORand with plaintext to generate the cipher text.

J. RC5
In cryptography, RC5 is a symmetric-key block cipher algorithm. RC5 is developed by Ronald Rivest. It is a user defined key length, data block size and the number of encryption rounds.

K. RC6
RC6 is a derived from RC5. RC6 is designed by Matt Robshaw, Ron Rivest Ray Sidney. RC6 is a symmetric key block cipher which is used to meet the requirements of the Advanced Encryption Standard (AES). RC6 encryption algorithm is a new federal Advanced Encryption Standard (AES).RC6 is a Feistel Structured private key algorithm. It uses a 128 bit plain text with 20 rounds and a variable Key Length of 128, 192, and 256 bit. RC6 does not contain S- boxes.

L. Serpent
Serpent is a very fast and reasonably secure block cipher developed by Ross Anderson, Eli Biham and Lars Knudsen. Serpent be able to work with dissimilar combinations of key lengths. Serpent uses Advanced Encryption Standard (AES). Serpent is a symmetric key algorithm which is based on substitution-permutation set of connectionsarrangement. It consists of a 128 bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It has 8 S- boxes.

M. TEA
TEA is a Tiny Encryption Algorithm which is very fast and moderately secure cipher. TEA is a Feistel Structured symmetric key algorithm. TEA is a block cipher. It uses a 64 bit plain text with 64 rounds and its Key Length is 128-bit with variable rounds having 32 cycles. It does not contain S- boxes.TEA is designed to use a hash function.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

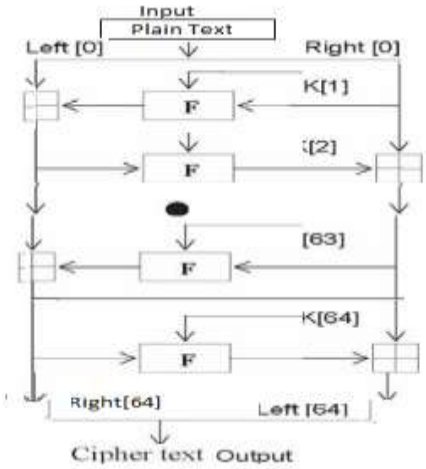

Figure: 9 Structure of TEA Encryption Routine

N. CAST
CAST stands for Carlisle Adams and Stafford Tavares. CAST is symmetric key algorithm based Feistel Structure. The CAST is a 64-bit block cipher solid algorithm. It uses a 64 bit plain text with 12 or 16 rounds. It contains 4 S- boxes. It uses Substitution-Permutation Network (SPN) cryptosystem. CAST supports variable key lengths between 40 and 128 bits.

O. Diffie-Hellman
Diffie-Hellman algorithm was introduced in 1976 by Diffie-Hellman. It is a first asymmetric encryption algorithm. Diffie Hellman is an algorithm used to share the secret between two parties. It is primary method to exchange cryptography keys using the symmetric encryption algorithms like AES. This algorithm is very simple. It is a key exchange algorithm. The Diffie-Hellman algorithm provides two users to establish the shared secret key and to communicate over an insecure communication channel. Authentication is free in Diffie-Hellman algorithm. It is not implemented in hardware.

P. MD5
MD5 is Message-Digest algorithm. The MD5 is a cryptographic algorithm..MD5 is derived from MD4& was designed by RonaldRivest in 1991. MD5 uses hash function with 128-bit which is 32 digit hexadecimal number. It is also used to verify data integrity.

Q. EIGamal
EIGamal is a public key cipherand asymmetric key encryption algorithm. It is used for public key cryptographywhich is based on Diffie-Hellman algorithm. El Gamal is an algorithm used for transmitting digital signatures and exchange of keys. This method is based on calculating logarithms The Digital Signature Algorithm (DSA) is based on El Gamal algorithm.

