A REVIEW PAPER ON CRYPTOGRAPHY AND NETWORK SECURITY

V. Agaphi Bob
Assistant Professor, Ramachandra College of Engineering,
Eluru, Andhra Pradesh, India.
vagaphib.932@gmail.com

Abstract:

With the rise of the World Wide Web and the proliferation of e-commerce platforms and social networks, organizations worldwide are generating vast volumes of data on a daily basis. With the explosively increasing internet that has been merging with our lives for the past few decades, data and network security has been of greatest importance as society moves towards the age of digital information. As the number of users connected to the web increases, the threat faced by the network because of attackers also increases. Cryptography, the science of information security derived from the inherent needs of humans to converse and share information or communicate selectively at times, has the primary function of sending correct data over the network without any undesirable modifications. In cryptography, the original message is masked or encrypted by the sender and has to be decoded or decrypted by the receiver using a predefined set of algorithms decided before the commencement of the data transmission. Thereby, successfully avoiding redundant people from accessing or understanding the message as it is converted to content unreadable by the human eye. This paper aims to provide an overview of network security and explore various techniques for enhancing it, particularly focusing on cryptography.

Keywords*: Security, Vulnerabilities, Cryptographic Methods, Encoding, Deciphering*

1. INTRODUCTION

The rapid advancement of modern internet and information technology has led to increased connectivity of individuals, businesses, educational institutions, and government departments to the internet. Consequently, this has attracted a surge in illicit users who employ tactics like fake websites, deceptive emails, Trojan horses, and backdoor viruses to launch attacks and disrupt networks. The primary targets of these attacks are computers, and once infiltrated, they can render thousands of networked computers inoperative. Furthermore, malicious actors with ulterior motives often target military and government entities, posing significant threats to social and national security. Cryptography, derived from the term "Hidden Secrets," revolves around the concept of encryption and secure communication. It plays a crucial role in studying protocols associated with various aspects of information security, including authentication, data confidentiality, data integrity, and non-repudiation. Cryptography is the art of encoding messages in secret code and involves designing and analyzing protocols to thwart adversaries. It addresses essential elements of modern information security, ensuring data remains confidential, intact, and authenticated. A key challenge lies in the effective sharing of encrypted data.

Due to the growing safety concerns with the pandemic, contactless lifestyle with the help of digitalization has been getting a boost now more than ever. Increasing convenience through online services such as e-commerce, e-mail, ebanking, e-schools, e-records, etc. increases the threat of cyber-attacks by illegal users through trojan horses, backdoor viruses, fake websites and emails. The security of the information and network is not

compromised by the study of secure communication. One of the most reliable ways is using Cryptography whose historical roots date back to 2000 B.C. The Greek term Cryptography, originated from 'Krypto' meaning hidden and 'graphene' signifying writing, is the art and science of concealing messages with images, symbols, numbers or alphabets. Here, data is encrypted using the security key which is known only to the respective sender and receiver. Keys can be of two types namely, symmetric key and asymmetric key. Cryptographic goals that are access control, authentication, confidentiality, data integrity and non-repudiation play a major role in modern cryptography. Even though cryptography is extremely useful, it is also considered highly brittle, as cryptographic systems' reliability can be compromised due to a single programming or specification error. CIA Triad is another important concept in cyber security. It stands for confidentiality, indicating only the authorized information is trustworthy and accurate and lastly, availability, meaning that authorized users have access to the systems and the resources they need.

2. IMPORTANT COMPONENTS OF CRYPTOSYSTEM

Cryptography is the process of transforming the secret data or information into an unreadable or scrambled form. Execution of cryptographic techniques and their associated transportation providing security services is known as a cryptosystem or cipher scheme. The various mechanisms of a basic cryptosystem are as follows

(a) Plain text: The initial message or information that we want to send secretly.
(b) Cipher text: It is the scrambled or unreadable form of the initial information or message.
(c) Key: It is the rule used to scramble or unscramble the data.
(d) Encryption Function: It is the method using which the cipher text is generated
(e) Decryption Function: It is the inverse of encryption. It is generation of the original message on the receiver's end.
(f) Encryption Key: The encryption key is inputted in the encrypted algorithm by the sender along with the plaintext to calculate the ciphertext.
(g) Decryption Key: The decryption key and encryption key share a connection but are not identical all the time. In order to compute the plaintext, receiver inputs the decryption key into the decryption algorithm along with the ciphertext.

