International Journal of Academic Research & Technology (IJART)
Volume: 01 Issue: 01

AN ILLUSTRATIVE REVIEWS ON CRYPTOGRAPHIC ALGORITHMS USED IN NETWORKING APPLICATIONS FOR SECURITY

Dr Vijayakumar Thota
Associate Professor
Department of Management
NSB Bangalore
Email: vijayakumarthota@nsb.edu.in

Abstract

The computational applications that can be performed through mobile and wireless networks have expanded at an exponential rate, and so have the aspects of network protection. In recent years, there has been an increase in the number of cyberattacks and other types of illegal behavior carried out on the networks of businesses and private persons. Firewalls and security code are two methods that are insufficient and ineffective when it comes to protecting computer networks. Users of personal gadgets, employees of businesses, and members of the armed forces have all come to realize how important it is to defend networks. This article provides protection for email conversations by using an algorithmic encryption approach based on RC4. Ever since the introduction of the internet, protection has been one of the most pressing issues, and having a grasp of how security has evolved is necessary for the production of new security technologies. The enormous rise in demand for computers among businesses and other types of organizations has resulted in the establishment of a number of different networks. In recent years, there has been a marked increase in the number of assaults that are launched against computer networks. In order to ensure the safety of wireless networks and mobile devices, it is necessary to create brand-new frameworks employing certain procedures. Taking into consideration the possibility that one of our networks or edge devices may be the target of one of many assaults. In this article, we'll investigate a variety of potential protective measures for our network. People make touch with one another in a variety of ways every day, some of which include the use of print media, direct mail, SMTP, social networking, search engines, bookmarking services, and promotional email. This authentication interval is controlled and regulated by the encryption and decryption methodsWithin the scope of this paper, an effort has been made to investigate a variety of cryptographic and network security principles. This article covers a wide variety of cryptographic algorithms that are utilized in networking applications and explores the current state of the art for these algorithms.

Keywords: Decryption, Encryption, RC4 Algorithm, Electronic Mail Security, SMTP, Cryptography Networking Applications.

1. Introduction

The word "cryptology" comes from the Greek phrase "Krypto’s logos," which translates to "hidden, secret." The purpose of cryptology is to safeguard communications between sender and recipient, both of whom must be assured that no one on the receiving end may overhear (the communication of the receiver is not disrupted in any way). hints that there could be humans living in Figure 1, given the information provided.

