iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

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: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Symmetric and Asymmetric System Cryptanalysis

Jyoti Chandwani[1], Kavita Sharma[2]
[1, 2]*Department of CSE, Arya Institute of Engineering and Technology, Jaipur*

Abstract: ***Cryptanalysis has always been a concerning issue in research appertain to information and network security. Cryptanalysis involves analysing encryption schemes, ciphers and encrypted texts for the purpose of finding weaknesses in ciphers and cryptosystems.***
Thus, it is the art of breaking codes and looking for points where security of an information system may fail. From frequency analysis attacks to differential cryptanalysis has helped to improve the security of an information systems. Cryptanalysts use various mathematical formulas to find vulnerabilities in cryptographic ciphers. These potential weaknesses can be exploited by an attacker to break into information security systems. Cryptographic algorithms are rigorously cryptanalyzed to minimize attacks on a system and meet security goals.
This paper primarily aims at describing existing cryptanalysis attacks on various modern ciphers on the basis of information available to attackers such as memory requirements, computational time requirements or the information available to the attacker.
Cryptanalytic attacks try to attack various mathematical weaknesses in the algorithms and Implementation attacks try to attack specific implementation of ciphers. This paper mainly focuses on various types of timing and analytic attacks based on the information at the hand, on symmetric and asymmetric cryptography algorithms. With the rise in computation power and advent of Quantum Computer, modern cryptosystems are at a greater risk of comprising its users' security. The study of potential attacks on information systems is essential, so that while developing a new and more secure cipher, these attacks can be taken under consideration.
In effect, by applying the countermeasures of these attacks, the new implementation or design can be made secure against studied attacks.
Keywords: Cryptanalysis, cryptosystem, cryptography, ciphers, security.

I. INTRODUCTION TO CRYPTOLOGY

Cryptology is outlined because the science of constructing communication incomprehensible to any or all individuals except those that have a right to scan and know it. It's sometimes separated into two distinct however related sciences: Cryptography and Cryptanalysis. The goal of cryptography is to change two individuals, commonly referred as Alice and Bob, to speak over an insecure channel in such a way that an opponent Oscar, cannot perceive the data that is being exchanged or intercept the communication. The channel may well be a wireless network or a telephone line. In cryptography, a cryptosystem provides confidentiality(encryption) by incorporating a collection of scientific discipline algorithms to implement security services for an application.

II. CRYTOGRAPHY

Cryptography is defined as the study of understanding, implementing, and information obfuscation techniques. It includes procedures of converting ordinary plaintext into untelligibale text, referred as cipher text. These procedures are known as cryptography algorithms or ciphers.

1) *Plaintext* - The initial intelligible message; i.e. data that may be directly read by humans or a machine.
2) *Ciphertext* - The remodeled message; i.e. encrypted text/data.
3) *Cipher* - the arithmetic (or algorithm) that is employed to rework the plaintext into ciphertext and reverting ciphertext to plaintext.
4) *Key*- The knowledge utilised in cipher best-known solely to sender or receiver. Key is used to encrypt the data, either that key or mathematically related key is used to decrypt the data back to a usable form.
5) *Encryption* - the method of changing plaintext to ciphertext typically known as 'encipherment'.
6) *Decryption* - the method of reverting ciphertext to plaintext typically known as 'decipherment.'

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

III. TYPES OF CRYPTOGRAPHY

1) *Symmetric-Key Encryption:* It uses one key to encrypt and decrypt messages. Conjointly known as even cryptography or single-ley encryption. Primarily used for confidentiality and privacy. DES, Triple DES, AES, RC5 etc. are example of symmetric ciphers.
2) *Asymmetic-Key Encryption:* It uses one key to encrypt and another for decrypting messages; conjointly known as uneven cryptography (or asymmetric encryption). Primarily used for nonrepudiation, key exchange and authentication. RSA, Elliptic Curve etc. are example of asymmetric ciphers.
3) *Hash Function:* It uses a mathematical transformation to irreversibly "encrypt" data, providing a digital fingerprint. Primarily used for message integrity.

IV. CRYPTANALYSIS

Cryptanalysis encompasses the study of defeating and strengthening techniques; that's finding, exploiting, and correcting weaknesses in either the algorithm themselves or above all implementations. In other words, it is the study of ways to crack encoding algorithms or their implementations. Often, a significant number of modern ciphers for their security rely on the difficulty of computing discrete logarithms or factoring.

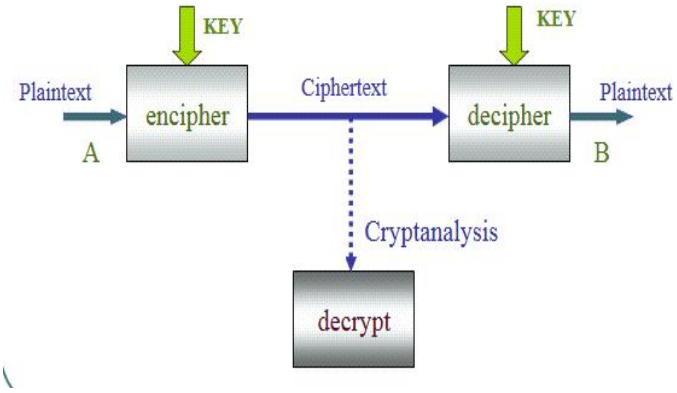


Fig. 1 Cryptanalysis

A. *Problem Definition*

The matter of cryptanalysis: Given some data associated with the cryptosystem (at least the ciphertext), and determines the plaintext and/or the key. The goal of the designer is to create this drawback as tough as attainable for the cryptanalyst. The security of a cryptosystem is ultimately determined by the scale of its key area. However, this can be the higher limit of this security live.
There may be a problem in the design of cryptosystems that can cause a significant reduction in the effective key space. The task of the cryptanalyst is to search out this pitfall and use it to attack the system.

TABLE 1
Example of Key Space Size

Key space – 40 bits	1×10^{12}
Key space – 56 bits (DES)	7×10^{16}
Key space – 128 bits	3×10^{38}
Key space – 256 bits	1×10^{77}
Number of 256-bit primes	1×10^{72}
Age of the Sun in seconds	1×10^{16}
Number of clock pulses of a 3GHz computer clock through the Sun's age	5.4×10^{26}

B. Classification of Attacks

The main objective of cryptanalyst is to get maximum information about the data regarding plaintext (original data). Classification of attack can be done on following basis:

1) *Quantity of knowledge accessible to attacker:* The main objective of adversary is to access the encryption key in order to decode the information. Attacks can be classified on the premise of knowledge accessible to attacker.
2) *Ciphertext-only Attack:* During this sort of attack, the attacker has solely the encoded message from that to determine the plaintext, with no data whatsoever of the latter. A ciphertext solely attack is typically presumed to be possible, and a code's resistance to that is taken into the account as the basis of cryptosystem's security.
3) *Known-Plaintext Attack:* During this attack, a cryptographer has plaintext and their corresponding cipher text. Attacker tries to seek out the key or relation between two.
4) *Chosen-Plaintext Attack:* The attacker gets the assorted ciphertext corresponding to an arbitrary set of plain text. This attack is one of the least realistic, but often most powerful. It states that not only we can intercept an encrypted message, but also we have some degree of control over what the plaintext message is for that. Selected plaintext attacks typically suppose making plaintext with certain properties with hope of affecting some measurable amendment within the ciphertext to derive data about the key. This attack is one amongst the least realistic, however usually most powerful.
5) *Chosen-Ciphertext:* The attacker obtains the assorted plain text like associate degree discretional set of cipher text. An extension to a chosen plaintext attack could be a chosen-ciphertext attack, that is, one during which we are able to opt for ciphertexts to be decrypted with a definite key. This attack is one amongst the least realistic, especially when combined with a chosen-plaintext attack.
6) *Related Key Attacks:* Like the chosen plaintext, attack in which attacker can obtain only cipher text encrypted with the help of two keys. Although the keys are unknown but the relationship between them is known. Example two keys dissent by one bit.

C. Computational Resources Required

Attacks may also be classified on the premise of resources needed. Those resources are:

1) *Time:* the quantity of computation steps (like encryption) that has be performed.
2) *Memory:* the quantity of memory required to perform the task.
3) *Data:* the quantity of plain text or cipher text required.

Actually, it's terribly troublesome to seek out these resources precisely, particularly once the attack is not sensible to truly implement for testing. However tutorial cryptanalysts tend to supply a minimum of associate degree calculable order of magnitude of their attacks problem.

V. GENERAL CRYPTOGRAPHIC METHODS

A few variety of algorithms, for their security rely solely on comprising mathematical operations like problem of computing distinct logarithms or resolution massive numbers. Yet a big variety of ciphers area unit are designed with techniques like substitution-permutation networks, Feistal structures, and shift registers.

1) *Brute-Force:* The quality known-ciphertext or known-plaintext attack is merely a brute- force attack, so named as a result of we have a tendency to simply attempt all possible keys and see which of them provides us the proper plaintext-ciphertext pairs.
2) *Time-Space Trade-Offs:* It needs a trade-off should be made between period of time and areas needed. Generally, it's possible to require less time to try to do certain computational process tasks at the price of skyrocketing the area needs.
3) *Rainbow Tables:* Rainbow tables are pre-computed tables used for reversing hash functions. They were designed to avoid collisions and to slightly increase the chance of success. Using the time-space tradeoffs. Rainbow tables accomplish this, by victimization completely different reduction perform anytime.
4) *Slide Attacks:* It is used as either a known-plaintext or chosen-plaintext attack. Slide attack has two requirements: first, cryptological algorithm program have a weak round function; and second, the algorithm program employs weak key scheduling algorithms. Although, these requirements may not be practical for most ciphers, slide attacks are used with success on many ciphers as well as variants of Blowfish and DES.
5) *Cryptanalysis of Hash Functions*: One goal of hash function is to come up with a digest of a source that cannot provide information about that source. However, the main goal of cryptanalysis of hash function is to get data regarding about the initial source text or to provide a duplicate hash.
6) *Cryptanalysis of Random Number Generators:* A primary reason for cryptanalyzing random selection generators is to do to work out into a couple of key utilized in a regular cipher and determine information about a key used in a standard cipher.

VI. CRYPTANALYSIS OF SYMMETRIC CIPHERS

There are various types of attack that can be done on symmetric ciphers. There are many cryptanalytic strategies that might rely on deep analysis of cipher which utilizes deep structure of cipher by gathering information about encryptions, recovering actually some or all of the sub-key bits. And if necessary then thoroughly look for the rest. These are usually referred as stastical attacks.

1) *Linear Cryptanalysis:* Linear cryptanalysis is a stastical method. This can be known-plaintext attack initial elaborate by Mitsuru Matsui and Atsuhiro Yamagishi within the early nineteen nineties against FEAL and DES. It requires access to a large amount of plaintext and ciphertext pairs which are encrypted with same keys. This formal method makes an attempt to relate the inputs and outputs of algorithm program elements along so that solving a system of linear equations can yield information regarding the bits of the key want to encrypt them. This method is that the initial attack against DES to operate in less time than an exhaustive search. The drawback is that an oversized range of plaintext-ciphertext pairs should be collected, which as a result of the attack is probabilistic, it is not bound to work for each key.
2) *Differential Cryptanalysis:* The standard differential cryptanalysis is a chosen-plainext attack. Differential Cryptanalysis was first made public in 1990 by Eli Biham and Adi Shamir and Murphy; in the years following, it has proven to be one of the most important discoveries in Cryptanalysis. Instead of analyzing linear relationships between input and output bit of Sboxes, as in linear cryptanalysis, differential cryptanalysis focuses on finding a relationship between the changes that occur within the output bits as a results of dynamic a number of the input bits. Differential Cryptanalysis is complex, given a known difference in the input and searching for a known difference in the output. In this method, the difference can be specified in several ways but exclusive-OR (XOR) operation is mostly used. It performs attack by repeatedly encrypting plaintext pairs with known input XOR until obtain desired output XOR. Once it's found; if intermediate rounds match needed XOR have a right pair, if not then have a wrong pair. Cryptanalyst can deduce keys values for the rounds, that is, right pairs suggest same key bits while wrong pairs give random values.
3) *Boomerang Attack:* This is a technique of cryptanalysis of block ciphers which is based on differential cryptanalysis. This type of attack provides different ways of attacks on various ciphers which are same from the basic differential cryptanalysis. Boomerang attack permit "differentials: cover only part of cipher. In order to produce the so called "quarter", this attack is applied at the point halfway through the cipher.
4) *Integral Cryptanalysis:* Attacks under integral cryptanalysis are appropriate on block ciphers based on substitution-permutation networks. In dissimilar differential cryptanalysis, the square attack uses sets or multi-sets of chosen plaintext of that half is held stable and Alternative half varies with all prospects.
5) *Davies' Attack*: This attack can be a plaintext attack that is based on non-uniform division of output pairs of adjacent S-boxes in DES. For attacking the DES, Davies' attack works by calculating empirical distribution of its characteristics and gathering various plaintext/ciphertext pairs.
6) *Man-in-the-Middle Attack:* This attack is a wellknown plaintext attack. It happens when cryptanalyst attempts to embed themselves into the communication channel between two parties who wish to trade their keys for secure communication through symmetric or public key infrastructure.

