International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 2, January-February 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Survey on Encrypted and Decrypted Text Algorithm Using CRC, SHA-256, MD5 and Caesar Cipher

Raghini Sharma[1], Dr. Umarani Chellapandy[2]

[1]Student, [2]Professor,
[1,2]Department of MCA, Jain Deemed-to-be-University, Bangalore, Karnataka, India

ABSTRACT

In this advanced universe of correspondences, cryptography has a significant job in the security of information transmission and is the best strategy for information security against detached and dynamic misrepresentation. Cryptography is an algorithmic cycle of changing over a plaintext or clear text message to a ciphertext or cipher message in view of a calculation that both the sender and beneficiary know. There are various calculations for performing encryption and decryption, however similarly scarcely any such calculations have stood the trial of time. The best calculations utilize a key. Encryption is the way toward interpreting plain content information (plaintext) into something that gives off an impression of being irregular and pointless (ciphertext). Decryption is the way toward changing over ciphertext back to plaintext. In this paper, we may gain knowledge about cryptography algorithms and their role in Encryption and Decryption. This paper performs near examination of Four calculations.

KEYWORDS: *CRC, MD5, SHA-256 and Caesar Cipher*

How to cite this paper: Raghini Sharma | Dr. Umarani Chellapandy "A Survey on Encrypted and Decrypted Text Algorithm Using CRC, SHA-256, MD5 and Caesar Cipher" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-2, February 2022, pp.1366-1369, URL: www.ijtsrd.com/papers/ijtsrd49436.pdf

IJTSRD49436

INTRODUCTION

A plaintext message can be hidden in one of the ways. The techniques of steganography hide the life of the message, while the techniques of cryptography render the message unintelligible to outsiders through diverse ameliorations of the textual content. Cryptography is extra directed to the encrypted message whilst steganography is extra directed on the hidden message. However, each techniques have the identical goal, it's far a mystery message. This is feasible due to the fact generally, a textual content message unreadable offers a person suspicion that the textual content message includes a positive that means for the proprietor of the message. Cryptography allows you to shop touchy records or transmit it throughout insecure networks in order that it cannot be study through all people besides the supposed recipient. Accordingly, the cryptanalyst tries to interrupt the encrypted message. A easy shape of cryptography, however one this is time-eating to construct, is one wherein an association of phrases or letters inside an reputedly harmless textual content spells out the actual message.

Plaintext – data that may be immediately examine through human beings or a machine. Plaintext is an anciental time period pre-relationship pc, whilst encryption became simplest used for hardcopy text, in recent times its miles related to many codecs together with music, films and pc programs.

Ciphertext – the encrypted data

A Cipher – the mathematics (or algorithm) liable for turning plaintext into ciphertext and reverting ciphertext to plaintext (you would possibly additionally see the word 'code' used – there may be a technical distinction among the 2 however it wants now no longer issue us now)

Encryption – the procedure of converting plaintext to ciphertext.

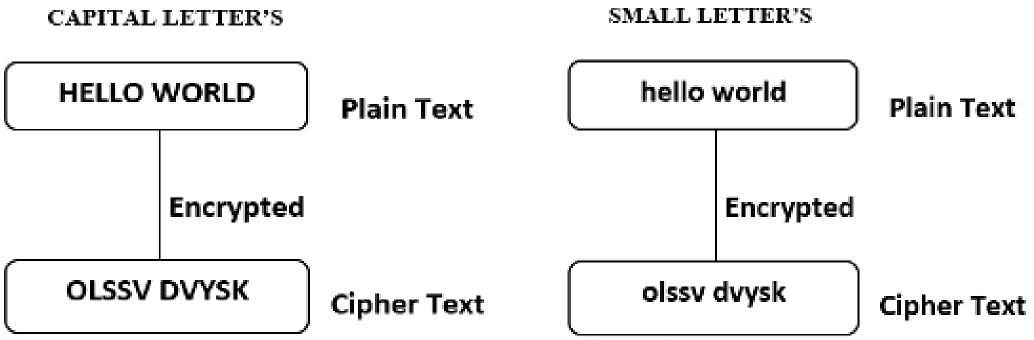
Decryption – the procedure of reverting ciphertext to plaintext.

Key -a few mysteries piece of data.

A. Caesar Cipher:

The Caesar Cipher strategy is one of the earliest and most straightforward techniques for encryption procedures. It's essentially a sort of replacement figure, i.e., each letter of a given message is supplanted by a letter with some decent number of positions down the letters in order. For instance, with a shift of 1, A would be supplanted by B, B would become C, etc. The technique is obviously named after Julius Caesar, who evidently utilized it to speak with his authorities. Accordingly, to encode a given text we really want a number worth, known as a shift which shows the quantity of position each letter of the text has been dropped down. The encryption can be addressed utilizing particular math by initial changing the letters into numbers, as indicated by the plan, A = 0, B = 1…, Z = 25. Encryption of a letter by a shift n can be depicted numerically.

In Caesar Cipher when any text is written in Small Alphabet, the decrypted text will be in the smaller letter and if it's written in Capital Alphabet the decrypted text will be in Capital Latter's too



When a Plaintext is written in both capital as well as the small letter's then the Encrypted letters will combination of both. For example, if "Hello World" is written using both Alphabet then the Encrypted Hash Value will be "OlssvDvysk" and if plaintext "Hello@123World" will be in Symbols and Alphanumeric characters then the Encrypted hash value will be "Lipps@123Asvph" where only Alphabet letters have Hash Value but Numbers and Symbols remain same.

B. CRC Algorithm:

Cyclic Redundancy Check (CRC) is a square code that was created by W. Wesley Peterson in 1961. It is regularly used to identify inadvertent changes to information sent through broadcast communications organizations and capacity gadgets. CRC includes paired division of the information pieces being sent by a foreordained divisor settled upon by the conveying framework. The divisor is produced utilizing polynomials. Along these lines, CRC is additionally called polynomial code checksum. Prior to sending the message over network channels, the shipper encodes the message utilizing CRC. The recipient disentangles the approaching message to recognize the blunder. In the event that the message is sans mistake, it is acknowledged, in any case, the beneficiary requests re-transmission of the message.

E.g., Plaintext: Hello World

Ciphertext: da895c06

In Cyclic Redundancy Check (CRC) plaintext is Encrypted not only in small or capital Alphabets but CRC uses combinations of Alphanumeric Characters whether the plaintext is in Symbols and Characters.

C. MD5 Algorithm:

MD5 (Message Digest Method 5) is a cryptographic hash calculation used to create a 128-digit digest from a line of any length. It addresses the summaries as 32-digit hexadecimal numbers. Ronald Rivest planned this calculation in 1991 to give the means to computerized signature checks. Ultimately, it was incorporated into different structures to support security files. The review size is consistently 128 pieces, and gratitude to hashing capacity rules, a minor change in the info string creates a radically unique summary. This is fundamental to forestall comparable hash age however much as could be expected, otherwise called a hash impact.

E.g., Plaintext: Hello123World

Ciphertext:10efb8334e8191f4a42fc9aef2897d82

The Ciphertext presented in MD5 and CRC uses both Alphanumeric Characters but the Encrypted text does not use capital letters even though Plain Text is in the form of small letters, Capital letters as well as Numbers.

D. SHA -256 Algorithm:

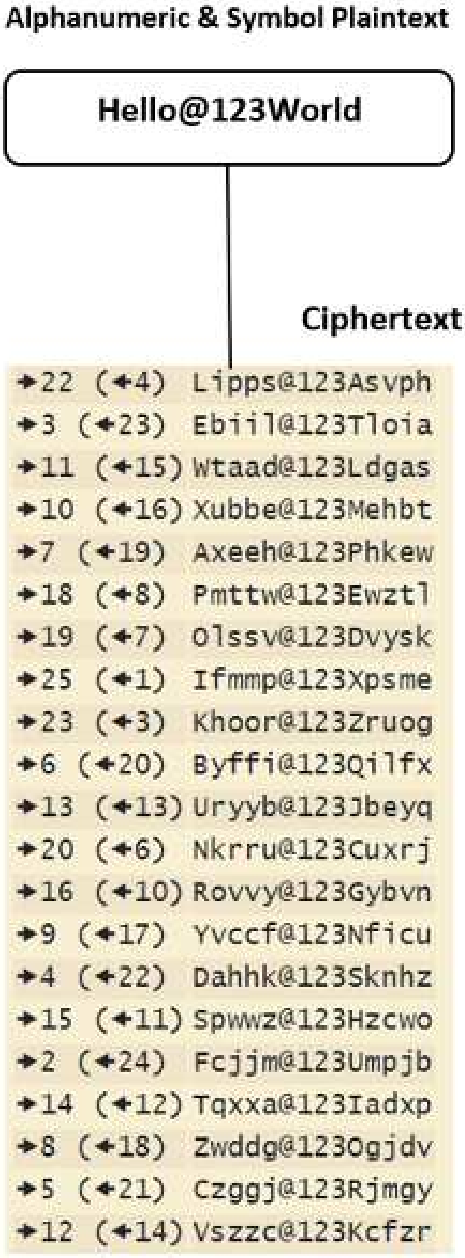
SHA 256 is a piece of the SHA 2 group of calculations, where SHA represents the Secure Hash Algorithm. Distributed in 2001, it was a joint exertion between the NSA and NIST to acquaint a replacement with the SHA 1 family, which was gradually losing strength against animal power assaults. The meaning of the 256 in the name represents the last hash digest esteem, for example regardless of the size of plaintext/cleartext, the hash worth will continuously be 256 pieces. Different calculations in the SHA family are pretty much like SHA 256. SHA-256 is a licensed cryptographic hash work that yields a worth that is 256 pieces in length.