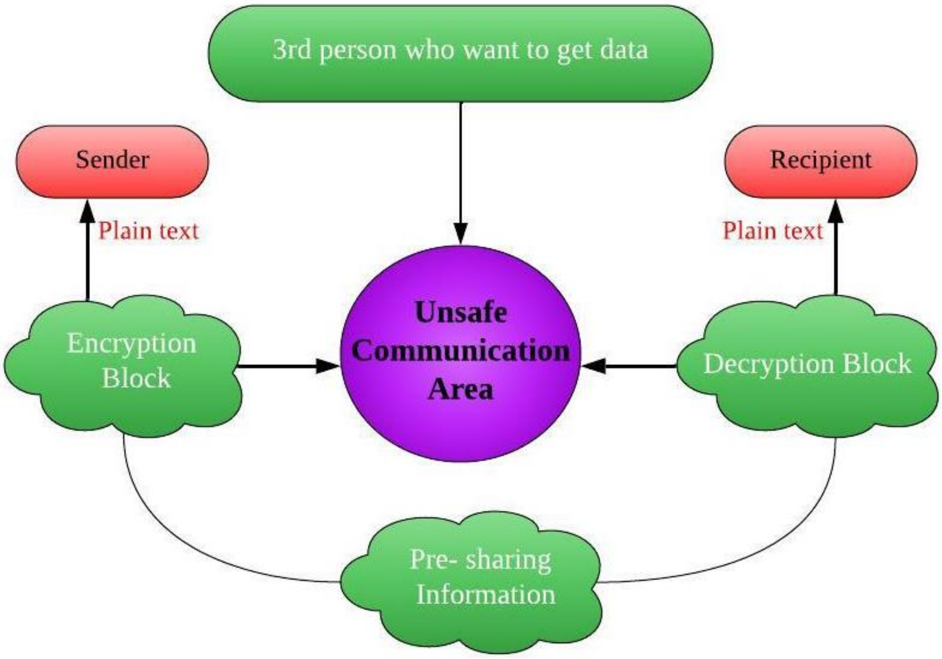

Figure 1: Communication channels over the unsafe area

It's possible that machine 3 will arrive at the conclusion that the text is encoded after it (reduces) understands that its sources of heat originate from ventilation, radiation, radiation, and conduction. The concepts of encryption and decryption, as well as asymmetric keys, are phrases that relate to the two primary categories of encryption techniques that fall within the broader category of symmetric encryption and decryption. This method of encrypting electronic communication (such as email) relies on the use of symmetric algorithms and is based on the usage of paper. The privacy of this method cannot be guaranteed by using the symmetrical key cryptosystem's secret since the rules and the keys both need to be kept a secret.

Either two keys that share the same key or an algorithm with a single key may be used for the symmetrical encryption's two different varieties. These are known as block ciphers and bit ciphers, and they are characterized by the fact that they enable the expansion or contraction of a single bit at a single position in a stream. 1987 was the year in which a stream cipher theory that was created by RC4 and presented in this article was able to prove the existence of a cipher. This concept's usefulness and convenience were improved through the use of a variety of methods, some of which included Secure Socket Layer (SSL), Wi-Fi Protected Access (WPA) for wireless internet security, which made secure communication possible, was advantageous, and was done, and was helpful; and was likely also preferred over Wired Equivalent Privacy (WEP), which made easy and expedient communication convenient; even in some cases, it might harm. Numerous developments, frameworks, protocols, and methods contribute to an increased level of safety inside the e-expanded network. Every user's primary email account need to be protected with a password that is exclusive to that account. The public key infrastructure (PKI) may enable individuals to connect with one another while also relying on a private key database (either their own or a shared one), which may make it possible to use all keys obtained from common authority. In public key infrastructures, key management, also known as key administration, may make this possible. Even though it is possible for a sender to include a recipient's public key into an encrypted Mail session, public key receivers must still be created before encrypted sessions. This is the case even if email encryption makes it possible for a sender to do so. It is possible to find a solution to this problem by using identity-based decryption, often known as expanding on ER. IBE makes use of the I.P address, which is sometimes referred to as a URL on occasion, as a name or domain, and the literal meaning of the name or IP address is used as a key in the system. Within the body of published research, several different types of protected email security framework implementations may be found. Lu and Geva are putting a distributed search engine into place, and this is happening regardless of any email communication that is taking place via the encrypted GE. It employs the attribute and public key standard known as X.509 in its operation. It does this by using an email server that links emails to their corresponding properties.

The proliferation of social networking and e-commerce apps, both of which need vast quantities of data to be entered, has led to an increase in the quantity of data that is often generated by enterprises all over the globe. When it comes to maintaining the smooth flow of data across all of these goals, data security is by far the most important goal. It is imperative that we replace antiquated methods of information sharing with ones that are more in line with the current times as our culture evolves into the modern century. As more people have access to the internet, there is also an increase in the number of malicious hackers who participate in online attacks. Authorizing network access refers to the process by which a network administrator grants users permission to view or modify any information stored on a network that is managed by the administrator.

The Internet's reach continues to grow across all aspects of society. Because of this, every person is now at risk, even those who have given permission to the network to monitor us as well as those who have not given permission. The goal of data security is to safeguard not just the network but also the data processing that takes place on it. In most cases, a network security strategy will include aspects of networking administration as well as security, and it will use a number of different levels of protection. When each component works together as intended, there is an improvement in the overall level of stability within the network. One of the many approaches to data security that are accessible, which is known as cryptography, is the one that is used the most often.

The use of cryptography in network security systems is still in its infancy, which leads one to the conclusion that these systems are still in their infant stages. One might use a cryptosystem in order to It has been shown that neural networks are capable of providing an efficient defense. The network's defenses are going to be significantly improved thanks to the use of neural networks and encryption on PCs. The neural network is constructed via the use of computational procedures that are difficult to manipulate and are represented as connected weight arrays. If you use the information from our content data to assist you in the construction of cryptographic algorithms, the information will be completely unintelligible to your adversary, which means they won't be able to comprehend the data you work with. Concepts from the theory, application, and stochastic behaviour of neural networks and related algorithms can be beneficial to the many facets of public-key cryptography. These include neural synchronization of shared concepts, self-learning techniques to the distribution of keys, and hashing methods, which can be used to cooperatively learn with the user. Neural networks additionally make advantage of the "expand" and "zoomed training signals" in order to split images into non-linear components. Each of these components is then given its own unique area to operate in independently. Regardless of whether a neural network is active or inactive, the activation level of the network is determined by a number of different factors. Cryptanalysis might benefit quite a bit by considering this concept.

2. Review Of Literature

The characteristics of network protection have evolved as a result of the exponential growth in computing applications of mobile and wireless networks. There has been an uptick in internet attacks and certain malicious activities on businesses and individual networks in recent years. Firewalls and security coding are insufficient and ineffective for defending computer networks. Personal device users, businesses, and the military have also realised the importance of network protection. The RC4-based encryption algorithmic rule is used to protect email correspondence in this article. With the introduction of the internet, protection has become a huge issue, and studying the evolution of security makes for a greater understanding of how security technologies emerged. Many networks have been developed as a result of the rapid demand for computers in businesses and other organisations. Attacks on computer networks have been even more common in recent years. As a result, certain approaches for designing new frameworks to secure wireless networks and mobile devices are needed. This paper would be extremely helpful and critical for network protection. Since our networks or edge devices may be infiltrated by a variety of assaults. We will examine various available mechanisms to defend our network in this article. People use contact mechanisms such as e-mail promotional, text messaging, SMTP, social networking, search engines, bookmarking services, partner systems, print media, and direct mail on a daily basis. This authentication intervals are controlled by the encryption and decryption techniques. The role of network protection entails not just the security of end systems but also the security of the whole network. An effort has been made in this paper to study numerous Network Security and Cryptographic principles. The current state of the art for a wide variety of cryptographic algorithms used in networking applications is discussed in this article.

In the excellent growth of internet environment, there is a challenge to send data in secure. Security means sending information without any modification or hacking done by unauthorized users. Network security has the component of cryptography technique which acts like guard to the information. The general concept of cryptography is encryption and decryption. There are many cryptographic algorithms are used to send the information as cipher text which cannot be understood by the intruders. So experts have taken the existing algorithms to provide security over the network and they want to apply the benefits of those algorithms in the suitable places. First step of getting the help from algorithm is to be studied and compared their parameters. This paper presents a review that comparative study of algorithms taken by many authors.

Internet of things has be broadly applied for home, industry, and many other applications. For these applications, secure information transmission becomes a critical issue to ensure the system safety. Hybrid encryption technique is a new cryptographic paradigm and it can be applied to the Internet of Things. It provides the benefit of the symmetric key and asymmetric key performance. It enables strong security and low computational complexity. In this paper, we proposed a mixed encryption algorithm to provide information integrity, confidentiality, non-repudiation on the data transmission for Internet of Things. We demonstrate the security efficiency with the comparison with traditional encryption algorithms.

Cryptography plays a major role in securing data. It is used to ensure that the contents of a message are confidentially transmitted and would not be altered. Network security is most vital component in information security as it refers to all hardware and software function, characteristics, features, operational procedures, accountability, access control, and administrative and management policy. Cryptography is central to IT security challenges, since it underpins privacy, confidentiality and identity, which together provide the fundamentals for trusted e-commerce and secure communication. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication.

Data security has been a major and challenging aspect in the modern era of information technology involving the internet and network applications. Especially it becomes serious in the cloud environment because the data is located in different places all over the world. The purpose of securing data is that only concerned and authorized users can access it. Different encryption algorithms provide the necessary protection against the data intruders' attacks by converting information from its normal form into an unreadable form. Security of data can be done by a technique called cryptography. Recently, the range of cryptography applications has expanded a lot in the area of network and the development of communication means. Cryptography is essentially required to ensure that data are protected against penetrations and to prevent the practice of spying. In this paper, the basic characteristics of different cryptographic algorithms i.e., Symmetric (secret) key cryptography, Asymmetric (public) key cryptography and Hashing cryptography are described. The application of these cryptographic algorithms has been explored in data and network security.

3. Components Used In Network Security

Before the development of public key encryption in the late 1970s, the only kind of encryption that was put into practice was symmetric encryption. This form of encryption is sometimes referred to as conventional encryption or single-key encryption. Up to the present day, symmetric encryption has been used for the purpose of clandestine communication by a wide range of individuals and organizations, including those operating in the military, commercial, and diplomatic spheres. A symmetric encryption technique is comprised of the following five components.

- ***Plaintext:*** This serves as the very first message or piece of data that the algorithm takes in as its input. Plaintext, also known as clear text, is a term used in the field of cryptography to refer to data that can be read and understood without the use of any additional methods.
- ***Encryption algorithm***: Encryption is the technique of hiding the contents of plaintext by dressing it up in a way that is unreadable. Encryption is a well-known method for protecting sensitive data from unauthorized access. During the encryption process, the plaintext is changed and altered in a variety of ways, including being exposed to a number of replacements.
- ***Secret key:*** The private key is another thing that the encryption technique needs. The key is used to specify precisely which alterations and replacements the algorithm will do.
- ***Cipher text:*** When plaintext is encrypted, cipher text, which is a type of data that cannot be understood, is produced. The result of having the message jumbled looks like this. Both the plaintext and the secret key are important components of this puzzle. Encryption is used as a consequence to protect sensitive information from being seen by unauthorized parties, even those who are capable of decrypting the data. If you use two different keys to encrypt the same message, you will get two completely different ciphertexts.
- ***Decryption algorithm:*** The process of turning encrypted material back to its original plain text format is referred to as decryption. In its most basic form, this is

the same encryption procedure but performed in reverse. Through the use of the private key and the ciphertext, it produces the initial plaintext (Figure 2).

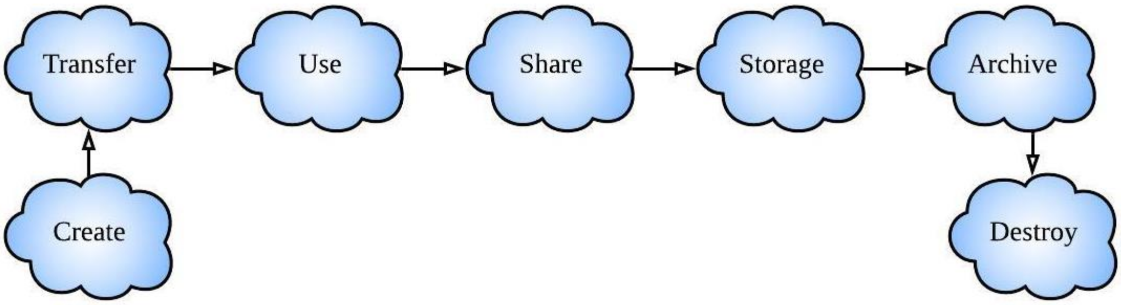

Figure 2: Data life cycle. The whole process from data production and storage through data destruction is referred to as a data security life cycle.

Encryption and decryption, as they are understood in the modern day, are believed to be combinations of three distinct types of algorithms. (i) symmetric key algorithms, in which the same key is used for both data encryption and decryption; (ii) asymmetric key algorithms, in which the sender uses a public key to encrypt data and the receiver uses a private key to decode it; and (iii) hashing. (i) asymmetric key algorithms, in which the sender uses a public key to encrypt data and the recipient uses a private key to decode it. The confidentiality of data is maintained with the help of hashing methods. In this way, cryptography may be used for user authentication in addition to protecting data from theft and alteration. The employment of cryptographic methods is very necessary to ensure the safety of data users. Because of the high degree of complexity of the method, there is a decreased chance of successfully deciphering the cipher text and regaining access to the plaintext.

4. Research Methodology

The strategy that is being suggested for this article may be divided down into four different categories. There is a new post, as well as a conventional message, and an MRC4 message. The programming language that is being used here is Java. Following the creation of a new Email package contract by the new message class, the encrypt function of the MRC4 class is used in order to cipher both the email entity and the content of the message. The default class is where you'll find the session instructions for registering with SMTP and POP3 servers. The messages class is then given control over the newly arrived data at that moment. When the messages class establishes a connection to the POP3 server in order to get encrypted email, the encrypted email is decoded using the MRC4 class's decrypt method. After the SMTP client has been created, the usage data is then fed into it for the first time. SMTP is the protocol that is used in order to transmit the customer email set. The sender and the receiver must first determine the RC4 key management points that were suggested in the Elgamal encryption technique for key contract before they can encrypt the subject and content of the letter using MRC4 in the MRC4 class. Figure 3 provides an illustration of the framework of the basic agreement.

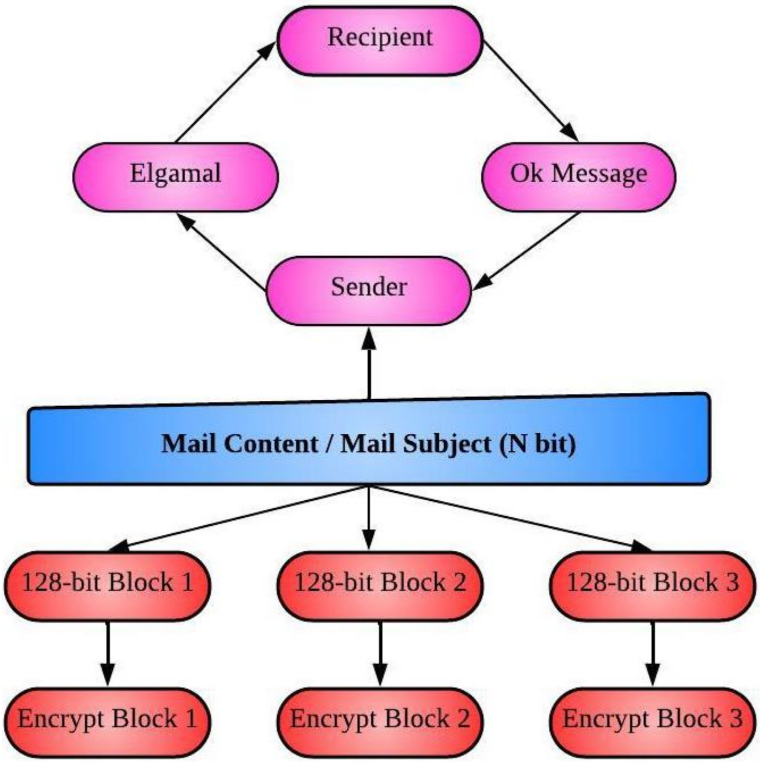

Figure 2: The Encryption Process of Each Block with Mrc4 Algorithm

- **RC4 ALGORITHM**

There are two basic cryptographic algorithms; these are.