VI. CRYPTANALYSIS OF ASYMMETRIC CIPHERS

In public-key encryption, two keys are used; one key (the private key) is used for the decryption and another key (the public key) is used for encryption (or vice versa). The major points to solve the "assumed hardness" of the mathematical problem used to construct the public-key system. Consequently, the security of modern public-key cryptosystem depends on a wide range of mathematical techniques for key generation and distribution. For example, RSA's security rests on the complexity of integer factorization, while the security of Diffie-Hellman key exchange depends on computing the discrete logarithm. Asymmetric cryptosystems give the chance to make the use of knowledge gained from the public key for (crypt) analysing the secrecy of any information system.

1) *Cryptanalysis of Hash System*: The most representative attack on cryptographic hash functions could be Birthday Attack. Birthday attack is an attack which can find out collisions in the hashing algorithm. Birthday paradox may be a base for this attack. This kind of attack is generally used on hash algorithm such as SHA-1 and MD5 etc.
2) *Side Channel Attacks*: This kind of attack is done by using additional information obtained from the physical implementation of the cipher. This is often principally associated with the hardware used to encrypt or decrypt the data. Attacker in other cryptographic attack has access to plaintext or ciphertext pairs or cryptographic algorithm. While in side channel attacks, analysis is based on algorithm realization. It uses the leakage of confidential information that maybe found like energy consumption, running time or running errors. It represents a mainstream of the recent block cipher analysis techniques.

VII. QUANTUM COMPUTING APPLICATION FOR CRYPTANALYSIS

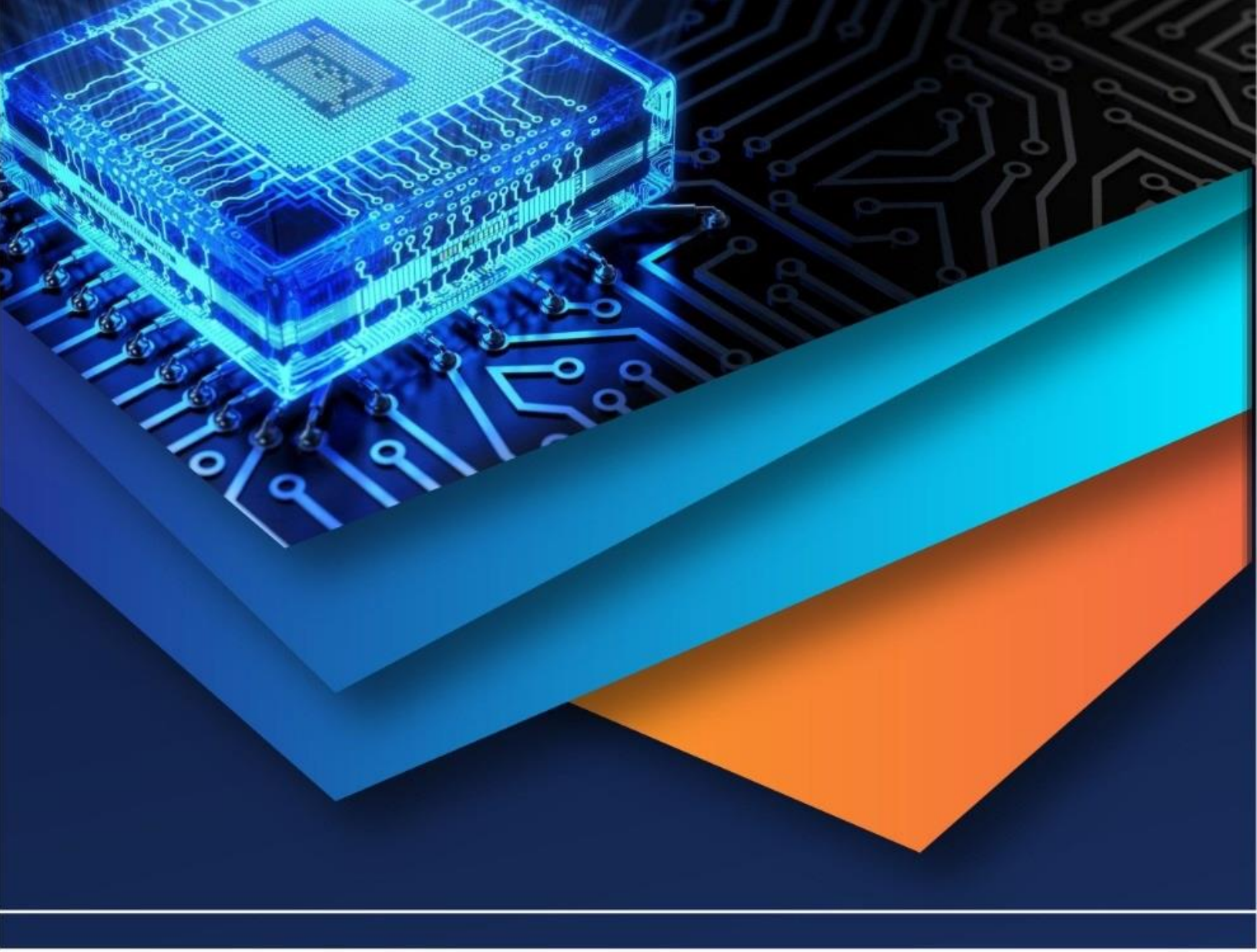
Modern cryptography has gotten significantly more impenetrable to cryptanalysis, and now appears to have the high ground against unadulterated cryptanalysis. Quantum computers that are still in the early in phases of analysis, have potential use in cryptanalysis.
For example: Shor's Algorithm could factor large numbers in polynomial time, in breaking some unremarkably used varieties of public-key encryption. By using Grover's formula on a quantum computer, brute-force key search is usually created quadratically quicker. However, this might be countered by doubling the key length.

VIII. CONCLUSIONS

In this paper we studied about cryptosystems, the objective was to specifically identify various types of attacks on cryptosystems and techniques of cryptanalysis. We studied various cryptanalysis attacks on secret- and public-key cryptosystems as well as hash functions. The knowledge of potential attacks helps to make our system safe from any cryptanalysis attack. By considering the possibility and practicability of these attacks, the existing algorithms can be improved. We can improve existing systems and minimize threats by identifying vulnerabilities and improving cipher's implementation and/or design. We also studied tersely about applications of Quantum Computers in Cryptanalysis and their effect on existing cryptosystems.

REFERENCE

[1] Stalling Williams, “Cryptography and Network Security: Principles and Practices”, 4th Edition, Pearson Education, 2006.
[2] Ashish Kumar Kendhe, Himani Agrawal “A Survey Report on Various Cryptanalysis Techniques”, International Journal of Soft Computing and Engineering (IJSCE), 2013
[3] Eli Biham “New Types of Cryptanalytic Attacks Using Realted Keys”, Technion – Israel Institute of Technology
[4] Crytanalysis, http://capec.mitre.org/data/definitions/97.html
[5] Ross J. Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” , 2nd Edition, John Wiley & Sons, 2008
[6] Sufyan Al-Janabi, Wael Ali Hussien “Architectural Design of General Cryptanalysis Platform for Pedagogical Purposes” i-manager’s Journal on Software Engineering, Vol. 11, No. 1, July- September 2016.
[7] Christopher Swenson, “Modern Cryptanalysis: Techniques For Advanced Code Breaking” Wiley Publishing, Inc., 2008.
[8] Steam and Block Cipher Operations, HYPERLINK "http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/Block%20cipher%20and%20stream%20cipher.html"
[9] Douglas R. Stinson, “Cryptography: Theory and Practice”, 3rd Edition, Chapman & Hall/CRC, 2006.
[10] Niels Ferguson, Bruce Schneier “Practical Cryptography”, Wiley Publishing Inc., 1st Edition, 2004.
[11] Cipher,https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7cphr1.html.
[12] Alan Kaminsky, Michael Kurdziel, Stanislaw Radziszowski “An Overview of Cryptanalytic Research for the Advanced Encryption Standard”, Rochester Institute of Technology.
[13] Jovan Golic “Recent Advances in Stream Cipher Cryptanalysis”, Publications de l'Institut Mathématique.
[14] Amandeep, G. Geetha “Research Problems in Block Cipher Cryptanalysis: An Experimental Analysis”, International Journal of Innovative Technology and Exploring Engineering(IJITEE).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY