IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Review and Analysis of Cryptography Techniques

[1]Twinkal, [2] Mohit Sharma
[1]MTech (CSE), [2]HOD. Of CSE DEPTT
[1]Computer Science of Engineering
[1]Yaduvanshi College of Engineering&Technology,
Narnaul, Mahendergarh (Haryana)

Abstract: With the internet blending into our lives and increasing at a breakneck pace over the last few decades, data communication has become based on digital data transmission,

Data security as a top priority in order for data to reach the intended user. It is often necessary to send sensitive information to a single person or a small group of people, and if this communication is intercepted and altered, it can be disastrous. Linked to the internet our information is only shared with those that need it, accessible to the intended recipient, and prohibits any unauthorized access and data change or alteration.To safeguard data during transmission or storage, various algorithms and methods have been developed in the field of security. A wide range of cryptography approaches are employed, each with its own set of strengths and limitations that are used to provide data security. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender. It encrypts data using a set of algorithms such as symmetric and asymmetric algorithms. These encryption methods vary in terms of strength, speed, and use of resources (CPU usage, memory, and power).

It is used to protect personal identifiable information (PII) and other confidential data, authenticate identities, prevent document tampering, and build trust between servers. Cryptography is one of the most significant techniques used by digital businesses to safeguard the systems that store their most valuable asset – data – whether it is at rest or in motion. Customer PII, employee PII, intellectual property, company strategies, and any other confidential information are examples of data. As a result, cryptography is a vital infrastructure, as the protection of sensitive data increasingly relies on cryptographic solutions.

It is a dynamic and mandatory component of digital business. Organizations need visibility into their cryptographic instances as well as guidance from not only standards groups such as NIST and ISO (International Organization for Standardization), but also the web browsers who control the user interfaces that connect businesses with consumers via secure online communications. Crypto agility is the key to keeping pace with the latest cryptographic compliance requirements, standards, and recommendations that sustain and secure digital business.Different asymmetric cryptography algorithms are discussed:

RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), and ECC (Elliptic Curve Cryptography) are some examples.The purpose of this research is to present the most popular and fascinating algorithms in use right now

Keywords: Cryptography, Algorithms, Diffe-Hellman

I. INTRODUCTION

Although cryptography is an old concept and discipline, it still exists and plays an important part in modernity. Cryptographic algorithms today are based on traditional cryptographic approaches. Internally, in performance, and in implementation, the various groups of algorithms have distinct characteristics. Cryptographic techniques and mechanisms have been improved over time. Cryptography has become more widely used, ranging from restricted use in government organizations to broad use by private persons and businesses. Increased Internet usage has had a profound impact on the nature of applications and how we communicate.

In the presence of an adversary, cryptographic procedures are used to ensure data secrecy and integrity. Various cryptographic approaches, such as symmetric-key cryptography or public-key cryptography, can be utilized during data transportation and storage depending on the security demands and dangers involved.

Furthermore, cryptography enables various computations on encrypted data without the need to decode the data for processing. These approaches are important for protecting personal information from being leaked during transportation and from storage servers from a privacy standpoint. A multi-layered security plan should include cryptographic approaches. Some security measures, such as the usage of a firewall and access permissions, try to keep intruders out of the network or computer entirely, similar to how fences and door locks try to keep robbers off the property or out of the house. An inner line of defense is provided by cryptography.

Cryptography protects data from intruders who are able to penetrate the outer network defenses and from those who are authorized to access the network but not this particular data, much like a wall safe protects valuables from people who are authorized to enter your house but not this particular data.

Different cryptographic techniques are required for data security. As a result, we examine the various coding strategies in-depth, rating their effectiveness and efficiency. There are new cryptographic systems that demand comprehensive study and analysis in light of the new cryptographic paradigms. Classical cryptography is the earliest algorithm, having been utilized long before the cryptographic system was discovered. Currently, the technology is being used to safeguard data and to improve old ways by applying new approaches. We examine many cryptographic techniques in this thesis.

Proposed Goal:

The goal of this study is to examine cryptography techniques in a more practical approach so that we can accomplish more, and we will discover more techniques than we were taught in theoretical practice. Because the amount of data is expanding every day, the field of evaluating vast amounts of data is current. When analyzing, it's also vital to compare and contrast cryptographic techniques. Cryptography is a large subject of study because each technique has its own unique qualities. Algorithms and approaches from various areas are used. To begin, it is necessary to specify the data to be studied in order to determine how to choose an algorithm.

To draw conclusions about the performance of cryptographic approaches, this study will employ comparative methods. All studies will be conducted in a practical manner. The growing popularity of the Internet has had a tremendous impact on the nature of applications and how we communicate. Different cryptographic techniques are required for data security. As a result, we examine the various coping strategies in-depth, rating their effectiveness and efficiency. Knowing the large range of applications and services where sensitive data is stored is enough to appreciate the necessity of cryptographic approaches. Data storage is one of the most essential personal, as well as operational, requirements for the success of a commercial venture, such as a bank or a company. Format encoding, symmetric search encryption, functional encryption, and homomorphism encryption are some of the new encryption forms imposed by the computational problems of specific schemes. They all involve data processing without possessing a private key to the data. There are new cryptographic systems that demand comprehensive study and analysis in light of the new cryptographic paradigms. Quantum cryptography and Turing-complete encryption programs are both very recent concepts with a strong theoretical foundation.

LITERATURE REVIEW

Cryptography is a method of ensuring message confidentiality. In Greek, the phrase has a special meaning: "hidden writing." Nowadays, however, individuals and organisations' privacy is protected by high-level cryptography, which ensures that information delivered is safe and only the authorised receiver has access to it [14]. Cryptography is a traditional technique that is continually being developed, with historical roots. Examples date back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as additional evidence from ancient Greece and Rome, such as secret writings and the renowned Caesar cypher [15] \Security is likewise applied to e-learning which includes e-exams, whose systems require authentication, privacy, encryption and confidentiality [16].Data communication, according to Nitin Jirwan et al. [11], is primarily based on digital data transmission, in which data security is prioritised when utilising encryption techniques to ensure that data reaches the intended users safely and without being compromised. They also exhibited several cryptography approaches, such as symmetric and asymmetric methods, that are used in the data communication process. Sandeep Tayal et al. [12] stated in a review on network security and cryptography that the rise of social networks and commerce apps has resulted in massive amounts of data being produced daily by organizations all over the world. As a result, information security becomes a major concern when it comes to ensuring the secure transmission of data over the internet. This issue emphasizes the importance of cryptographic approaches as more people connect to the internet. This paper gives an overview of the many security approaches employed by networks, including cryptography.Anjula Gupta et al. [13] discussed the history and significance of cryptography, as well as how information security has become a difficult problem in the computer and communications areas.This paper also provides various asymmetric algorithms that have given us the ability to protect and secure data, in addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by providing security and privacy.The Diffie–Hellman key is used in RSA methods to encrypt and decrypt data. Furthermore, RSA and Diffie–Hellman are touted as being strong enough for commercial use. The Diffie–Hellman key can be used to encrypt and decrypt messages using RSA, DES, AES, and elliptical curve encryption. [17].

Significance of Literature Review

This research is significant because it provides a comprehensive definition of the many cryptographic methods that we use in our daily lives in today's digital world. It provides us with the necessary understanding of various algorithms. It provides a thorough understanding of cryptographic approaches, such as which algorithm is best for data secrecy, integrity, authentication, and nonrepudiation. This research makes it simple to determine which algorithm is more safe, which algorithm is faster, which algorithm has more sophisticated computing, the advantages and disadvantages of various algorithms, and so on. This study provide foundation of the thesis and it tells about the areas need to work on. Each study has their own significance and have different reviews. This study tell us that among all algorithms RSA is more secure but has low speed due to its complex and long computation, and ECC is faster than all other cryptographic algorithms. So this literature review helps me to find out all these facts and proof about Asymmetric key cryptography algorithms.

Overview from Review of Literature & Problem Formulation

Authentication, integrity, confidentiality, and no-repudiation are only a few of the major security goals that cryptography helps to achieve. To fulfil these objectives, cryptographic algorithms are created. The objective of cryptography is to provide reliable, strong, and robust network and data security. We presented a summary of some of the research that has been done in the subject of cryptography, as well as an explanation of how the various algorithms used in cryptography for various security goals function in this paper. In order to protect personal, financial, medical, and ecommerce data while maintaining a reasonable level of privacy, cryptography will continue to be used in IT and business plans. Algorithms, mathematics, information theory, transmission, encryption, and other techniques and technologies are all included in cryptography. Individuals, institutions, and businesses all across the world are concerned about information security. Without encryption technology, it is difficult to consider a computer system completely secure nowadays. Basic means for safeguarding data and communications are cryptographic figures and algorithms.

RESULT AND ANALYSIS

The goal of qualitative data analysis is to transform raw data by looking for, evaluating, detecting, coding, mapping, exploring, and documenting patterns, trends, themes, and categories in order to comprehend and give their underlying meanings. Inductive analysis and creative synthesis are the terms Patton uses to describe this process.

This chapter looks at different approaches to qualitative data analysis and interpretation. It also highlights the importance of rigour and quality in qualitative data analysis. Much has been written about qualitative data analysis, as seen by the list of references in this chapter. The profusion of literature has undoubtedly added to the complexity of the qualitative data analysis technique.

According to Birks: “When starting a study, a rookie researcher may feel overwhelmed by the complexity of qualitative research terminology and some of the original work on the issue.”

In the presence of malevolent third parties, known as adversaries, cryptography ensures safe communication. Encryption transforms a plaintext input into an encrypted output using an algorithm and a key (i.e., cipher text).

Cryptography is becoming increasingly popular and powerful as the world gets more globalised. One of the most important aspects of computer security is cryptography. To satisfy a user's needs, a cryptographic method must be chosen based on factors such as security and performance.

Cryptography is one method for ensuring the secrecy, authenticity, integrity, availability, and identification of user data, as well as providing security and privacy to the user. By using mathematical changes or equations, encryption transforms ordinary data or plaintext into something incomprehensible or cipher text. Algorithms are mathematical changes or equations used in encryption operations.

The research article gives a general review of cryptography, including public and private key encryption.

Conclusion Algorithms, mathematics, information theory, transmission, encryption, and other techniques and technologies are all included in cryptography. Individuals, institutions, and businesses all across the world are concerned about information security. Without encryption technology, it is difficult to consider a computer system totally secure nowadays. Basic means for safeguarding data and communications are cryptographic figures and algorithms. We researched cryptographic algorithms, their cryptographic properties, and developed an application to encrypt and decrypt various texts in this article. Then we demonstrated each method with an example of how it works, and we contrasted several of the algorithms in depth. New attack tactics, ideas, and implementations of widely studied algorithms are all progressing in cryptography. As a result, based on our requirements, it's critical to examine their structure, efficiency, and scalability criteria. New coding paradigms with access to computational theory that are important in new systems and technologies. The relationship between efficiency and computational power is inextricably linked. As a result, we must tackle new tough problems in order to improve cryptographic techniques.The parameters of cryptographic algorithms vary, including encipherment and decipherment time, memory, throughput, and CPU use. This study examines the need to enhance a combined encryption algorithm that combines several encryption algorithms based on all relevant criteria in order to improve the overall safety and security of encryption methods. After going through all of the above-mentioned cryptographic approaches, it's clear that ECC is faster than RSA because it utilises a smaller key. However, in comparison to RSA, its mathematical operation is more difficult. Secret keys are exchanged between two users in the Diffie-Hellman cryptography algorithm. In DSA, the receiver uses a digital signature to certify that the signal received is unchanged

Future Scope: The world of computers and cyber security is constantly evolving, with new techniques like machine learning and artificial intelligence being developed on a daily basis. Quantum computing is one concept that has progressively evolved into much more than a concept. New encryption algorithms that are several times more powerful than the classical cryptography we use today can be constructed using quantum computing. While quantum computing has several benefits for cryptography, threat actors can utilize it to develop new malware that can break traditional cryptographic algorithms in half the time or less. Fortunately, quantum computers are still a long way from being fully developed and useful, but your company may start planning for the quantum revolution now.

Quantum Computing: The way traditional computing works is that operations are carried out in the form of bits. At any given time, these bits can have a value of 0 or 1. The quantum physics concept of superposition is used in quantum computing. When anything, such as a bit, is in two states at the same time, it is called a superposition. This means that quantum bits, also known as qubits, can be in both the 1 and 0 states at the same time. Because the bits might be set to 00, 11, 01, or 10, doing computation on a set of two classical bits takes four calculations. Because qubits can be in all four states at the same time in quantum computing, the quantum computer can execute calculations on all four states. This creates a slew of problems for today's encryption technologies. The private key for some encryption algorithms, such as RSA, which is used in the majority of eCommerce transaction encryptions, is obtained by factoring a number that is the product of two large prime integers. This is incredibly difficult to achieve with traditional computers, and with a long enough key length, it may take thousands of years to break. The usage of qubits in quantum computers, on the other hand, greatly reduces the time it takes to crack an algorithm like RSA. Although the key length can be increased for added security, a 256-bit key is now only as secure as a 128-bit key in the face of quantum computing.

REFERENCES

1. "Security In Wireless Sensor Networks," ACM, Vol. 47, No. 653.2004. A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No. 653.2004.

2. "Analysis Of Publickey Cryptography For Wireless Sensor Networks Security," by F. Amin, A. H. Jahangir, and H. Rasifard, in World Academy of Science Proceedings, ISSN 1 307-6884, Engineering and Technology 2008.

3. Wikipedia, “http://en.wikipedia.org/wiki/Diffie%E2%80%93 Hellman_key_exchange,”

4. Simon Blake Wilson et al., “Key agreement protocols and their security analysis,” 9-sep-1997.

5. David A. Carts, “A Review of the DiffieHellman Algorithm and its Use in Secure Internet Protocols,” SANS institute, 5-nov-2001.

6. Vocal, “http://www.vocal.com/cryptography/dsadigital-signature-algorithm/,”

7. Erfaneh Noorouzil et al, “A New Digital Signature Algorithm”, International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.

8. William-Stallings, “http://williamstallings.com/Extras/Security Notes/lectures/authent.html”

9. Robert Zuccherato, “Elliptic Curve Cryptography Support in Entrust,” Entrust ltd. in Canada

10. Kristin Lauter, “The Advantages of Elliptic Curve Cryptography for Wireless security,” IEEE Wireless Communication, Feb 2004.

11. N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .

12. S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763- 770, 2017.

13. A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.

14. N. Sharma , Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.

15. B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

16. D. Costinela-Luminita, "Information security in e-learning platforms," Procedia - Soc. Behav. Sci., 15, 2011, pp. 2689-2693.

17. R. Kumar, and C. C. Ravindranath, "Analysis of Diffie Hellman Key Exchange Algorithm with proposed Key Exchange Algorithm," Int. J. Emerg. Trends Technol. Comput. Sci., 4(1), 2015