iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2017 **Issue:** Conference **Month of publication:** September 15, 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Comparative Analysis of Various Encryption Algorithms and Techniques

Hemangi Zope[1], Prof. Savita Sangam[2]
[1]*Student, Computer Engineering, SESGOIFE Diksal, Bhivpuri,*
[2]*Associate Professor & HOD, IT, Shivajirao S. Jondhale college of Engineering Dombivali*

Abstract*: *Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. Classification is one of the main tasks in data mining. For the past few years due to the increment in various privacy problem many conceptual and feasible solution to the classification problem have been proposed under different certainty prototype.
Keywords: Security, k-NN classifier, encryption, Information security.

I. INTRODUCTION

Encryption is a method for a user to securely share data over an insecure network or storage site. Encryption is the one of the way to protect data. Data security is an essential part of an organization. It can be achieved by using various methods. The encrypted data is safe for some time but never think it is permanently safe. The information about the key is present in the encrypt data which solves the problem of secure transport of keys from the transmitter to the receiver. In case of practical system, encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format cipher text with the help of key[1].

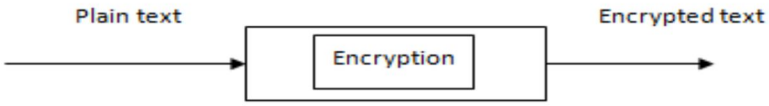


Figure1. Encryption

The system in which first data(Plain text) in encrypted at sender side and decrypted into plain text again at receiver end using a unique key or some particular formula is called a Cryptographic system. Encrypted messages can sometimes be broken by cryptanalysis also called code-breaking.

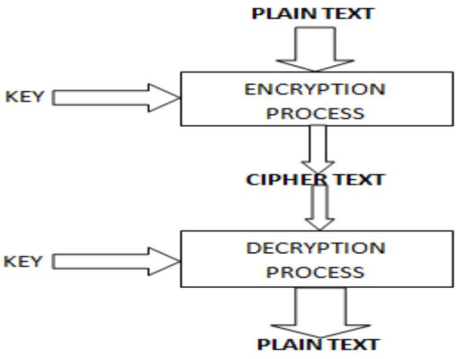


Figure 2. Encryption Process

II. METHODOLOGY

In this paper, we have considered DES, RSA, AES, BLOWFISH, ECC, 3DES Encryption Algorithms and Techniques for improving secured data Communication, Information Security using cryptography detailed description of Information security using cryptography and algorithms.

©IJRASET (UGC Approved Journal): All Rights are Reserved

A. *Basic Terminology Used In Cryptography*

There are some terms which we should know for better understanding of encryption algorithms. This terminology is very important to understand because in every algorithm description we are going to discuss these common terms. The encryption terminology shown in Fig.3[2]:

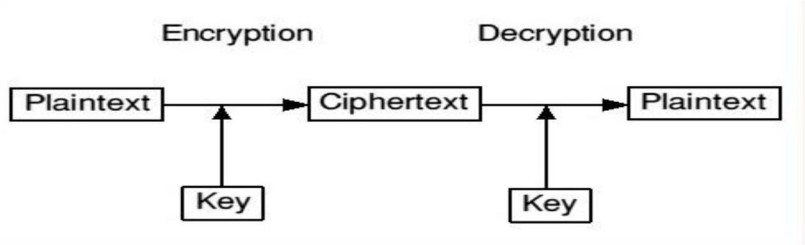


Figure 3. Encryption Terminology

B. *Plain Text or Normal Text*

The original text or message used in communication in called as Plain text.
Example: John sends “Hello” to Perry. Here “Hello” is Plain text or Original message.

C. *Cipher Text*

The plain text is encrypted in un-readable message. This meaningless message is called Cipher Text.
Example: “Hello” message is converted in “-&tt%”. This meaningless message is Cipher Text.

D. *Encryption*

Encryption is a process of converting Plain text into Cipher text. This non-readable message can securely be communicated over the unsecure network. Encryption process is done using encryption algorithm.

E. *Decryption*

Decryption process is the reverse of Encryption process i.e. Cipher text is converted into plain text using particular encryption algorithm.

F. *Key*

A key is a numeric or Alpha-numeric text (mathematical formula). In encryption process it takes place on Plain text and in decryption process it takes place on cipher text.

G. *Key Size*

Size is the measure of length of key in bits used in any algorithm.

H. *Block Size*

Key cipher works on fixed length string of bits. This fix length of string in bits is called Block size. This block size depends upon algorithm.

I. *Round*

Round of encryption means that how much time encryption function is executed in complete encryption process till it gives cipher text as output [3]. Cryptography systems can be broadly classified into two categories: Symmetric encryption algorithms Asymmetric encryption algorithms

III. MAIN OBJECTIVES OF CRYPTOGRAPHY

Encryption or Cryptography have some goals that needs to be fulfilled for user benefit. Modern cryptography concerns itself with the following four objectives [4]:

A. *Confidentiality*

The information cannot be understood by anyone for whom it was unintended.

