Security and Authentication through Text Encryption and Decryption based on Substitution Method

Munish Mehta, Vijay Goyar, Vishnu Bairwa

Abstract**:** ***In order to maintain security, privacy and integrity of important information or data is a great challenge in today's world. Cryptography is a technique to prevent important data from hackers and intruder by converting important information in encrypted text by using an encryption algorithm. This paper is a review of various symmetric and asymmetric cryptography techniques. In this paper some gaps have been identified after reviewing some algorithms like they don't work for case sensitive data but merely works for uppercase alphabets, they don't encrypt numerically, spaces and they don't run on the special symbol. In our proposed solution an effort to expand the original 5X5 character set of the Play Fair algorithm will be done so as to include lower case alphabets(a-z), some symbols, numeric(0-9) and a special character '\0' for space. So, a new algorithm will encrypt lowercase, numeric, symbols as well as spaces.***

Keyword: Cipher, Cryptanalysis, Decryption, Encryption, Private Key, Public Key, Substitution, Transposition.

I. INTRODUCTION

A. Cryptography

Encryption and Decryption is a security mechanism by which information is converted in such a way that only authorized user can read it.[6] It uses an encryption algorithm to generate ciphertext that can only be read after decrypted. As we know the security of data is of prime importance and can be achieved by encoding the original messages by applying encryption technology to make them non-readable. Decryption can be performed without the interference of user and encryption of the data can be done by user using cryptography method. Cryptography not only provides authentication to the user but also protects the data. As the user share much of their information on the internet due to advancement in the network technology there is again a big issue for data security. Cryptography technique is again required to maintain the security of the data. The data which is in an understandable format, more reliable and readable without distinctive methods are recognized as plain text. Encryption provides security for data at every time even when we move data from one location to another over network then data is most vulnerable[2][6].

Revised Manuscript Received on July 02, 2019.

Dr. Munish Mehta, Department of Computer Application, NIT Kurukshetra ,India.

Vijay Goyar, Department of Computer Application, NIT Kurukshetra, India.

Vishnu Bairwa, Department of Computer Application, NIT Kurukshetra, India.

Encryption does its work during data transfer so as to make it an ideal solution and it does not matter where the data has been stored or how it is used. The transfer of data from a mobile device to another is a risk for data theft. Encryption can help to protect the data by storing it across all devices while transferring it.

Classical cryptanalysis involves an interesting combination of the analytical reasoning, application of the mathematical tools, the pattern finding, patience, determination, and also the luck. Cryptanalysts are also known as attackers. Cryptology embraces both the cryptography and the cryptanalysis.

There is mainly two types of keys in cryptography. i.e.

- Symmetric key
- Asymmetric key

Classification and definition of keys

Symmetric key cryptography: Symmetric key encryption is the use of a single key for both the encryption and decryption process. it is also known as private key cryptography. For Example In private key cryptography, the information transmitter 'X' encrypts the information with the private key and sends the encrypted text to 'Y' The recipient 'Y' decrypts the encrypted text using the same key which the transmitter used to encrypt the plain text. To establish communication between 'X' and 'Y' this key was used. If 'X' requires to connect with other user let us say 'Z' then another key will be used. In a network of n nodes, n* (n-1) /2 keys are necessary which is an order of the square of n which is very big.[5][3]

Asymmetric key cryptography: In Asymmetric key cryptography, encryption had two keys, i.e. a secret key and a public key. For encryption, the public key is used and for decryption private key is used. This is also known as public key encryption. For example, While using Public key cryptography, when a sender 'X' sending a message encrypts the message by using the recipient's public key which is able to be seen by everyone and sends the text to 'X' after encryption. If 3rd party desires to decrypt the message and tries to using B's public key, then resultant will turn out to splutter because the only private key of B can decrypt this message which is not like the public key. So, to make secure communication a pair of keys like public and private keys will be used by every node in the network In a network of n nodes, 2*n keys are required which is an order of n [5][3].

Substitution: In the substitution technique, the letters of the plaintext are replaced by other letters/numbers/ symbols. It can be done by keys in the case of letters, Normal text is always in small letters, The encrypted text is a capital letter. The most important values are shown in italics. There are many other substitution techniques available like a mono-alphabet cipher, César cipher, Hill cipher, Play-fair cipher, poly-alphabet cipher, etc.[4].

There are some substitution techniques:-

a) Mono-Alphabetic Cipher:-Predictability of Caesar Cipher was its weakness once any key replacement of a single alphabet is known then, the whole message can we decipher and almost 25 attempts are required to break it. In this technique, simply we substitute any random key for each alphabet letter, that is 'X' can be being replaced with any letters from A to Z. Let's say we substitute A with E that doesn't mean that B will be replaced by F. Mathematically, we have 26 alphabet permutation which means (26 x 25 x 24 x...2) which is about 4 x 1026 possibilities.

b) Poly-Alphabetic Substitution Cipher: Polyalphabetic Substitution cipher was introduced by Leon Battista in the year 1568, and its prominent examples are Vigenère cipher and Beaufort cipher. We use several one-character keys, each key encrypts one plain-text character. This first key encrypts the first plain-text character, the second key encrypt the second plain-text character. Similar is the case for third-fourth key etc. After all, keys are used then they are recycled. If 50 one-letter keys, every 50th character in the plain text would be placed with the same key and this number (in our case, 50) is a period of the cipher. The key points of the polyalphabetic substation cipher are the following: It uses a set of related mono-alphabetic substitution rules. The rule used for transformations determined by the key it uses.

c) Hill Cipher: it is a polygraphic substitution cipher based on the linear algebra. Each letter is represented by using a number modulo 26. In general, the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not necessary to be followed by the cipher. For message encryption, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decipher the message, each block is multiplied by the inverse of the matrix used for encoding.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).hi

d) Playfair Cipher: In Playfair cipher, primarily a key table is produced[5]. The by and the large key table is a 5×5 matrix of alphabets that acts as the key for encrypting the plaintext. Apice of the 25 alphabets must be unique and one letter of the alphabet "usually J" is omitted from the table as we require only 25 alphabets instead of 26.

If the plaintext contains J, then it is replaced by I, it is not necessary I and J come together in one block we add any alphabet in the table, I and J come less in a sequence of the letter that's why we use I and J together.

The sender 'A' and the receiver 'B' decide on a particular key, say 'CIPHAR'. In a key table, the first characters check from "left to right" if the same alphabet comes we take single alphabet like 'soon' there are two 'O'. Duplication is not allowed there take only 26 unique letters. The remaining table will be filled with the left out letters of the alphabet, in the natural order.

The encryption of Play fair was the first practical digraphs of encryption of substitution. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair, who promoted the use of encryption.

The technique encrypts pairs of letters (digraphs) instead of simple letters as in the simple substitution cipher. The game fair is much harder to break because the frequency analysis for simple substitution codes does not work. Frequency analysis can still be performed, but for the 25 * 25 = 625 possible digraphs instead of the 25 possible monographs. Therefore, frequency analysis requires much more encrypted text to function.[5][8]

The play-fair code begins with the creation of a key table. The key table is a 5 × 5 letter grid that will act as a key to encrypt the text without formatting. Each of the 25 letters must be unique and one letter of the alphabet (usually Q) is omitted from the table (since there are 25 points and 26 letters in the alphabet).

Let's take an example like we have key "vishnu vijay" and the plain text is "we are friends". The first characters "going from left to right" in the table will be the sentence, with the duplicate letters removed. The rest of the table will be filled with the remaining letters of the alphabet, in order. Our key table would look like this:

Table 1: 5*5 matrix

V	I/J	S	H	N
U	A	Y	B	C
D	E	F	G	K
L	M	O	P	Q
R	T	W	X	Z

Now, first of all, we make the two-two pair of the alphabet like "we ar ef ri en ds" now convert into cipher text it will look like "tf ut fg tv kj fv" this is our ciphertext after conversion The following figure is showing conversion process of plain text into cipher text:

Table 2: Encrypting 'FW'

E	F
M	O
T	W

Our first pair is “we” its equivalent ciphertext is ‘tf’. Similarly, conversion of the remaining pair of alphabets into ciphertext is as follows:

Rules of the play-fair technique [1][7]:

- If alphabet ‘e’ and ‘g’ or any alphabet come in the same row what we do in this situation we take the next value of the alphabet.
- If alphabet came in the same column what we do is to take the down value of the alphabet.
- If alphabet comes in the matrix of n * m order like “d and s” in Table 3, they are not in the same row or column. They are different from each other. In this case, what we do actually, we pick the last value of the same row.[1][7] Like:

Table 3: Encrypting ‘SD’

V	I/J	S
U	A	Y
D	E	F

In Table 3 ‘D’ is converted to ‘F’ & ‘S’ is converted to ‘V’.

With reference to the previous rules, if the data is "FRIENDS", in the first place they are divided into pairs that are "FR", “IE”, “ND” and "SZ". Now, these pairs of the alphabet will check in figure 1. To encrypt the "FR" message, alphabet "FR" is replaced by the characters in their corresponding intersection line, as shown in Table 2.

Table 4: Encrypting ‘FR’

V	I/J	S	H	N
U	A	Y	B	C
D	E	F	G	K
L	M	O	P	Q
R	T	W	X	Z

The alphabet F and R they are not in the same row or column they different from each then replace each plaintext with the letter that forms the other corner of the rectangle that lies on the same row as that plaintext letter (being careful to maintain the order). Plaintext ‘FR’ is encrypted to ciphertext ‘DW’.

Table 5: Encrypting ‘IE’

V	I/J	S	H	N
U	A	Y	B	C
D	E	F	G	K
L	M	O	P	Q
R	T	W	X	Z

The alphabet came in the same column what we do take down the value of the alphabet. Plaintext ‘IE’ is encrypted to ciphertext ‘AM’.

Table 6: Encrypting ‘ND’

V	I/J	S	H	N
U	A	Y	B	C
D	E	F	G	K
L	M	O	P	Q
R	T	W	X	Z

The alphabet N and D are not in the same row or column. So we apply the same rule of above. Plaintext ‘ND’ is encrypted to ciphertext ‘VK’.

Table 7: Encrypting ‘SZ’

V	I/J	S	H	N
U	A	Y	B	C
D	E	F	G	K
L	M	O	P	Q
R	T	W	X	Z

The alphabet ‘S’ and ‘Z’ are not in the same row or column. So we apply the same rule of above. Plaintext ‘ND’ is encrypted to ciphertext ‘NW’.

II. CRYPTOGRAPHY INTENT

Users use cryptography for several reasons. The goal of modern cryptography is **to ensure the preservation of information properties** through various techniques. Various attributes of information can be preserves like its confidentiality, integrity and authenticity.

Confidentiality means assurance regarding only the intended recipient of a message can read it. Exactly what most people think of when word comes "cryptography” and that is the prime goal of classical cryptography.

Integrity means assurance regarding a piece of information has not been altered. This is the purpose of message authentication codes (MACs), message digests, and cryptographic hashing.

Authenticity means assurance regarding the sender of a message is who they say they are. This is the territory of digital signature and public-key cryptography in general. So to attain the confidentiality, integrity & authenticity of the information being sent we will modify the existing algorithm in such a way that it will overcome the problem of case sensitive, ambiguity and by adding a new capability of lower case alphabets, numeric data ranges from 0 (zero) to nine and other special characters used in the English language. To accomplish the use of Play Fair Cipher technique of substitution cipher method will be preferable.

III. OBJECTIVE

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The primary aim of this paper is to practice and study of techniques for secure communication in the presence of third parties and finding demerits in the existing algorithms if any. More broadly, it is about building and analyzing the rules that overcome the influence of attackers or strangers and that are linked to various facets of information security, such as information confidentiality, authentication and non-repudiation. Encryption applications include ATM cards, computer passwords etc.

A. GAPS IDENTIFIED

The algorithms studied till now it seems that there is a lack of the following:[1][7]

- They don't work for case sensitive data (only works for Upper case alphabets).
- They don't encrypt numeric, spaces.
- They don't work on a special symbol.

B. SCOPE

The scope of this proposed solution includes the following features:

- Easy and convenient for encryption.
- All the outliers can be detected by the program in a two-phase manner.
- The performance of the software package depends on the volume of data that have the number of objects in the dataset.
- The inputs in terms of file size in a dataset have to be entered manually.
- Efficient in terms of memory utilization.

It is expected that the proposed solution will protect the privacy of information/data and sensitive files. Encryption works with all types of data, text and files. We want to select what we encrypt, encryption and decryption algorithm helps us to keep documents, private information and files in a confidential way. Encryption is also used to ensure the hiding of data/files and documents.

Data encryption is also used to provide the security of files and other important documents also get safe from the opponent so that while sending the files or documents nobody else other than the recipient can see it. Today due to exponential use of the internet, the transfers of files and confidential information over the internet demands the security and safety of the data and this can be performed by using encryption and decryption. In the current scenario, encryption and decryption are most widely used in every field like defence, banking, Real-time environment, online money transfer etc.

IV. CONCLUSION

We will try to expand the original 5X5 character set of the Play Fair algorithm and to include lower case alphabets(a-z), some symbols, numeric(0-9) and a special character '\0' for space. So, our algorithm will encrypt lowercase, numeric, symbols as well as spaces.

Our proposed algorithm will encrypt case sensitive data, spaces, numeric and special symbols. In future, we will extend the given table to include more symbols.

REFERENCES

[1] Jitendra Choudhary, Prof. Ravindra Kumar Gupta, Dr Shailendra Singh, " A GENERALIZED VERSION OF PLAY FAIR CIPHER", COMPUSOFT, An international journal of advanced computer technology, 2 (6), June-2013 (Volume-II, Issue-VI).

[2] Mohammed Haris, Bhavya Alankar, "A Survey Paper on Different Modification of Playfair Cipher", International International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017.

[3] Mohit Marwah, Rajeev Bedi, *Amritpal Singh, Tejinder Singh, "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS", Singh et al., International Journal of Advanced Engineering Technology, E-ISSN 0976-3945, Int J Adv Engg Tech/IV/III/July-Sept.,2013/16-18.

[4] Ravindra Babu K[1], S. Uday Kumar [2], A. Vinay Babu [3], I.V.N.S Aditya4, P. Komuraiah5, "An Extension to Traditional Playfair Cryptographic Method", Volume 17– No.5, March 2011.

[5] Sanjay Kumar Mathur1, Sandeep Srivastava2, "Extended 16x16 Play-Fair Algorithm for Secure Key Exchange Using RSA Algorithm", Volume: 4 Issue: 2.

[6] V.Subhashini1, Dr.N.Geethanjali2, P.Vidyasagar3, P.Amrutha4 1Research Scholar, "A Novel Approach on Encryption and Decryption of 5X5 Playfair Cipher Algorithm", International Journal of Advanced Scientific Technologies, Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017.

[7] S.S.Dhenakaran, PhD. Assistant Professor, M. llayaraja research socholar , "Extension of Playfair Cipher using 16X16 Matrix", International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012.

[8] Reena singh, Shaurya taneja, Kavneet kaur, "Modified Play-fair Encryption Method using Quantum concept", DIACom-2016; ISSN 0973-7529; ISBN 978-93-80544-20-5

AUTHORS PROFILE

Munish Mehta Assistant Professor at NIT Kurukshetra Doctor of Philosophy (PhD), Master of Computer Application.

Vijay Goyar MCA Student at NIT Kurukshetra, Bachelor of Application from the University of Rajasthan

Vishnu bairwa MCA Student at NIT Kurukshetra, Bachelor of Application from the University of Rajasthan.