International Journal of Computing and Applications | **ISSN: 0973-5704**
Volume 13, Number 2, (July-December 2018), pp 349-354

COMPARATIVE ANALYSIS OF CRYPTOGRAPHY CIPHER TECHNIQUES WITH CLCT TECHNIQUE

Sandeep Kumar[1], Rahul Johari[2] and Laukendra Singh[3]

[1-3]University School of Information & Communication Technology, GGSIPU, Dwarka, New Delhi-78, India.
Email: [1]sandeepkumar.ipu@ieee.org, [2]rahul.johari.in@ieee.org, [3]laukendrasingh.ipu@gmail.com

Abstract: Now a days, Internet based network applications are growing at a very fast rate. So the value and importance of the exchanged data over the internet or other type of media are increasing. To handle security threats latest data transfers methodologies uses cryptography as an effective, efficient, and essential component for secure transmission of information by implementing security parameters naming Confidentiality, Authentication, integrity, availability and accuracy. Cryptography is an example of the data security that transforms information from its plain normal form into an unintelligible form by using secure encryption techniques and vice-versa. In current work, comparison has been carried out of the cipher techniques like Caesar Cipher, Affine Cipher, Rail Fence Cipher, with proposed CLCT Cipher technique. The simulation has been carried out by programming Eclipse IDE Tool, using JAVA, an open source programming language. The analysis shows the CLCT cipher technique is stronger in nature due to diffusion property.

Keywords: Security, Cryptography, Caesar Cipher, Affine Cipher, Rail Fence Cipher, CLCT Cipher.

1. INTRODUCTION

Today Organization's realize the need for security of data. Organizations use wired or wireless network to carry out their daily commercial transactions or operations including sensitive data transfer. Various sensitive information like banking transactions, confidential data, and credit information is transferred over internet. To protect this type of information or data there is a great need of security of customer data such as Credit and Debit Card Information as mandated by various security controls. So organizations have to pay a huge price in case data is compromised, especially customer's confidential data. Basically data security means protecting its confidentiality, integrity, authentication and availability[1]. Now the term cryptography is introduced to provide the solution for these types of security issues. Cryptography is the subdivision of cryptology in which encryption and decryption are deployed, to guarantee the security and authentication of data.

The term cryptography is also defined as "Cryptography is an art or science of encompassing the principles and methods of transforming an intelligible data text into one that is unintelligible and then retransforming that data text back to its original form". Figure 1 shows the concept of cryptography. Cryptography is classified as symmetric key cryptography and asymmetric key cryptography [1][2].

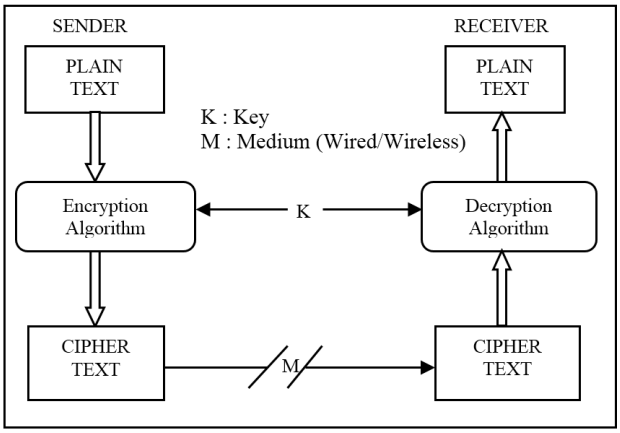

Figure 1: Functional diagram of cryptography

1.1. Security Issues

If the scope to a specific organization is defined to focus on the consequences of security attacks in case of Software Company, it can be summarized as :

- Stealing the plans and strategy of the organization for their own profit.
- Stealing the company database to capture the market.
- Stealing the organization's code and technology and changing the code to generate problem for the company.
- Stealing the address, location details of the customer.

1.2. Ciphers

As Well known, a cipher is an algorithm that contains a series of well-enumerated steps for performing encryption or decryption [2]. Most ciphers can broadly be classified in several ways. Figure 2 shows a classification of ciphers in two categories i.e. Traditional Cipher and Modern cipher.

Block Cipher: Block cipher works on set of symbols usually of a fixed and finite size called block that is entire message is divided into blocks which have the same fixed size and after then text is encrypted block by block.

Stream Cipher: Whereas stream cipher works on continuous stream of symbols/characters.

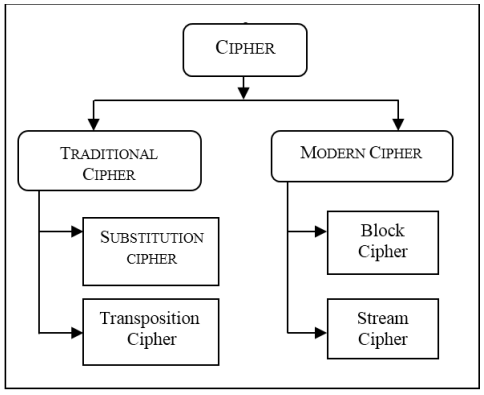

Figure 2: Classification of Cipher

Substitution cipher: In such a cipher technique, cipher substitute one symbol with another. Substitution cipher is categorized into two categories that is monoalphabetic cipher and polyalphabetic cipher. In monoalphabetic cipher, a symbol or word or a character in the original text is changed to the exactly same symbol or character in the ciphertext regardless of its position in the text. In polyalphabetic cipher, each occurrence of symbol probably can have a different substitute. The relationship between the symbols in the plaintext and symbols in the ciphertext is one-to-many relationship.

Transposition Cipher: There is absolutely no substitution of characters; instead their location or position change. In other words, a transposition cipher permutes or reorganize the order of symbols in a block of symbols.

1.3. Cipher Model

Cipher model scheme has majorly five ingredients [2]:

Plaintext: This is the original readable text or message that is usually fed into the algorithm as main input.

Cipher-text: This is an unreadable message produced as output. It depends on the plain-text and the secret/public key. For a given message, two different keys will generate two different ciphertexts. The ciphertext generated is an random stream of data or digits and, as it usually unintelligible.

Secret/Public key: Secret key is also an input to the symmetric encryption algorithm and private-public key combination is used in asymmetric encryption algorithm. The key value is independent of the plaintext and of the algorithm. The algorithm will generate a result as output depending on that particular key being used at that point of time.

Encryption algorithm: The algorithm performs various transformations and substitution on the plain text with the help of secret/public key and result unintelligible text (cipher text).

Decryption algorithm: This is a reverse method of the encryption algorithm. As Well known, it takes the cipher text and the secret/public key as the main source of inputs and thereby produces the actual plaintext.

1.4. Cipher Techniques

There are various cipher techniques proposed by researchers as per the need for secure transmission of data. Some of the cipher techniques which were proposed earlier are listed here:

Caesar Cipher: Caesar cipher or Additive cipher is one of the simplest and most widely known cipher techniques. This is type of substitution cipher [2]. Encryption and decryption operations are described as follows:

Encryption: Ciphertext = (Plaintext + Key) mod26.

Decryption: Plaintext = (Ciphertext − Key) mod26

Affine Cipher: Affine cipher is an example of a mono-alphabetic cipher that performs two arithmetic operations multiplication and addition that is two secret keys are used, one for multiplication and other for addition in this cipher technique. Encryption and decryption operations are described in the following:

Encryption: $\text{Ciphertext} = ((\text{Plaintext} \times \text{Key1}) + \text{Key2}) \bmod 26$.

Decryption: $\text{Plaintext} = (\text{Key}^{-1} \times (\text{Ciphertext} - \text{Key2})) \bmod 26$

Rail Fence Cipher: It is very interesting and intelligent cipher that has been used for decades. In Rail Fence cipher, plaintext is written downwards diagonally, then moving up when we reach the bottom rail. When we reach the top rail, the text or message is written downwards again until the whole text is written out. In Rail Fence cipher, key is used as the number of rails. The message or text is then read off in rows.

Example: If we have 3 rails and plaintext "CRYPTOGRAPHY IS AN ART", then it is arranged as:

C . . . T . . . A . . . I . . . A . . .

. R . P . O . R . P . Y . S . N . R .

. . Y . . G . . . H . . . A . . . T

Now, Ciphertext obtained is: CTAIA RPORP YSNRY GHAT

CLCT Cipher: [6]Cross Language Cipher Technique (CLCT) is a new type of cipher technique that uses two functions: Language Converter and Encryption with their different functionalities at sender side and results in a more powerful encrypted text. The function Language Converter (LC) replaces the English text value to the Hindi text value. Encryption function performs the operation like Caesar cipher function. The same functions are also used at destination side to produce the plaintext. Encryption and decryption functions are defined as follows:

Encryption: Ciphertext = (LC(Plaintext) + Key)) mod2416.

Decryption: Plaintext = (LC(Ciphertext − Key)) mod2416

2. RELATED WORK

In[3] author(s) have worked on information retrieval technique without performing any scrutiny on questions and answer authorization steps. The process is initiated by forming two different groups of a joint team naming, IXA NLP group and Elhuyar foundation. A foreign language naming Basque, basically belonging to the area around the Pyrennes in Spain and France is taken into account, as this language have not a large number of speakers in the world, and is also not related to any other language. The information retrieval tasks have been performed on two criterions: Mono lingual (English-English) and Bi-Lingual (Basque-English). In[4] author(s) have introduced a model based communication tool that have been focussed on online collaborations with respect to cross language collaborations leading to product development and, termed as Cross Language Transformation based on Recursive Object Model(CLT-ROM). A secure ROM is generated after the transformation of the sentence that is written in natural language, target ROM works on a transformation algorithm. Concept of using ROM is used as it provides clear description of the requirements. English sentences have been translated to the Chinese ROMs for collaboration that leads to the product development. The semantics are captured and also the information that is present in the natural language is preserved. In [5] author(s) have designed a Java based tool to depict the exploitation of Injection through SQL Injection attack and Broken Authentication using Brute Force Attack and Dictionary Attack. In[6] authors(s) introduce the Cross Language Cipher (CLCT) Technique, in which the plain

text file is fetched and then the cipher text generated is stored in language different from the original natural language. The plain text file is of English language and then it is converted to Hindi language along with an encryption process, making it difficult for the intruder to successfully attack the text file. In[7] author (s) describes the increased use of Hindi language subject matter over the web and other offline purposes over the last decade. Based upon this, an enhanced Cross Language Information Retrieval (CLIR), a sub-domain of Information Retrieval technique has been designed with the help of Näive Bayes algorithm accompanied by Particle Swarm Optimization (PSO) algorithm for improvements of ranking and searching aspects of CLIR systems, especially with respect to Hindi-English based CLIR. A document corpus for performing documents pre-processing and existing Microsoft Bi-Lingual dictionary are the integral part of the approach. As the word is featured in English language, it is clustered and ranked with the above said algorithms and PSO is implemented inside the clusters for ranking of the documents. In[8] author(s) describe the new cryptographic technique of using three keys for protecting the plaintext. In[9] author(s) have designed METHS technique in which mapping of confidential credit card number is done to Hindi language and then encrypted using affine cipher technique. Various types of testing have been conducted on an artificial e-commerce transaction environment designed on HTML page. In[10] author(s) attempts to develop a bi-lingual machine translation tool for sentences in simple present and past sentences. The translation of the user interface of a knowledge based system has been automated. The project executes the transformation process of well structured simple present and past sentences written in Arabic language to a well structured English sentence by using dictionary as a means for translation. The methodology which has been adopted is dependent on the basic structural components such as the parts of speech of a language that are necessary for translations.

3. PROPOSED WORK

The process of encryption and decryption has been accomplished in Java language. The already existing ciphers that is Caesar cipher, Affine cipher, Rail Fence and CLCT cipher are tried to convert plain-text to cipher-text.

3.1. Adopted Methodology

Program to implement Caesar cipher, Affine cipher, Rail Fence cipher, and CLCT cipher techniques were developed and designed in open source programming language : JAVA. The process used is defined in the following steps:

- A java program was written to read the text/ contents of the file.
- Stored, the text of the file in a variable.
- Read, the text from variable and print the same.
- Applied the encryption techniques: Caesar cipher, Affine cipher, Rail Fence cipher, CLCT cipher.
- Printed the encrypted contents of the file with execution time.

Cipher techniques like Caesar cipher, Affine cipher, and Rail Fence cipher were compared for their performance with CLCT cipher technique. The simulation was carried out using Java programming language. The relationship among the ciphers for a fixed size input text with their LOC, occupied memory, and execution time were performed and results are showcased in Table 1.

Table 1
Comparative Analysis of Cipher Techniques

Cipher Techniques	*Input Text Size (in bytes)*	*Program (LOC)*	*Execution Time (nano -seconds)*	*Memory Used (MB)*
Caesar Cipher	614	58	1.992	0.2546
Affine Cipher	614	83	2.778	0.2598
Rail fence Cipher	614	122	4.646	0.2523
CLCT Cipher	614	141	2.091	0.4889

The comparison shows that CLCT cipher technique takes less time than Affine Cipher Technique and it has more security advantage. The reason is that it is not vulnerable and not easy to find the plaintext due to the diffusion property. Figure 3 illustrates the graphical representation of the comparative results of Cipher techniques which is described in Table 1.

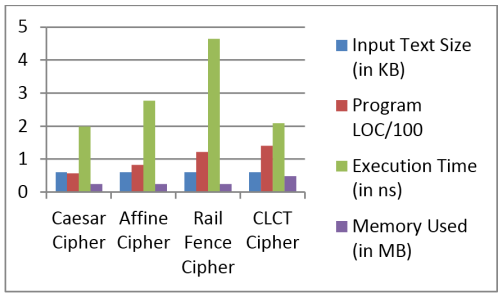

Figure 3: Graphical representation of relationship of ciphers

4. SIMULATION AND ANALYSIS

ECLIPSE IDE software has been used as simulator for implementation of Caesar Cipher, Affine Cipher, Rail Fence Cipher, and CLCT technique. The reason for using the Eclipse IDE 7.1 is that, it is open source. The code has been written entirely in java programming language because besides being open source it offers the flexibility of easy to code cryptographic functions. In hardware configuration, 32 bit Intel Atom Processor and 2GB main memory has been used. The snapshots are illustrated in the Figures 4 to 8.

Figure 4 illustrates the input text or plain text which is common for all the analyzing cipher techniques. Figure 5, Figure 6, Figure 7 and Figure 8 are illustrating the execution time and encrypted text of Caesar cipher, Affine cipher, Rail Fence cipher, and CLCT cipher technique respectively.

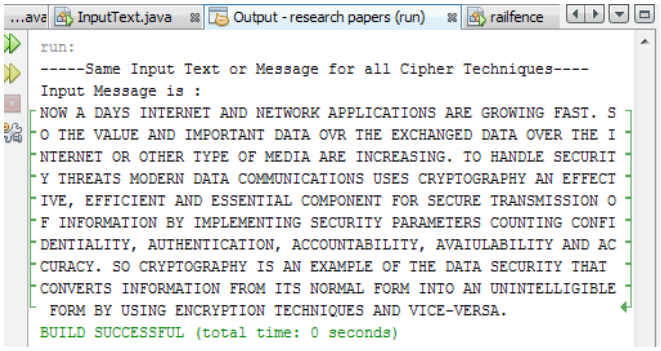

Figure 4: Input Text Common for All Cipher Techniques

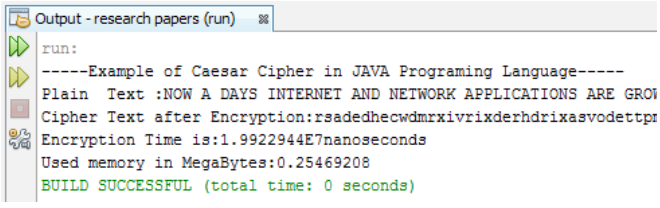

Figure 5: Encrypted Text of Caesar Cipher Technique with Encryption Time and Memory Used

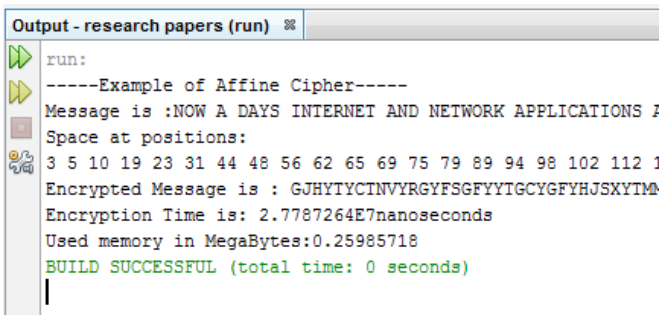

Figure 6: Encrypted Text of Affine Cipher Technique with Encryption Time and Memory Used

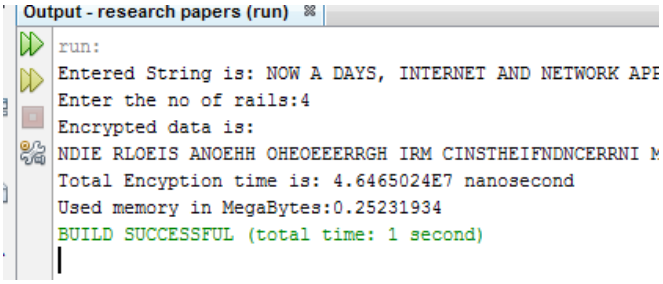

Figure 7: Encrypted Text of Rail Fence Cipher Technique with Execution Time and Memory Used

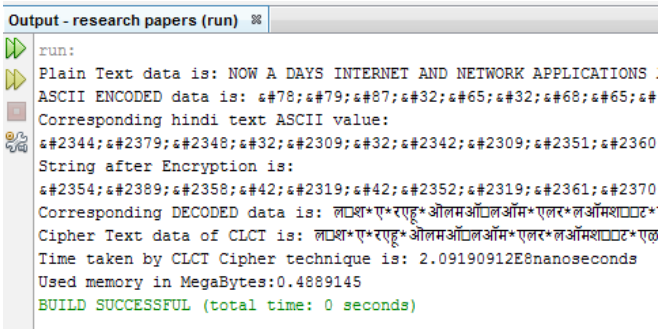

Figure 8: Encrypted Text of CLCT Cipher Technique with Execution Time and Memory Used

5. CONCLUSION AND FUTURE WORK

In this paper, useful aspects of various substitution encryption techniques have been discussed. Performance analysis of various cipher techniques has been discussed. Each technique is unique in its way, which is suitable for different applications. Everyday new encryption technique is evolving, hence fast and secure encryption techniques will always work out with high rate of security. After calculation of the execution time of the Caesar cipher, Affine cipher, Rail Fence cipher and CLCT cipher for the same input text/data size, result shows that CLCT cipher takes less time to execute the program and it is very strong in nature;

means that attacker could not able to find out the plain text easily.

In future work, it is proposed to compare the results of the CLCT cipher technique with many other cipher techniques like transposition cipher, Vigenere cipher, Hill cipher et.al with the security, time and space complexity parameters.

References

[1] Behrouz A. Farouzan "Cryptography and Network Security", Mc. Graw-Hill Special Indian Edition 2007.

[2] William Stallings "Cryptography and Network Security-Principles and Practices" Pearson fourth Edition 2007.

[3] Eneko Agirre, Olatz Ansa, Xabier Arregi1, Maddalen Lopez de Lacalle, Arantxa Otegi1, Xabier Saralegi and Hugo Zaragoza, "Elhuyar-IXA: Semantic Relatedness and Cross-Lingual Passage Retrieval", Springer-Verlag Berlin Heidelberg, 2010.

[4] Kunmei Wen, Suo Tan, Jie Wang, Ruixuan Li, Yuan Gao, "A model based transformation paradigm for cross-language collaborations", Advanced Engineering Informatics, Elsevier 2012.

[5] I. Jain, R. Johari, R.L Ujjwal "CAVEAT: Credit Card Vulnerability Exhibition and Authentication Tool". In: Second International Symposium on Security in Computing and Communications (SSCC-14), pp. 391-399. Springer 2014 .

[6] Laukendra Singh, Rahul Johari "CLCT: Cross Language Cipher Technique." In International Symposium on Security in Computing and Communication, Springer International Publishing. pp. 217-227. Springer International Publishing, 2015.

[7] Eva Katta, Anuja Arora, "An Improved approach to English-Hindi based Cross Language Information Retrieval System", In Eighth International Conference on Contemporary Computing (IC3), IEEE, 2015.

[8] R. Johari, H. Bhatia, S. Singh, and M. Chauhan. "Triplicative Cipher Technique." *Procedia Computer Science* 78 : 217-223, 2016.

[9] A. Gupta, S. Semwal, R. Johari "METHS: Mapping from English Language to Hindi Language for Secure Commercial Transactions" IEEE International Conference on Computing Communication and Automation 2016.

[10] Ismail Hmeidi, Ahmad Al-Aiad, Sama Al-Momani, Mohammad Ibnian, "A Simple Present and Past Sentences Machine Translation from Arabic Language (AL) to English language", In International Conference on Engineering & MIS (ICEMIS), IEEE, 2016.