Role of Encryption/Decryption Key in Cryptography

Meenu[1], Sarbjeet[2]

[1]Assistant Professor, Computer Science, Innocent Hearts Group of Institutions, Jalandhar, India
[2]Assistant Professor, Satyam Inst. Of Mgt & Tech, Nakodar

Abstract

Cryptography is a powerful technique for securing data and communication. cryptography is a technique used to encrypt and decrypt the data. A technique encryption (hiding information) data will be encoded which is used to provide secure data to prevent from fraud user and hackers where decryption is used to convert the encoded data into user readable format. It is used for storage and transmission compression is a reduction in the number of bits needed to represent the data."Cryptography algorithms serve the crucial purpose of safeguarding sensitive data. As the internet has seamlessly integrated into our daily lives, experiencing rapid growth over recent decades, ensuring data security has emerged as a paramount concern for every individual connected to the web.

Data security guarantees that our information remains accessible solely to its intended recipient while thwarting any unauthorized alterations or tampering attempts. Achieving this high level of security necessitates the utilization of diverse algorithms and techniques. Cryptography encompasses methods that encode data through specific algorithms, rendering it indecipherable to the naked eye unless decoded using predetermined algorithms set by the sender.

Keywords: Cryptography, Algorithm, Cipher, Encryption, Decryption, Data Security.

INTRODUCTION

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: “secret writing”."In contemporary times, the safeguarding of both individual and institutional privacy relies significantly on advanced cryptographic methods. These measures ensure that transmitted data remains secure, accessible only to authorized recipients. Despite its historical origins, cryptography persists as an age-old practice continually evolving and refining its techniques."This prevents the loss of sensitive information. Data Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext. Here's a rephrased version: "Symmetric encryption is employed when encrypting larger volumes of data, surpassing a small amount."

Countless individuals worldwide rely on cryptography daily to safeguard their data and information, often unaware of its utilization. Despite its immense utility, cryptography is recognized for its susceptibility, given that a solitary programming or specification mistake can compromise cryptographic systems.

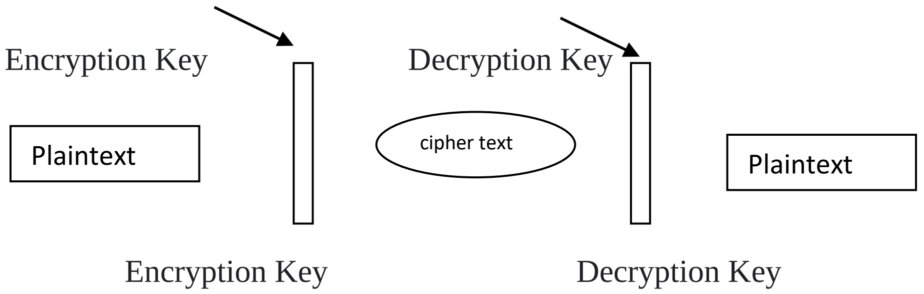
Cryptography Concerns Itself With The Following Four Objectives:

1. **Confidentiality:** The information cannot be understood by anyone for whom it was unintended.
2. **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3. **Non-repudiation:** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.
4. **Authentication:** The sender and receiver can confirm each other's identity and the origin/destination of the information.

CRYPTOGRAPHY:

Cryptography serves as a technique for securing data and communications via encoding, ensuring that only the intended recipients have the ability to access and interpret the information.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.Cryptography not only protects It not only safeguards data against theft or modification but also finds application in user authentication.



Keys In Cryptography: A cryptographic key comprises a sequence of characters utilized in encryption algorithms to transform data, rendering it seemingly random. Similar to a physical key, it encrypts data, permitting only individuals possessing the correct key to decrypt and access it.

Common Terms Used in Cryptography:

Plaintext: The original and understandable text. As an instance, 'Y' needs to transmit a “Computer” message to 'Z'. Here, “Computer” is the plaintext or the original message.

Ciphertext: Gibberish text, like "A@$&J9," refers to text that is unintelligible and incomprehensible to anyone attempting to read it.

Encryption: Encryption involves transforming readable text into an unintelligible format. This transformation relies on an encipherment algorithm and a specific key for the process to take place. Encipherment occurs on the sender side.

Decryption: A reverse method of encode. It is a method of converting ciphertext into plaintext. Key: A key is character, number/special character. It is used at the time of "encoding”on the original text and at the time of decode on the ciphertext.

Cryptography Techniques:

Cryptography is closely related to the specialized fields of cryptology and cryptanalysis. It Comprises techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is mosty associated with scrambling plaintext (ordinary text, sometimes referred to as *cleartext*) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice in this field are known as cryptographers. The basic idea behind cryptography is to use an encryption key to encrypt information so that only those who have access to it can read it.

All other people will see the random letters instead of the original message. To decrypt a message, all you need is the correct key.Cryptography is not limited to computer science or mathematics,it involves mathematics from other fields, such as economics, statistics, and physics etc. It also requires engineering because most cryptographic algorithms are based on mathematical principles such as linear algebra (matrixes) and number theory (arithmetic)etc.

Techniques Used For Cryptography

The most commonly used techniques in cryptography:

- Symmetric Key Cryptography,
- Asymmetric Key Cryptography,
- Hashing,
- Secret Sharing,
- Digital Signatures,
- Elliptic Curve Cryptography,
- Quantum Cryptography,
- Steganography,
- Zero-Knowledge Proofs,
- Homomorphic Encryption.

The two fundamental techniques for encrypting data are "**symmetric cryptography**," which entails the usage of the same key to encrypt/ decode information; and **"asymmetric cryptography,"** which makes use of public and private keys to encrypt/ decode information.

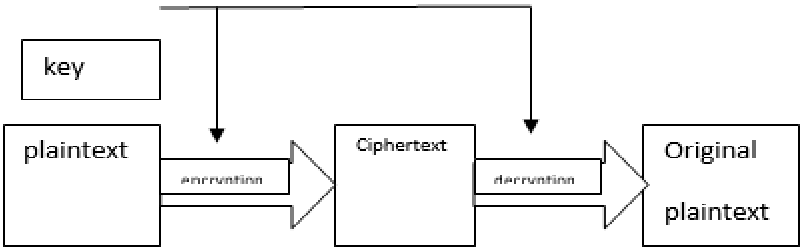


Fig:1. Symmetric cryptosystem

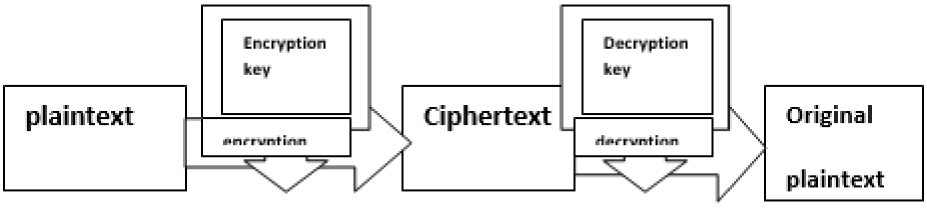


Fig:2. Asymmetric cryptosystem

Uses of Encryption:

Encryption is used to protect data being transmitted. This ensures the data does not fall into the wrong hands of cybercriminals, hackers, internet service providers, spammers, and even government institutions etc. Any time you access ATM or sending the messages across devices such as Snapchat, these messages are encrypted to ensure that no-one other than the person it was sent to can access it.

Examples of asymmetric encryption include RSA(Rivest-Shamir-Adleman) and DSA. RC4 and DES are two instances of symmetric encryption.

Types Of Encryption Systems

- Advanced Encryption Standard (AES)
- Triple DES
- Blowfish
- Rivest-Shamir-Adleman (RSA)

DES, AES, and RSA are the three main encryption types. A more recent 3DES is a block cipher that is still in used in today. The Triple Data Encryption Standard (3DES) are For triple protection, it employs three independent 56-bit keys rather than a single 56-bit key. "Various entities, including governments, security organizations, and businesses, utilize the Advanced Encryption Standard to secure private communications." "Rivest-Shamir-Adleman," or RSA, is another common encryption system.

It is often used to encrypt data transferred over the internet and depends on a public key to do so. Those receiving the data will be given their own private keys to decode the communications.

Applications Of Cryptography:

- **Electronic Commerce:** Cryptography is used in e-commerce to protect data from theft and misuse.Digital signature encryption and authentication protocols secure online transaction etc.
- **Secure Storage:** Encryption is used to store data securely on storage devices like external hard drives, USBs, memory cards, etc.
- **Wireless Network Security**: Cryptography plays a role in safeguarding wireless networks against potential attacks. Its operations include verifying user identities and encoding data transmitted through the internet.
- **Online Banking:** Cryptography is used to secure online banking transactions. Its purpose involves confirming user identities, encoding information, and ensuring secure money transfers.
- **Secure Email:** Cryptography is used to send emails securely. It serves the purpose of verifying users, encoding information, and guaranteeing the secure transmission of emails.

LITERATURE REVIEW

Computer security is a new and fast-moving technology within the computer science field with computer security teaching to be a target that never stop moving. Security courses predominantly concentrate on algorithmic and mathematical components, highlighting areas like hashing techniques and encryption as primary focal points.

As crackers find ways to hack network system new courses are created that latest type of attacks but each of these attacks become outdated daily due to the response from new security software, with the continuous maturity of security terminology security techniques and skills continue to emerge in the practice of business network optimization security architecture and legal foundation.

CONCLUSION:

In this paper it tells about the security of the data by using encryption which translates the data into a secret code. It is the most effective way to achieve data security which access to a secret key or password that enables to decrypt it. Data that hasn't undergone encryption is commonly known as plain text, while encrypted data is typically termed as cipher text.

Cryptography serves to ensure the secrecy, authenticity, and verification of message senders. Its fundamental operations include encryption, decryption, and cryptographic hashing, forming the core functions of ensuring message confidentiality and integrity alongside sender authentication. For data security, cryptographic techniques are used. Encryption acts as a safeguard against unauthorized or fraudulent users.

REFERENCES:

1. A Review Paper on Cryptography Abdalbasit Mohammed Qadir ,Software Engineering Department, Firat University,
2. Elazig, Turkey.
3. Research on Various Cryptography Techniques Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi.
4. A Research Paper On Cryptography Gurdeep Singh1 , Prateek Kumar2 , Nishant Taneja3 , Gurpreet Kaur4 1,2,3b.Tech Student Department Of Mechanical Engineering,Mvsit Sonipat 4asst. Professor Department Of Mechanical Engineering,Mvsit Sonipat Mahavir Swami Institute Of Technology, Sonipat Haryana-131030.
5. https://www.ijcsma.com/articles/information-security-through-compression-and-cryptography-techniques.pdf
6. https://www.researchgate.net/profile/Abdalbasit-Mohammed/publication/334418542_A_Review_Paper_on_Cryptography/links/5db07f61299bf111d4c01521/A-Review-Paper-on-Cryptography.pdf
7. https://www.cloudflare.com/learning/ssl/what-is-encryption/
8. https://www.academia.edu/111610589/A_study_of_data_security_using_cryptography
9. https://www.slideshare.net/ABHIJEETKHIRE/steganography-final-report
10. https://www.simplilearn.com/cryptography-techniques-article