Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography

R. Venkateswaran
Research Scholar- Ph.D
Karpagam Academy of Higher Education
Karpagam University
Coimbatore, Tamilnadu, India.

Dr. V. Sundaram
Director- Computer Applications
Karpagam College of Engineering
(Affiliated to Anna University)
Coimbatore, Tamilnadu, India.

ABSTRACT

This paper shows the possibility of exploiting the features of Genetic Algorithm with poly substitution methods in a linear way, to generate ASCII values of the given text and then applying conversion, transposition with the features of Cryptography.

In polyalphabetic substitution ciphers 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.

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.

Key words
Encryption, Decryption, Genetic Keys, Mono Substitution, Poly Substitution.

1. INTRODUCTION

The demand for effective network security is increasing exponentially day by day. Businesses have an obligation to protect sensitive data from loss or theft. Not only businesses see to the security needs; they have to understand where the computer is vulnerable and how to protect it. In the present scenario, where a user needs to be connected anyhow, anywhere, anytime.

2. HISTORY

The word cryptography comes from the Greek word *kryptos*, which means hidden and *graphein*, which means writing. There has always been a need for exchanging information secretly. History is filled with examples where people have tried to keep information secret from adversaries. Cryptography, the science of encrypting and decrypting information can be traced back all the way to year 2000 BC in Egypt. Here it was first used with the help of the standard hieroglyphics in order to communicate secretly. Julius Caesar (100-44 BC) used a simple substitution cipher which has been named after him today. During the first and the second war the demand for secrecy increased dramatically and all kinds of new cryptographic techniques evolved.

Today’s society has evolved, and the need for more sophisticated methods for protecting data has increased. As the world becomes more connected, the demand for information and electronic services is growing, and with the increased demand comes increased dependency on electronic systems. Exchanging sensitive information over the Internet, such as credit card numbers is common practice. In today's information society, cryptography is one of the main tools for privacy, trust, access control, electronic payments, corporate security, authentication and many other fields. The use of cryptography is not something used only by governments and highly skilled Specialists it is available for everyone.

This paper will present some basic knowledge about Cryptography. It will focus on some new approach on text encryption and description and describe their functions and flaws.

3. SECURE COMMUNICATION BASIC TERMS

Let’s consider two parties that want to communicate secretly, Alice and Bob. If Alice wants to send something to Bob, some information, we call that information a plaintext. After encrypting the plaintext a ciphertext is produced. Bob 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.

4. OBJECTIVES OF THE PROJECT

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 provide 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.

5. POLY SUBSTITUTION METHODS

In polyalphabetic substitution ciphers 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.

Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or verify the correctness of a message to the recipient (authentication) forms the basis of many technological solutions to computer and communications security problems.

6. SYMMETRIC AND ASYMMETRIC SYSTEM MODEL

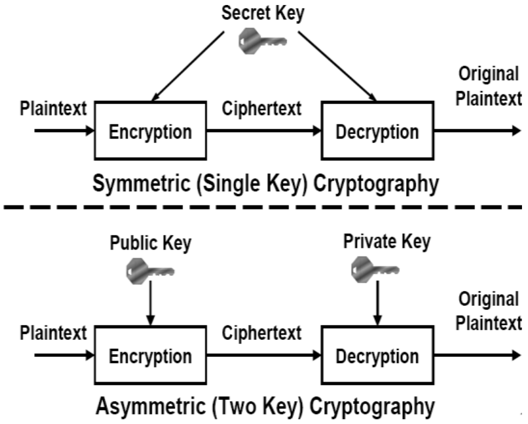

Figure 1
Symmetric and Asymmetric System Model

6.1 Encryption Process

- Take the example text “ Welcome”.
- Take three key e1, e2, e3 and assign a character e1 be ‘a’ and e2 be ‘D’ and e3 be ‘s’.
- 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.
- Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.
- 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.
- 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.
- Finally takes the decimal values of each updated character in the given text and print and this process shown in Table 1.

6.2 Decryption Process

- Takes the ASCII values of each updated character in the given text and converted into binary format.
- Transposition takes place in each character after all the process are over that is moves or change one bit either LSB or MSB .
- Subtract ASCII value of all values of given text, the resultant text is a decrypted messages, and it generate a combination of 3* (256 * 256 * 256) letters decrypted coded text.
- Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.
- Subtract ASCII value of e1 from the value of first character, and e2 from the second character and e3 from third character, alternatively subtract the value of e1, e2, e3 to consecutive characters.
- Transposition takes place in each character after all the process are over that is moves or change one bit either LSB or MSB , the end result is some binary value
- Finally takes the decimal values of each updated binary value in the given text and print.
- Decrypted message “ Welcome ” and this process shown in Table 2.

6. 3 . RESULT

6.3.1 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 1 : Encryption Process Result

Character	ASCII values	Add Con. letter	Binary values	Alter LSB	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}

I.e. cyber text.

6.3.2 Decryption Result

The Encrypted Text is applied to decrypted formula

By applying the reverse process

Table 2 : Decryption Process Result

Cyber Result	Binary Values	Alter LSB	Subtract Con. Letter	Remaining ASCII Values	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”

7. TYPES OF SUBSTITUTION CIPHER

- Mono Alphabetic Substitution Cipher
- Homophonic Substitution Cipher
- PolyGram Substitution Cipher
- Transposition Cipher
- Poly Alphabetic Substitution Cipher

8 .KEY TERMS

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.

Ciphertext 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 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 ciphertext (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.

Key A relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into ciphertext (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.

Scoreboard Method of determining the fitness of a possible solution - takes a small list of the most common diagrams and trigrams and gives each chromosome a score based on how often these combinations occur.

Trigram Sequence of three consecutive characters.

Unigram Single character.

9. CONCLUSION

The Proposed methodology will give the new area of research on cryptography and genetic algorithms.

This new methodology for text encrypts and decrypt using genetic algorithm is definitely an effective method while compared with other cryptography systems.

10. REFERENCES

[1] Aleksey Gorodilov,Vladimir Morozenko,'Genetic Algorithms for finding the key's length and crypto analysis of the permutation cipher', International Journal "information Theories and Applications vol.15/2008.

[2] Bethany Delman,'Genetic Algorithms in Cryptography' published in web; July 2004.

[3] Darrell Whitley,' A Genetic Algorithm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.

[4] Introduction to Cryptography – Ranjan Bose – 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] A K Verma, Mauyank Dave and R.C Joshi,'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Subsitution 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, 1999.