A Classical Cipher Approach for Securing Web User Data

Pradeep Kumar Sadh[1]* Dr. Pratima Gautam[2] Dr. Rajendra Gupta[3]

[1]Research Scholar, AISECT University, Bhopal (M.P.) India

[2]Dean, Dept of CSE, AISECT University, Bhopal (M.P.) India

[3]Assistant Professor, AISECT University, Bhopal (M.P.) India

Abstract – In Cryptography, when the data is converted in other form, some methods are required to convert the data. This method is using encryption and decryption technique and the converted data is called cipher text. In this paper, three methods of cipher are discussed with solution. The understanding of decryption techniques such as functional analysis, security attack and classical cipher attack has studied and also focused on how these techniques work and how they differ with each other. The study shows the cipher techniques are safe but time consuming as compared to other encryption and decryption techniques.

Keywords: Cipher, Shift Cipher, Affine Cipher, Transposition Cipher

---------------------------♦-----------------------------

I. INTRODUCTION

When a user send the message to another web user over the network, the data or text is converted in secure form for the security purposes. The text which a user sends over the network is treated as plain text and when it is converted in another form, call cipher text. Cipher text is also being referred as encrypted text. Before encryption the text is called plaintext. In cryptography, cipher is an algorithm which is applied over the plain text to get the cipher text. Other name for cipher text is encrypted or encoded information because it is unreadable or not understandable by a user or computer without the proper algorithm. The reverse of encryption is called decryption. It is the process of turning the cipher text into readable form which is called plaintext. Coded text and cipher text are completely different. Coded text is a result of a code, but not a cipher.

Plain text is not mandatory text only. It can be another form of media like an audio, video, an image also. The plain text and cipher text is a generic name for the input to the Encryption algorithm. The Encryption algorithm is suggested a short name like Cipher. The output of this cipher is called cipher text. Cipher text is generally in hexadecimal notation or in binary.

When a user sends any text using any media software or application, it is first be encrypted. So, no other third party or person can read the text. Whereas the receiver for whom a user sends the message or text can read the message in its original form of text.

II. AN OVERVIEW OF CIPHER TECHNIQUES

The simple data is known as Plain text and data after encryption is known as Cipher text. The process of encryption hides the data in such a way that an attacker cannot hack the data. The main purpose of encryption is to hide the data from unauthorized parties from viewing and altering the data. Encryption techniques occur or used by using shifting techniques and mathematical operations over the data.

A transposition cipher can easily be recognized by an analysing the character frequencies. Some of the iterating transposition ciphers greatly increase the security, but as with substitution ciphers, almost all such ciphers can be studied and can be broken. However, many modern cryptosystems incorporate transposition cipher in which the operation on large data sets has the disadvantage of requiring enough memory that consumes time.

One of the cipher techniques called polyalphabetic were invented in the year 1467 by the Florentine architect Alberti, who devised a cipher disk with a larger outer and smaller inner wheel respectively and indexed it by plaintext and cipher text characters. In this technique, letter alignments are defined with a simple substitution and modified by rotating the disk after enciphering few words. In the year 1918, the first printed book on cryptography was published on this technique Polygraphia, written by the German monk Trithemius. This book demonstrate the concept of polyalphabetic in which a square tableau is proposed with 24 characters listing all shift substitutions for a fixed ordering of plain text alphabet characters. The tableau rows were used sequentially to substitute one plain text character each for 24 letters. In the year 1553 a researcher Belaso suggested the use of easily changing key to define the fixed alphabetic (shift) substitutions in a polyalphabetic substitution. A Polyalphabetic cipher has many advantages over simple substitution ciphers. However, it is also noticed that the polyalphabetic ciphers are not significantly more difficult to crypt analyze, because the approach is very much similar to the simple substitution cipher. Once the block length is determined in this cipher, the cipher text letters can be divided into groups and a frequency analysis can be done on each group.

Following are the most popular techniques for converting the plain text into cipher text. These are Shift Cipher, Affine Cipher and Transposition Cipher. The detailed description of these techniques is as given below:

(a) **Shift Cipher-** Shift Ciphers work with the use of modulo operator to encrypt and decrypt the messages. The Shift Cipher uses a key K, which contains an integer from 0 to 25. The shift cipher can be checked by sharing this key K with the person to whom we want to see the sending message.

Following is the procedure of encrypting the message:

For every letter in the message say M :

(i) Convert the letter in the form of numbers that matches its order in the alphabet and that should be started from 0; say this number X.

[A = 0, B = 1, C = 2, D = 3, ...,Y = 24, Z = 25]

(ii) Than calculate: Y = (X + K) mod 26 where K is key

(iii) Convert the number **Y** into its equivalent letter that matches its order in the alphabet which starts from 0. [i.e. A = 0, B = 1, C = 2, D = 3, …….,Y = 24, Z = 25]

When user A is sending some message to user B on the network, the data of A can be encrypted using key K (suppose K = 19) in the following way;

The user A is sending message KHAS to user B, which can be encrypted as follows:

K H A S

10 7 0 18

+ 19 19 19 19

------------------------

(29 26 19 37) mod 26

3 0 19 11

------------------------

D A T L

So, after applying the Shift Cipher with key K = 19 the message of user A "KHAS" produce the cipher text "DATL". This encrypted date is sent to user B. This encrypted data is decrypted using decryption process in which the cipher text is converted in plaintext.

Following is the procedure of decrypting the encrypted message:

For every letter in the cipher text C :

Convert the letter into its corresponding number that matches its order in the alphabet which starts from 0, and say this number Y.

(i) [A = 0, B = 1, C = 2, D = 3, ..., Y = 24, Z = 25]

(ii) Than Calculate : X = (Y - K) mod 26 where K is a Key

(iii) Convert the number X into a letter that matches its order in the alphabet which starts from 0.

(iv) [A = 0, B = 1, C = 2, D = 3, ..., Y = 24, Z = 25]

With the same key K having value 19, user B can decrypt the encrypted message in the following way:

D A T L

3 0 19 11

- 19 19 19 19

------------------------

(-16 -19 0 -8) mod 26

10 7 0 18

K H A S

So, after decrypting the Shift Cipher with the use of same key value K = 19, the user B deciphers the cipher text "DATL" with the message text "KHAS".

This process of encryption and decryption is very simple and having single stage to convert plain text into cipher text and vice-versa. The limitation of this cipher technique is the fix letter numbers (i.e. 26 always for key). Someone can easily try all the 26 letters one by one until the recovery of the user message. This is one of the types of brute force attack.

(b) Affine Cipher

As seen in the above procedure of cipher, a shift cipher can produce only 25 different transformations for the given text. This type of encryption method is not called secure method. The affine cipher method is a generalization of the shift cipher which provides a little bit additional security. The affine ciphers do apply multiplication and addition to each character using the following function:

$y = (ax + b)$ MOD m

here x is the numerical value of the letter in the plain text, m is assigned as the number of letters in the plain text alphabets, a and b which are the secret numbers in the process and y is the output of the transformation. The letter y can be decrypted again to x by using following formula:

x = inverse (a) ($y – b$) MOD m

here inverse(a) is a value such that if it is multiplied with a MOD m the output would be 1, which mean a * inverse(a) MOD m = 1

Let the secret numbers are a = 11 and b = 4. Applying these numbers in the above equation that gives encryption function

$y = 11x + 4$ MOD 26

here letter E and S will be encoded to W and U as shown in example below. Since the computation involves modulo 26 arithmetic, several letters may fail to be uniquely decoded if the multiplier has a common divisor with 26. Therefore, the greatest common divisor of a and m must be 1.