Table: 1 Common Symmetric Key Algorithm with its Description

Algorithm	Description	Key Length
DES	DES adopted as a U.S. government standard in 1977	56 bits
AES	Subset of Rijndael cipher developed by Joan Daemen and Vincent Rijmen	128-256 bits
Triple-DES	A three-fold application of the DES algorithm	168, 112 or 56 bits
Blowfish	Block cipher developed by Bruce Schneier	32–448 bits
IDEA	Block cipher developed by Massey and Xuejia	128 bits
Twofish	It is symmetric keyblock cipher of AES	256 bits.
RSA	Developed by Ron Rivest, Adi Shamir ,Leonard Adleman for encryption algorithm in 1977	3072 bits
RC2	Block cipher developed by Rivest	1-2048 bits
RC4	Stream cipher developed by Rivest	1-2048 bits

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

RC5	Block cipher developed by Rivest and published in 1994	128-256 bits
RC6	AES finalist developed by RSA Labs	128-256 bits
Serpent	AES finalist developed by Anderson, Biham, and Knudsen	128-256 bits
TEA	Designed by David Wheeler and Roger Needham	64 bits
CAST	Created by Carlisle Adams and Stafford Tavares in 1996	128 bits
Diffie-Hellman	Created by Ralph Merkle and named after Whitfield Diffie and Martin Hellman	3072-bit
MD2, MD4, MD5, MD6	Designed by Ronald Rivest	128-512 bits
EIGamal	Described by TaherElgamal in 1985	128 bits
IDEA	Block cipher developed by Massey and Xuejia	128 bits

IV. CONCLUSION

Network security and cryptography challenges and issues are discussed by various researchers. This paper gives a detailed description of the symmetric key encryption algorithms which is called as secrete key algorithms like AES, DES, TRIPLE DES and BLOWFISH. This paper also provides description of the Asymmetric key which is called as Public key algorithms like RSA, Diffie-Hellman,andEIGammal. Among these algorithms the Blowfish algorithm uses the bits which ranges from 32 to 448 bits and . It uses 16-round Feistel cipher and uses large key-dependent S-boxes for encrypting the data. So it is not possible for a hacker to decrypt the original data.

REFERENCES

[1]Chia Long Wu, Chen Hao Hu,"Computational complexity Theoretical Analyses on cryptographic Algorithms for computer Security Application", Innovations in Bio-inspired computing and Applications(IBICA), 2012, pp.307 – 311.
[2] Quing Liu, Yunfei Li, Lin Hao, "On the Design implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), 2010, pp.533-536.
[3]MandalB.K. , Bhattacharyya , BandyopadhyayS.K , "Designing and Performance Analysis of a proposed Symmetric Cryptography Algorithm", Communication Systems and Network Technologies (CSNT), 2013.
[4] Wang, Suli, Liu, Ganjai, "File encryption and decryption system based on RSA algorithm", 2011,pp. 797 – 800.
[5] Da Silva, J.C.L, "Factoring semi primes and possible implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2010,pp.182-183.
[6]GeethavaniB. ,Prasad, E.V. Roona R. " A new Approach for secure data transfer in audio signals using DWT", pp. 1-6, Sept 2013.
[7]Chong Fu, Zhi-jiang Zhu, "An Efficient implementation of Rsa Digital signature", Wireless Communications, Networking and Mobile computing, oct. 2008, pp.1-4.
[8] Afolabi, A.O and E.R. Adagunodo, 2012. Implementation of an Improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.
[9] WulingRen College of Computer and Information Engineering Zhejiang Gongshang University. 2010. A hybrid encryption algorithm based on DES and RSA in Bluetooth communication. Second International Conference on Modeling,Simulation and Visualization methods.
[10] Jonathan Katz and Yehuda Lindell. 2014.Introduction to Modern Cryptography. CRC Press.A. De Santis, G. Di Crescenzo, and G. Persiano. 1994. Secret Sharing and Perfect Zero Knowledge.Springer–Verlag, 73–84.
[11] J.SairaBanu , Dr.S.Subha,"Loop Parallelization And Pipelining Implementation Of AES Algorithm Using OpenMP And FPGA", IEEE international conference 2013.
[12] RituPahal,VikasKumar,"Efficient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.
[13] SwetaK.Parnar,Prof. K.C.Dave,"A review on various most common symmetric encryption algorithm", International journal for scientific research and development,volume1,issue 4,2013.