IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

Analysis of Information Security through Crypto-Stenography with Reference to E-Cipher Methods

Padmaja Patel[1], Sibo Prasad Patro[2]

Assistant Professor, Department of CSE, GIET, Gunupur[1, 2]

Abstract: This paper shows the possibility of exploiting the features of E- cipher method by using both cryptography as well as Steganography methods to send and receive the message in more secured way and shows the different methods are available and an comparative study on Substitution cipher. Proposed methodology shows that successfully using these Poly substitutions methods (Proposed E-Cipher) to evolve a new method for Encrypting and decrypting the messages. In poly-alphabetic substitution ciphers (E-Cipher) the plaintext letters are enciphered differently depending upon their placement in the text. As the name poly-alphabetic suggests this is achieved by using several two, three keys and random keys. Combinations instead of just one, as is the case in most of the simpler crypto systems. We can use Poly substitution method combining the features of cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated. After this process, file is compressed; the compressed file is hidden in image file using LSB method, the same process is applied reversely to retrieve the source message by Genetic keys.

Keywords: Genetic Algorithm, Encryption, Decryption, Genetic Keys, Mono Substitution, Poly Substitution., object.

I. INTRODUCTION

The core objective of the research is to protect information leakage what so ever manner it may be, the use of appropriate technology.To provide a high level of confidentiality, integrity, non reputability and authenticity to information that is exchanges over networks.

Confidentiality: Data is protected by hiding information using encryption technique

Integrity: Ensures that a message remains unchanged from the time it is created and opened by recipient.

Non – reputability: It provides a way of proving that the message came from someone even it they try to deny it.

Authentication: It verifies the identity of user in the system and continues to verify their identity in case someone tries to break into the system.

II. SECRET KEY CRYPTOGRAPHY

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the Plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

III. PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

IV. SECURED COMMUNICATION BASIC TERMS

Let's consider two parties that want to communicate secretly, A and B. If A wants to send something to B, some information, we call that information a plaintext. After encrypting the plaintext a cipher text is produced. B knows the encryption method since he is the intended receiver and since he must use the same method together with his secret key to decrypt the cipher text and reveal the plaintext.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

4.1. Secured Communication System Model

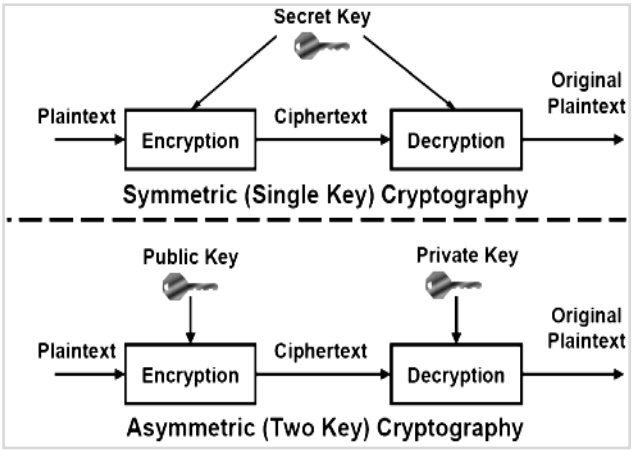

Figure 1: Symmetric and Asymmetric System Model

V. TYPES OF SUBSTITUTIONS CIPHER

There are 4 kinds of substitution cipher; Mono -alphabetic, Homophonic, PolyGram, Transposition Cipher and Poly - alphabetic methods.

5.1. Caesar Cipher

- Good in theory but not so good in practice.
- How to make the cipher more difficult can complicate?
- Cipher text alphabets corresponding to the original plain text alphabets may not necessarily be 3 places down the order, instead, can be any places down the order.
- Thus, alphabet A in plain text would not necessarily be replaced with D. It can be replaced by any other alphabet.
- Once the replacement scheme is decided, it would be constant and will be used for all other alphabets in given message
- English languages contain 26 alphabets. Thus, A can be replaced by any order in the English alphabet set (B through Z). Not make sense to replace A with A
- So, each alphabet have 25 possibilities of replacement.
- The major weakness of Caesar Cipher is its predictability.
- Rather than using a uniform scheme, use random substitution. This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z) and so on
- The crucial difference, there is no relation between the replacement of B and replacement of A. That is, if decided to replace A with D, not necessarily replace each B with E – can replace B with other character
- To put it mathematically, the cipher can have any permutation or combination of the 26 alphabets which means (26 x 25 x 24 x 23 x …2) or 4 x 1026 possibilities!
- This is extremely hard to crack. It might actually take years to try out these many combinations even with the most modern computers.

5.2. Homophonic Substitution Cipher

- Very similar to Mono-alphabetic Cipher.
- The difference between the 2 techniques is that replacement alphabet set in simple substitution technique is fixed (A with D..) whereas in the case of Homophonic, one plain text alphabet can map to more than one cipher text alphabet.
  e.g A can be replaced by D, H, P, R; B can be replaced by E, I, Q, S….
- Difficult to analyze compare with mono-alphabetic because the frequency didn't show the real usage of each alphabet.

5.3. PolyGram Substitution Cipher

- Rather replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets is replaced with another block.
- It is done by dividing plain text to a group of alphabet. This group can be 2 alphabets or more than that.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

- Play-fair Cipher and Hill Cipher are examples of cipher that used Polygram Substitution Cipher.

5.4. Poly-alphabetic Substitution Cipher

- Leon Battista invented the Polyalphabetic Cipher in 1568. This cipher has been broken many times, and yet it has been used extensively. The Vigenere Cipher and Beaufort Cipher are the examples of it.
- The cipher uses multiple one-character keys. Each of the keys encrypts one plain text character.
- The first key encrypts the first plain text character; the second key encrypts the second plain text character and so on.
- After all the keys are used, they are recycled. Thus, if we have 30 one-letter keys, every 30th character in the plain text would be replaced with the same key.

VI. PROPOSED E-CIPHER METHODS

In poly-alphabetic substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text. As the name poly-alphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems.

Method 1: **using E-Cipher Method**

Algorithm

1. Take the example text “Welcome”.
2. Take three key e1, e2, e3 and assign a character e1 be ‘a’ and e2 be ‘D’ and e3 be‘s’.
3. Let ASCII value of e1 be 1 and e2 be 2 and e3 be 3 and take the text, add ASCII value of e1 to value of first character, and e2 to second character and e3 to third character, alternatively add the value of e1, e2, e3 to consecutive characters.
4. Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.
5. After adding ASCII value of all values of given text, the resultant text is an encrypted message, and it generate a combination of 3* (256 * 256 * 256) letters encrypted coded text with 128 bit manner.
6. Transposition takes place in each character after all the process is over that is moves or change one bit either LSB or MSB, the end result is increasing security.
7. Finally takes the decimal values of each updated character in the given text and print and this process shown in Table 1.

Method 2: **Cyrpto-steganographic method**

Algorithm

Encrypted message is then compressed; this file is hidden in Image file using LSB method, The resultant object send to the receiver.

In the receiver side, object is received and then unzipped using the methods then the result is decrypted with substitutions cipher methods.

We can use Poly substitution method combining the features of genetic Algorithms and cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.

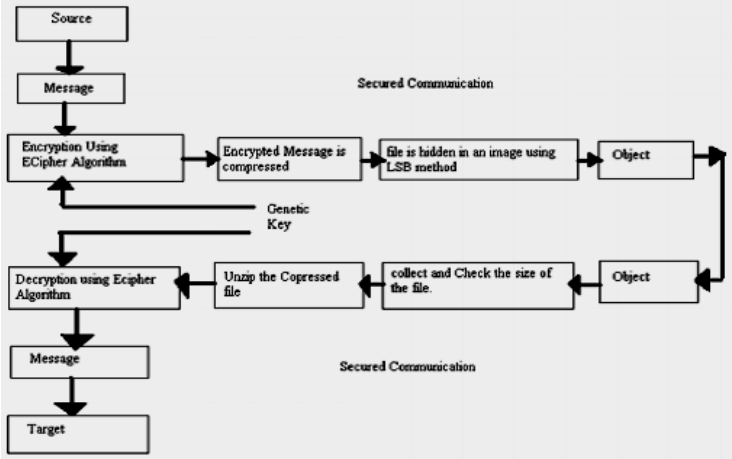

Figure: 2 Lay-out Flow Diagram

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

VII. METHODOLOGY

In poly-alphabetic substitution ciphers (E-Cipher) the plaintext letters are enciphered differently depending upon their placement in the text. As the name polyalphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems.

Using two keys, we take 2 keys e1,e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character. Alternatively add the value of e1 and e2 to consecutive characters. Encrypted message is then compressed; this file is hidden in Image file using LSB method, The resultant object send to the receiver.

In the receiver side, object is received and then unzipped using the methods then the result is decrypted with substitutions cipher methods.

Poly substitution method(e-cipher) combining the features of genetic keys methods with features of Steganography with cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.

6.2.1. Encryption Result

Keys X,Y,Z and message “WELCOME”
Let X – a, Y – b and Z - c
ASCII VALUES for a – 97 b –98 c-99

Table 1Encryption Result Data – Method 1

i/P	ASCII values	AddCon. letter	Binary values	Alter MSB	Final Result
W	87	184	10111000	10111001	185
E	69	167	10100111	10100110	166
L	76	175	10101111	10101110	174
C	67	164	10100100	10100101	165
O	79	177	10110001	10110000	176
M	77	176	10110000	10110001	177
E	69	166	10100110	10100111	167

The Encrypted message is
{185,166,174,165,176,177,167}
ie., Encrypted Text
6.2.2. Decryption Result

The Encrypted Text is applied to decrypted formula By applying the reverse process

Table 2Decryption Result Data – Method -1

Cyber result	Binary Values	Alter MSB Letter	Subtract Con. Value	Rem. ASCII	Plain Text
185	10111001	10111000	184	87	W
166	10100110	10100111	167	69	E
174	10101110	10101111	175	76	L
165	10100101	10100100	164	67	C
176	10110000	10110001	177	79	O
177	10110001	10110000	176	77	M
167	10100111	10100110	166	69	E

The Plain text is “WELCOME”
convert cipher text (encrypted data) into plaintext.

VIII. KEYWORDS

Encryption The process of putting text into encoded form
Genetic algorithm (GA) Search/optimization
algorithm based on the mechanics of natural selection and natural genetics

Key A relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into cipher text (during encryption) or vice versa (during Decryption)
Key length The size of the key - how many values comprise the key?
Monoalphabetic Using one alphabet - refers to a cryptosystem where each alphabetic character is mapped to a unique alphabetic character
Mutation Simulation of transcription errors that occur in nature with a low probability - a child is randomly changed from what its parents produced in mating
Order-based GA A form of GA where the chromosomes represent permutations. Special care must be taken to avoid illegal permutations
Plaintext A message before encryption or after decryption, i.e., in its usual form which anyone can read, as opposed to its Encrypted form.
Polyalphabetic Using many alphabets - refers to a
cipher where each alphabetic character can be mapped to one of many possible alphabetic characters
Population The possible solutions (chromosomes) currently under investigation, as well as the number of solutions that can be investigated at one time, i.e., per generation
Block A sequence of consecutive characters encoded at one time.
Block length The number of characters in a block
Chromosome The genetic material of an individual - represents the information about a possible solution to the given problem.
Cipher An algorithm for performing encryption (and the reverse, decryption) - a series of well-defined steps that can be followed as a procedure. Works at the level of individual letters, or small groups of letters.
Cipher text A text in the encrypted form produced by some cryptosystem. The convention is for cipher texts to contain no white space or punctuation.
Crossover (mating) Crossover is the process by which two chromosomes combine some portion of their genetic material to produce a child or children.
Cryptanalysis The analysis and deciphering of c cryptographic writings or systems.
Cryptography The process or skill of communicating in or deciphering Secret writings or ciphers
Cryptosystem The package of all processes, formulae, and instructions for encoding and decoding messages using cryptography.
Decryption Any procedure used in cryptography to convert cipher text (encrypted data) into plaintext.
Diagram Sequence of two consecutive characters.
Encryption The process of putting text into encoded form.
Fitness The extent to which a possible solution successfully solves the given problem - usually a numerical value.
Generation The average interval of time between the birth of parents and the birth of their offspring - in the genetic algorithm Case, this is one iteration of the main loop of code.
Genetic algorithm (GA) Search/optimization algorithm based on the mechanics of natural selection and natural genetics.
Mutation Simulation of transcription errors that occur in nature with a low probability - a child is randomly changed from what its parents produced in mating.
Trigram Sequence of three consecutive characters.
Unigram Single character.

IX. CONCLUSION

The Proposed methodology will give the new area of research on cryptography with combined features of Steganography with reference to Substitution ciphers(E-Cipher) Methods. This new methodology for text encrypts and decrypt using E- Cipher Methods with reference to Unicode / ASCII code method is definitely an effective method while compared with other cryptography information security systems.

REFERENCES

(1) AlekseyGorodilov,Vladimir Morozenko, 'Genetic Algorithms for Finding the Key's Length and Cryptoanalysis of the Permutation Cipher', International Journal Information Theories and Applications, 15/2008.
(2) Bethany Delman,'Genetic Algorithms in Cryptography' published in web; July 2004.
(3) Darrell Whitley, 'A Genetic Algorthm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.
(4) Ranjan Bose ,Introduction to Cryptography –Tata Mc-Grew –Hill Publisher ltd, 2001.
(5) N. Koblitz,'A Course in Number Theory and Cryptography', Springer-Verlag, New York, INc, 1994.
(6) Nalani N., G. Raghavendra Rao, 'Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics; IJCSNS, Vol. 6 No.1B, January 2006.
(7) Sean Simmons,'Algebric Cryptoanalysis of Simplified AES', October 2009;33,4;Proquest Science Journals Pg. 305.
(8) Sujith Ravi, Kevin Knight, 'Attacking Letter Substitution Ciphers with Integer Programming',Oct 2009,33,4; Proquest Science Journals Pg.321.
(9) Verma, Mauyank Dave and R.C Joshi,'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Substitution Cipher in Adhoc Networks; Journal of Computer Science **3**(3): 134-137, 2007.
(10) William Stallings, "Cryptography and Network Security: Principles and Practice",2/3e Prentice Hall, 2008.