Encipher Process

Assume the message is encrypted by the function $y = (11x + 4)$ MOD 26 To encrypt the plaintext MONKEY, we first convert each letter in plaintext into a numerical value between 0 and 25 according to following list

A	-	0
B	-	1
C	-	2
D	-	3
.		
.		
.		
Z	-	25

Thus, the numerical values corresponding to the plaintext MONKEY are 12, 14, 13, 10, 4, and 24.

Applying the given function for each numerical value, we have

M : y = (11*12 + 4) MOD 26 = 6

O : y = (11*14 + 4) MOD 26 = 2

N : y = (11*13 + 4) MOD 26 = 17

K : y = (11*10 + 4) MOD 26 = 10

E : y = (11*4 + 4) MOD 26 = 22

Y : y = (11*24 + 4) MOD 26 = 8

The corresponding letters are **GCRLWI,** which is the cipher text.

Decipher Process

To decipher, we transform the function y as:

x = inverse (a) ($y – b$) MOD m

Then we have, x = inverse (11) ($y – 4$) MOD 26

Inverse (11) MOD 26 = 19, and the decryption function will be $x = 19 (y – 4)$ MOD 26

We now decipher the cipher text GCRLWI by applying the decryption function. We have:

G : y = 19* (6 - 4) MOD 26 = 12

C : y = 19* (2 - 4) MOD 26 = 14

R : y = 19* (17 - 4) MOD 26 = 13

L : y = 19* (10 - 4) MOD 26 = 10

W : y = 19* (22 - 4) MOD 26 = 4

I : y = 19* (8 - 4) MOD 26 = 24

The corresponding plaintext letters are **MONKEY**.

Since each letter in plaintext is enciphered in this algorithm using function of $y = (ax + b)$ MOD m, the user can break the affine cipher by solving two linear mathematical equations with two examples of variable x and y. Once the values of a and b is obtained, the plain text can be decipher the entire cipher text.

The above concept can be explained in following way,

Assume that the word "**IF**" is enciphered as "**PQ**".

I → P : 8a + b = 15 MOD 26

F → Q : 5a + b = 16 MOD 26

After solving the above equations, the value of *a* and *b* would be 17 and 9 respectively.

(c) **Transposition Cipher-** The transposition cipher is one another kind of cipher technique in which Instead of replacing characters with other characters, it just change the order of the characters. Generally, the text to be encrypted is set in a number of columns. These columns are again reordered and produce encrypted text. Here to decrypt a cipher text using a transposition cipher, we need to find the number of columns and then rearrange the columns according to that.

The Columnar Transposition is one of the best examples of a Transposition Cipher. To understand the concept of transposition cipher, take a message (plaintext) and arrange it into some columns. Suppose the phrase is "WE ARE DISCOVERED FLY AT ONCE" – and add a bit of padding (random characters) to the end to make each column equal.

W E A R E D

I S C O V E

R E D F L Y

A T O N C E

Q K J E U

Now, each column can be converted vertically to create the cipher text.

In this way, we can reach at a relatively secure cipher text. In order to decrypt and read the message, there can be two options: Either read through the message letter by letter (by skipping to the next word) or rearrange the letters in columns. The key can be decided by watching the number of columns and how many letters fit into each column. With this information in hand, decrypting this message is easy.

One more explanation of a transposition cipher is as follows;

A transposition cipher is a method in which letters are rearranged in an order in the cipher text (encoded text), according to some predetermined procedure without making any substitution.

Let us encrypt the following text message;

"Now run along and do not get into mischief, I am going out". In this sentence, remove the punctuation and the blank spaces between words. Finally, the following sentence is obtained.

"now run a long and do not get in to mischief i am going out".

These are 46 letters in length. Now add 4 extra padding characters, suppose "a", at the end to now get:

"now run a long and do not get in to mischief i am going out a a a a".

We can now write this message in 4 rows, having each 12 letters long.

n o w r u n a l o n g a

n d d o n o t g e t i n t

o m i s c h i e f i a m

g o i n g o u t a a a a

By taking the letters in a order down the columns, instead of along the rows, the following sentence is obtained :

"nnog odmo wdii rosh uncg ntho agiu leet otfx niix gnax atmx"

Now this sentence can be sent to another user with removing the spaces, and the message is "hidden".

Suppose the hacker try to intercept and wants to decipher the above message. Let's check to how to decipher a message encoded in this way:

48 characters can be encoded using grids of one of these dimensions:

1 × 48, 2 × 24, 3 × 16, 4 × 12, 6 × 8, 8×6, 12×4 ...

The first of these doesn't rearrange the message at all.

The second size gives:

n n o g o d m o w d i i r o s n u n c g n t h o

a g i u l e e t o t f x n i i x g n a x a t m x

Reading down the columns gives "nangoigu....". Definitely not English!

The next arrangement is a 3 by 16 grid:

n n o g o d m o w d i i r o s n

u n c g n t h o a g i u l e e t

o t f x n i l x g n a x a t m x

A 4 by 12 grid gives:

n n o g o d m o w d i i

r o s n u n c g n t h o

a g i u l e e t o t f x "nrannogi..."

n i l x g n a x a t m x

and a 6 by 8 grid gives:

n n o g o d m o

w d i i r o s n

u n c g n t h o "nwuaog.."

a g i u l e e t

o t f x n i l x

g n a x a t m x

An 8 by 6 arrangement gives:

n n o g o d

m o w d i i

r o s n u n "nmrcaena...."

c g n t h o

a g i u l e

e t o t f x

n i l x g n

a x a t m x

A 12 by 4 sized grid gives:

n n o g

o d m o

w d i i

r o s n

u n c g

n t h o

In the above procedure, a plain text can be converted into cipher text using different ways of arrangement. But this is a very simple substitution ciphers which uses a single mapping from plaintext to cipher text letters. Also the same plaintext is having the same cipher text. This characteristic is not always better in cryptography from the security point of view.

III. LITERATURE REVIEW

To protect the user from unauthorized access and data hacking, several encryption and decryption methods have been proposed by researcher.

In cryptography, an Attribute-based encryption (ABE) scheme in proposed in which messages are encrypted and the decryption keys are calculated according to the given set of attributes and an access structure on the set of attributes. In a traditional KP-ABE method, the characteristics of specified attributes have been treated at the same level. In real environment applications, each attribute has a different weight according to its significance (Liu, et. al., 2014).

In the current time, web technology has become faster and stronger. Large number of users are using it to store sensitive data on third party servers, either for cost saving or for simplicity of sharing of data (Wan, et. al., 2012).

The applications which run in clouds can balance several factors including load balancing, bandwidth, size of data and security. One of the major problems to cloud adoption is data security and privacy. Because the data owner and the service provider do not remains within the same trusted domain (Balamurugan and Venkata Krishna, 2014).

Attribute-Based Encryption (ABE) is proposed as public key cryptographic technique that works in one-to-many fashion and it is also called fuzzy encryption technique. Public key encryption methods store encrypted data on third party servers, while distributing decryption keys to authorized users. But this concept is having many drawbacks. First, it is difficult to efficiently manage the distribution of secret keys for authorized user. Secondly there is a lack of flexibility and scalability in the system. Third, data owners should be online, whenever encrypting or re-encrypting the data or during the distribution of the secret keys. The proposed algorithm ABE minimizes these limitations by reducing the communication overhead of the internet and increasing scalability, flexibility for large scale systems (Li, et. al., 2013).

In the cloud environment, the data security is crucial to protect against inside attack, denial of service attack and collision attack. Additionally, the different expressive access control policies are used to protect user data stored locally and the data stored remotely (Purushothama and Amberker, 2012).

The enormous number of transfer of data and the information takes place using web that is considered to be the most efficient even though it is definitely a public access medium. To counterpart this limitation, many researchers have come up with emerging algorithms to encrypt the information from plain text into cipher text (Kester, 2013. Kester, & Paul, 2012).

In the field of information security, the encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those are having good knowledge, usually referred to as a security key. The result of this process is called encrypted message. The reverse process of this is referred to as decryption (Sinkov, 1966).

There are two main algorithmic approaches are there for encryption, symmetric and asymmetric. Symmetric-key algorithms (Courtois & Pieprzyk (2002). are a special type of algorithms under cryptography that uses the same cryptographic keys for both encryption of plaintext and decryption of cipher text. These security keys may be identical or not. The keys, in practice, represent shared secret information between two or more parties that can be used to maintain private information links (Hans & Helmut (2007). This requirement that both parties have access to the secret key is one of the main drawbacks of the symmetric key encryption method as compared to public-key encryption. Typical examples of symmetrical algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent (Gary & Carl, 2007).

On the other hand, Asymmetric or Public key encryption is an encryption method where a message is encrypted with a recipient's public key that cannot be decrypted by anyone except a possessor of having private key and the person associated with the public key used. This is used for confidentiality purposes (Kester & Koumadi, 2012).

In present days, the cryptography entails complex and advance mathematical algorithms that are applied for encryption of text and cryptographic techniques for image encryption based on the RGB pixel displacement where pixels of image are shuffled to obtained a cipher image (Aiden & Mario, 2011).

According to one of the researcher, in case of all single alphabet substitution ciphers, the Caesar cipher is easily broken and the present study offers essentially no communication security (Encryption, 2011).

The Vigenère cipher is one of the security methods of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. This is a simple form of polyalphabetic substitution (Aiden & Mario, 2011). (Martin, 2012). This type of Cipher spoils the statistics of a simple Caesar cipher by using multiple Caesar ciphers. The technique is named for its inventor, Blaise de Vigenère from the court of Henry III of France in the sixteenth century, and was considered unbreakable for around 300 years (Reinhard, 2001).

According to Wobst and Reinhard, the greater character set allows more type of messages to be encrypted like passwords. It is also increases the key domain and hence provides more security (Rahmani, et. al., 2012).

Alfred Tennyson has encrypted the text according to the keyword "Emily", which is the first name of Tennyson's wife. Studies of Babbage's notes reveal that he had used the method later published by Kasiski (Hans & Helmut (2007). [20]. In the field of cryptography, a transposition cipher is a process of encryption by which the positions of the text is altered by units of plaintext and shifted according to a regular pattern, so that the cipher text constitutes a permutation of that plaintext. Mathematically, an objective function is used to change the characters' positions to encrypt the text and an inverse function to decrypt it. The letters themselves are kept unchanged, which implies that the effect is only on their positions only. Making of their order within the message scrambled according to some well-defined scheme. A number of transposition ciphers are done according to a geometrical design (Rahmani, et. al., 2012). Franksen, 1985).

In a columnar transposition approach, the message is written out in rows of a fixed length and then it is read out again column by column, and the columns are also chosen in some scrambled order wise. In this case, both the width of the rows and the permutation of the columns are usually defined by a keyword (i.e. key) The advanced form of columnar encryption technique is used for encryption purposes in a matrix representation form (Kester, 2012).

IV. DISCUSSION

After studying various cipher techniques, cryptanalysis and cryptography proposed by many researchers, it is found that the study of cryptanalysis is very much needed for securing the web user data over the network.

By applying already proposed algorithms of cipher over the data, almost same result is found and by applying same algorithm over different types of data items, the algorithm performed differently.

It is also noticed that how Symmetric and Asymmetric ciphers differ and how they both have pros and cons. An example is taken in the study of cipher to get the proper understanding of encryption and decryption. In some cases, the studied cipher techniques don't found good result. So these techniques have been implemented in the current study and found satisfactorily outcomes.

The researcher has gained knowledge and better understanding of encryption/decryption techniques and its most popular algorithms like Transposition, Hill, Affine, Shift cipher algorithms and the researcher states that further study is required to protect user data using implementation in above proposed techniques to decrypt substitution.

V. CONCLUSION

Three cipher techniques; shift cipher, affine cipher and transposition cipher are explained with the example to show how much cipher data is secured over the network. The security in cipher should have keywords (password) that should be easy to remember and understand, should be easy to apply without errors and offer a good security. Different stages and procedures are required like substitution, transposition as well as fractionation to resist cryptanalysis. The user must determine whether he is eager on security, applicability or speed on the net. The cipher techniques as described in this study provide the latest and strongest encryption combinations before the era of digitalization in networking cryptography and providing a guideline to the development of encryption scheme. Many combinations, extensions and adaptations has been taken in the above explained techniques are possible. It is noticed that although attacking some of these ciphers requires extensive and complex cryptanalytic techniques, the modern computational system can break them by a powerful brute force.

VI. REFERENCES

Abraham Sinkov (1966). Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966. ISBN 0-88385-622-0

B. Balamurugan and P. Venkata Krishna (2014). Extensive survey on usage of attribute based encryption in cloud, Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, pp. 263–272.

B. R. Purushothama and B. B. Amberker (2012). Access control mechanisms for outsourced data in cloud, in Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on. IEEE.

Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. http://books.google.com/books?id=fd2LtVgFzoMC& pg=PA21.

Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. http://books.google.com/books?id=fd2LtVgFzoMC& pg=PA21.

Classical cipher, Transposition ciphers, Retrieved from http://en.wikipedia. org /wiki/Classical_cipher

Delfs, Hans & Knebl, Helmut (2007). "Symmetrickey encryption". Introduction to cryptography: principles and applications. Springer.

Encryption (2011). Wellesley college Computer Science Department lecture note retrieved from : http://cs110.wellesley.edu/lectures/L18-encryption/

Franksen, O. I. (1985). Mr. Babbage's Secret: The Tale of a Cipher—and APL. Prentice Hall.

Kester, Q. A., & Koumadi, K. M. (2012). Cryptographie technique for image encryption based on the RGB pixel displacement. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on (pp. 74-77). IEEE.

Kester, Q.-A. (2012). "A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference, Vol., No., pp.78-81, 25-27 Oct. 2012

Kester, Quist- Aphetsi., & Danquah, Paul (2012). A novel cryptographic key technique. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on (pp. 70-73).

Kester, Quist-Aphetsi (2013). "A cryptosystem based on Vigenère cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology(IJARCET) [Online], 1.10 (2012): pp: 108-113.

M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143.

Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. http://books.google.com/books?id=1NHli2uzt_EC&p g=PT142.

Mullen, Gary & Mummert, Carl (2007). Finite fields and applications. American Mathematical Society. p. 112 IEEE 1363: Standard Specifications for Public-Key Cryptography

Nicolas Courtois, Josef Pieprzyk (2002). "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT.

Rahmani, M. K. I., Wadhwa, N., & Malhotra, V. (2012). Advanced Computing: An International Jour nal (ACIJ). Alpha-Qwerty Cipher: An Extended Vigenere Cipher, 3 (3), pp. 107-118.

Transposition ciphers, columnar transposition Retrieved from http://en.wikipedia.org/wiki/Transposition_cipher

Wobst, Reinhard (2001). Cryptology Unlocked. Wiley. pp. 19. ISBN 978-0-470-06064-3.

X. Liu, H. Zhu, J. Ma, and S. Ma (2014). Key-policy weighted attribute based encryption for fine-grained access control, in ICC14-W5: Workshop on Secure Networking and Forensic Computing.

Z. Wan, J. E. Liu, and R. H. Deng (2012). A hierarchical attribute based solution for flexible and scalable access control, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754.

Corresponding Author

Pradeep Kumar Sadh*

Research Scholar, AISECT University, Bhopal (M.P.) India

E-Mail – rajendragupta1@yahoo.com