International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 2, Mar.-Apr. 2023 pp: 229-232 www.ijemh.com

Cryptography for Beginners

Suparnesh Bhattacharyya
[1,2]*Faculty Member, Gobardanga Hindu college, Gobardanga, Westbengal, India*

Date of Submission: 14-04-2023 Date of Acceptance: 29-04-2023

ABSTRACT: The study of secure communication methods that enable information to be sent discreetly between two parties is known as cryptography. Online financial transactions and our personal information are protected by cryptography, a crucial piece of technology. The fundamental ideas of digital signatures, decryption, and encryption are covered in this article's beginner-friendly introduction to cryptography. We'll go over the various varieties of cryptography, such as symmetric key and public key cryptography, as well as popular encryption formulas like AES and RSA. We'll also look at how cryptography protects our online activities, such as banking online and sending secure emails. Readers will have a fundamental understanding of cryptography and its significance in contemporary life by the end of this article.

KEYWORDS: Cryptography, Plain text, Cipher text, Transformation algorithm.

I. INTRODUCTION

Securing communication while third parties are present is done through the use of cryptography. It includes converting plaintext messages into cipher text using mathematical techniques so that they can be sent securely via an unsecured channel. Because it allows for secure online transactions, private chat, and the protection of sensitive data from unauthorised access, cryptography has become an indispensable component of modern life.

Beginners, who are interested in learning about the fundamentals of cryptography, including the various kinds of encryption algorithms, how they operate, and their applications, should read this essay.

1. **Symmetric Encryption**:

The same key is used for both the encryption and decryption of the message in a method of encryption known as symmetric encryption. AES (Advanced Encryption Standard) is the most widely used symmetric encryption method, and it is employed by many businesses to safeguard sensitive data.

Each fixed-length block of the plaintext message is encrypted individually using a secret key in AES. The final cipher text is created by combining the encrypted blocks. The decryption procedure is just the opposite of the encryption procedure; it involves utilising the same key to unlock the cipher text.

2. **Asymmetric Encryption:** Asymmetric encryption, commonly referred to as public-key cryptography, encrypts and decrypts data using a set of two keys: a public key and a private key. While the private key is required for decryption, the public key is utilised for encryption.

The most extensively used asymmetric encryption algorithm is RSA (Rivest-Shamir-Adleman), which is also used for key exchange and safe online transactions. In RSA, the recipient's private key is used to decrypt the message after it has been encrypted using the sender's public key.

3. Hashing: Hashing is a method for examining the message's integrity. The plaintext message is the input to a hash function, which produces a fixed-length output known as a hash value. The hash value is used to confirm that the message was not changed during transmission because it is specific to the input message.

The most well-known hash function is SHA-256, which produces hash values that are 256 bits long. In digital signatures and password storage, hashing is frequently utilised.

.

II Applications of cryptography:

Cryptography has a wide range of uses, such as:

• Secure online transactions: Online payments, e-commerce, and online banking are all protected by cryptography.
• Digital signatures: To confirm the veracity and integrity of digital documents and signatures, cryptography is used.
• Password storage: Passwords are securely stored using cryptography, preventing unauthorised access to important information.

• Key exchange: Parties safely exchange secret keys using cryptography.

[1]Secure online transactions: Online payments, e-commerce, and online banking are all protected by cryptography:

Our daily lives now include secure internet transactions on a regular basis. We depend on the security of our online transactions, whether we are making purchases, paying bills, or transferring money. Our sensitive information is protected by cryptography during online transactions.

Cryptography is used to secure online banking, e-commerce, and payments. The transaction is encrypted using a cryptographic technique when we make an online payment. Our payment information cannot be intercepted or altered during transit thanks to this encryption. Only the intended recipient will be able to access our payment information thanks to the encryption.

Cryptography is also used by e-commerce websites to safeguard user data. The data is encrypted using cryptography when we submit our personal and payment information into an online store. Our information is kept secure and private thanks to this encryption. Digital certificates and digital signatures are also used by e-commerce sites to confirm their validity and make sure we are not connecting with a counterfeit website.

Cryptography is also frequently utilised in online banking to safeguard our financial data. Strong cryptographic techniques are used to encrypt the data when we access our online bank account. Our login information, account information, and transaction data are all secured against unauthorised access thanks to this encryption. Digital certificates and digital signatures are often used by banks to validate their websites and make sure communicating with the genuine website.

To sum up, cryptography is essential for protecting our internet transactions. It makes sure that our private and secure personal and financial data is transmitted. A high level of security is provided and fraud and identity theft are deterred via the use of encryption, digital certificates, and digital signatures. Cryptography will be more and more necessary as online transactions become more common.

[2] **Digital signatures: To confirm the veracity and integrity of digital documents and signatures, cryptography is used:**

Modern cryptography relies heavily on digital signatures because they give us a mechanism to verify the veracity and integrity of digital documents and signatures. Digital data, such as documents, emails, and software code, can be authenticated and its integrity confirmed using a mathematical technique called a digital signature.

Data must first be hashed, or turned into a fixed-length string of characters, in order to establish a digital signature. A digital signature is created once the hash has been encrypted with the signer's private key. The document has a digital signature that can be validated by anybody with access to the signer's public key**.** The hashing operation is repeated on the document during the digital signature verification procedure, and the outcome is contrasted with the initial hash value saved in the digital signature. The document has not been tampered with if the hash values match, and the signature is regarded as legitimate. The document has been altered and the signature is deemed invalid if the hash values do not match.

Several advantages of digital signatures include non-repudiation, integrity, and authentication. Authentication makes ensuring that the identity of the signer is confirmed and that the document is not a forgery. Integrity guarantees that nothing has been changed since the document was signed. In order to prevent the signer from retracting their signature, non-repudiation is used. To verify the integrity and authenticity of digital documents and transactions, digital signatures are frequently employed in e-commerce, banking, legal, and government applications. Software code is also signed using digital signatures to guarantee that it hasn't been altered and is secure to install.

To sum up, digital signatures are an essential part of contemporary cryptography since they offer a mechanism to verify the veracity and integrity of digital documents and signatures. The security of digital transactions is ensured by the widespread usage of digital signatures, which offer authenticity, integrity, and non-repudiation.

[3]Password storage: Passwords are securely stored using cryptography, preventing unauthorised access to important information: A key component of contemporary cyber security is password storage. Users are authenticated using passwords in order to grant access to sensitive data and services like email and online banking. Passwords can, however, be readily stolen or compromised if they are not kept in a safe location, endangering user data and computer systems.

Passwords are securely stored using cryptography, which also prevents unauthorised access to sensitive data. When a user creates a password, the password is first transformed using a cryptographic technique into a fixed-length string of characters. The plain text password is subsequently substituted in a database for the hash value. The user's password is hashed and compared to a value that has been previously stored when they log in. By using cryptographic hashing, it is guaranteed that the attacker will not be able to recover the original password even if the database is hacked. They will only have access to the hash value, which is useless as a login method. Some systems also use additional security safeguards to further increase the security of password storage, such as salting the hash value.
Numerous apps, including online banking, email, and social networking, use cryptographic password storage. However, in order to prevent passwords from being quickly deciphered or guessed, it is crucial to choose strong and original passwords.

[4]Key exchange: Parties safely exchange secret keys using cryptography: Modern cryptography relies heavily on key exchange because it gives two parties a mechanism to securely exchange secret keys without exposing them to unauthorised access. Symmetric encryption techniques encrypt and decode messages using secret keys, guaranteeing that the communication is secure and confidential.
To safely exchange secret keys between two parties, cryptography is utilised. The Diffie-Hellman key exchange, which was initially developed in 1976, is the technique for key exchange that is most Users should also exercise caution when inputting their credentials to make sure they are not entering them into phishing or fraudulent websites. In conclusion, utilising cryptography to store passwords is a crucial component of contemporary cyber security. Passwords are saved securely and cannot be easily cracked thanks to cryptographic hashing, preventing unauthorised access to user data and systems. Users must, however, take precautions to make sure they create secure, one-of-a-kind passwords and use caution while entering them online.

EXPERIMENTATION:

I. Cryptography is the application of mathematical methods to encrypt plain text into a message in order to conduct secure communication in the presence of outsiders.
II.Bengali words and phrases can be encoded using a number of cryptographic methods, such as transposition ciphers and substitution ciphers. While replacement ciphers replace the alphabetic characters with different letters or symbols, transposition ciphers rearrange the letters in the plaintext message.
III. For instance, by replacing each letter in the alphabet with the one that follows it, the Bengali word "Bangla" may be encoded as "Boknog" using a simple

A transposition cypher modifies the letter order of the plaintext message in line with a set of rules.
For instance, the Bengali word "kaj" might be written as "jak" by flipping the letters.
These fundamental encryption techniques are, however, vulnerable to emerging cryptographic attacks that can easily and affordably break them. Modern cryptography uses the advanced algorithms RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) to encrypt data and ensure its security. These algorithms use public-private key pairs and difficult mathematical equations to protect the authenticity, secrecy, and integrity of transmitted data.

WHAT ARE THE RESEARCH AREA IN CRYPTOGRAPHY IN EDUCATION

Particularly in the areas of computer science and information security, cryptography has taken on greater significance in education. There are various cryptography-related study fields in the field of education, including:

1. Cryptography instruction techniques: This field of study focuses on the best methods for teaching the subject of cryptography to pupils. This entails looking into the application of diverse

teaching strategies, including practical projects, interactive learning settings, and game-based learning.

2. Creation of a curriculum for cryptography: The goal of this research is to create a thorough and efficient cryptography curriculum for students at various educational levels. This entails determining the fundamental ideas and abilities that students must master as well as developing teaching strategies and tools that facilitate efficient learning.

3. Encryption assessment and evaluation: Research in this area focuses on creating accurate and valid assessment instruments to gauge how well pupils comprehend encryption. Investigating the use of different assessment techniques, such as written exams, practical exercises, and performance-based evaluations, is part of this.

4. Cryptography and diversity: Research in this area focuses on finding ways to make cryptography more inclusive and accessible to underrepresented groups as well as on boosting diversity in the field of education. This entails looking into the use of culturally sensitive teaching strategies, developing tools and resources that reflect many viewpoints, and tackling prejudices and preconceptions in the teaching of cryptography.

The overall goal of research in cryptography education is to raise the standard of cryptography instruction, boost student engagement and comprehension, and prepare students for careers in cyber security and other related industries.

REFERENCES

[1]. Cybersecurity, Cryptography And Network Security For Beginners: Learn Fast How To Get A Job In Cybersecurity HUGO HOFFMAN **Nov** 2020 · HUGO HOFFMAN · Narrated by Matyas J. and Scott Clem.

[2]. Cryptography and Network Security | 3rd Edition Paperback – 1 January 2015 by Forouzan .

[3]. Handbook of Applied Cryptography, Paul C Van Oorschot, Scoot A Vanstone, A. J. Menezes

[4]. Introduction to Modern Cryptography by Jonathan Katz, Yehuda Lindell

[5]. New Direction on Cryptography, Democratizing Cryptography: The work of Whitfield Diffie and Martin Hellman. August 2022, Page 365-390, https://doi.org/10.1145/3549993.3550007

[6]. R. Merkle, "Secure Communication over an insecure channel" submitted to communications of the ACM [This was subsequently published in volume 21. No .4.pp. 294-299, April.

[7]. A review on steganography and cryptography, Publisher: IEEE, Rina Mishra, Praveen Bhanodiya,

[8]. Published in: - 2015 International Conference on Advances Computer Engineering and Application.