iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8180

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

A Study of Implemented Classical Cipher Techniques for Better Security Solution

Dr. Rajendra Gupta[1], Pradeep Kumar Sadh[2], Dr. Pratima Gautam[3]
[1]*Assistant Professor,* [2]*Research Scholar,* [3]*Dean, Dept. of Computer Application, AISECT University, Raisen*

Abstract: ***The cryptography is a method of converting plan text data into non-readable form so that the data can be protected from hacking. There are two main techniques used for converting data into other form; Transposition technique and Substitution technique. The main objective of this paper is to explain some classical cipher techniques along with its solution. In this paper, two implemented cipher technique 'Two Way Cipher Transposition' and 'Disorder Cipher Transpositions' have been studied and implemented over original message. The analysis of these two implemented techniques found that these techniques are more strong and convenient than the previous transposition techniques.***
Keywords : Classical Cipher, Two Way Cipher Transposition, Disorder Cipher Transpositions

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. 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 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 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 cryptanalyze, 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:

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 [1].

In present days, 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 [2].

The applications which run in clouds can balance several factors including load balancing, bandwidth, size of data and security. One of the major problem to cloud adoption is data security and privacy. Because the data owner and the service provider do not remains within the same trusted domain[3].

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 [4].

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 [5].

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 [6 - 7].

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 [8].

There are two main algorithmic approaches are symmetric and asymmetric. Symmetric-key algorithms [9] 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 [10]. 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 [11].

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 [12].

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 [13].

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 [14].

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 [15][16]. 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 [17].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

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 [18].

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 [10] [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 ciphertext 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 [18-19].

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) [20]. The advanced form of columnar encryption technique is used for encryption purposes in a matrix representation form [21-23].

IV. IMPLEMENTED CIPHER ALGORITHMS

To overcome the problem of cipher algorithms, some implementations have been done on transpositions schemes. The functioning of the implemented cipher algorithms is described as below.

A. Two Way Cipher Transposition

The two way cipher transposition or double columnar transposition was most probably much secure and very popular cipher techniques during the time of Second World War. At that time, this security algorithms was used by both allied and axis forces of army and a periodical changes of good keys ensured a very good resistance against cryptanalytic attacks. These algorithms were very easy to apply, although it was found that the process was time consuming for long messages. The disadvantage of the algorithms was that letter frequency analysis show a normal linguistic distribution, as similar to plaintext, which points to transposition. When enough ciphertext available, encrypted with the same key, an attack by anagramming could be successful, although it was very difficult. A very efficient way to beat the anagramming is to first fractionate the characters of the plaintext. The following explanation describes the functioning of the two way cipher transposition.

Suppose, the message to encrypt is :

WE ENSURES THE DELIVERY OF THE DOCUMENTS A

Now, suppose the keywords are : **SYSTEM** and **CONSPIRACY**

After getting the text message and keyword, we can make first transposition. Create a matrix and write the first keyword into that matrix. Beneath the keyword, make the sequence of how we read off the letters. Assign number 1 to the keyword letter that is first in the alphabet. The second letter 2 and continue the process. If two identical (same) letters occur in the keyword, the most left letter get the lowest digit. Now the first transposition matrix would be:

```
S Y S T E M
3 6 4 5 1 2
-----------
W E E N S U
R E S T H E
D E L I V E
R Y O F T H
E D O C U M
E N T S X
```

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Next, it is the time of creating a second matrix with the chosen second keyword. Again we will precede the same procedure to assign digits according to the order of the letters in the alphabet. Now read off the letters from the first transposition matrix column by column, according to the key order sequence and apply them row by row into the second matrix.
The second transposition matrix would be :

C O N S P I R A C Y
2 6 5 9 7 4 8 1 3 10

S H V T U U E E H M
W R D R E E S L O O
N T I F C E E E Y D

The final ciphetext is again read off column by column according to the key order sequence of the second keyword.

By watching the shifted letters in matrix, the final ciphertext in groups would be:

ELE SWN HOY UEE VDI HRT UEC ESE TRF

To decipher the two way transposition, we follow the reverse procedure or opposite direction to get plain text. Now, starting with creation of a matrix with the second keyword and determine the long and short columns (keep free places at the end) according to the length of the message. The ciphertext is arranged according to the matrix column-by-column and according to the keyword sequence. In the next step, first we create the matrix for the first keyword and determine the long and short columns according to the length of the message. Now, read off the matrix from the second keyword row-by-row and write it into the matrix of the first matrix, column-by-column, according to the keyword sequence of that matrix. Finally, the text should be read off row by row.
Here, the point to be noticed is that in much larger keywords or key sentences, 15 letters or more used to enable the encryption of large pieces of plaintext.

B. Disorder Cipher Transpositions

The disorder cipher transposition is a further complication to the normal transposition. In place of filling the matrix row by row, the rows are all filled in a very irregular fashion, resulting in two separate areas. This results in a very complex transposition of the characters. First, we determine the exact number of rows and columns to fill in the matrix. Next we fill a row until we reach the digit from the keyword sequence. If the first digit is at 8th place, we will only fill that row up to that position. We continue the next row until the second position and so on is filled. If we have reached the end position of the last line, we continue by filling the remaining empty places at each line. In the following example, the difference between two areas is visible by the lower and upper case characters.

Algorithm

Step 1: First select the plaintext which is to be encrypted from the sender side.
Step 2: Write down the plaintext randomly in a row of matrix or depth= 2 (two rows).
Step 3: Select a key K randomly as password
Step 4: A table is defined and set with column equal to the number of alphabet of the key K with rows that are sufficient to accommodate all the characters of the plaintext.
Step 5: The password is arranged in such a way that its occurrence in the alphabet i.e the alphabet closest to letter ‘a’ is assigned the first position in whatever column may be.
Step 6: The position of the alphabets is used to write the cipher text (CT1) in a row wise until the alphabet are getting over. This process is continued till all the characters position has been exhausted. If CT1 include some of the remaining characters then the blanks of the table in a row wise to fill left characters of cipher text in lower case, then we get cipher text CT2.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Step7: Apply the cipher text CT2 into classical Caesar cipher with key K2 and finally we get the cipher text (CT3). This cipher text is required Cipher text.
Suppose the plan text is as given below in capital letters;

WE ENSURE THE DELIVERY OF THE DOCUMENTS AND WILL SEND FURTHER INSTRUCTIONS A

We use the key CONSPIRACY

On the left we see the matrix after filling the first area and on the right we see the same matrix filled completely:

C O N S P I R A C Y	C O N S P I R A C Y
2 6 5 9 7 4 8 1 3 1 0	2 6 5 9 7 4 8 1 3 10
W E E N S U R E . .	W E E N S U R E a n
M	M d w I l l s e n d
T H E D E L I V E . .	T H E D E L I V E f
R Y O F T H . . .	R Y O F T H u r t h
E D O … … … . .	E D O e r i n s t r
CU … … … … . .	C U u c t i o n s x
M E N T S … … … .	M E N T S … … … ..

Once the matrix is filled up properly, we read it off by the columns, as per the keyword sequence.

According to this, several types of disruption are possible. Another possible method is that of large triangles. Usually the disruption method is used in one of the two transpositions of a double transposition, making it much stronger.

V. DISCUSSION

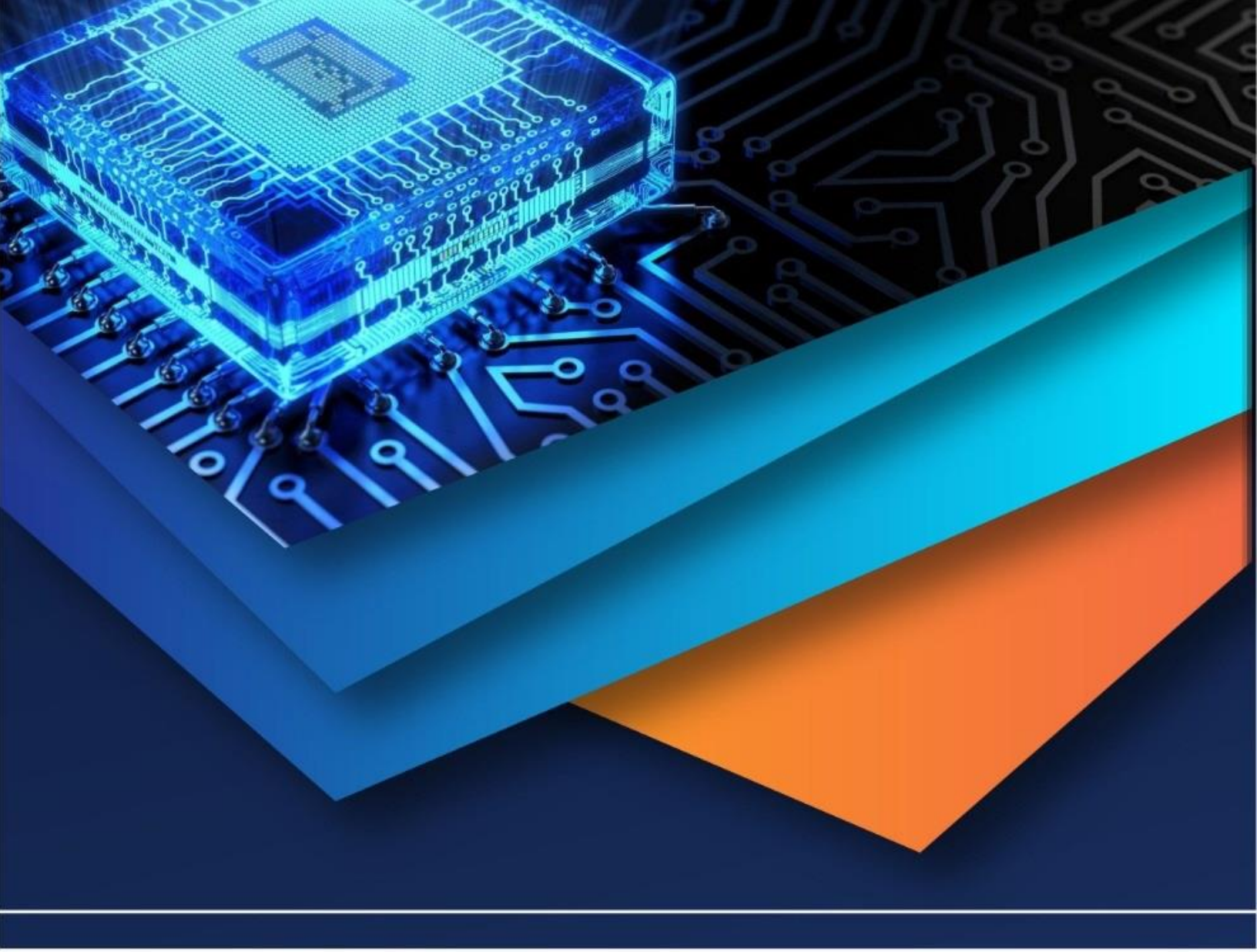
After studying various cipher techniques, cryptanalysis and cryptography proposed by many researchers, it is found that the study of cryptanalysis is very much needed for securing the web user data over the network.
By applying already proposed algorithms of cipher over the users data, almost same result is found and by applying same algorithm over different types of data items, the algorithms has 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 results. So these techniques have been implemented in the current study and found satisfactorily outcomes.
The understanding of decryption techniques such as functional analysis, security attack and classical cipher attack has studied and also investigated that how all these techniques work and how they differ with each other. The researcher has a solid idea of how the frequency analysis and security attack are implemented as they have been implemented in real life tests within their study.
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.

VI. CONCLUSION

The proposed cipher techniques 'Two way Cipher Transposition' and 'Disorder Cipher Transposition' provide valuable knowledge of cryptography and can be implemented in software design to secure the data. The algorithms are stronger than the previous one where the problem of encryption the bigger text message was arriving. The proposed algorithms are easy to understand and it is easy to apply in security purposes. The two way cipher transposition or double columnar transposition was most probably much secure and very popular cipher techniques in earlier time but the implementation in this technique performs better results. Further study of these two transposition techniques at different applications can produce valuable result.

REFERENCES

[1] X. Liu, H. Zhu, J. Ma, and S. Ma, Key-policy weighted attribute based encryption for fine-grained access control, in Icc14-W5: Workshop on Secure Networking and Forensic Computing, 2014.
[2] Z. Wan, J. E. Liu, and R. H. Deng, A hierarchical attributebased solution for flexible and scalable access control, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.
[3] Balamurugan and P. Venkata Krishna, Extensive survey on usage of attribute based encryption in cloud, Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, pp. 263–272, 2014.
[4] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, 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, 2013.
[5] B. R. Purushothama and B. B. Amberker, Access control mechanisms for outsourced data in cloud, in Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on. IEEE, 2012.
[6] Kester, Quist-Aphetsi. "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. Web. 16 Jan. 2013
[7] 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).
[8] Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966. ISBN 0-88385-622-0
[9] Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT 2002
[10] Delfs, Hans & Knebl, Helmut (2007). "Symmetrickey encryption". Introduction to cryptography: principles and applications. Springer, 2007
[11] Mullen, Gary & Mummert, Carl. Finite fields and applications. American Mathematical Society. p. 112. 2007
[12] IEEE 1363: Standard Specifications for Public-Key Cryptography
[13] Kester, Q. A., & Koumadi, K. M. (2012, October). 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.
[14] 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.
[15] Encryption. Wellesley college Computer Science Department lecture note retrieved from : http://cs110.wellesley.edu/lectures/L18-encryption/
[16] 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.
[17] Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. http://books.google.com/books?id=1NHli2uzt_EC&p g=PT142.
[18] Wobst, Reinhard (2001). Cryptology Unlocked. Wiley. pp. 19. ISBN 978-0-470-06064-3.
[19] 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), 107-118.
[20] Franksen, O. I. (1985) Mr. Babbage's Secret: The Tale of a Cipher—and APL. Prentice Hall..
[21] Classical cipher, Transposition ciphers, Retrieved from http://en.wikipedia. org /wiki/Classical_cipher
[22] Transposition ciphers, columnar transposition Retrieved from http://en.wikipedia.org/wiki/Transposition_cipher
[23] Kester, Q.-A.; , "A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY