VOLUME V
ISBN No.: 978-81-953602-8-4
Computational Science

Estd. 1957

NALLAMUTHU GOUNDER MAHALINGAM COLLEGE

An Autonomous Institution, Affiliated to Bharathiar University, An ISO 9001:2015 Certified Institution,

Pollachi-642001

SUPPORTED BY

ABT Industries Ltd.,
Dairy Division

PROCEEDING

One day International Conference

EMERGING TRENDS IN SCIENCE AND TECHNOLOGY (ETIST-2021)

27th October 2021

Jointly Organized by

Department of Biological Science, Physical Science and Computational Science

NALLAMUTHU GOUNDER MAHALINGAM COLLEGE

An Autonomous Institution, Affiliated to Bharathiar University

An ISO 9001:2015 Certified Institution, Pollachi-642001.

Estd. 1957

Proceeding of the

One day International Conference on

EMERGING TRENDS IN SCIENCE AND TECHNOLOGY (ETIST-2021)

27th October 2021

Jointly Organized by

Department of Biological Science, Physical Science and Computational Science

ISBN No: 978-81-953602-8-4

Nallamuthu Gounder Mahalingam College

An Autonomous Institution, Affiliated to Bharathiar University

An ISO 9001:2015 Certified Institution, 90 Palghat Road, Pollachi-642001.

www.ngmc.org

ABOUT THE INSTITUTION

A nations's growth is in proportion to education and intelligence spread among the masses. Having this idealistic vision, two great philanthropists late. S.P. Nallamuthu Gounder and Late. Arutchelver Padmabhushan Dr.N.Mahalingam formed an organization called Pollachi Kalvi Kazhagam, which started NGM College in 1957, to impart holistic education with an objective to cater to the higher educational needs of those who wish to aspire for excellence in knowledge and values. The College has achieved greater academic distinctions with the introduction of autonomous system from the academic year 1987-88. The college has been Re-Accredited by NAAC and it is ISO 9001 : 2015 Certified Institution. The total student strength is around 6000. Having celebrated its Diamond Jubilee in 2017, the college has blossomed into a premier Post-Graduate and Research Institution, offering 26 UG, 12 PG, 13 M.Phil and 10 Ph.D Programmes, apart from Diploma and Certificate Courses. The college has been ranked within Top 100 (72nd Rank) in India by NIRF 2021.

ABOUT CONFERENCE

The International conference on “Emerging Trends in Science and Technology (ETIST-2021)” is being jointly organized by Departments of Biological Science, Physical Science and Computational Science - Nallamuthu Gounder Mahalingam College, Pollachi along with ISTE, CSI, IETE, IEE & RIYASA LABS on 27th OCT 2021. The Conference will provide common platform for faculties, research scholars, industrialists to exchange and discus the innovative ideas and will promote to work in interdisciplinary mode.

EDITORIAL BOARD

LIST OF ARTICLES

International Conference on Emerging Trends in Science and Technology (ETIST 2021)
Jointly Organized by Department of Biological Science, Physical Science and Computational Science
Nallamuthu Gounder Mahalingam College, Affiliated to Bharathiar University, Tamilnadu, India.
Published by NGMC - November 2021

A Study of Cryptography Encryption and Compression Techniques

Dr.P.Logeswari[1]- G.Banupriya[2]- J.Gokulapriya[3]- S.Sudha[4] – S.Sharmila[5]

ABSTRACT: Data is any sort of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to stop unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of knowledge and authentication of other users. Compression is that the process of reducing the amount of bits or bytes needed to represent a given set of knowledge .It allows saving more data. Cryptography may be a popular ways of sending vital information during a secret way. There are many cryptographic techniques available and among them AES is one among the foremost powerful techniques. The scenario of present day of data security system includes confidentiality, authenticity, integrity, non repudiation. the safety of communication may be a crucial issue on World Wide Web. it's about confidentiality, integrity, authentication during access or editing of confidential internal documents.

Keywords: Encoding and decryption, Compression, Cryptography Concept, Security, Integrity.

1. INTRODUCTION

To secure the data, compression is used because it use less disk space (saves money), more data can be transfer via internet. It increases speed of data transfer from disk to memory. Security goals for data security are Confidential, Authentication, Integrity, and Non-repudiation. Data security delivers data protection across enterprise. Information security is a growing issue among IT organizations of all sizes. To tackle this growing concern, more and more IT firms are moving towards cryptography to protect their valuable information. In addition to above concerns over securing stored data, IT organizations are also facing challenges with ever-increasing costs of storage required to make sure that there is enough storage capacity to meet the organization’s current and future demands. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Currently compression and encryption methods are done separately. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information

Dr.P.Logeswari[1] , Assistant Professor, Sri Krishna arts and Science College, logeswarip@skasc.ac.in
G.Banupriya[2], Research scholar, Sri Krishna arts and Science College, logeswarip@skasc.ac.in
J.Gokulapriya[3], Research scholar, Sri Krishna arts and Science College, logeswarip@skasc.ac.in
S.Sudha[4], Research scholar, Sri Krishna arts and Science College, logeswarip@skasc.ac.in
S.Sharmila[5], Assistant Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, Tamilnadu, India. Email: mcasharmi2007@gmail.com

from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

2. CRYPTOGRAPHY

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction.

The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster’s Collegiate Dictionary defines cipher as ―a method of transforming a text in order to conceal its meaning.‖ The information that is being hidden is called plaintext; once it has been encrypted, it is called ciphertext.

To hide any data two techniques are mainly used one is Cryptography other is Steganography. In this paper we use Cryptography. Cryptography is the science of protecting data, which provides methods of converting data into unreadable form, so that Valid User can access Information at the Destination. Cryptography is the science of using mathematics to encrypt and decrypt data.

3. BASIC TERMINOLOGY OF CRYPTOGRAPHY

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing.

The information that we need to hide, is called plaintext , It’s the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.

The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks.

Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks, and to detect attacks on information-based systems.

4. CRYPTOGRAPHY GOALS

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them.

These goals are:

1. **Confidentiality:** it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.
2. **Authentication:** it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don’t have personal knowledge of their identities.
3. **Data Integrity:** its ensures that the received message has not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
4. **Non-Repudiation:** it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

5. **Access Control:** it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

5. DATA ENCRYPTION

A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

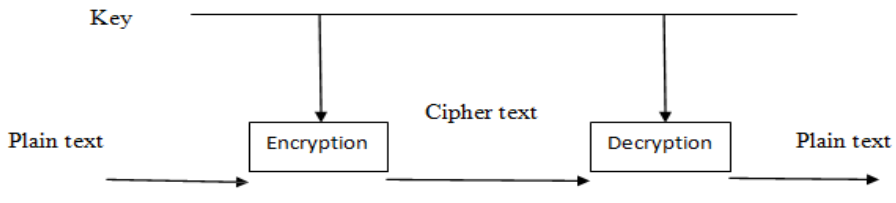
Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

6. DATA DECRYPTION

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

7. SYMMETRIC KEY CRYPTOGRAPHY

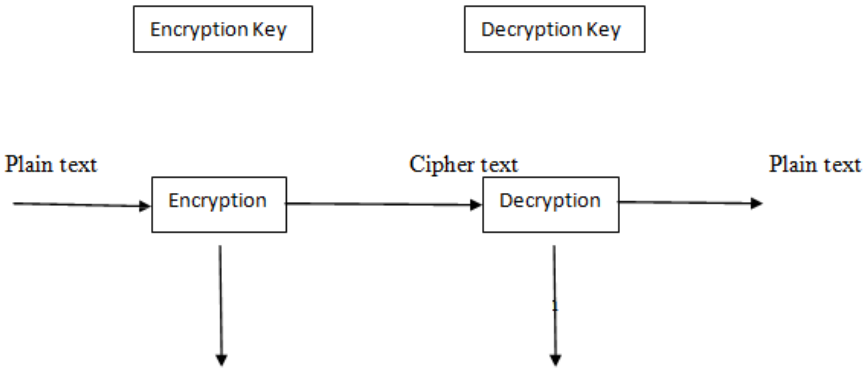
In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.



Symmetric Cryptosystem

8. ASYMMETRIC KEY CRYPTOGRAPHY

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.



Asymmetric Cryptosystem

9. COMPRESSION

Data compression offers an attractive approach for reducing communication costs by using available bandwidth effectively. Compression algorithms reduce the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs etc.

Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time. Many methods are used for this purpose, in general these methods can be divided into two broad categories: Lossy and Lossless methods. Lossy Compression generally used for compress an images. In this original data is not identical to compressed data that means there is some loss e.g. Block Truncation Coding, Transform Coding, etc... Lossless Compression used for compress any textual data.

SUMMARY

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified.

REFERENCES

[1] Author1, Initials, Author2, Initials and Author3, Initials, Book With Three Or More Authors, Name of Publisher, Place of Publisher, Year of publication
[2] Swarnalata Bollavarapu and Ruchita Sharma-— Data Security using Compression and Cryptography Techniques‖
[3] Manoj Patil, Prof. Vinay Sahu—— A Survey of Compression and Encryption Techniques for SMS‖
[4] Bobby Jasuja and Abhishek Pandya —— Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding‖
[5] https://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx
[6] https://www.techopedia.com/definition/1773/decryption [6]www.computerhope.com/jargon/d/decrpti.htm

[7] https://en.wikipedia.org/wiki/Cryptography
[8] https://www.techopedia.com/definition/25403/encryption-key
[9] http://searchsecurity.techtarget.com/definition/private-key
[10] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf
[11] Dr. P.Logeswari "Extraction of Subset- Want in Data Stream using EMDMICA Algorithm " Volume 7 Issue VI, June 2019.
[12] Dr. P.Logeswari, J.Gokulapriya "A Literature Review on Data Mining Techniques "in July Volume -7 Issue -7.
[13] Dr. P.Logeswari, J.Gokulapriya "Literature Survey on Big Data mining And Its Algorithmic Techniques "in July Volume -8 Issue7.
[14] Dr. P.Logeswari, G.Banupriya "A Survey on Implementations Solutions for Attack Prevention Cryptography Technique's in WSN UsingNS2" Volume 7,Issue 6 June 2021.
[15] Dr. P.Logeswari, G.Banupriya "Review on Cryptography Techniques in WSN for Attack Prevention" volume 8, Issue 8.
[16] Dr. P.Logeswari, J.Gokulapriya "Data Mining Approaches and Applications" (Conference Paper).
[17] Dr. P.Logeswari, G.Banupriya "Image processing and its Application" (Conference Paper).
[18] Dr. P.Logeswari, G.Banupriya "Cryptography Techniques and its analysis" (Conference Paper).
[19] Dr. P.Logeswari, S.Sudha "Survey on Privacy Preserving Secure Mining" (Conference Paper).
[20] Dr. P.Logeswari, J.Gokulapriya "Analysis of Data Mining Techniques and its Application" (Conference Paper).
[21] Dr. P.Logeswari, G.Banupriya "Cryptography Techniques and its Analysis" (Conference Paper).
[22] Dr. P.Logeswari, S.Sudha "A Survey on Privacy Preserving in Data Mining"Volume- 7, Issue-8 August 2021.
[23] Dr. P.Logeswari, S.Sudha "A Review on Privacy Preserving in Data Mining" Volume-8, Issue-6 June2021.
[24] Dr. P.Logeswari, J.Gokulapriya "Research Paper on Big Data and Hadoop" (Conference Paper).
[25] Dr. P.Logeswari, J.Gokulapriya "Data Mining for Security Applications" (Conference Paper).