A Novel Cryptographic Method for Information security with Low Computational Cost

Nahida Nazir, Pushpendra Kumar Pateriya
School of Computer Science & Engineering
Lovely Professional University, Punjab, India

Abstract: Encryption and decryption techniques are gaining importance in the cryptographic system.In this context a new encrypting and decrypting technique have been designed to secure the plain text over the internet and preventing all the prone attacks like man in middle attack and other vulnerable threats. It is actually encrypting and decrypting the text with the special characters and symbols along with the variations in mapping that makes it impossible for the intruder to breach the ethics of security like confidentiality,availability, integrity, Denial of Service. This paper also highlights the strengths and drawbacks of the designed system.

1. INTRODUCTION

Cryptography is a technique of coding the data so that it cannot be interpreted by all the humans and the subject that deals with the breaking of the coding information and creating its meaning text or data is called cryptanalysis[1] .In cryptography the human readable text is known as plain text and the text that is in coded form is called cipher text[2].There are number of techniques that can be implemented to create cipher text like substitution techniques and transposition techniques[7]. In substitution technique the plain text is coded either with numbers, letters or with some special characters .In transposition technique the letters are rearranged[3] .In former technique the position remains unchanged only the letters change .But in transposition technique the position of letters is also changed. The substitution technique is further categorized in mono alphabetic and polyalphabetic cipher techniques .Key and keyless ciphers belong to the
Transpositiontechnique. Symmetric key encryption it is based on single key arrangement
Block cipher and stream ciphers are the two types of symmetric approach .Symmetric algorithm is fast but the major drawback of this technique is how the keys can be shared between the sender and the receiver for encryption and decryption process. In asymmetric encryption also known as public private encryption that involves two separate keys for coding and decoding process[5].Private key is kept confidential and the public key is exchanged[8].

This research work is intended to investigate how secure the data is when it is travelled from one person to another. We know that the highly confidential data is transferred over network in an encrypted form. There are many types of encryption algorithms which are being used. Most of the modern encryption-decryption algorithms are complicated and require more computational power, so there is a scope of designing new cryptographic algorithms which will be robust in nature and perform the encryption/decryption in optimal period of time.The Cryptographic Algorithm is used to keep the message confidential and at the same time it allows us the facility of sending it from one person to another person through any medium either be it online or offline. This cryptography Cipher makes sure that your data is secure in the process of transmission. This Crypt Cipher is very easy to use as this Crypto Graphical Cipher is shared only between the sender and receiver. This Crypt Cipher uniqueness comes with its features like replaceable, replicable, complicated decryption, cannot be broke by using brute force algorithms as it is generated according to the user.

2. Literature Review

Secure data communication over network is essential and Challenging incurrent situations to ensure datasecurity over networks. Number of cryptographic algorithms or cipher techniques are present and the techniques chosen for coding and decoding should meet the basic fundamentals of network security research by Jitendra Singh Chauhan and S. K. Sharma in 2015 provided the comparison of various existing algorithms like Advanced Encryption Standard algorithm, Data Encryption Standard

,Blow Fish algorithm ,Secure Hash Algorithm and Message Digest 5 and highlighted a proper way how to use these techniques to secure the data over networks.

In paper [3] by AlHasib et al in 2008 two most important techniques were used namely RSA and AES .Confidentiality and authorization were major concerns about the data transmitted over the internet .Mathematical analysis of both the techniques were taken into account, strengths, computational speed .Different attacks were also implemented on these techniques but both proved to be very strong against any attack.

J. Pradhan et al in 2008 to achieve the security for electronic business application usually different organization follow the encoding and decoding techniques .The techniques to secure the business data were data encryption standard and advanced encryption standard both are based on different keys first one is based on the symmetric approach and the second algorithm is based on asymmetric approach.AES out performed than the respective algorithm because problem occurred in sharing the key in business organization.

Y. Abouelseoud, M. Mikhail, and G. Elkobrosy in 2014 implemented the techniques and algorithms in industrial world. Information leakage in such an environment can be problematic even they may lose the financial status since every transaction is done via online and the primary requirement is to secure the transaction over the internet.ElGamal and variation of ElGamal were used to secure the data and information that is transmitted between the organizations so the variation of ElGamal provided the secure transactions.

In 2008[12] by A. Naureen, A. Akram et al operated the encryption and decryption methods on the sensor environment. A cluster based framework was used where the base station served as the distribution center for keys containing public keys of all the nodes in the network. Public key cryptography and private key cryptography were used. Public key cryptography is an efficient way to provide security than the private key in a sensor environment.

T. Nawaz S. Farah, M. Y. Javed, A. Shamim in 2012[13].Authors presented the comparison of different techniques and the techniques were ElGamal,RSA and Pallier asymmetric algorithms .The comparison was based on resource utilization like CPU memory,computational speed to code and decode the text and key size.

In 2014 by S. Agrawal and R. Tripathi [14] security of the data as a major challenge for all fields is highlighted. Cryptography is a solution to all the existing prominent problems like confidentiality, masquerading and spoofing.A comparison of symmetric and asymmetric techniques were presented both of the techniques performed better,efficiency comparison was based amount of the data to be transmitted.

S. R. Kumari and B. Padmavathi in 2013[15].Due to security reasons the sharing of information via the internet has become an issue because of the security breaches.so more techniques are implemented in a bulk to secure the data transmission .Here the focus is on combining the steganography techniques with the cryptographic ones .The first step is to encrypt the data with the different cryptographic techniques then after creating the coded text hide the data in either audio orvideo with the steganography techniques.Authors implemented techniques like AES,DES and RSA to achieve the goal for securing the data.

In 2013 by Int. J Comput.Appl and G. Singh, scrambling of the plain textare known as encryption as it can only read by the man that created this coded form.With the advancement in the digital world more security measures should be taken to protect the data from the security threats .Here the concern is not only to provide the security over the internet but to the databases as well as computers that stores the confidential data so double security is provided to secure the data at both the levels.Authors like R. Goudar and Patil in 2008.Internet surfing is the common way of exchanging data or messages .Security issues are not only related to e commerce but e government information is of prime concern.So here different encryption techniques have been implemented for data transmission like message digest, SHA.

3. Proposed Methodology: To decrease the complexity of the cryptographic algorithm which will include both the encryption as well as decryption process without compromising the security. In a short period

of time, not only this, it also provides additional security. This approach avoids repetition of the ciphers and the mapping presented here is so difficult that its security cannot be breached.

Workflow steps:

1. Creating new ciphers for all the alphabets.
2. Creating a database which consists of ciphers with mappings to alphabets.
3. Creating a new encryption and decryption algorithm using java compiler
4. Using Steganography concepts for hiding messages.
5. Creating a user's guide to guide the users how to use the code.
6. Giving privileges to the user to change the mapping of the ciphers.

Description to design a new cryptographic algorithm, we need to consider the advantages and disadvantages of the already present traditional cipher has. Ciphers like Caesar have a key which always remains the same. Some properties from Shift cipher, Transportation cipher and Permutation ciphers can also be inherited. To make it easy but difficult to break, we may want to use the properties that all the above-mentioned ciphers have. The Cryptographic Cipher that we are going to create is purely based on the concept of inheriting the traditional ciphers by creating a different structural representation of alphabets and numbers which are going to be called as ciphers. Creating a database for ciphers which are particularly generated for alphabet/number. This may change from person to person. But a significant number of alphabets and numbers have fixed ciphers which cannot be changed. Creating a new cipher which is flexible and dependable for the safety and security of the data is our objective.

The Cryptography System works on the principle of dedicating ciphers for every alphabet and number. It is completely dependent on the rules created by the founder of the cryptosystem. Different cryptosystems have different rules. Cipher can be anything like symbols, numbers, and alphabets. A cryptosystem is designed for maintaining confidentiality and secrecy of messages. There are many cryptosystems available presently in Cryptography. Some of them are Substitution cipher, Permutation ciphers, RSA, Advanced Encryption System(AES), DES etc. In asymmetric key cryptography there are various keys to generate the secret key. Many rounds of mathematical executions take place for a piece of message. Each round has a key which generates for the next round of encryption. Symmetric key cryptosystem has a primary key and private key which is only shared between the sender and receiver. The encryption takes place manually or programmatically.

To design a strong cryptosystem, we need to create the ciphers for every alphabet and number. Ciphers can be unique and can be repeated. They should solely depend on the individuality of the variables. Ciphers can be of any symbols given in the number system or anything that is derived from any mathematical expression. We need to create a database representing ciphers for numbers and alphabets. We need to create a computational program on the base of C++ or Java program, in which the database is inherited into the language which is used. Executing the program is based on the message that is given to encrypt.

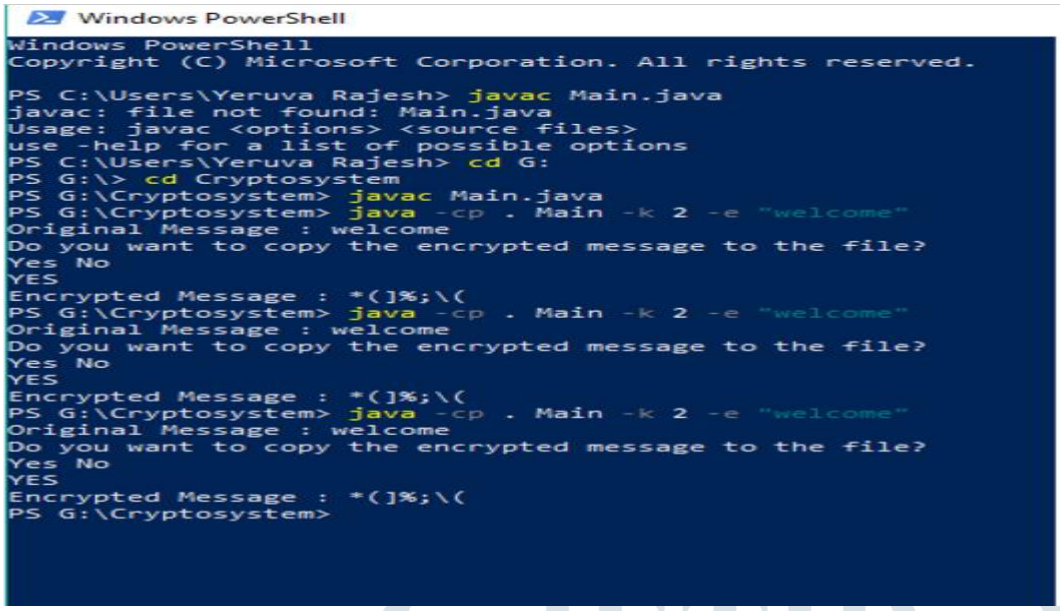
Creating the ciphers which are the special characters that can be used. Maintaining records of the ciphers in a database so that it will be used for any chances of changing the mapping procedure to keep the cryptosystem more secure. Record of the default cipher database should be maintained.

So we are inheriting the properties of both symmetric and asymmetric variations to find an Cipher algorithm of its own which is very easy to use and yet difficult to break the cipher. The Limitations of this Algorithm is anyone can create cipher numbers in their databases. The databases can be changed, and uniqueness should be maintained.

The default cipher numerals which are to be created will be inherited from already present traditional ciphers like Caesar cipher, Shift cipher, Monoalphabetic& Polyalphabetic cipher, Substitution cipher, Transportation cipher, Play fair cipher and Vigenere cipher. The Cipher numeric is dedicated to any alphabet or numerical. Those alphabets and numerical should be denoted by their ciphers only. Source code is developed with INTELLIJ IDE. Encryption of the text message we used the Comma-separated values (CSV) file for the building the database so that clients can modify it easily. A python oriented tool is also used here. The plain text is encrypted using Caesar cipher which is a round one encryption and then to the round two encryption using Vigenere cipher.

4. Result and Discussions

Experimental Result



Screenshot of the message that has been encrypted

Strengths:

- Database can be changed by their user according to their wish
- Ciphers are not fixed and can be changed. So Brute force and Dictionary attacks won't work
- Messages are hidden with the help of steganography. So provides an extra level of encryption.
- Message in the picture or audio is in encrypted form. But the encryption is in special characters. Till now there is no encryption done by special characters so makes it unique.
- All the letters have different keys.
- Name of the image totally depends on the Message. So, the key is difficult to find.
- Even intruder gets the Image or the Message he cannot find the key and doesn't understand what the special characters are for.

Drawbacks

The main drawback of this technique is that every special character cannot be used because there are few special characters that cannot be recognized.

5. Conclusion and Future Scope:

Here random message was created and after generating the text the proposed encryption technique was applied to create the coded text that could not be easily computed to decode the text .Moreover the number of resources consumed by this technique were low as compared to other techniques This paper presents the development in the encryption and decryption technique with the help of special characters .Also with the shortcomings and strengths of the techniques have been highlighted .This paper prevents the attacks like snooping ,spoofing and other attacks that are prone to the plain text Implementation of this technique on Digital Signatures.

References

[1] Ci, Yunfei, et al. "Design and Implementation of the Components of the Symmetric Cryptographic Algorithm." *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*.IEEE, 2017.

[2] Stallings, W. Cryptography and Network security.In W. Stallings, Cryptography and Network security (p. 786).Pearson; 7 edition (March 5, 2016).

Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction".Introduction to Modern Cryptography.

[3] Cocks, Clifford (20 November 1973). "A Note on 'Non-Secret Encryption'" (PDF). CESG Research Report.

[4] Shannon, Claude; Weaver, Warren (1963).The Mathematical Theory of Communication.University of Illinois Press.ISBN 0-252-72548-4.

[5] M. Kumar, V. Kumar and A. Sharma," A Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, 2014.

[6] A. Abdullah et al , "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Cryptography and Network Security, 2017.

[7] A. Majare, G. Yadav " A Comparative Study of Performance Analysis of Various Encryption Algorithms", International Conference on Emanations in Modern Technology and Engineering (ICEMTE), Volume: 5 Issue: 3, 2017.

[8] L. Saikia, D. Talukdar " A Review On Different Encryption Techniques: A Comparative Study", International Journal of Engineering Research and General Science, Volume 3, Issue 3, 2015.

[9] B. Thomas, S. Swathi, P. Lahari et al " Encryption Algorithms: A Survey", International Journal of Advanced Research in Computer Science & Technology (IJARCST), Volume 4, Issue 2, 2016.

[10] N. Singh, "Survey Paper on Steganography", International Refereed Journal of Engineering and Science (IRJES), Volume 6, Issue 1, 2017.

[11] M. Rahim, A. Rashid "Critical Analysis of Steganography "An Art of Hidden Writing"", International Journal of Security and Its Applications, Volume 10, No. 3, 2016. [14] S. Asbeh, H. Al-Sewadi, S. Hammoudeh and A. Hammoudeh, "Hex Symbols Algorithm for AntiForensic Artifacts on Android Devices",

[12] A. Naureen, A. Akram, T. Maqsood, R.Riaz, K. H. Kim, and H. F. Ahmed, "Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks," IEEE Veh. Technol. Conf., pp. 163–167, 2008

[13] S. Farah, M. Y. Javed, A. Shamim, and T.Nawaz, "An experimental study on Performance International Journal of Pure and Applied Mathematics Special Issue 676 Evaluation of Asymmetric Encryption Algorithms,"Recentadvaces Inf. Sci., vol. 8, pp. 121– 124, 2012.

[14] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," Int. J. Adv. Found. Res. Comput., vol.1, no. 6, pp. 68–76, 2014. [8] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES , AES and RSA Algorithm along with LSB Substitution Technique,"Int. J. Sci. Res., vol. 2, no. 4, pp. 170–174, 2013.

[15] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES , AES and RSA Algorithm along with LSB Substitution Technique,"Int. J. Sci. Res., vol. 2, no. 4, pp. 170–174, 2013