©IJRASET (UGC Approved Journal): All Rights are Reserved

B. Integrity

The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

C. Non-repudiation

The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

D. Authentication

The sender and receiver can confirm each other's identity and the origin/destination of the information.

E. Access Control

Only authorized users can access the data. This is done to avoid unauthorized user access.

A plain text is encrypted using an algorithm called "encryption algorithm". A cipher text is decrypted using an algorithm called "decryption algorithm". A key is used at the time of encryption and decryption process. The security level of cryptography is determined by the key space or key length (size of key).

IV. OVERVIEW OF ENCRYPTION ALGORITHMS

In this section we will discuss about the various cryptographic algorithms to be analysed for their performance evaluation. To start the algorithm analysis firstly we should know that what is Algorithm actually. "An algorithm is a sequence of unambiguous instructions for solving a problem" i.e. for obtaining a required output for any legitimate input in a finite amount of time. We are taking some encryption algorithms under consideration those are DES, RSA, AES, BLOWFISH, ECC, 3DES[5].

A. DES (Data Encryption Standard)

It was developed in the early 1975 at IBM labs by Horst Fiestel. The DES was approved by the NBS (National Bureau of Stadards, now called NIST -National Institute of Standards and Technology) in 1978. The DES was standardized by the ANSI (American National Standard Institute) under the name of ANSI X3.92, better known as DEA (Data Encryption Algorithm). But now it is an outdated symmetric key data encryption method. It completes the 16 rounds of encryption on each 64 bits block of data. Data encryption standard works on a particular principle.The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm.

B. 3DES (Triple Data Encryption Standard)

In cryptography techniques Triple Data Encryption Standard (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block [5]. Triple-DES is also proposed by IBM in 1978 as a substitute to DES. So 3DES is simply the DES symmetric encryption algorithm used three times on the same data. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text shown in Figure 4.

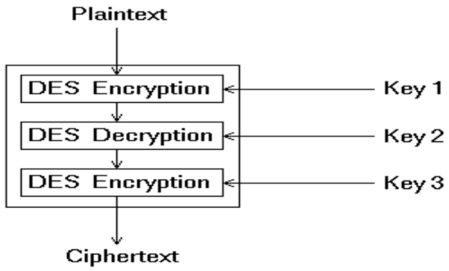


Figure 4. 3DES Structure

C. RSA (Rivest-Shamir-Adleman Algorithm)

The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is best known and widely used public key scheme. It uses large integers like 1,024 bits in size. It has only one round of encryption. It is asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages[6]. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process.

©IJRASET (UGC Approved Journal): All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

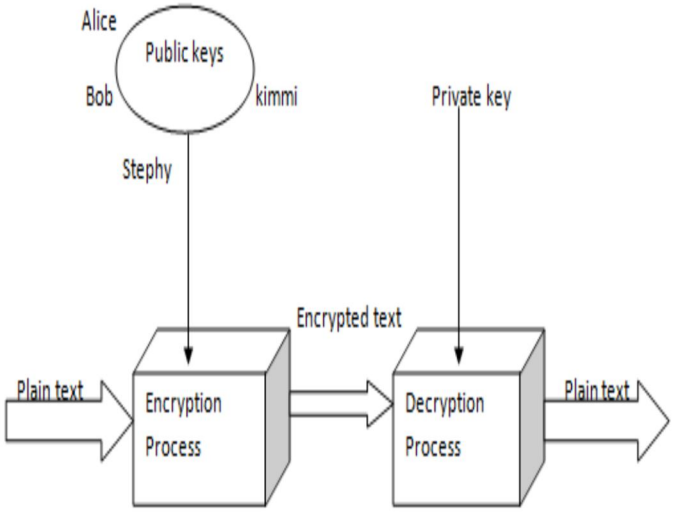


Figure 5. RSA Algorithm (Asymmetric Key Cryptography)

D. ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller from IBM and Neil Koblitz from University of Washington as an alternative mechanism for implementing public-key cryptography. This ECC (Elliptic Curve Cryptography) is Based on algebraic structures of elliptic curves over finite fields i.e. Elliptic curve theory[6]. ECC Create Faster, Smaller and more efficient keys as compared to other encryption algorithm. In this encryption is done in elliptic curve equation (used in mathematics) form.

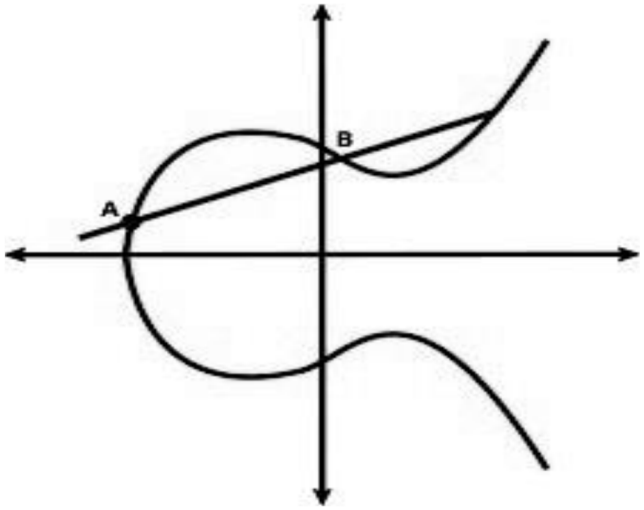


Figure 6. Elliptic Curve Representation

E. AES (Advanced Encryption Standard)

In 1997, the National Institute of Standards and Technology (NIST) announced an initiative to choose a successor to DES in 2001. It selected the Advanced Encryption Standard as a replacement to DES and 3DES. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually three block ciphers, AES-128, AES-192 and AES-256[7]. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

©IJRASET (UGC Approved Journal): All Rights are Reserved

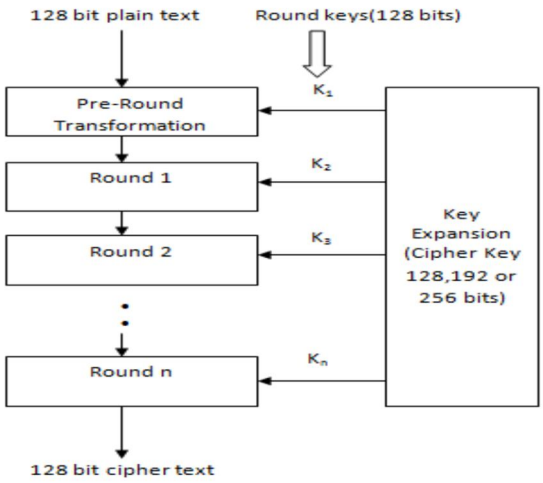


Figure 7. AES Algorithm

F. Blowfish

Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round Feistel cipher and uses large key dependent S-Boxes. Each S-box contains 32 bits of data.

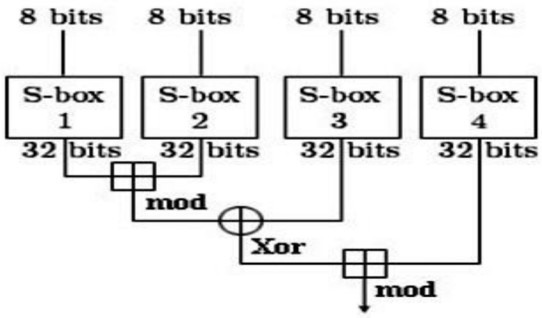


Figure 8. Blowfish Function F.

V. COMPARATIVE TABLE

Table 1. Comparison of Various Algorithms on the basis of Different Parameters

PARAMETERS	DES	3DES	ECC	RSA	BLOWFISH	AES
DEVELOPMENT	In early 1970 by IBM and Published in 1977.	IBM in 1978.	Victor Miller from IBM and Neil Koblitz in 1985	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993	Vincent Rijmen, Joan Daeman in 2001
KEY LENGTH (Bits)	64 (56 usable)	168,112	Smaller but effective key	Key length depends on no. of bits in the module	Variable key length i.e. 32 – 448	128,192, 256
ROUNDS	16	48	1	1	16	10,12,14
BLOCK SIZE (Bits)	64	64	Stream size is variable	Variable block size	64	18

©IJRASET (UGC Approved Journal): All Rights are Reserved

ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attack	Doubling attack	Brute force attack, timing attack	No attack is found to be successful against blowfish.	Key recovery attack, Side channel attack
LEVEL OF SECURITY	Adequate security	Adequate security	Highly secure	Good level of security	Highly secure	Excellent security
Flexibility	NO	YES	YES	NO	YES	YES
ENCRYPTION SPEED	Very slow	Very slow	Very Fast	Average	Very fast	Faster

VI. CONCLUSION

In this paper, we have analysed various encryption algorithms. We have found that each algorithm has its own benefits according to different parameters. From the work completed in this paper it is observed that that the strength of the each encryption algorithm depends upon the key management type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption that will lead to more heat dissipation. So, it is not advisable to use short data sequence and key lengths. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. From above analysis we have found that ECC and Blowfish, these two encryption algorithms are leading with the security level that they provide and faster encryption speed. ECC is having some attacks on it but on Blowfish, no attack is successful yet. So from this review and analysis we have shortlisted ECC and Blowfish encryption algorithm. These two encryption algorithms are more secure and fast to work with and in future there is wide scope of improvement in these both encryption algorithms [7].

REFERENCES

[1] M. Kumar and E. G. Dharma, “A comparative analysis of symmetric key encryption algorithm”, IJARCET, vol. 3, no. 2, (2014).

[2] Mital Maheta ”Design and simulation of AES algorithm Encryption using VHDL”, International Journal of Engineering Development and Research Volume 2, Issue 1, 2014.

[3] M. Kumar and E. G. Dharma,“A comparative analysis of symmetric key encryption algorithm”,IJARCET (2014).

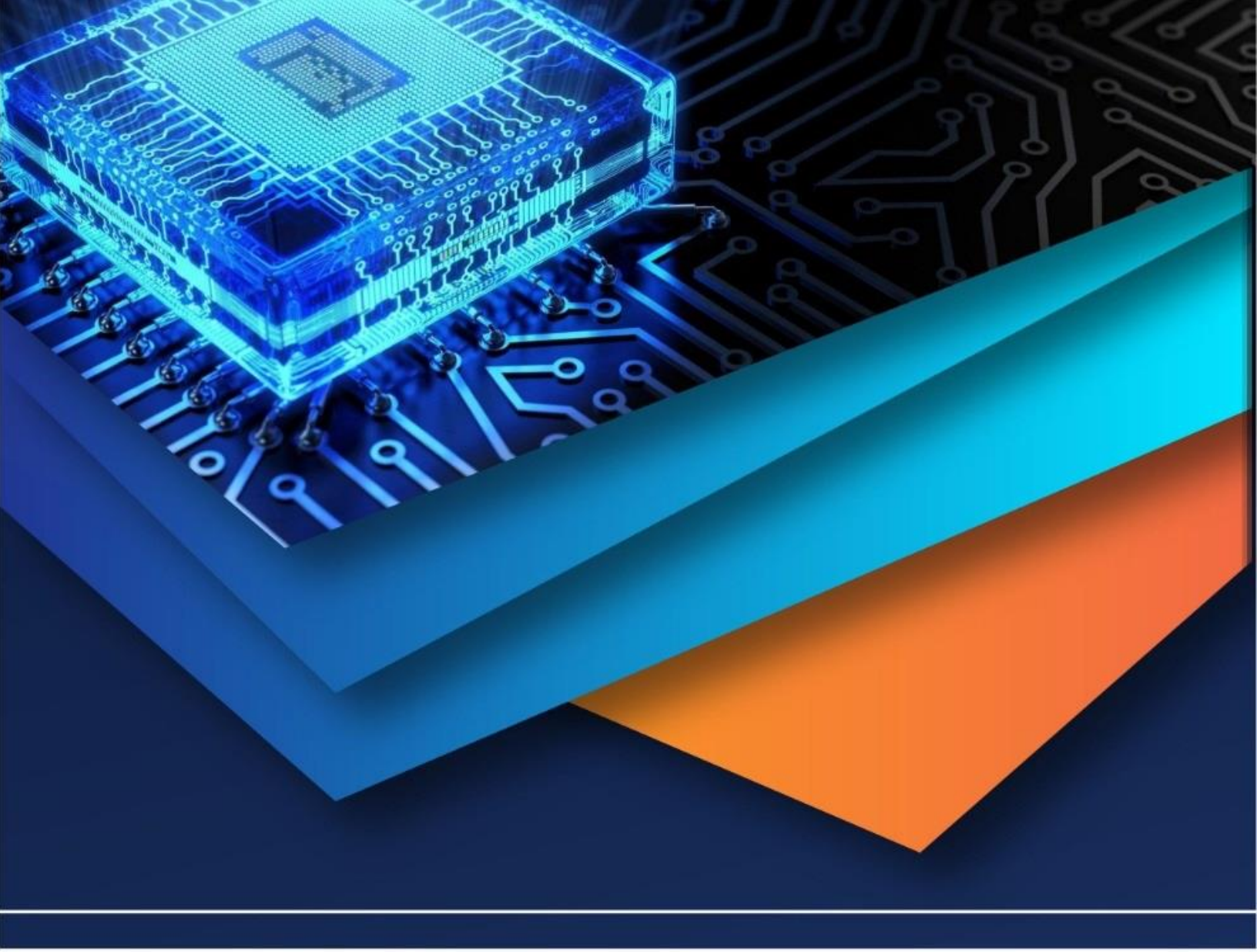
[4] Ajay Kakkar, M. L. Singh, P.K. Bansal," Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology Volume 2 No. 1, January, 2012.

[5] Suyash Verma, Rajnish Choubey,Roopali soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", International Journal of Emerging Technology and Advanced Engineering.

[6] E. Biham and A. shamir, "A differential cryptoanalysis of data encryption stamdard", Springer-verlag, (1999).

[7] Vishwa gupta, Gajendra Singh," Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering”, Issue 1, January 2012.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)