e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:12/December-2021 Impact Factor- 6.752 www.irjmets.com

A CRITICAL REVIEW ON CRYPTOGRAPHY AND HASHING ALGORITHM SHA-512

Jai Verma*1, Md Shahrukh*2, Mukul Krishna*3, Ruchi Goel*4

*1,2,3,4MAIT Department Of Computer Science Engineering, Delhi, India

ABSTRACT

Data privacy plays a very important role today. All people are concerned about whether their data is safe or not because there are multiple threats online from phishing scams to data thefts, which continuously try to steal users' information. There were many algorithms that were previously used to secure user data like Transposition Cipher, Symmetric Key Encryption and Asymmetric Key Encryption but now they are outdated and less secure. Here we propose to use a more secure and up to date, Secure Hashing Algorithm (SHA-512) to encrypt user data (Image, video, audio, word file, multiple folders) in the user system. In SHA-512 ,512 bits encrypted code is generated which is not possible to break. Because of Secure Hashing Algorithm (SHA-512) providing strong encryption it is used in various places like (BTS), LBRT Credits (LBC) and android studio while some websites are also now providing SHA encrypted download links to provide better security to their users like cloud flare.

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

I. INTRODUCTION

Cryptography is a manner to reach restrictions of undisclosed messages. This phrase has a particular sense in Greek: “secret message”. In present time , however, the privateness of persons and corporations is delivered through cryptography at an effective measure ,ensuring that particulars of data transmitted is secured in such a manner that only the intended receiver can retreive the particulars of data [1]Everyday around the globe many individuals and corporations make utilize cryptography on an everyday basis to safeguard particulars of data and its details, in spite of the fact that most users don't realise it while making use of it. Furthermore being considered of excessive use , it is regarded highly delicate, as cryptography machines can be jeopardized due to a single programming or instruction error.[2]

With ancient origins, cryptography could be termed as an old approach that is upto this time maturing. Examples dated in the past as old as 2000 B.C., when the early Egyptians adopted “secret” symbols, in addition other proofs like secret messages in prehistoric Greece or the famed Caesar cipher of prehistoric Rome [3].

This application is aimed to provide users a simple and hassle free platform that they can use to encrypt their data easily to protect their data from unwanted access and theft .Therefore for this purpose here we are proposing the use of SHA-512 algorithm, the reason being to keep the data of user more protected as it is one of the most up to date algorithm for encryption of data and is hard to decrypt if someone unwanted tries to access user data. It is part of SHA-2 family that was published by US, National Security Agency in year 2001.

SHA-512 is a hashing algorithm based on non-linear functions that performs a hashing function on given data, it is designed in such way that it prevents any method of decryption and uncrackable. Here by performing hashing user data is encrypted in 128 bit hexadecimal characters i.e 512 bits for example - 0123456789abcdef Hashing algorithms help is taken in many different domains like internet security, digital certificates and blockchain for secured password hashing. Hashing functions take user data as their input and produce an output (called hash digest) of fixed length for the given input data. The output should, however, satisfy some conditions to be useful which are .[4]

1. Uniform distribution:
2. Fixed Length
3. Collision resistance

SHA-512 does its work in a few stages. These stages go as follows:

1. Input formatting
2. Hash buffer initialization

3. Message Processing
4. Output

II. RELATED WORK

Existing system was able to encrypt the data with 160-bit which is easy to break using brute force approach and the file size was limited due to limitation of file size firstly we compress the data then encrypt the file. In Existing System only one type file at a time of encryption is possible. It was not able to perform validation checkup and display the type of data during the uploading session. It was not able to create multiple virtual drives and can create a single virtual drive only under the desktop or laptop and not to other removable media.[5]

By performing security checkups here that are performed while performing operation of encryption and decryption of documents. By using this SHA, which generates 512-bit it is much larger than the existing system and so it is not possible to break the file because the combination generated by SHA-512 is 2^256. Here in the present system file size does not matter while performing the encrypt and decrypt action . It takes merely 5 secs for the users to encrypt as well as decrypt the file. It supports multiple types of files within the single click with the same type of Encryption. If anyone tries to decrypt the file without using the correct key by changing its extension, then the file is corrupted permanently.[6]

III. TERMINOLOGY OF CRYPTOGRAPHY

Encryption:-By encryption we mean the execution to conceal information in such a method that only the user who has a corresponding key can decrypt and read the information. Encryption is a two-way function. When users are encrypting some data , they're doing it with keeping in mind that they have to decrypt the data later.

Decryption:- By decryption we mean the conversion of the data that is encrypted to keep it safe, in encrypted extension the data is not in readable format and it has to be decrypted to read it. It is just like the coded message which has to be deciphered to get the original message that is intended to be read by specific person/persons. It uses the concept of a secret key or password to decode/decrypt the file, without it the file can not be opened and if tried to be opened forcefully it will be corrupted permanently[7]

Hash:- Hash algorithm is an arithmetical operation that performs the conversion of given data into a numerical fixed length size. So, if we take an example, for better understanding on how hash works…

"The Quick Brown Fox Jumps Over The Lazy Dog"

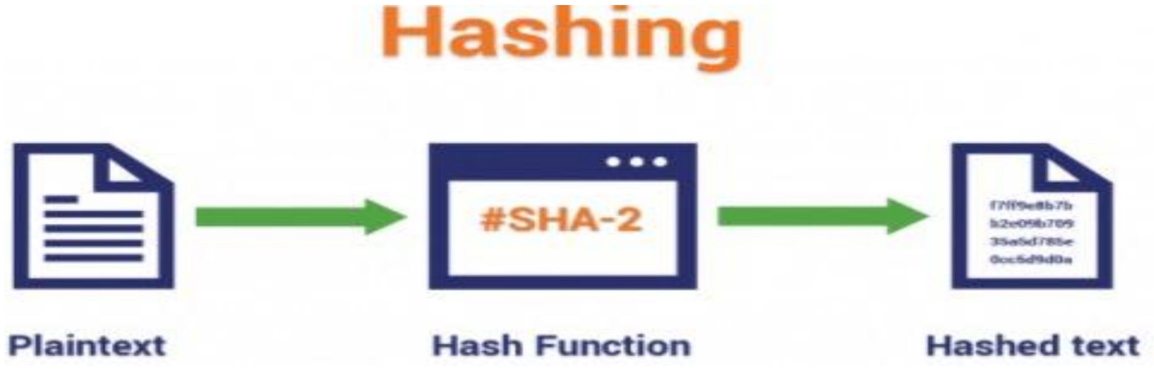
Now if run this into a specific hash algorithm called crc32 we will get: "07606bb6"

The result is called a hash or hash value. Occasionally hash is also called 1 way encryption.[8]

Asymmetric encryption – This is the Public Key example we just gave. One key encrypts the other key decrypts. The encryption only goes one way. This is the concept that forms the foundation for PKI (public key infrastructure), which is the trust model that undergirds SSL/TLS.

Symmetric Encryption – This is closer to a form of private key encryption. Each party has its own key that can both encrypt and decrypt. As we discussed in the example above, after the a symmetric encryption that occurs in the SSL handshake, the browser and server communicate using the symmetric session key that is passed along.

Hashing:- Hashing is the practice of using an algorithm to map data of any size to a fixed length. This is called a hash value (or sometimes hash code or hash sums or even a hash digest if you're feeling fancy). Whereas encryption is a two-way function, hashing is a one-way function. While it's technically possible to reverse-hash something, the computing power required makes it unfeasible. Hashing is one-way[9]



IV. PROPOSED ARCHITECTURE

Now we will describe the steps of the project that how the file is encrypted and how the file is decrypted. Classification of steps during execution of projects are-

1- For Encryption-

- Select the file(Image, video, audio, word file, multiple folders)
- Enter the password
- Pass this password through SHA-512
- Generate key of 128-bits
- File is Encrypted

2- For Decryption

- Select the file(Image, video, audio, word file, multiple folders)
- Enter the password
- Generate key of Given Password
- Match the key of both hashes
- If it is Matched, the file will be decrypted or it will show an error message

V. RESULT

Based on the results of research and discussion it can be concluded that the Secure Hashing Algorithm is advanced than other cryptography functions and after researching more about SHA family functions we can here conclude that SHA-512 is the most secure option to encrypt user data. The other cryptographic function like transposition cipher lacks security and are not viable to encrypt sensitive data.. Implementation of the SHA 512 algorithm method produces the longest number of bits of 512 bits so as to ensure system security and data confidentiality. Penetration Testing against Brute Force attacks using the Hashcat tool indicates that the SHA 512 algorithm is better in terms of endurance and strength for brute force testing because it has longer time to find the plaintext of the hash value of the algorithm thus indicating that the hash function is more reliable and robust. It produces the length of 512-bits hash Size and makes 2^256 combinations which are not possible to break. Due to high security this algorithm is also implemented in Blockchain .

Author	Year of publication	Title	Outcome
ABDALBA SIT MOHAMM ED AND NURHAYAT VAROL	2019	A Review Paper On Cryptograph y	Here the concept of cryptography was discussed with its history and ever changing need of algorithms and their need in digital security. some historical algorithms were also discussed here like caesar cipher, simple substituition ciphers, transposition ciphers, stream ciphers and modern hash algorithms

Dr. R.K Gupta	2020	A Review Paper On Concepts Of Cryptograph y And Cryptograph ic Hash Function	Here we observed different properties, characteristics of different hashing algorithms. we observed DES,RSA,MD family and SHA family. we also observed the basic concept of cryptography and different type of keys used for encryption. Shortcomings or limitations of different algorithms were also discussed here as DES is not viable for encrypting sensitive data while in RSA it is difficult to decide large p and q
ARADHAN A SAHU AND SAMAREN DRA MOHAN GHOSH	2017	A review paper on secure hash algorithms with its variants	Different secure hash algorithms from the SHA family were compared on different parameters and how they differ from each other in respect of their construction and working was observed. SHA-0,SHA-1,SHA-2,SHA-3 were compared here.SHA-256 and SHA-512 novel hash algorithms were also discussed here. Working of hash algorithms differ from each other and they work on different principles
PIYUSH GARG AND NAMITA TIWARI	2012	Performance Analysis of SHA Algorithms (SHA - 1 and SHA-192): A Review	Here after comparison between SHA-160 and SHA-192 it was concluded that they are better in their respective field. SHA-192 is more secure when it was tested against the number of brute force attacks that were needed to break it and SHA-160 was proven to be fast when it was compared with other SHA algorithms
PIYUSH GUPTA AND SANDEEP KUMAR	2014	A Comparative Analysis of SHA and MD5 Algorithm	After doing comparison here it was found that SHA provided more security than MD5 but MD5 was faster than SHA on 32 bit machines

VI. CONCLUSION

This research paper consists of all the information about Cryptography and Hashing algorithms. Cryptography perform crucial role in the accomplishment of primary goals to protect, authenticity integrity and confidentiality of data. In Cryptography the algorithms are developed in such a way to obtain one's goals. The set of rules takes the time for the computation of hash price. Cryptography will keep emerging with IT and commercial enterprise plans in regard to protecting private, monetary, medical, and e-trade information and providing a decent degree of privateers. We would like to extend this work to variations by creating android based applications and web applications making changes in UI according to our needs. This research paper consists of comparisons between different secure hashing algorithms and its variants. Each algorithm takes the time for the computation of hash value. By computing the time required from each of these algorithm and finding the algorithm which will require the less amount of time for computation of the hash value.

VII. REFERENCE

[1] Abdalbasit Mohammed, Nurhayat Varol.2019. A review paper on cryptography. DOI:10.1109/ISDFS.2019.8757514,

[2] https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography

[3] J. Katz and Y.Lindell. 2008. Introduction to Modern Cryptography, London: Taylor &Francis Group, LLC, 2008.

[4] B. Prenee.2010., Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[5] 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

[6] "Symmetric Cryptography | Science

[7] Direct."|https://www.sciencedirect.com/topics/computer-science/symmetric-cryptography

[8] Aradhana sahu, Samarendra Mohan Ghosh.2017.A review paper on secure hash algorithms with its variants

https://www.researchgate.net/publication/326009898_Review_Paper_on_Secure_Hash_Algorithm_With_Its_Variants

[9] "Cryptography Tutorial | Tutorial point." Cryptography Tutorial |

https://www.tutorialspoint.com/cryptography/index.htm

[10] William Stallings "Cryptography and Network Security — Principles and Practise",

[11] Pearson Education Limited 2017

[12] "SHA-512 Hash in Java | GeeksforGeeks " SHA-512 Hash in Java |

[13] https://www.google.com/amp/s/www.geeksforgeeks.org/sha-512-hash-in-java/amp/

[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] https://www.researchgate.net/publication/327392778_Analysis_of_Secure_Hash_Algorithm_SHA_512_for_Encryption_Process_on_Web_Based_Application

[16] Dr. RK. Gupta. 2020 . A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function. European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 07, 2020.

[17] https://ejmcm.com/pdf_5157_596c1024e1fb468438347e8ab5322db2.html

[18] Piyush Garg, Namita Tiwari. 2012. Performance Analysis of SHA Algorithms (SHA -1 and SHA-192):A Review . http://www.ijctee.org/

[19] Piyush Gupta and Sandeep Kumar. 2014. A Comparative Analysis of SHA and MD5 Algorithm. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4492-4495

[20] https://www.academia.edu/7330547/A_Comparative_Analysis_of_SHA_and_MD5_algor ithms

[21] "Cryptography Functions | Microsoft." Cryptography Functions| https://docs.microsoft.com/en-us/windows/win32/seccrypto/cryptography-functions