IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review Paper On Cryptography

D.KALAIVANI
Assistant Professor of Computer Science
Government Arts and Science College
Harur, Dharmapuri (Dt)-636903

Abstract: Data is any kind of digital information that has been stored. Asset protection is the focus of security. Protective digital privacy measures used to stop unwanted access to computers, personal databases, and websites are referred to as data security. Cryptography is constantly evolving. By offering features for encryption of information and verification of identities, secure communication protects users. The process of lowering the quantity of bits or bytes required to represent a specific set of data is known as compression. It enables more data to be saved. One common method for transmitting important information covertly is cryptography. AES represents one of the most powerful methods for cryptography given the many that are available. Today's security of information systems scenario includes confidentiality, authenticity, integrity, and non-repudiation are all part of the modern information security system. One of the most important concerns on the global web is privacy when communicating. When accessing or editing private internal documents, it concerns confidentiality, integrity, and authentication.

Keywords: Compression, Cryptography Concept, Security, Integrity, Data Encryption and Decryption.

I. Introduction

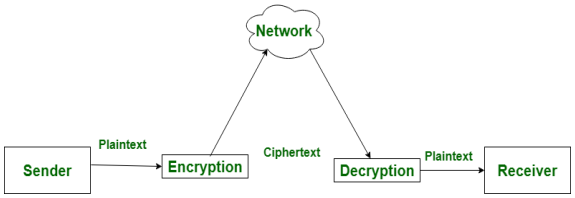
Compression uses less disk space (saving money) and allows for more data to be transferred over the internet, it is used to secure data. It speeds up the movement of data from the disk to the memory. Confidentiality, authenticity, integrity, and non-repudiation are the four security objectives for data security. Enterprise-wide data protection is provided by data security. IT companies of all sizes are becoming increasingly concerned about information security. An increasing number of IT companies are turning to cryptography to address this growing issue and safeguard their sensitive data. Apart from the aforementioned worries about protecting stored data, IT companies are also dealing with the rising storage expenses necessary to ensure that there is adequate storage space to satisfy the organization's present and future needs. It is well known that data compression lowers communication and storage expenses. It entails converting data in a specific format, known as a source message, into data in a smaller format, known as a code word. It is well known that data encryption keeps information safe from prying eyes. Using an encryption key, it converts data in one format known as plaintext to another known as cipher text. At the moment, encryption and compression are done independently.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Since cryptographic algorithms are built on the assumption of computational hardness, it is difficult for an adversary to break them in practice. Modern cryptography is largely based on mathematical theory and computer science practice. Theoretically, such a system could be broken, but there are currently no practical methods for doing so. In the information age, the development of cryptographic technology has brought up several legal concerns. Many governments have classified cryptography as a weapon and restricted or outright banned its use and export due to its potential for use as a tool for espionage and sedition.

II. Cryptography

Encryption- The process of transforming a regular message (plain text) into a meaningless message (ciphertext) is known as encryption. By transforming data into an unintelligible format that only someone with the right decryption key can decipher, encryption can protect data. It is often used to protect sensitive data, such as financial and personal information and online communications.

Decryption- is the process of returning a meaningless message (ciphertext) to its plaintext form. Converting a message into an unintelligible format that cannot be decoded is the primary difference between secret writing and related secret writing. On the other hand, recovering the initial message from the encrypted data is known as secret writing.



III. Types of Cryptography

While hybrid systems like the SSL internet protocols do exist, most encryption techniques fall into one of three categories: hash functions, symmetric cryptography algorithms, or asymmetric cryptography algorithms. 1. Cryptography with Symmetric Keys 2. Cryptography with Asymmetric Keys 3.Hash Functions

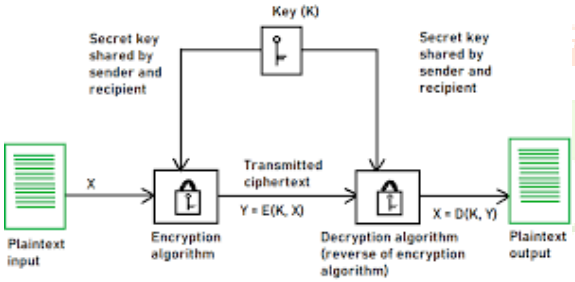


Fig 3.1 Cryptography with Symmetric Keys

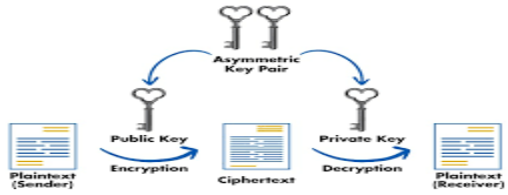


Fig 3.2 Cryptography with Asymmetric Keys

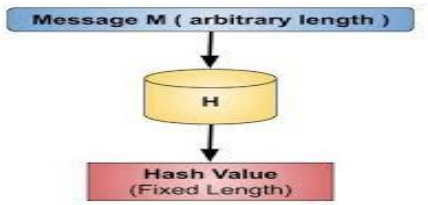


Fig 3.3 Hash Functions

Symmetric Key Cryptography

A single key is used for both the encryption and decryption processes in symmetric key encryption, also known as private key cryptography, secret key cryptography, or single key encryption. In such systems, the same private key must be available to all users[1]. A Diffie-Hellman key agreement or, more precisely, a secure key exchange method, such as a previously established secure communication channel like a private courier or secured line, can be used to exchange private keys.

There are two types of symmetric key algorithms: **Block Cipher:** In a block cipher, a fixed-size block of data is subject to the cipher algorithm. For instance, if the block size is eight, then eight bytes of plaintext are encrypted simultaneously. The encrypt/decrypt process's user interface usually calls the low-level cipher function several times when working with data that is larger than the block size. **Stream Cipher**: Rather than working on a block basis, stream ciphers change data one bit (or one byte) at a time. To put it simply, a stream cipher creates a keystream using a specified key. The generated key stream is then XORed with the plaintext data. Examples of Symmetric Cryptography are DES, Triple DES, Blowfish, and AES. The synchronous stream cipher is the first of two kinds of stream ciphers, where the key stream

depends on the key; however, the cipher text in the asynchronous cipher depends on the key stream.

Asymmetric Key Cryptography

In contrast to symmetric encryption, this type of cryptography uses two keys: one for encryption and another for decryption. These keys don't need to be kept secret because they can be used repeatedly and only once per message. The most popular application of asymmetric key cryptography is in public-key systems. Asymmetric encryption [2] uses two keys: a public key and a secret key. As a result, these algorithms are also known as public key algorithms (PKA). Even though one key is made public, public key cryptography is generally regarded as more secure than symmetric encryption techniques because only the private key of the intended recipient can be used to decrypt an encrypted message. Asymmetric key cryptography has many examples, Rivest, Shamier, and Adleman (RSA), Elliptic curve cryptography (ECC)

Hash Functions

Similar to a unique mathematical function, a hash function transforms an input of arbitrary data—such as text, numbers, or files—into a fixed-length string known as a hash[3]. It can be compared to your data's

fingerprint. Although a hash function can process data of any size, it always produces output with a fixed length. The input is substantially larger than the output. **Collision-resistant**: Every time a piece of data is altered, a new hash is generated to preserve data integrity. **One-way**: It is impossible to reverse this function. A digest must make it impossible to find the original data in order to guarantee data security.

IV. Futures of Cryptography

Quantum cryptography: To keep up with the rapid advancement of technology and the high frequency of cyber attacks, the field of cryptography is constantly evolving. Quantum cryptography, also known as quantum encryption, is the applied science of effectively encrypting and transferring data based on the permanent and naturally occurring laws of quantum physics for use in cyber security. **Post-quantum cryptography:** In contrast to quantum cryptography, which relies on natural laws to construct secure cryptosystems, post-quantum cryptographic algorithms employ a variety of mathematical cryptography techniques to construct quantum computer-proof encryption.

Confidentiality: Information is hidden by cryptography, making it accessible only to those who possess

The proper key.

Integrity: It helps ensure that information remains unchanged during transmission or storage. Additionally, specialized tools are able to detect attempts to alter it.

Authentication: It assists in verifying the identity of those involved in messages or transactions. utilizing tools such as digital signatures and identity verification systems.

Non-repudiation: It prevents people from denying their actions. Similar to sending a message and identifying the sender with special marks.

Access control: It helps protect confidential information by limiting access to specific individuals with designated keys.

V. Applications of Cryptography

Secure Communication: Voice-over-IP (VoIP) calls, instant messaging, and emails are just a few of the communication channels that are frequently secured with cryptography. The confidentiality and integrity of the information exchanged are guaranteed by encrypting the transmitted data, which also stops eavesdropping.

Data protection: It's essential for protecting private information kept on computers, servers, and other electronic devices. By encrypting files, directories, and entire storage volumes, it guards against data breaches and illegal access.

Online Transactions: Cryptography is used in online banking and e-commerce to protect online transactions. It makes it possible to encrypt financial information, such as bank account information and credit card numbers, preventing hackers from intercepting it.

Digital signatures and authentication: It's made possible by cryptography, which enables users to authenticate themselves and confirm the accuracy of digital documents. Cryptographic techniques are used to create digital signatures, which guarantee non-repudiation and the signer's inability to retract their involvement in the transaction.

VI. Compression Technology

By efficiently utilizing available bandwidth, data compression presents an alluring method of lowering communication expenses. In order to reduce the amount of storage needed for that data, compression algorithms eliminate redundancy in the data representation. The amount of digital data such as text, photos, videos, sound, computer programs, etc. Transmitted over the Internet has increased at an unprecedented rate over the past ten years. Sending or storing fewer bits is the idea behind data compression. Data compression is the process of reducing data size to conserve transmission time or space. There are numerous approaches used for this, but they can generally be categorized into two main groups: lossy and lossless approaches[4]. Lossy compression is typically used to reduce the size of an image. Since the compressed and original data are not the same, there is some loss, such as with block truncation coding, transform coding, etc. Any textual data can be compressed using lossless compression.

VI. Uses of Cryptography

Cryptography can;

a. Provide secrecy.

b. Authenticate that a message has not changed in transit.

c. Implicitly authenticate the sender.

d. Hides words

e. Protect ordinary commerce and ordinary people.

f. Hide secrets, either from others, or during communication.

VII. Short-Comings of Cryptography

Cryptography can only hide information after it is encrypted as long as it is encrypted, but it cannot hide:

a. Physical contraband,

b. Cash,

c. Physical meetings and training,

d. Movement to and from a central location,

e. An extravagant lifestyle with no visible means of support, or
f. Actions.
And cryptography simply cannot protect against:
a. Informants,
b. Undercover spying,
c. Bugs,
d. Photographic evidence, or
f. Testimony.

VIII. Conclusion

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] Schneier, B. (1996) Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth), John Wiley & Sons, Inc., New Jersey.
[2] Gupta, R. K. (2020) A Review Paper on Concepts of Cryptography and Cryptographic Hash Function, European Journal of Molecular & Clinical Medicine, 7(7), 3397-3408.
[3] Kumari, S. (2017) Cryptography Encryption and Compression Techniques, International Journal of Engineering and Computer Science, 6(4), 20915-20919. DOI: 10.18535/ijecs/v6i4.20 [20] http://all.net/edu/curr/ip/Chap2-4.html
[4] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf