JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

GROUP THEORY AND CRYPTOGRAPHY

Name of Author: DEEPA JAISWAL
Designation of Author: Assistant Professor
Name of Department: Computer Science and Engineering
Name of organization: MANGALAYATAN UNIVERSITY JABALPUR (M.P) ,
City: Jabalpur, Country: India

Abstract*:* Group theory provides a strong foundation for creating efficient and safe cryptography systems. Its use extends to a number of public-key cryptography techniques, including the commonly used RSA and ECC as well as more recent advancements in post-quantum cryptography**.** Groups are a fairly common algebraic object, and they are used in some capacity in most cryptographic techniques. Particularly, finite cyclic groups are used in Diffie–Hellman key exchange. Therefore, cryptographic algorithms that employ infinite non-abelian groups, are primarily referred to as group-based encryption.

Index Terms: Group Theory, Cryptography.

I. INTRODUCTION

Algebraic structure research has significant applications in cryptography, particularly in the development of public-key cryptosystems. In order to provide safe communication while third parties are present, group theory is used in cryptographic methods. Group theory is primarily concerned with structures called groups, which are made up of a set and an operation (such as addition or multiplication) that joins any two components to create a third element that is part of the same set. Closure, associativity, the presence of an identity element, and the existence of inverse elements are the four essential requirements that the operation must meet. Groups offer a foundation for building sophisticated, secure algorithms based on comparatively straight forward algebraic operations in the context of cryptograph. In cryptography, group theory is used primarily in the creation and evaluation of cryptographic algorithms. Additionally, it is employed in the research of error-correcting codes, which are crucial for the storage and transmission of data.

What is a cryptographic algorithm, or cryptography?

The process of encrypting and decrypting data to keep it secret and safe from unauthorized parties is known as cryptography. In order to protect communication, cryptography was initially employed in Ancient Egypt circa 1900 BC, replacing hieroglyphic writing. An algorithm used in cryptography is a mathematical formula that jumbles plain text and renders it unintelligible. They are employed in digital signatures, authentication, and data encryption.

The process of creating and utilizing coded algorithms to conceal and safeguard transmitted data so that only those with the authorization and skills to decrypt it can read it is known as cryptography. Stated differently, communications are hidden via cryptography, making them unreadable by outsiders.

Different Cryptography Types 3

Symmetric and asymmetric encryption are the two basic forms of cryptography. Asymmetric key cryptography and symmetric key cryptography:

Symmetric Encryption: A single shared key is used by symmetric key cryptography for both encryption and decryption. In symmetric cryptography, the secret key is shared by the sender and the recipient of an encrypted message.Symmetric encryption locks and unlocks messages using a single key called a private key. Using this key, the sender can quickly and easily conceal the

message. Additionally, the receiver reads it with the same key. Nonetheless, it might be challenging to safely share the key with the appropriate person; therefore handling it properly is crucial.

Some of the main attributes of symmetric encryption include:

- **Speed:** The encryption process is comparatively fast.
- **Efficiency:** Single key encryption is well suited for large amounts of data and requires fewer resources.
- **Confidential**: Symmetrical encryption effectively secures data and prevents anyone without the key from decrypting the information.

Asymmetric Encryption: One private key and one public key are used in asymmetric cryptography, commonly known as public key cryptography. To decode data encrypted with a public and private key, one needs both the recipient's private key and the public key. Because the public key is only utilized during the encryption process and not during the decryption process, public key cryptography allows for secure key exchange over an insecure medium without requiring the sharing of a private decryption key. This is how asymmetric encryption raises the security ante because a person's private key is never disclosed. Asymmetric encryption locks data with a public key and unlocks it with a private key. The private key encryption needs to be kept confidential, whereas the public key can be shared by everybody. As soon as a message is sent.

Some of the main attributes of symmetric encryption include:

- **Security**: Asymmetric encryption is considered more secure.
- **Robust**: Public key cryptography offers more benefits, providing confidentiality, authenticity and non-repudiation.
- **Resource intensive:** Unlike single key encryption, asymmetrical encryption is slow and requires greater resources, which can be prohibitively expensive in some cases.

Public Key Cryptography: Asymmetric cryptography, sometimes referred to as public key cryptography, creates a pair of keys—a public and private key pair—by means of an asymmetric algorithm for the purpose of encrypting and decrypting messages. Symmetric encryption, which encrypts and decrypts data using a single key, is not the same as public key cryptography. Diffie-Hellman, RSA, and elliptic curve cryptographic systems (ECC) are a few instances of public key cryptography, also known as asymmetric algorithms. Public key cryptography is used by Certificate Authorities (CAs) to issue digital certificates. The virtual keys, or public and private keys, are really big numbers that are used to encrypt and decrypt data. Both sides provide the keys, which are generated by a reliable CA. Typically, the key pair's generator holds the private key.

RSA cryptography: The letters RSA stand for Ron Rivest, Adi Shamir, and Leonard Adleman, who were the ones who initially revealed the method to the world in 1977. The foundation of RSA cryptography is the assumption that factoring large integers (integer factorization) is hard. On the assumption that there is no effective solution for integer factorization, full decryption of an RSA cipher text is considered to be impossible. The public key of an RSA cryptography user is the result of multiplying two huge prime integers by an additional value, which is then made public. The key components need to remain undisclosed. A message can be plausibly decoded by anyone with the prime factors, but anyone can encrypt it with the public key.

Key management and cryptographic keys:

To utilize encryption techniques securely, you need cryptographic keys. A difficult part of cryptography is key management, which includes creating, exchanging, storing, using, destroying, and replacing keys. Using the Diffie-Hellman key exchange technique that is while transferring data over a public network, the Diffie-Hellman algorithm is being used to create a shared secret that may be utilized for private communications. The elliptic curve is being used to produce points and obtain the secret key using the parameters. Cryptographic keys can be safely sent over an open channel. A crucial element of key exchange protocols is asymmetric key cryptography. In symmetric key cryptography, the sender encrypts plain text using a single key that is shared with the receiver.Once the recipient receives the encrypted text, they can use the same key to decrypt it and obtain the sender's plain text back. Public-key or asymmetric cryptography: ECC is an alternative to RSA that can provide the same degree of cryptographic strength at significantly smaller key sizes, improving security while requiring less processing and storage power.

Hash-function: In cryptography, a hash function is similar to a mathematical function that converts different inputs, such as messages or data, into fixed-length character strings. This indicates that while the hash function's output is always a set length, its input can be any length. It's similar to trying to squeeze a big balloon into a little ball. This procedure is significant because it

creates a distinct "fingerprint" for every input. A fingerprint that is significantly altered by even small changes in the input is said to possess "collision resistance." Digital signatures, data integrity checks, and password storage—applications that use hash values rather than actual passwords—all depend heavily on hash functions. A hash function yields values known as hash values, or message digests.

(a) Hash functions are mathematical operations that "map" or change a given collection of data into a fixed-length bit string that is referred to as the "hash value."

(b)Hash functions have a variety of complexity and difficulty levels and are used in cryptography.

(c) Crypto currency, password security, and communication security all use hash functions.

Characteristics of Cryptography

Cryptography ensures that data remains authentic, private, and unaltered while also preventing users from retracting their activities. Finally, the following are some crucial aspects of cryptography:

Confidentiality: Information is hidden by cryptography so that only those possessing the proper key can decrypt it: Integrity: It ensures that information is not altered during transmission or storage. Additionally, specialized instruments can detect any attempts to alter it.

Authentication: It assists in determining the parties to messages or transactions. employing methods such as digital signatures and identity verification systems.

Non-repudiation: It prevents anyone from denying their involvement in an incident. similar to sending a message and utilizing special symbols to identify the sender. Cryptography is used in many different fields to ensure that messages sent by users are secure. Here are a few noteworthy uses:

Secure Communication: Voice-over-IP (VoIP) calls, emails, and instant messaging are just a few of the channels that are protected by cryptography. Transmitting data encrypted protects the integrity and security of the information shared while preventing eavesdropping. Data protection is essential for protecting private information kept on computers, servers, and other electronic devices. It prevents data breaches and illegal access by encrypting files, directories, and entire storage volumes.

Online Transactions: Cryptography is used to safeguard transactions made over the Internet in online banking and e-commerce. It makes financial data, such as credit card numbers and banking credentials, encrypted so they can be shielded.

Cryptography's future:

The field of cryptography is always changing to keep up with the rapid advancements in technology and the sophistication of cyber-attack. The state-of-the-art in cryptography is represented by next-generation advanced protocols like elliptic curve cryptography (ECC) and quantum encryption.

Conclusion:

To sum up, cryptography plays a critical role in protecting our digital data. assisting with safe communication, data protection, and identity verification on the internet. as we become familiar with its various varieties. along with its functions and applications. We can see why, given the digital age we live in today, protecting our personal information is so important.ly allowing specific individuals to access it with unique keys.

REFERENCES:

- Carter, Nathan C. (2009), Visual group theory, Classroom Resource Materials Series, Mathematical Association of America, ISBN 978-0-88385-757-1, MR 2504193
- Cannon, John J. (1969), "Computers in group theory: A survey", Communications of the ACM, 12: 3–12, doi:10.1145/362835.362837, MR 0290613, S2CID 18226463
- Frucht, R. (1939), "Herstellung von Graphen mit vorgegebener abstrakter Gruppe", Compositio Mathematica, 6: 239–50, ISSN 0010-437X, archived from the original on 2008-12-01

- Golubitsky, Martin; Stewart, Ian (2006), "Nonlinear dynamics of networks: the groupoid formalism", Bull. Amer. Math. Soc. (N.S.), 43 (3): 305–364, doi:10.1090/S0273-0979-06-01108-6, MR 2223010 Shows the advantage of generalising from group to groupoid.
- Judson, Thomas W. (1997), Abstract Algebra: Theory and Applications An introductory undergraduate text in the spirit of texts by Gallian or Herstein, covering groups, rings, integral domains, fields and Galois theory. Free downloadable PDF with open-source GFDL license.
- Kleiner, Israel (1986), "The evolution of group theory: a brief survey", Mathematics Magazine, 59 (4): 195–215, doi:10.2307/2690312, ISSN 0025-570X, JSTOR 2690312, MR 0863090
- La Harpe, Pierre de (2000), Topics in geometric group theory, University of Chicago Press, ISBN 978-0-226-31721-2
- Livio, M. (2005), The Equation That Couldn't Be Solved: How Mathematical Genius Discovered the Language of Symmetry, Simon & Schuster, ISBN 0-7432-5820-7 Conveys the practical value of group theory by explaining how it points to symmetries in physics and other sciences.