International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# An Introduction of Advanced Encryption Algorithm: A Preview

**Asfiya Shireen Shaikh Mukhtar[1], Ghousiya Farheen Shaikh Mukhtar[2]**

Master of Computer Application Radhikatai Pandav College of Engineering, Nagpur, Maharashtra, India

Master of Computer Application, S S Maniyar College of computer and Management, Nagpur, Maharashtra, India

**Abstract:** ***In a recent era, Network security is playing the important role in communication system. Almost all organization either private or government can transfer the data over internet. So the security of electronic data is very important issue. Cryptography is technique to secure the data by using Encryption and Decryption Process. Cryptography is science of "secret information "it is the art of hiding the information by Encryption and Decryption. Encryption is the process to convert the Plaintext into unreadable format known ciphertext and Decryption is the process to convert cipher text into plaintext. Numbers of algorithm used for encryption and Decryption like DES, 2DES, 3DES, RSA, RC2, RC4, RSA, IDEA, Blowfish, AES but AES algorithm is more efficient and Effective AES algorithm is 128 bit block oriented symmetric key encryption algorithm. In this paper I describe the brief introduction of AES algorithm .My paper is divide into following Section. In I Section I Present the brief introduction of AES (Advance Encryption Standard) Algorithm, In II Section I Present the different Cryptography algorithm, In III Section I Present comparison of AES algorithm with different cryptography algorithm, In IV Section I Present the Modified AES algorithm and Text and Image Encryption by using AES algorithm, In V Section I Present Future Enhancement of AES algorithm and Conclusion.***

**Keywords:** component: AES, DES RC2, RC4, Blowfish

## 1. Introduction

Cryptography is a science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure network. So that it cannot read by anyone except the intended recipient. Cryptography provide the confidentiality, integrity, authentication, non repudiation Confidentiality is the process of maintaining the secrecy of information and data. Confidentiality can be achieved by encryption and decryption. The method of disguising plaintext result in such a way as to hide its substance is called encryption. Encryption plaintext result in unreadable gibberish called ciphertext. The process of reverting ciphertext to its original plaintext is called decryption. Encryption and decryption process used mathematical calculation with some shifting and rotating operation with or without a key. Cryptography can be divided into three types of algorithm Symmetric key algorithm, asymmetric key algorithm and hash function.

Modern ciphers are classified into stream a cipher which encrypts the inputs data bit by bit and block ciphers which encrypts a block of bits at a time Here we are interested to work on block ciphers. The block cipher transforms a block of plain text to a block of cipher text. Many block cipher algorithms were proposed. But Data Encryption Standard (DES) was considered to be the most dominant till 1990s.DES has a key length of 56 bit .This key length is considered small and easily be broken. Hence National Institute of Standards and Technology (NIST) called for the Proposal of new block cipher algorithm. In August 2000 NIST selected five algorithm: Mars, RC2, Rajndeal, Surpent and twofish are the final competitors. In 2000 NIST announced Rajndeal algorithm was the winner by analyzing various security parameters and other characteristics, Rajndeal algorithm developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen was crowned as new AES algorithm in the year 2001.

## 2. AES Rijndeal Algorithm

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. The Rijndael algorithm allows the block and key size of 128, 160, 192, 224, 256 bits. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128,192,256 bits. Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design Simplicity.

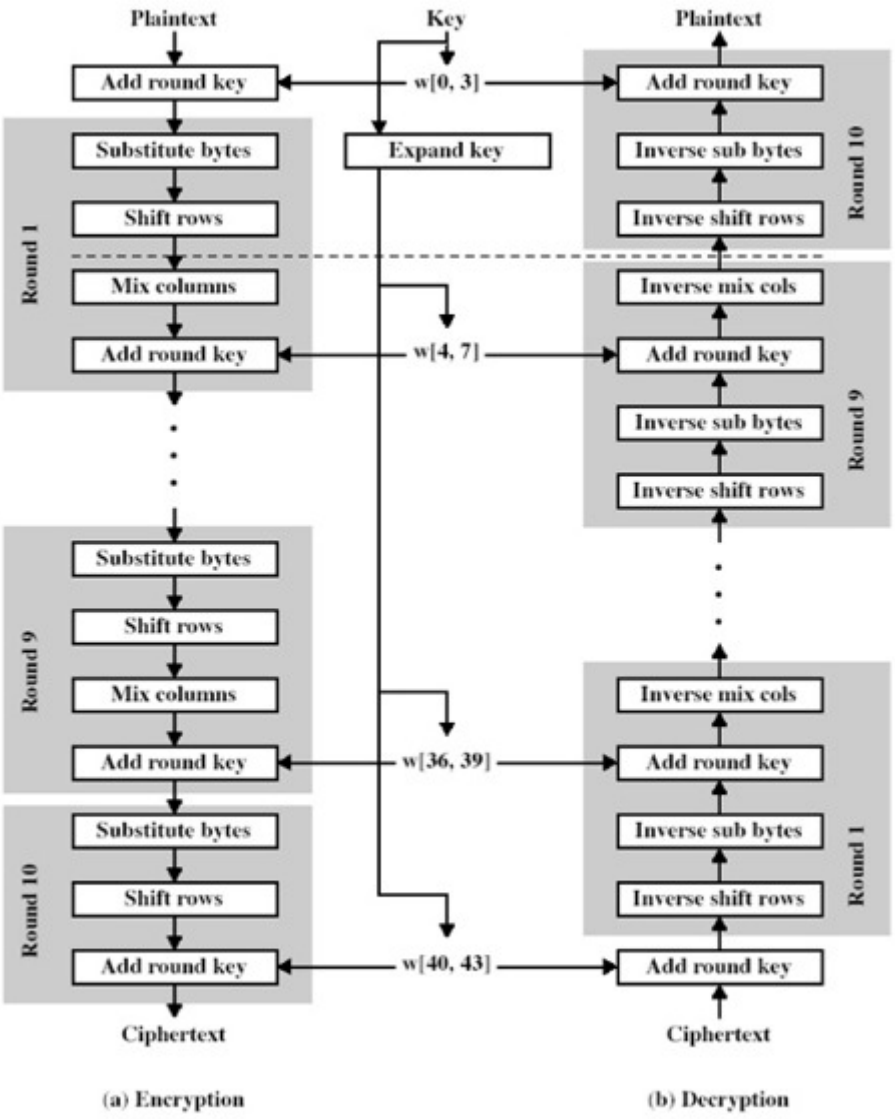
## 3. Workings of a Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes 3. Inverse Add Round Key




## 4. Compared Algorithms

**RC2:** RC2 is a block cipher with 64-bits block cipher and variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts.

**DES:** (Data Encryption Standard): DES was the first encryption standard published by NIST (National Institute of Standards and Technology) [3].It is a symmetric algorithm; It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation; 8 bits are used for error detection.DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text.

**3DES:** It uses 64 bit block size with 192 bits of key size . The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. 3DES is slower than other block cipher methods.

**AES:** It was recognized that DES was not secure because of advancement in computer processing power. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies . It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible.

**RC6:** RC6 is block cipher derived from RC5. It was designed to meet the necessities of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard .

**Blowfish:** Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a

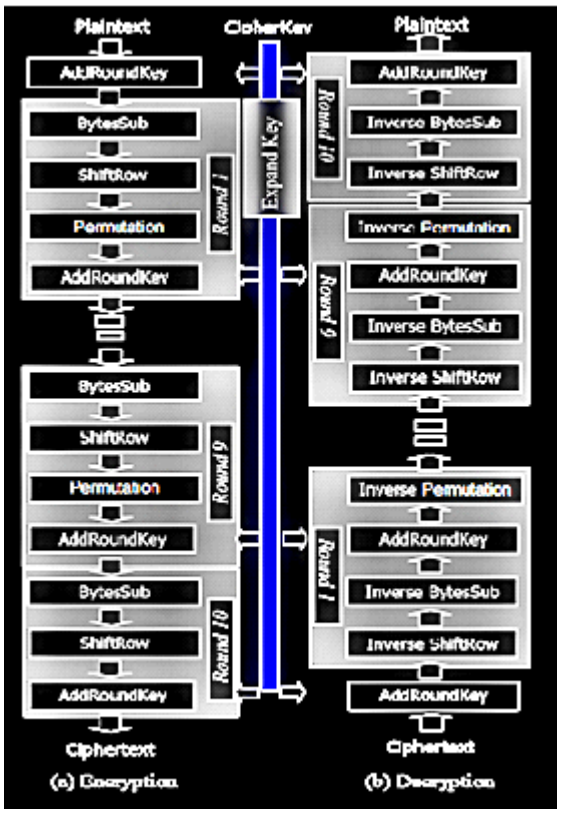
variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less . Blowfish is one of the fastest block ciphers which has developed to date. Slowness kept Blowfish from being used in some applications. Blowfish was created to allow anyone to use encryption free of patents and copyrights. Blowfish has remained in the public domain to this day. No attack is known to be successful against it, though it suffers from weak keys problem (Bruce, 1996).

**Table 1**: Comparison of DES, 3DES, AES and Blowfish algorithm

| Algorithm | Key size | Blok size | Structure | Rounds |
|---|---|---|---|---|
| DES | 56 bits | 64 bit | Feistal Network | 16 |
| 3DES | 112 or 168 bits | 64 bits | Feistal Network | 48 |
| AES | 128,192,256 bits | 128 Bits | Substitution-Permutation Network | 10,12 |
| Blowfish | 32-448 bit in steps of 8 bits. 128 bits by default | 64 bits | Feistal Network | 14 |

## 5. Modified AES Algorithm

To overcome the problem of high calculation and computational overhead, we analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. So we develop and implement a modified AES based Algorithm for all kind of data. The basic aim to modify AES is to provide less computation and better security for data. The modify AES algorithm adjusts to provide better encryption speed. In Modified-AES the block length and the key length are specified according to AES specification. Three key length alternatives 128,192 or 256 bits and block length of 128 bits. We assume a key length of 128 bits, which is commonly implemented. In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mix column step and add the permutation step. Mixcolumn gives better security but it takes large calculation that makes the encryption algorithm slow. The other three junctures remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithms. This block is a 4×4 square matrix consisting of 16 bytes. This block is copied into the state array. The state array is modified at each stage of encryption or decryption. Similarly the 128-bit key is also depicted into a square matrix. The 128-bit key is expressed into an array of key schedule words: each word is of four bytes. The total key schedule words for ten rounds are 44 words; each round key is similar to one state. The block diagram of the Modified-AES algorithm with 128 bits data is shown below.




The algorithm is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and is flexible for key size of 128 bits. These four operational blocks represent one round of Modified-AES. There are 10 rounds for full encryption. The four different stages that we use for Modified-AES Algorithm are:

- Substitution bytes
- Substitution bytes
- Shift Rows
- Permutation
- Add Round Key

## 6. Text and Image Encryption

Many digital services like multimedia systems, medical and military imaging systems, internet communication require reliable security in storage and transmission of digital images. Due to growth of internet, cell phones, multimedia technology in our society digital image security is the most critical problem. In these technology digital images plays more significant role than the traditional texts. It demands serious protection of users' privacy for all applications. Therefore image encryption techniques are usually used to avoid intrusion attack Correlation among pixels and high redundancy, these characteristics are varies according to type of multimedia data. Therefore generally same technique cannot be used to protect all types of multimedia data. We may not use the traditional encryption algorithms to encrypt images directly because two reasons.

1) The size of image is often larger than text. Hence traditional encryption algorithms take larger time to encrypt and decrypt images compared to text.

2) In text encryption both decrypted and original text must be equal. This condition is never true for images. Because due to human perception; decrypted image with small distortion is usually acceptable (Chang et al, 2001), (Jiri Jan, 2005), (David Salomon, 2005). We can reduce this perceivable information by decreasing the correlation among image elements using certain transformation techniques (Mitra et al, 2006). Considering the above points, this research of image encryption is divided into two parts. 1) First encryption and decryption of image data is perform by Code Block Chaining method with PKC 5 padding of Advanced Encryption standard. 2) After this we will perform password based encryption and decryption of image with the help of using MD5 and DES algorithm together

## 7. Digital Image Formats

There are many types of digital image formats like.bmp, .gif, .jpg, .pict, .eps and .png. This project can use any kind of format. The results obtain in this paper are mainly using .gif format only. Therefore the detail explanation regarding .gif file format is given below.

**GIF Files**

The Graphics Interchange Format (GIF) was originally invented by CompuServe in 1987. It is mainly used file formats for web graphics and exchanging graphics files between computers. GIF format a supports 8 bits of colors information. This information is limited to 8 bit palette and 256 colors. Therefore 256 different colors are available in this format to represent the picture. GIF also support transparency, interlacing and animation.(Gardner and Betcher, 2006), (Robert Fry, 2006). When we use LZW (Lempel-Ziv-Welch) method to save GIF images, GIF images are degrade any image quality. Features of GIF format transparency, interlacing, file compression, and primitive animation. The interlacing feature browser can display portions of the image as it updates. Because of updating of interlacing part the original poor image becomes more and better.

## 8. Future Enhancement of AES algorithm

The proposed system can be extended to standard video coding systems such as those using MPEG and other video formats. All the existing costly encryption products will have no use in future if the video encryption also invented with royalty free open source software. Therefore it will be the most flexible and cheaper solution.

## 9. Conclusion

In this paper we describe the brief introduction of AES algorithm, we examine and compare various cryptography algorithm and Text and Image Encryption and Decryption using AES algorithm .This paper is useful for research scholars who research on cryptography.

## References

[1] Pratap Chandra Mandal, ”Superiority of Blowfish Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE)ISSN: 2277 128X, Volume 2, Issue 9, September 2012

[2] W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005

[3] Shashi Mehrotra Seth, Rajan Mishra on “ Comparative Analysis Of Encryption Algorithms For Data communication ” in IJCST Vol. 2, Issue 2, June 2011 I ,pp. 292-294

[4] Monika Agrawal, Pradeep Mishra “A Comparative Survey on Symmetric Key Encryption Techniques” International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882. [15]