INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

Cryptography- A Fundamental Tool for Directions of Research Process-An Overview

Dr. V. Venkateswara Rao
Professor in Management,
Pace Institute of Technology & Sciences: Ongole
venkatpacemba2010@gmail.com

D. Pushpa Sri
Assistant Professor,
Pace Institute of Technology & Sciences: Ongole
pushpasri_d@pace.ac.in

Abstract: In Today's, Digital communications Era sharing of information is increasing significantly. The Information being transmitted is vulnerable to various passive and active attacks. Therefore the information security is one of the most challenging aspects of communication. Cryptography plays an integral role in secure communication and it provides an excellent solution to offer the necessary protection against the Data Intruders. Over period of time, Data encryption techniques took a massive leap from simple methods to complicated mathematical circulations. In order to achieve secure communications, however still with its complexity erypgraphic algorithms are prone to one or many attacks. Therefore this paper presents a detailed study about the Directions of safety, protection that leads to Research process. The various symmetric key encryption techniques, its comparison and the attacks to which they are vulnerable to.

Keywords: Cryptography, Systematic Key, Cryptanalysis' etc.

INTRODUCTION

Cryptography is the art of achieving security by encoding messages to make them Non-readaptable. Cryptography not only protects the information but also provider's authentication to the user. Here the original information and encrypted information are referred as plaintext and cipher text respectively. The Transformation of plaintext in to unintelligible Data known as cipher text in the process of Encryption. During communication, the sender performs the Encryption with the help of a shared secrets key and the receiver performs the decryption. Cryptographic algorithms are broadly classified in to sysmmatively key cryptography and Asymmetrical key cryptography. This section elucidate about services and mechanisms of cryptography.

NEED &SCOPE OF CRYPTOSYSTEMS

In the present scenario of cryptosystems, the algorithms make use of keys in to ciphering process which is a good alternative process which is goal alternative. But multiple keys are hard to generate and exchange. It also consumes network bandwidth with high traffic. Some algorithms are introduced the encryption of images and video streams by using various transformations like DCT, or Orthogonal transformations, confusion and diffusions. But they don't guarantee lossless operation in decryption process. In order to overcome these problems, we have designed dynamic symmetric key algorithms to achieve fast, accurate and Zero less results in Research areas. The Research work proposed here suggests a technique which uses a dynamic bit pattern key to encrypt the data analysis of research areas. We can apply this technique to many types of multimedia files. As the dynamic key is generated from the multimedia a research file, greater the size of the file, the greater the number of keys for encryption. Also Pixel depth, bit position and any other multimedia file properties are the past of the bit pattern and hence, enhance the security without affecting the cryptography process.

OBJECTIVES OF THE STUDY

The Objectives are as follows:

1. Development of multimedia based Dynamic systematic key cryptography Algorithms.
2. Coding of Algorithms in an appropriate programming package ensuring its profitability.
3. To ensure maximum security of data by using multiple keys.
4. To take advantage of both stegonography and cryptography for innovation & Research of new dynamic key symmetric encryption algorithms.

FOOT STEPS FOR PROPOSED RESEARCH APPROACH

1. Generation of parametric INC to decide the bit pattern as key from the multimedia file.
2. Generation of Dynamic key from multimedia file repeatedly for each set of data values in the process of Research.
3. Applying the key with minimum computations on user data to get cipher data in research areas.
4. Sharing the key generation is parametric.

REVIEW OF LITERATURE

Various Encryption Algorithms have been developed in the past decade. Some Algorithms worked very efficiently but they still have some overheads relating to them. There has been a miraculous improvement in the field of cryptographic particularly in case of Research. Some internet security has come in to existence, the old algorithms, have still their importance in various applications and so before discussing the current Research work. It is important to have a glance on the old popular symmetric key algorithms. Aditee Gotham (2011) has proposed a new approach concept of technique by using a block based transformation on which is used for image encryption. In this algorithms image is transformed in to other image before encryption processes is done. Mazola (2011) has proposed a new symmetric way of using a new Algorithms using of 128 Bits which are propounded with secrecy of Business research.

PERFORMANCE/EFFICIENCY METRICS

The organizations suffer big losses due to growing number of attacks. The wastage of time and resources caused to users result in lost revenues as time is money in on-line businesses. Also, the Terrorist organizations can harm a country by stealing the valuable secret information from the network. As most of the cryptic techniques don't assure complete efficient security, there is a need to analyze their features in detail, so as to come up with an innovative approach that resolves all the issues. In current work, we propose a powerful and efficient technique that ensures safety of users' data from nearly all types of attacks. To measure the efficiency and performance of Algorithms it is required to be compared with similar existing algorithms using the benchmarked performance metrics.

MECHANISMS OF CRYPTOGRAPHY

Cryptography provides four types of services such as confidentiality, integrity, authentication, Non- repudiation. A service that embraces the security of data processing systems and the information transfers of an organization. Confidentiality is production of data from unauthorized disclosure. Integrity providers assurance that the information received are exactly as sent by an authorized entity etc., information certain no modification, deletion etc., Authentication ensures that the identity of the sender and receiver of the information. It provides assurance that the communicating entity is the one that it claims to be. Cryptography having security mechanisms that is designed to detect, prevent or recovered from a security attacks. Security mechanisms of cryptography are divided in to 2 types such as specific security mechanisms and passive security mechanisms. Specific security mechanisms may be incorporated in to appropriate protocol layer in order to provide some of the OSI security services for Research Development purpose. Digital signature, encipherment are the best examples for Research process. Pervasive security mechanisms may be incorporated in order to provide OSI security aspects of Research information which are not specific to any particular OSI security service, security label, event Detection etc.,

RESEARCH PROCESSING APPROACHES OF

A block cipher is another symmetric key operating on full length of groups of bets called blocks, with an unvarying transformation. Block cipher uses modes of operations to provide an information services such as confidentiality or Authenticity. Modes of operation in Research are 1. Electronic code Book 2. Cipher Block chaining 3. Cipher feedback, output feedback 4. Counter mode in Research Process. A mode of research operation describes how to repeatedly apply a ciphers single block operation to security transform amounts of Research data larger than a Block.

RESEARCH –KEY DISTRIBUTION PROCESS

The major problem in symmetric key cryptography is that of the key Distribution because the key of Research must be shared secretly. Keys can be distributed by any of the following ways:

1. Sender can select the key and physically delivered it to the receiver.

2. A trusted third party can select the key and physically deliver it to the sender and the receiver.

3. If sender and receiver have previously and recently used a key, are party can transmit the new key to the others, encrypted using the old key.

4. If sender and receiver each has encrypted connection to the third party, then the Third party can deliver a key on the encrypted links to the sender and receiver.

CRYPTOANALYSIS- A BRIEF VIEW OF RESEARCH PROCESS

The scientific Analysis of securing Data, cryptanalysis of securing Data, crypto analysis is the science of analyzing and breaking up of information. The crypto analyst might have cipher text of Research and wanted to discover Encryption key that was used to encrypt it. The Application of mathematical, statistical tools, Research pattern findings must deliver the fact and accurate information to the receiver. Cryptographic attacks are mainly classified in to two types.

1. Positive attack
2. 2. Active attack.

A goal of the positive attack is just read the information it does not change the content of the message, where as the active attack, not only read the information and also modifying the content of the message.

VARIOUS SYSMMETRIC KEY ENCRYPTION TECHENIQUES

Regarding Research areas, general cryptographic techniques are classified as classical and modern based on periods which they are developed and used in. Classical cryptographic methods are still used purposefully to the several areas of research concepts for providing confidentiality techniques are developed in recent years of providing best research services like confidentiality, Authentication to the research information. In order to increase the degree of security, the modern cryptographic techniques algorithms are in creditably complex applicable for Research conceptive.

CONCLUSION

Cryptography plays a pivotal role in explosive growth of digital data storage and communication. In Research it is used to achieve the mains of security goals like confidentiality, Integrity, Authentication and Non-repudiation. In order to achieve these goals, various cryptographic Algorithms are developed to conduct research in a systematic way. In which some of the Algorithms are failed due to lack of confidentiality. Algorithms for encryption of research data is selected based on the purpose, and the type of channel which the data is being communicated. The main purpose of this paper is to disseminate the basic research knowledge about the purpose, importance and significant regarding cryptographic algorithms and comparison of available symmetric key encryption techniques based on some parameters like vulnerability of research, uniqueness and Techniques

REFERENCES

1. Cryptography Analysis- A Parametric view by Ronald Risdon pp.231-239.
2. Algorithems for research areas development- Pearson's publications for new researchers. Pp.89-95.
3. Topo research process- The incidental base. Translate publications pp.564-629. 6th Edition.
4. Cryptographic Algorithms- A need of the Hour. Pearson's publications pp.64-98.
5. Analytical Aspective of Research Values- A Confidential movements of follow-up- crimsons research work- Value theory pp.23-48.

