ISBN 978-93-5156-328-0
International Conference of Advance Research and Innovation (ICARI-2015)

Comparative Analysis of Cryptography Cipher Techniques

Laukendra Singh, Rahul Johari
Department of Computer Engineering, USICT, GGSIP University New Delhi, India

Article Info
Article history:
Received 8 January 2015
Received in revised form
15 January 2015
Accepted 22 January 2015
Available online 31 January 2015

Keywords
Cryptography,
Security,
Encryption,
Decryption,
Caesar Cipher,
Playfair Cipher,
Feistel Cipher

Abstract
In today's scenario, Information Security is the most challenging aspects in the web and network application. Internet and network applications are growing fast. So the value and importance of the exchanged data over the internet or other type of media are increasing. To handle security threats modern data communications uses cryptography an effective, efficient, and essential component for secure transmission of information by implementing security parameters counting Confidentiality, Authentication, accountability, and accuracy. So, Cryptography is an example of the data security that converts information from its normal form into an unreadable form by using encryption techniques.. There are various encryption techniques have been proposed by the researchers over a period of time. But in our literature survey we compared the cipher techniques like Caesar Cipher, Playfair Cipher, and Feistel Cipher by using C programming language code with their execution time. In this paper, we have analysis and compare Caesar Cipher, Playfair Cipher, and Feistel Cipher and found relationships among them.

1. Introduction

Basically data security means protecting its confidentiality, integrity, and availability [1]. The consequences of a failure to protect any of the three of these aspects will incur losses in business, loss of company's goodwill, loss of customer trust, and legal liability. Organizations are spread across states and across countries. Organizations use the internet as a backbone to carry out their day to day operating including sensitive data transfer. There is a need to protect customer data as mandated by various security controls. So organizations have to pay a large number of prices in case of compromise of data, specially customer's confidential data. With the rapid growth of information technology and science of encryption, an innovative area for cryptographic products has stimulated. Cryptography is the subdivision of cryptology in which encryption and decryption are designed, to guarantee the security and authentication of data [figure 1]. Cryptography also can be further classified as symmetric key cryptography and asymmetric key cryptography [1, 2].

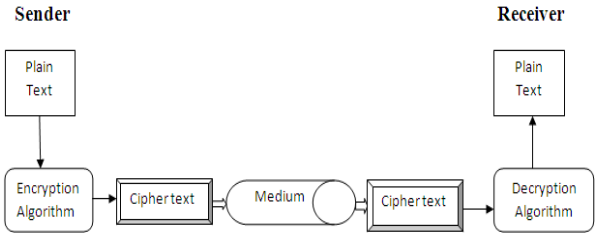

Fig: 1. Concept of Cryptography

If we define the scope only to a specific organization to focus on the consequences of security attacks in case of Software Company like:

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

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on [2]. All the techniques for providing security have two components:

a. A security related transformation on the information to be sent. Example include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
b. Some secret information shared by two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

1.1 Ciphers

In cryptography, a cipher is an algorithm for performing encryption or decryption – a series of well defined steps that can be followed as a procedure [2]. An alternative, less common term is Encipherment. Most modern ciphers can be categorized in several ways:

- By whether they work on blocks of symbols usually of a fixed size called Block Cipher, or on a continuous stream of symbols called Stream Cipher.
- By whether the same key is used for both encryption and decryption called symmetric key algorithms, or if a different key is used for each called asymmetric key algorithms. If the algorithm is symmetric, key must be known to the sender and recipient and no one else. If the algorithm is an asymmetric, the enciphering key is different from, but closely related to the deciphering key. Asymmetric key algorithm has public-private key property and one of the keys may be made public without loss of confidentiality.
- Ciphers are also categorized as follows:

Corresponding Author,
E-mail address: jonulaukendra@gmail.com

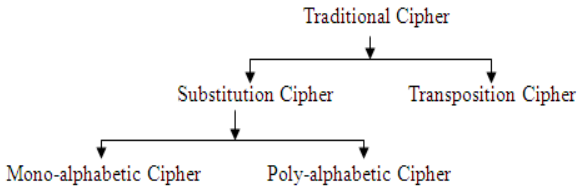

Fig: 2. Categories of Ciphers

Substitution Cipher: In substitution cipher, cipher substitutes one symbol with another. In a mono-alphabetic cipher, a symbol or character in the plaintext is always changed to the same symbol or character in the cipher-text regardless of its position in the text. The relationship between symbols in the plaintext and the cipher-text is a one-to-one relationship. Whereas In poly-alphabetic cipher, each occurrence of a symbol can have a different substitute. The relationship between the symbol in the plaintext to a symbol in the cipher-text is a one-to-many relationship.

Transposition Cipher: In transposition cipher, there is no substitution of characters; instead their location change. In other words, a transposition cipher reorders (permutes) the symbols in a block of symbols.

1.2 Cipher Model

An encryption scheme has five ingredients [2]:

- Plaintext: This is the original readable text or message that is fed into the algorithm as input.
- Encryption algorithm: The algorithm performs various transformation and substitution on the plain-text.
- 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 produce a result as output depending on that particular key being used at that time.
- 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 cipher-texts. The cipher-text is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm: This is a reverse of the encryption algorithm. It takes the cipher-text and the secret/public key as the inputs and produces the original plaintext.

1.3 Basic Requirement for Secure Use of Encryption

There are two requirements for secure use of encryption [1, 2]:

a. We need a strong encryption algorithm. We would like the algorithm to be such that an opponent who known the algorithm and has access to one or more cipher-texts would be unable to decipher the cipher-text or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt cipher-text or discover the key.

b. Sender and receiver must have exchanged copies of the secret/private key in a secure fashion and must keep the key secure.

2. Related Work

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

- **Caesar Cipher:** Caesar cipher or Additive cipher or Shift cipher is one of the simplest and most widely known encryption techniques. This is type of substitution cipher [1, 2, 3].
- **Playfair Cipher:** Playfair cipher is an example of a poly-alphabetic cipher used by the British army during World War 1. The secret key in this cipher made of 25 alphabetic characters arranged in 5cross5 matrix. Different arrangement of the characters in the matrix can create many different secret keys [1, 2].
- **Feistel Cipher:** It is designed by Feistel. It is very interesting and intelligent cipher that has been used for decades [1, 2].

3. Proposed Work

Methodology Adopted: The process of encryption and decryption has been accomplished in C language platform. The already existing ciphers i.e. Caesar cipher, Playfair cipher, and Feistel cipher are tried to convert plain-text to cipher-text. The plain-text used for transformation to cipher-text had alphabetic text.

3.1 Working Step

In the step 1 it was planned to script a program to implement Caesar cipher, Play-fair cipher, and Feistel cipher techniques.

3.1.1 The process involved for working step

a. A program is developed to read the characters/contents of the file.
b. Stored the contents of the file in an array.
c. Read the contents from the array.
d. Print the same.
e. Applied the encryption techniques: Caesar cipher, Play-fair cipher, Feistel cipher.
f. Print the encrypted contents of the file with execution time.

We analysis few ciphers like Caesar cipher, Play-fair cipher, and Feistel cipher. We found the relationship among the ciphers for a fixed size input text with their execution time. The relationship among the ciphers is defined in the following [Table 1].

As we are seeing that Feistel cipher technique takes more time than the other type of ciphers which are mentioned in this report, but it has been used for some decades. The reason is that it is not vulnerable and not easy to find the key.

Name of the Cipher Technique	Input Text size (in bytes)	Program LOC	Execution Time (in Second)
Caesar Cipher	958	125	0.007
Playfair Cipher	958	102	0.165
Feistel Cipher	958	75	1.313

Table 1: Comparison among Ciphers

ISBN 978-93-5156-328-0

3.2 Snapshots: Given below are the Snapshots of the Running Programs

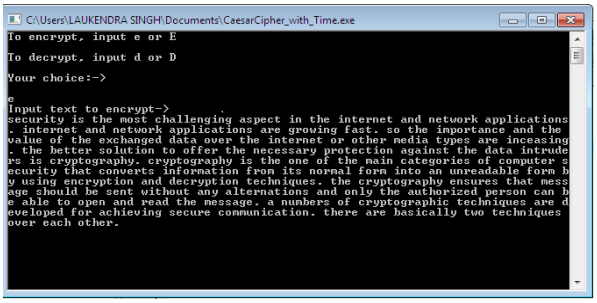

Fig: 3. Input Text for the Caesar Cipher

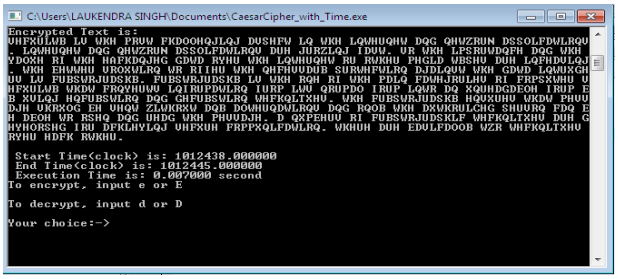

Fig: 4. Encrypted Text for the Caesar Cipher

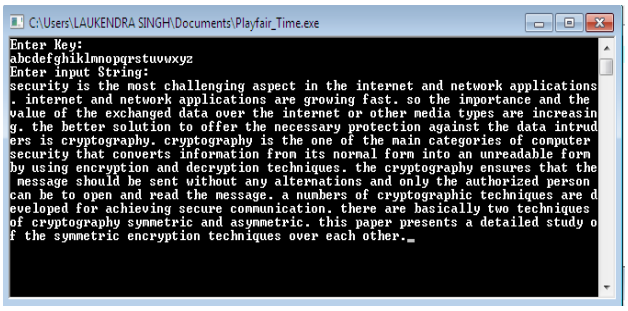

Fig: 5. Input text for the Playfair Cipher

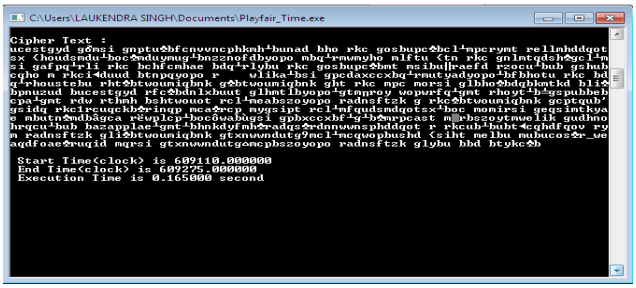

Fig: 6. Encrypted Text for the Playfair Cipher

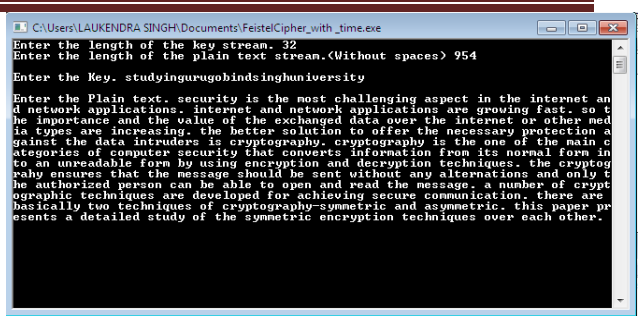

Fig: 7. Input Text for the Feistel Cipher

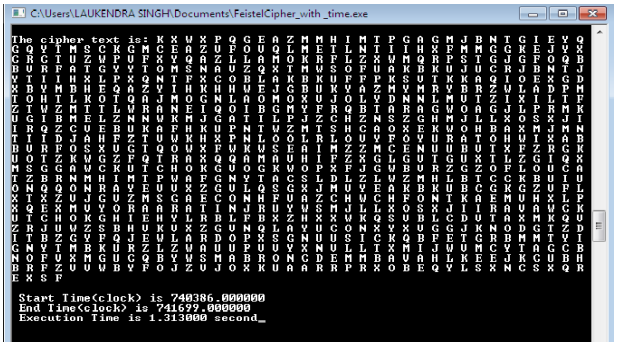

Fig: 8. Encrypted Text for the Feistel Cipher

4. Conclusion

In this wireless world, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceeding. To sum up, all the techniques are useful for real time encryption. Each technique is unique in its way, which might be suitable for different application. 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, Playfair cipher, and Feistel cipher for the same input text/data size, we analyzed that Caesar cipher is very simple cipher technique because it is easy to understand and implement. Caesar cipher technique takes lesser time to execute the program but it is very vulnerable in nature; means that key can be easily find out. And Playfair cipher takes more execution time than Caesar cipher but it is more secure. For more security in Playfair cipher, we need to change the key matrix in consequent time intervals. Whenever, Feistel cipher is more strong and secure than Playfair cipher and Caesar cipher but it takes more execution time. If the key size of the Feistel cipher will increase, it will will become more powerful in nature. So, attacking is not easy on Feistel cipher.

References

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

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

[3] L. Ruby, R. Johari, Designing a Secure Encryption Technique For Web Based Applications, International Journal of Advance Research in Science and Engineering, 3(7), 2014