IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOGRAPHIC SECURE HASH ALGORITHM WITH ITS VARIANTS

[1]Laya Rose Joseph, [2]Sreeji S, [3]Aiswarya p s, [4]Sandhya S, [5]Shivam Kumar

[1]Assistant professor, [1]Department of Computer Science, JCT College of Engineering and Technology, Coimbatore, India.

[2]Assistant professor, [2]Department of Computer Science, JCT College of Engineering and Technology, Coimbatore, India.

[3]Assistant professor, [3]Department of Computer Science, JCT College of Engineering and Technology, Coimbatore, India.

[4]Assistant professor, [4]Department of Computer Science, JCT College of Engineering and Technology, Coimbatore, India.

[5]B.E., Final year, [5]Department of Computer Science, JCT College of Engineering and Technology, Coimbatore, India.

ABSTRACT

Today, data privacy is of utmost importance. Everyone is worried about whether their data is secure because there are several online risks, such as phishing scams and data thefts, that attempt to take users' information constantly. In the past, numerous algorithms were employed to protect user data, including Asymmetric Key Encryption, Symmetric Key Encryption, and Transposition Cipher were once common , however they are now antiquated and less safe. Here, we suggest encrypting user data (images, videos, audio files, word documents, and numerous folders) on the user machine using the more secure and modern Secure Hashing Algorithm (SHA-512). A 512-bit encrypted code that is impossible to crack is produced using SHA-512. Because the Secure Hashing Algorithm (SHA-512) offers robust encryption, it is used in many locations, including (BTS), LBRT Credits (LBC), and Android Studio. Additionally, certain websites, as cloud flare, are now offering SHA-encrypted download links to improve user security.

Keywords: Integrity, Secure Hashing Algorithm, Data Encryption, Data Decryption, Cryptography Concept

INTRODUCTION

A way to circumvent limitations on undisclosed messages is through cryptography. Greek gives this term a specific meaning: "hidden communication." However, at this moment, cryptography effectively protects the privacy of individuals and businesses, ensuring that the details of data transferred are encrypted in a way that only the intended recipient can retrieve the details of data [1]. Despite the fact that the majority of users are unaware of it while using it, many people and businesses use cryptography on a daily basis to protect data and its specifics around the world. It is also seen as being overused and extremely delicate since cryptography devices can be compromised by a single programming or instruction error[2].

With ancient origins, cryptography could be nominated as an old approach that's upto this time growing. exemplifications dated in the history as old as 2000B.C., when the early Egyptians espoused " secret " symbols, in addition other attestations like secret dispatches in neolithic Greece or the celebrated Caesar cipher of neolithic Rome[3].

This operation is aimed to give druggies a simple and hassle free platform that they can use to cipher their data fluently to cover their data from unwanted access and theft. thus for this purpose then we're proposing the use of SHA- 512 algorithm, the reason being to keep the data of stoner more defended as it's one of the most over to date algorithm for encryption of data and is hard to decipher if someone unwanted tries to pierce Stoner data. It's part of SHA- 2 family that was published by US, National Security Agency in time 2001.

SHA- 512 is a mincing algorithm grounded on non-linear functions that performs a mincing function on given data, it is designed in similar way that it prevents any system of decryption and uncrackable. Then by performing mincing stoner data is translated in 128 bit hexadecimal characters i.e. 512 bits for illustration- 0123456789abcdef Hashing algorithms help is taken in numerous different disciplines like internet security, digital instruments and blockchain for secured word mincing. mincing functions take stoner data as their input and produce an affair(called hash condensation) of fixed length for the given input data. The affair should, still, satisfy some conditions to be useful which are.[4]

1. Fixed length
2. Collision Resistance
3. Uniform distribution

The work of SHA-512 in few stages. These stages are as follows:

1. Hash buffer initialization
2. Input formatting
3. Message processing
4. Output

III. RELATED WORK

Being system was suitable to cipher the data with 160- bit which is easy to break using brute force approach and the train size was limited due to limitation of train size originally we compress the data also cipher the train. In Being System only one type train at a time of encryption is possible. It wasn't suitable to perform confirmation scan and display the type of data during the uploading session. It wasn't suitable to produce multiple virtual drives and can produce a single virtual drive only under the desktop or laptop and not to other removable media.[5]

By running security audits here while running the encryption and decryption operations on the documents. By employing this SHA, which generates 512-bit, it is considerably larger than the current system, and because the combination produced by SHA-512 is 2^256, it is impossible to break the file. The size of the file is irrelevant on the current system while executing the encrypt and decrypt action. The users can encrypt and decrypt the file in about 5 seconds. With a single click, it supports many file kinds with the same encryption. The file is irreversibly ruined if someone attempts to decode it without using the right key by changing its extension.[6]

IV. TERMINOLOGY OFCRYPTOGRAPHY

Encryption:- By encryption, we imply the process of executing information concealment in a way that only a person with the appropriate key may decode and read the information. The function of encryption is two-way. Users encrypt data with the understanding that they will also need to decode it in the future.

Decryption:- By decryption we understand the conversion of the data that is encrypted to keep it safe, in the data is not in readable format and it has to be decrypted to read it. It is comparable to a coded message that must be cracked to reveal the original message that is meant to be read by a particular person or people. It employs the idea of a secret key or password to decode or decrypt the file; without it, it cannot be opened, and if it is attempted to open the file forcibly, it will become permanently ruined.[7]

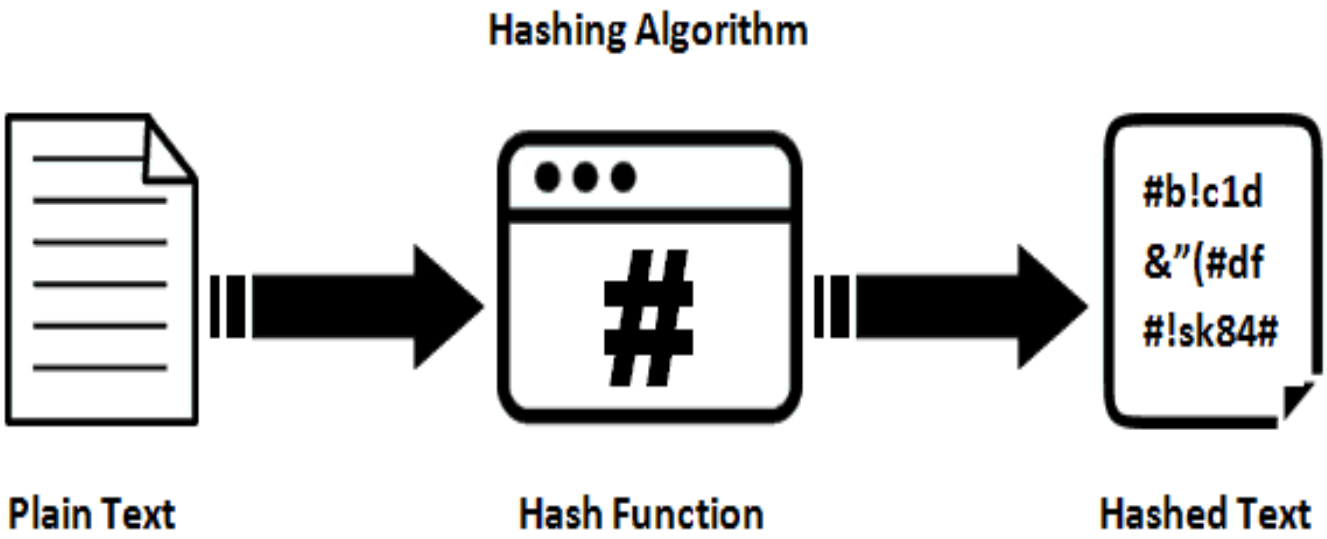
Hash:- The hash algorithm converts inputted data into a numerical string of a set length through the use of mathematics. So, using an example will help us better understand how hashing works.

"The Quick Brown Fox Jumps Over The Lazy Dog"
Now, if we run this via the crc32 hashing method, we will receive the result "07606bb6."
The outcome is referred to as a hash or hash value. Hash is occasionally referred to as one-way encryption.[8]

Asymmetric encryption:- This is the example of Public key, In which the one key encrypt the message while other decrypt the message. The encryption only goes one way. This idea serves as the cornerstone of PKI (public key infrastructure), the trust architecture that supports SSL/TLS.

Symmetric Encryption:- This is similar to the create a private key encryption, In which both party have own key for encryption and decryption. The browser and server communicate using the symmetric session key that is passed along after the symmetric encryption that takes place in the SSL handshake, as we mentioned in the example above.

Hashing:- Hashing is the process of mapping data of any size to a predetermined length using an algorithm. This is known as a hash value (or, if you're feeling sophisticated, a hash code, hash sum, or even a hash digest). Hashing is a one-way function as opposed to encryption, which is a two-way function. Although it is theoretically possible to reverse-hash something, the necessary computational power makes it impractical. One-way hashing.[9]



V. PROPOSED ARCHITECTURE

We will now go over the project's stages for both the encryption and decryption of the file. The classification of project execution steps is :-

1. **For Encryption:-**

- choose it (from among images, videos, audio files, word documents, and multiple folders).
- Give the password
- Verify this password using SHA-512
- Generate key of 128-bits
- Selected file is encrypted

2. **For Decryption:-**

- choose it (from among images, videos, audio files, word documents, and multiple folders).
- Give the password
- Verify key of given password
- Compare the keys of the two hashes.
- If it matches, the file will be decrypted otherwise an error message will appear.

VI. RESULTS

PIYUSH GUPTA AND SANDEEP KUMAR	2014	A Comparative Analysis of SHA and MD5 Algorithm	After comparison, it was discovered that SHA offered greater security than MD5, but that MD5 was faster on 32 bit platforms.

Based on the findings of the study and the debate, it can be said that the Secure Hashing Algorithm is more sophisticated than other cryptographic operations. After learning more about the SHA family of algorithms, we can say that SHA-512 is the most secure method for encrypting user data. Transposition cyphers, another cryptographic function, are insecure and unusable for encrypting sensitive data. To ensure data confidentiality and system security, the SHA 512 algorithm implementation method generates the longest number of bits possible from 512 bits. Penetration The SHA 512 method is superior in terms of endurance and strength for brute force testing, according to tests using the Hash-cat programme. This is because it takes the algorithm a longer time to find the plaintext of the hash value, showing that the hash function is more dependable and resilient. It generates 2256 combinations with a length of 512 bits that are impossible to crack. This method is used in Blockchain as well due to its high level of security.

Author	Year of publication	Title	Outcome
ABDALBA SIT MOHAMMED AND NURHAYAT VAROL	2019	A Review Paper On Cryptography	In this article, the idea of cryptography was covered along with its history, the always changing requirements for algorithms, and their role in digital security. Here, some ancient algorithms, like the Caesar cypher, stream cyphers, simple substitution cyphers, transposition cyphers, and recent hash algorithms, were also covered.
Dr. R.K Gupta	2020	A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function	Here, we noted several attributes and features of various hashing methods. We noticed the DES, RSA, MD, and SHA families. Additionally, we looked at the fundamentals of cryptography and the many kinds of keys that are employed in encryption. Here, flaws or restrictions of many algorithms were also examined, such as how DES is unsuitable for encrypting sensitive data and how choosing large p and q in RSA can be challenging.

ARADHAN A SAHU AND SAMARENDRA MOHAN GHOSH	2017	A review paper on secure hash Algorithm with its variant.	On a variety of criteria, the SHA family's several secure hash algorithms were compared to show how they differ from one another in terms of design and operation. SHA-O, SHA-1, SHA-2, and SHA-3 compared in this. Here, we also explored the innovative hash algorithms SHA-256 and SHA-512. The methods by which different hash algorithms operate and their differences from one another
PIYUSH GARG AND NAMITA TIWARI	2012	Performance Analysis of SHA Algorithms (SHA 1 and SHA-192): A Review	Here, it was determined that SHA-160 and SHA-192 are superior in their respective fields following comparison. When compared to the number of brute force attacks required to crack it, SHA-192 is more secure, and SHA-160 has been shown to be faster than other SHA algorithms.

VII. CONCLUSION

Everything you need to know about cryptography and hashing techniques is contained in this research paper. The completion of the main objectives to safeguard data's authenticity, integrity, and confidentiality depends critically on cryptography. The algorithms used in cryptography are designed to help one achieve their objectives. The computation of the hash price requires time due to the set of regulations. To protect personal, financial, medical, and e-commerce information and to offer a respectable level of privacy, cryptography will continue to advance with IT and business objectives. We want to expand on this work by building web and Android applications and altering the user interface to suit our requirements. This research study contrasts various secure hashing methods and their variations. Each algorithm requires time to calculate the hash value. by calculating the amount of time needed for each of these algorithms, then selecting the one that would compute the hash value in the shortest amount of time.

VIII. REFERENCE

1. (2014, Mar.). Keccak Website [Online]. Available: http://keccak. noekeon.org/
2. “SHA-512 Hash in Java | Geeks-For-Geeks " SHA-512 Hash in Java
3. M. Mozaffari-Kermani , M. Zhang, A. Raghunathan, and N. K. Jha ,"Emerging frontiers in embedded security," in Proc. Conf VLSI Design, Jan. 2013, pp. 203-208
4. D.-J. Bernstein and T. Lange. (2012). The new SHA-3 software shootout.e-Print [Online] Available: http://eprint.iacr.org/2012/004.pdf
5. (2014, Mar.). Keccak Website [Online]. Available: http://keccak. noekeon.org/
6. C.G Thomas and Robin Thomas Jose.2015. A Comparative Study on Different Hashing Algorithms. Vol. 3, Special Issue 7, October 2015. ISSN(Online): 2320-9801. https://www.ijircce.com/special-issues/pdf/2015/october/30_212.pdf
7. Piyush Garg, Namita Tiwari. 2012. Performance Analysis of SHA Algorithms (SHA -1 and SHA-192):A Review . http://www.ijctee.org/
8. Keccak Hash Function, NIST (National Institute of Standards and Technology),(2014, Mar.) [Online]. Available: http://csrc. nist.gov/groups/ST/hash/sha-3.
9. Saeid Nourizadeh and Mojtaba Javanmardi, "Cryptanalysis of the Reduced-Round Version of JH," iEEE 6'h international Symposium on Telecommunications (iST'2012).
10. Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. (7 December 2018). "Hash functions". *Handbook of Applied Cryptography*. CRC Press. pp. 33–. ISBN 978-0-429-88132-9
11. Cryptography and hash function | https://en.wikipedia.org/wiki/ Cryptographic_hash_function
12. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
13. https://brilliant.org/wiki/secure-hashing-algorithms/

14. Meiliana Sumagita, Imam Riadi.2018.Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 373-381The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001
15. Fatma Kahri , Belgacem BoualJegue, Mohsen Machhout and Rached Tourki, "An FPGA implementation of the SHA-3 : The Blake hash Function," IEEE 2013 JO'h international MultiConference on Systems, Signals & Devices (SSD) Hammamet, Tunisia, March 18-21,2013
16. media, w. *Hash Function*. Retrieved June 25, 2016, from https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Hash_function.svg/2000px-Hash_function.svg.png
17. Forum, G. *Intent to Deprecate: SHA-1 Certificates*. Retrieved June 25th, 2016, from https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/2-R4XziFc7A%5B101-125%5D