E.g., Plaintext: Hello123@#World

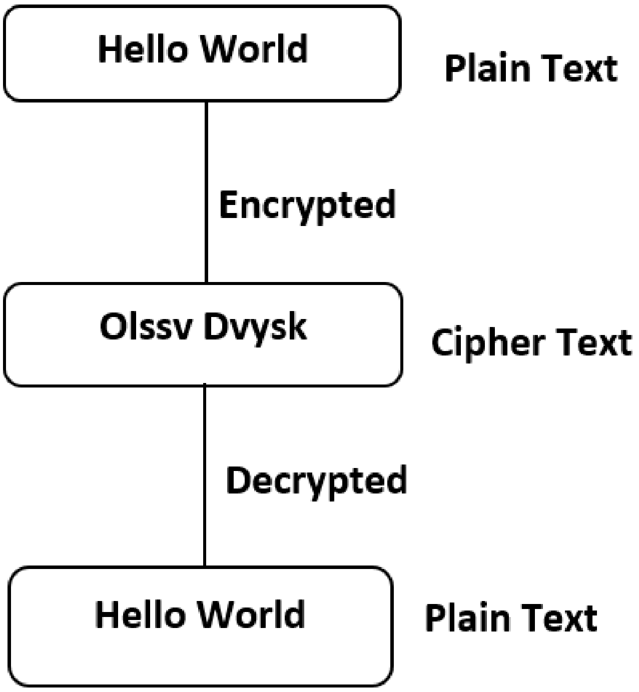
Ciphertext:8d0159485e43c2a5526b15bb8725dbbf3dad3307c538d4c3b901ae3982bf7fe6

In the SHA-256 Algorithm, we used Alphanumeric and Symbols characters as Plaintext but the Ciphertext is Alphanumeric without Capital letters and Symbols used in it.

Basically, let it be any Algorithm used to store password weather it is in Alphanumeric Characters and Symbols, but the Encrypted Hash values will be stored in Alphanumeric Characters without Capital letters unless if it is in Caesar Cipher since Caesar Cipher stores Capital letters encrypted in Capital letters only.



```
→22 (←4)  Lipps@123Asvph
→3 (←23)  Ebiil@123Tloia
→11 (←15) Wtaad@123Ldgas
→10 (←16) Xubbe@123Mehbt
→7 (←19)  Axeeh@123Phkew
→18 (←8)  Pmttw@123Ewztl
→19 (←7)  Olssv@123Dvysk
→25 (←1)  Ifmmp@123Xpsme
→23 (←3)  Khoor@123Zruog
→6 (←20)  Byffi@123Qilfx
→13 (←13) Uryyb@123Jbeyq
→20 (←6)  Nkrru@123Cuxrj
→16 (←10) Rovvy@123Gybvn
→9 (←17)  Yvccf@123Nficu
→4 (←22)  Dahhk@123Sknhz
→15 (←11) Spwwz@123Hzcwo
→2 (←24)  Fcjjm@123Umpjb
→14 (←12) Tqxxa@123Iadxp
→8 (←18)  Zwddg@123Ogjdv
→5 (←21)  Czggj@123Rjmgy
→12 (←14) Vszzc@123Kcfzr
```



As Shown in the Diagram in Caesar algorithm does not change the hash value of numbers and symbols, Even in Nihilist cipher the encrypted text is in only numbers instead of Alphanumeric.

LITERATURE REVIEW:

A few papers were inspected and observed unique views to execute the feasible method for encryption and unscrambling calculation for safety.

In 2014 Sukirty Jain proposed "Cyclic Redundancy Codes: Study and Implementation". This paper introduces a manner to authenticate the information transmitted over the community the use of the Cyclic Redundancy Check (CRC) mistakes detection approach which fit sat the idea of binary division. A community have to be able to transmitting the information from one cease to every other cease with accuracy. She speaks approximately shifting the information in a gadget have to be enriched with mistakes detection and mistakes correction strategies.

In 2017 D Rachmawati additionally proposed "A comparative look at of Message Digest 5(MD5) and SHA256 set of rules". They proposed a contrast among Message Digest 5(MD5) and Secure Hash Algorithm 256(SHA256). They in comparison algorithms primarily based totally on walking time and complexity. The studies consequences acquired from the complexity of the Algorithms MD5 and SHA256 is the same, however concerning the velocity is acquired that MD5 is higher in comparison to SHA256. They proposed that the complexity of the MD5 set of rules and SHA256 is identical and the price is Θ(N), however the walking time of MD5 is quicker than SHA256.

In 2018 Rohit Singh additionally proposed "A Review Paper on Cryptography of Modified Caesar Cipher". Encryption is accomplished at the sender facet and decryption is accomplished at the receiver facet. He represents Caesar cipher as one of the fine examples as it has much less complexity, restricted electricity consumption, and much less reminiscence consumption. The evaluation of Basic Caesar cipher, Delta formation Caesar cipher, and XOR Caesar cipher is accomplished on the premise of many parameters like Avalanche Effect, Frequency Test, and Brute pressure attack.

In 2019 Abdalbasit Mohammed, Nurhayat Varol additionally proposed "A Review Paper on Cryptography" They proposed a look at of present encryption strategies which can be analyzed to sell the overall performance of the encryption methods. They proven evaluation of a number of the studies that has been performed within side the subject of cryptography in addition to of ways the diverse algorithms utilized in cryptography for distinctive safety functions work.

CONCLUSION:

Cryptography assumes an imperative and basic part in accomplishing the essential points of safety objectives, like verification, trustworthiness, privacy, and no-renouncement. Cryptographic calculations are created to accomplish these objectives. Cryptography has the significant motivation behind giving solid, and hearty organization and information security. With the web having arrived at a level that converges with our lives, developing violently during the most recent a very long while, information security has turned into a fundamental worry for anybody associated with the web. Information security guarantees that our information is just open by the expected collector and forestalls any adjustment or modification of information. To accomplish this degree of safety, different calculations and strategies have been created. Cryptography may be described as strategies that cipher records, relying on precise algorithms that make the records unreadable to the human eye except decrypted via way of means of algorithms which are predefined via way of means of the sender.

In this paper, we exhibited a survey of a portion of the examination that has been directed in the area of cryptography as well as of how the different calculations utilized in cryptography for various security purposes work. The models referred to in all of the Algorithms show that every Algorithm has different code text regardless of when their plaintext is the same. Each and every calculation (Caesar Cipher, CRC, MD5, and SHA256) has different handiness, hash values, and Encryption and Decryption methodologies to encode anyway their code values contrasts. Cryptography will keep on arising with IT and field-tested strategies concerning safeguarding individual, monetary, clinical, and web-based business information and giving a decent degree of security.

REFERENCES:

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

[2] https://www.researchgate.net/publication/323806050_A_comparative_study_of_Message_Digest_5MD5_and_SHA256_algorithm

[3] http://www.unit-conversion.info/texttools/crc/

[4] https://10015.io/tools/sha256-encrypt-decrypt

[5] https://www.md5hashgenerator.com/

[6] https://cryptii.com/pipes/caesar-cipher

[7] https://www.dcode.fr/caesar-cipher

[8] https://cryptii.com/pipes/nihilist-cipher

[9] https://www.researchgate.net/publication/343979632_A_Review_Paper_on_Cryptography_of_Modified_Caesar_Cipher

[10] https://www.researchgate.net/publication/328578872_Cyclic_Redundancy_Codes_Study_and_Implementation