- Symmetric algorithms
- Asymmetric algorithms

A cryptographic code of activities is a series of actions meant to achieve a purpose utilizing two or more margins. This code is created via the use of cryptography. Stream cyphers are symmetrical algorithms that may come in a few different flavours, the most common of which being synchronous stream cyphers and self-synchronizing stream cyphers. As was previously explained, the stream cipher known as RC4 communicates with servers and web browsers through the SSL/TLS protocols. Additionally, the RC4 stream cypher makes use of a number of additional standards and protocols. Additionally, it is included into the WEP and WPA protocols. It also provides the phases of the ciphering process in addition to the essential structure. The acquisition of each new key calls for the fulfilment of all previous processes. During the process of setting up a l-bit key, the encryption key is used to build an encrypting vector. This vector is constructed using two arrays state and key and a l-number of mixing operations. L is the important length here. The concept of random permeation serves as the foundation for this approach. The main system and the plaintext source are completely distinct from one another. To initialize a 2-byte array, the method makes use of a key with a variable length, the length of which may range anywhere from 1 to 256 bytes. First, the plaintext and the ciphertext are XORed with some pseudo-random bytes taken from the array. Then, the ciphertext and the plaintext are combined to generate the ciphertext/plaintext.

- **Strengths of RC4**
  - The difficulty that comes with trying to find any value in the database.
  - The difficult task of figuring out which row or column in the database need to be used to choose each value in the sequence.
  - The speed of the encryption is ten times faster than that of des.
- **Limitations of RC4**
  - RC4 is no longer considered to be safe to use.
  - There is a one in 256 chance that each given key is a weak key. Cryptanalysis has the ability to identify keys by recognizing circumstances in which one or more created bytes are strongly related with a few bytes of the key.
  - There is just one possible usage for each given RC4 Algorithm key.

To begin using RC4 encryption, you will first require a key, which may be chosen by the user and can range in size from 40 bits to 256 bits. A five-character ASCII code is converted into its corresponding forty-character binary representation to form a 40-bit key (for example, the ASCII key "pwd12" is converted into binary as 0111000001110111011001000011000101).

5. Analysis and Interpretation

The experiment includes the examination of data in both its plaintext and image forms. The unencrypted and encrypted versions of the NLCA-128 photographs. The following is a comprehensive analysis of the experiments and the results they produced.

- **Image Histogram (Intensity Variation):** The Intensity Variation (Histogram) is an extremely helpful tool that can be used to evaluate how the encryption process impacts the entire picture. Following decryption using NLCA, the desired shape of the histogram should be a straight line. The performance of the architecture with 128 bits is satisfactory.

The initial pressure distribution in certain test pictures results in very little variations in the histogram. These variations are driven by the fact that the test photographs themselves contain very few variances.

No	Image	Dimension	Entropy (ORG)	Entropy (ENC)
1	Baboon	127x127	7.2611	7.9691
		210x210	7.1762	7.9658
		276x276	7.2091	7.9956
2	Lena	129x129	7.491	7.9865
		221x221	7.5518	7.9652
		356x356	7.4966	79997
3	Banda	255x255	7.9666	7.9329
		532x532	7.4517	7.9936
5	Peppers	258x258	7.5522	7.9971
		522x522	7.6666	7.9999

Table 1: Image Entropy Test for NLCA −128.

Everything is broken out into granular detail in Table 1. It has been shown that NLCA-128 results in an entropy change that is, on average, 10.23%. The findings make it very evident that the NLCA-128 method that was offered is the most appropriate option for image coding.

6. Result and Discussion

The performance characteristics of NTRU, RSA and ECC are observed by implementing the algorithms for computation using the open source Bouncy Castle 1.47 Java library and comparing their experimental run times. Open JDK-7 with Cacao Java Virtual Machine was used for faster execution. Our experiments were conducted on 700 MHz Raspberry Pi running Linux and Intel(R) Core(TM) i3 CPU @ 2.27GHz to facilitate performance comparison. In the first experiment, the run times for three fundamental primitives of a cryptosystem, i.e., encryption, decryption and key generation, were measured for NTRU and RSA with different key-sizes. Test was done for randomly generated message of size 32 bytes. Table 1 shows the results on an Intel machine and a Raspberry Pi device respectively.

Asymmetric Algorithm	**Key Generation (ms)**	**Encryption (ms)**	**Decryption (ms)**

RSA-2048	91.42	0.53	3.32
RSA-3072	235.7	0.61	9.51
NTRU-439	6.25	0.29	0.32
NTRU-743	10.25	0.35	0.65

Table 2: Comparison Of Key Generation, Encryption, And Decryption Speed On Intel Core @2.27ghz

The results show that RSA has a very poor performance in generating asymmetric keys in both cases. Also it was observed that NTRU decryption (private key operation) worked multiple times faster than its RSA counterpart for the same level of security (RSA-2048 can be compared to NTRU-439, RSA-3072 can be compared to NTRU-743).

7. Conclusions

To put the current state of secure e-mail systems into perspective, we might say that the goal of the software is to establish a level of confidence between two individuals or within a small group so that individuals in the group may communicate with one another using text-based e-mail. Even if such software has long been available for free download, the usability and quality of open implementations have recently seen significant improvements. Using free software to implement comparable safety precautions for MIME-based email is feasible, despite the fact that such software is uncommon and is often supplied for a fee. Even while local certificate administrations are now being put into place and are making substantial headway in their implementation, they are not yet widely used nor have they reached their full potential. As their use develops and a common security framework gets stronger, all email you send and approve will be accessible. Since then, the economic viability of using a single association software to construct enterprise-wide authorizing bodies has significantly increased. It is possible for enterprises to ensure the security of their communications without relying on any governmental licensing authority. Despite the seeming amount of unpredictability, there are reasons to believe that sending confidential messages over email would be possible. It is quite likely that all email tiers will make use of the same algorithmic standards, license types, and confidence management frameworks that are now in operation. The message layout is the only one of these four components that cannot be reused for several performances, and even then, it is unusual for that to happen. The other three components, however, may be shared.

8. References

1. Anjula Gupta , et.al. “Cryptography Algorithms: A Review “ *International Journal of Engineering Development and Research*, Vol.2 No.2, (2014).
2. Mini Malhotra et.al. “ Study of Various Cryptographic Algorithms”, *International Journal of Scientific Engineering and Research*, Vol.1, No.3, (2013), PP.77-88.
3. Shashi Mehrotra Seth et.al,” Comparative Analysis Of Encryption Algorithms For Data Communication”, *International Journal of Computer Science and Technology*, Vol.2, No.2 (2011) pp.292-294.
4. S G Suganya, Prasanna D, “Detection and Prevention of DDoS Attack Using Modern Cracking Algorithm”, *International Research Journal in Advanced Engineering and Technology*, Vol.2, Issue.3, Apr 2017.
5. E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques” *International Journal of Advanced Research in Computer Science and Software Engineering,* VOL. 2, Issue 7 July 2012, Page 226-233.
6. Sumedha Kaushik, Ankur Singhal, “Network Security Using Cryptographic Techniques” *International Journal of Advanced Research in Computer Science and Software Engineering*, VOL.2, Issue 12 December 2012, Page 105-107.
7. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." *Dr. Dobb's Journal*, March 2001.
8. Pranay Meshram,Pratibha Bhaisare, S.J.Karale,”,comparative study of selective encryption algorithm for wireless adhoc network” ,IJREAS Volume 2, Issue 2 , in *International Journal of Research in Engineering & Applied Sciences*.
9. Punita Mellu & Sitender Mali, “AES: Asymmetric key cryptographic System” *International Journal of Information Technology and Knowledge Management*, 2011, Vol, No. 4 pp. 113-117.
10. Wenye Wang, Zhuo Lu., “Cyber Security in the Smart Grid: Survey and challenges”, Computer Networks: *The International Journal of Computer and Telecommunications Networking*, Vol.57 Issue 5, April, 2013.
11. Martin Drahansky and Maricel Balitanas., “Cipher for Internet-based Supervisory Control and Data Acquisition Architecture,” *Journal of Security Engineering*, Jun, 2011.
12. Aamir Shahzad and Shahrulniza Musa., “Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication”, *International Journal of Society (IJS),* Vol.6, Issue.3, 2012.