Advancement in Data Security using Cryptography Techniques

[1]Anuj Chauhan, [1]Student, [2]Sangeeta Rani, [2]Assistant Professor

SGT University, Gurugram, India.

Anujchauhan1299@gmail.com

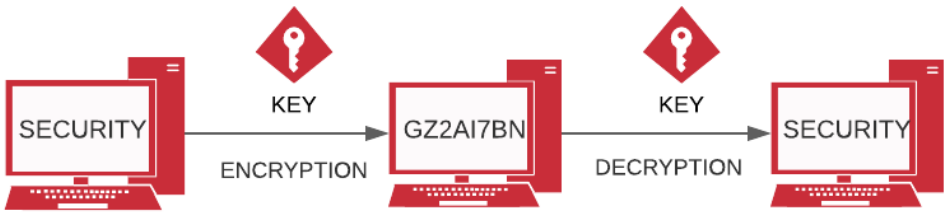
Abstract:**In today world data is everything. Data is a valuable asset that can lead an organisation to grow as well as the downfall of that organisation. If an organisation's data fell in corrupt and unauthorised people that organisation's reputation gets serious damage and recovering from that damage can be difficult. So, by any means, data must be protected from corruption and unauthorised access, by doing so an organisation can prevent financial loss, reputation damage, consumer confidence disintegration and brand erosion. To prevent unauthorised access to data, cryptography algorithms are used. In this paper, I am proposing a general idea that how we can fuse different cypher techniques and create a much-secured technique than the used techniques. Cryptography algorithms are very essential to protect your data. Cryptography algorithms simply work by encrypting the plain text into a secured cypher text which cannot be easily decrypted by third parties.**

Introduction:

The world today we know is far more advanced. Everything is digitalised. There is a lot of data around us. From advanced data centres, servers to common household items like fan, tv, AC, washing machine etc everything is digitalised. Everything is connected to the internet. So we are dealing with a lot of data. Managing and securing this data is very complex and require precision. A small mistake could lead to a breach in the system and loss of data. If this data fell into wrong hands, it can be very harmfulto an organisation or an individual. Data can protect life as well as can destroy them [1]. To secure the data cryptography is needed. It ensures that only authorised persons can access it.

Cryptography has become part of our life some use it knowingly and some use it unknowingly. But it is a must method to ensure the security of data. Cryptography is a Greek word that means 'Hidden' or 'Secret'. Cryptography is the science that keeps our data secure by transforming the normal data into cypher data by using compression and encryption. Cryptography takes plain text or data, apply encryption and give a cypher text which is very hard to decrypt [2].

Data is encrypted using an algorithm and a key is generated. This key is very important because it is used to encrypt and decrypt the data [3].



Historic Algorithm:

Caesar Cipher:

Caesar Cipher was developed by '*Gaius Julius Caesar'*. Gaius Caesar used this cypher to send messages to his generals. Caesar Cipher is the most commonly known cipher. This cipher works by substituting the letters with other letters using shifts. The shift can have any numeric value. example DATA using shift=2 can be written as FCVC.

Transposition Cipher:

The oldest implementation of transposition cipher was *'Scytale'* used by Spartans. The transposition cipher is different from other ciphers. In this cipher letters are rearranged in plain text using a specific key. The plain text is written in a rectangular form horizontally. There can be as many rows. There are two types: Complete Columnar and Incomplete Columnar, the only difference between these two are that the incomplete columnar column can be empty but the complete columnar column cannot be empty.

Simple Substitution Cipher:

In simple substitution cipher, the letters in plain text are substituted by different letters using some key. This key is used to both encrypt and decrypt the plain text [4].

Modern Algorithm:

Stream Cipher:

In-stream cipher, the plain text is converted into bits and then algorithm and key are applied to every single bit to form cipher text. A keystream generator generates a key in terms of bits then XOR is applied to bits of plain text and bits of the key to generate ciphertext.

Block Cipher:

In block cipher, plain text is divided into blocks and then a key is applied to each block to get cipher text. In block cipher, there is an algorithm for encryption and an algorithm fordecryption. To make cipher block more secure pseudorandom permutation is used.

Hash function:

In the hash function, plain text is passed through a hash function to get ciphertext. It maps arbitrary size data to fixed-size data. A hash function takes an arbitrary amount of data input and produces fixed-size output. This output also called a hash value. This hash value can be used as a password to verify the user [5].

Related Work:

This section gives an overview of previous research and study on cryptography in data security.

Simrandeep Singh Thapar and Himali Sarangal [1] concluded that we cannot protect the data for a longer time. Using better computer data can be decrypted. So, we need to find more ways to protect our data strong enough to secure data for a longer time.

Madhusudan Singh, Shiho Kim [2] proposed a crypto unique ID to create a much secure environment for data sharing and environment. This crypto unique ID can be able to solve many problems like deadlock etc.

Mark A. Will, et al [3] combined elliptic curve cryptography with AES. They stated that a simple anonymous routing protocol can be used for better performance. XORing nodes are good for internal network and AES is used to improve security furthermore.

Abdalbasit Mohammed Qadir, Nurhayat Varol [4] concluded that to achieve security, integrity, confidentiality cryptography plays a major role in it. It plays an important role in creating strong and robust networks. To protect data and provide privacy cryptography is needed.

William J. Buchanan, Shancang Li & Rameez Asif [5] combined various lightweight cryptography techniques. This combined technique is more secure than separately applied techniques.

Manju Khari, et al [6] proposed an EGC protocol that gives a high level of security during transferring of data. Due to the EGC protocol's enhanced embedding efficiency, more data hiding capacity is achieved.

Shariqua Izhar, et al [7] proposed three cryptography techniques by combining existing techniques. The combination of transposition and substitution cipher is used to such an extent that the brute force method cannot be used on them.

Anuj Kumar, Vinod Jain, Anupam Yadav [8], proposed a new technique. This technique is called the hybrid technique. This technique is a combination of DES and RSA algorithms. When applied combined, it is more secure than applied separately.

Marek R. Ogiela, Lidia Ogiela [9], told us about cognitive cryptography techniques. This technique is used to secure data that has high value and significance.

Sattar B.Sadkhan, Akbal O. Salman [10], states that any small change in computing change our lives. With change there comes the problem of security as well as data change. So, they use lightweight cryptography. It is a modern algorithm that is used to solve modern problems.

Proposed Work:

Here I have proposed some cryptography methods which can provide us with a base for further advancements in encryption techniques. These methods are mix up of already existed substitution encryption techniques such as:

1. Caesar Cipher
2. Vigenere cipher
3. A1Z26 Cipher

Method 1:

In this method, I combined Caesar cypher and Vigenere cypher

Step 1: Take the plain text.

Step 2: Apply Caesar cypher by using n number of shifts.

Step 3: Then further apply Vigenere cypher by using any keyword

Example:

Text = CRYPTOGRAPHY

By applying Caesar cypher:

Shift = 4

Caesar Text = GVCTXSKVETLC

Further Applying Vigenere Cypher:

Input Text: GVCTXSKVETLC

Keyword = LEMON

Cypher text = RZOHKDOHSGWG

Method 2:

In this method, we are going to combine Caesar cypher, Vigenere cypher and A1Z26 cypher.

Step 1: Take the plain text.

Step 2: Apply Caesar cypher by using n number of shifts.

Step 3: Then further apply Vigenere cypher by using any keyword.

Step 4: Further apply the A1Z26 cypher.

Example:

The cypher text generated in the above method: RZOHKDOHSGWG

Then applying A1Z26 cypher:

Cypher Text: 18-26-15-8-11-4-15-8-19-7-23-7

Conclusion:

Data has always been the most crucial part of us humans. Hackers, breachers etc always try to use this data for ill will and wrong purposes. A consistent threat is always there to the data. So, data must be secured and we must ensure that only authorised individuals can access it.

The solution to this problem is cryptography. To secure the data we can use compression and encryption techniques. Nowadays there are a lot of algorithms with help of which we can protect our data. But the problem is that some algorithms are very complex to implement and some are easily brute-forced. So, I have tried to mix up various simple techniques to create a more secure technique. When combined, this technique is more secure than individually applied.

Future Work:

In today's world where data is everything, the security of data is a major concern. If we create one technique to protect the data, hackers create other technique to crack that technique. As long as security concerns of data are their future scope of data security and cryptography are also there. There are a lot of peoples who are creating new algorithms to protect the data which are not easy to crack. In cryptography, compression and encryption techniques are used to protect the data from hackers.

There are some improvements in my work that can be done in future:

1. These algorithms must be tested on real-time simulators.

2. We can use other cryptography techniques combination to get more security.

3. More complex techniques can be used to raise the security of data which are not easier to get breached.

References:

[1] Simrandeep Singh Thapar, Himali Sarangal, “A Study of Data Threats and the Role of Cryptography Algorithms” 2018 IEEE

[2]Abdalbasit Mohammed Qadir, Nurhayat Varol,” A Review Paper on Cryptography” 2019 IEEE

[3] Mark A. Will, Ryan K. L. Ko,” Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography” 2017 IEEE

[4] Madhusudan Singh, Shiho Kim, “Crypto Trust Point (cTp) for Secure Data Sharing among Intelligent Vehicles” 2018 IEEE

[5] William J. Buchanan, Shancang Li & Rameez Asif,”Lightweight Cryptography Methods” 2018 Taylor and Francis

[6] Manju Khari, Aditya Kumar Garg, Amir H. Gandomi,” Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques” 2019 IEEE

[7]Shariqua Izhar, Anchal Kaushal, Ramsha Fatima, Mohammed A. Qadeer,” Enhancement in Data Security using Cryptography and Compression” 2017 IEEE

[8] Anuj Kumar, vinod Jain, Anupam Yadav,” A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique” 2020 IEEE

[9] Marek R. Ogiela, Lidia Ogiela," Cognitive cryptography techniques for intelligent information management" 2018 Elsevier

[10] Sattar B.Sadkhan, Akbal O. Salman," A Survey on Lightweight-Cryptography Status and Future Challenges" 2018 IEEE

[11] Je SenTeh, MoatsumAlawida, You ChengSii," Implementation and practical problems of chaos-based cryptography" 2020 Elsevier

[12] M Elhoseny, K Shankar, SK Lakshmanaprabu," Hybrid optimization with cryptography encryption for medical image security in Internet of Things" 2018 Springer

[13] MS Taha, MSM Rahim, SA Lafta," Combination of steganography and cryptography: A short survey" 2019 IOPScience

[14] S Padhye, RA Sahu, V Saraswat," Introduction to cryptography" 2018 TaylorFrancis

[15] LPI Ledwaba, GP Hancke, HS Venter, SJ Isaac,"Performance costs of software cryptography in securing new-generation Internet of energy endpoint devices" 2018 IEEE

[16]