3. HISTORY

The origin of cryptography or secretive writing can be dated back to the birth of the writing system of humans. As time went by, with evolution in mankind; groups, tribes and kingdoms came into being. This gave rise to power and political conflicts and the need to have confidentiality in the sent messages between kingdoms. Hieroglyph is a 4000-year-old technique developed at the beginning of secretive writing in Egypt where the messenger who would carry the

message on the king's behalf was the only person with the key needed to decrypt the message. Following are a few of the historic cryptographic algorithms.

4. LITERATURE REVIEW:

There is much skepticism surrounding cryptography. Fagin et al. (2008) indicates that there is progress being made in this area to remove the skepticism. The National Institute of Standards and Technology (NIST) has joined forces with the National Security Agency (NSA) to form the "Common Criteria" process known as the Common Criteria for Information Technology Security Evaluation 2005 whose aim it is to increase the confidence in cryptographic and information-related security products. Additionally, the Department of Defense (DoD) has enacted policy directives requiring Information Assurance (IA) professionals to receive information security training in addition to basic IA training for all of its DoD employees (Fagin et al.). Fagin et al. further notes that security today requires some level of skepticism and critical thinking.

Bhargav-Spantzel et al. (2007) contends that there is a recent paradigm in identify management called user-centricity identity management. The study conducted by Bhargav- Spantzel et al. differentiated between two predominant notions: relationship-focused and credential-focused identity management. In the former approach, a user only maintains relationships with identity providers (IDPs) and thus every transaction providing identity information is conveyed to the appropriate IDP. In the latter approach, the user must obtainlong-term credentials and store them in a local provider database.

In the area of wireless security, Tafaroji, & Falahati (2007) proposed a means of improving security of the code division multiple access (CDMA)—one of the most widely used wireless air link interfaces in 3G wireless communication—by applying an encryption algorithm over the spreading codes. In the Tafaroji et al. study the cross-correlation between outputs of encryption algorithm causing multi-user interference was studied thoroughly, since multi-user detection is the inherent characteristic of CDMA. A combination of encrypted and unencrypted M-sequence is used as the spreading code to mitigate system performance.

In the area of chosen ciphertext attacks (CCA), Boneh, Canetti, Halevi, & Katz (2006) proposed a CCA-secure public-key encryption scheme based on identity-based encryption (IBE). These schemes provide for a new paradigm for achieving CCA-security, which avoids "proofs of well-formedness" that was the basis for previous constructions. Furthermore, by instantiating their constructions using known IBE constructions, Boneh et al. was able to obtain CCA-secure public-key encryption schemes whose performance was competitive with other CCA-secure schemes already in existence.

Walters (2007) proposes a draft IS security curriculum that should be incorporated into the core body of knowledge of the business curriculum, and proposes that additional practical guidance to Accounting Information Security (AIS) educators who would like to incorporate IS security into

their existing curriculum needs to be undertaken.

Zanin, Di Pietro, & Mancini (2007) in their study present a new distributed signature protocol based on the RSA cryptographic algorithm, which is suitable for large-scale ad-hocmnetworks. This signature protocol is shown to be distributed, adaptive, and robust while remaining subject to tight security and architectural constraints. The study reveals that the robustness of this protocol scheme can be enhanced by involving only a fraction of the nodes on the network. Zanin et al. demonstrated that their protocol scheme is correct, because it allows a chosen number of nodes to produce a valid cryptographic signature; it is secure, because an attacker who compromises fewer than the given number of nodes is unable to disrupt the service or produce a bogus signature; and it is efficient, because of the low overhead in comparison to the number of features provided.

5. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Encryption and decryption of protected data are typically achieved through two primary techniques: Asymmetric and Symmetric encryption.

Symmetric Encryption

In Symmetric Encryption, the same cryptographic keys are employed for both encrypting plaintext and decrypting ciphertext. Symmetric key encryption is characterized by its speed and simplicity. However, its primary drawback is that both users involved in communication must securely exchange their keys

A single key serves for both the encryption and decryption of data.

Types of Symmetric-Key Algorithms

Symmetric-key encryption employs either stream ciphers or block ciphers. Stream ciphers encrypt individual digits (typically bytes) of a message one at a time.

Block ciphers take a set number of bits and encode them as a single unit, padding the plaintext to match the block size. Historically, 64-bit blocks were common, but the Advanced Encryption Standard (AES) algorithm, approved by NIST in December 2001, and the GCM block cipher mode of operation employ 128-bit blocks.

Asymmetric Encryption

Asymmetric encryption, also known as Public Key Cryptography, utilizes two keys: a public key, known to the public, and a private key, known only to the user.

In Asymmetric key Encryption, two different keys are used for encryption and decryption:

The Public key and the Private key.

Public key encryption involves encrypting message data with a recipient's public key. The message cannot be decrypted by anyone lacking the corresponding private key, which is assumed to be owned by the key's holder. This approach aims to ensure confidentiality.

Digital Signature involves signing a message with the sender's private key and can be verified by anyone with access to the public key, enhancing network security.

AES (Advanced Encryption Algorithm)

AES is an iterated symmetric block cipher characterized by repeating a predefined set of steps multiple times. AES is a symmetric key encryption algorithm operating on fixed-size bytes. With the rapid growth of digital data exchange in electronic communication, data security has become increasingly vital. Cryptography plays a pivotal role in safeguarding information systems against various threats. Two cryptographic methods are utilized: symmetric and asymmetric. This paper focuses on the symmetric cryptographic technique AES (Advanced Encryption Standard), using 200-bit block size and key size, alongside the conventional 128-bit block size. The AES algorithm is implemented using a 5x5 matrix for the 200-bit version. The proposed work is compared to 256-bit, 192-bit, and 128-bit AES systems in terms of encryption and decryption times and throughput on both sides.

Efficient Data Hiding Using AES & Advanced Hill Cipher Algorithm

This paper proposes a data hiding technique using the AES algorithm, combining steganography and cryptography for enhanced security. While cryptography alone cannot provide absolute security, combining it with steganography results in an advanced security solution. Among various cryptography techniques, AES encryption with a 128-bit key is employed to conceal the message. The proposed hybrid scheme, which incorporates the advanced Hill cipher algorithm and AES, enhances security, as indicated by several metrics.

6. CONCLUSION

In today's rapidly evolving digital landscape, network and data security have become essential concerns for any organization with an internal private network connected to the internet. The protection of data has become critically important, particularly when it comes to ensuring user data security in cloud environments. With the advancement of cryptographic techniques and the increasing use of multiple keys for a single application, the field of cryptography has become more flexible and adaptable. As the internet grows, the field of cryptography also grows continuously to provide more secure information transmission to all the users connected all over the world. As we face a constant threat of data integrity being at a risk, organizations consider confidentiality as a vital factor. Cryptography promises a robust, safe and strong network security along with data security. Therefore, development of a secure network for a firm's needs helps the network refrain from the risks it can face in an operational environment. Cryptography continues to emerge as the most powerful medium in the IT industry to provide privacy in e-commerce, medical, personal and financial data. A reliable security policy should ensure data or information confidentiality and authentication with no effect on its availability or integrity. This paper has introduced various cryptographic schemes used for network security purposes. The encryption of messages with highly secure keys, known only to the sender and recipient, plays a significant role in achieving robust security in the cloud. The secure exchange of keys between the sender and receiver is a crucial task, and key management is vital for maintaining the

confidentiality of sensitive information and verifying the integrity of exchanged messages to ensure authenticity

7. REFERENCES

1. *Disha Satyan Dahanukar and Durva Sanjay Shelke "A Review Paper on Cryptography and Network*
2. *Security" Shri Bhagubhai Mafatlal Polytechnic, Mumbai, Maharashtra, India. IJARSCT 2021*
3. *Sachin Ade, Shadab Khan "A Review Paper on Network Security and Cryptography" Jagadambha College Engineering & Technology Yavatmal, Maharashtra, India, IRJETS 2023*
4. *Mitesh Sharma, Review on Cryptography in Network Security, ETRASCT – 2014 (Volume 2 – Issue 03), IJERT, 30-07-2018*
5. *Ritu Pahal, Vikas Kumar, "Efficient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.*
6. *The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China*
7. *Dr. R.K Gupta "A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function" European Journal of Molecular & Clinical Medicine, ISSN 2515-8260, Volume 07, Issue 07, 2020*
8. *Abdalbasit Mohammed Qadir and Nurhayat Varol "A Review Paper on Cryptography" in 7th International Symposium on Digital Forensics and Security (ISDFS), June 2019.*