Playfair extended using Genetic Operators

Amritha Thekkumbadan Veetil

M.Tech, Computer Science, Invertis University, Bareilly, India

Abstract: Security plays an important role in day to day life. A stronger encryption method always makes a user happy when it comes to the security of their data. This paper extends the traditional playfair encryption method using genetic algorithm. The two main operators of genetic algorithm 'Crossover' and 'Mutation' are used for the extension. The extended playfair is secure and encrypts the data more effectively, providing double layer of protection.

Keywords: Genetic Algorithm, Crossover, Mutation, Encryption, Decryption, Playfair

I. INTRODUCTION

A. Cryptography

Cryptography deals with the encryption of data to restrict the access of data to only authorized person. Cryptography offers efficient solution to protect sensitive information including personal data security, internet security, military communication security, etc.

Symmetric key cryptography: The sender and receiver uses the same key for encryption and decryption and hence the key is shared between them [1][2]. Example: DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

Asymmetric key cryptography: The technique is also known as public key cryptography. In this cryptographic method, the sender and the receiver uses different keys for encryption and decryption and hence the key is not shared between them [1][2]. Example: RSA (Ron Rivest, Adi Shamir and Leonard Adleman).

Other than the above mentioned methods, there are other methods of performing encryption.

a) Substitution – Alphabets in a plaintext are replaced by other alphabets.

Example: Playfair

b) Transposition – The order of alphabets in the plaintext are changed.

Example: Transposition matrix

This paper uses the playfair method which works with a 5x5 table. The table is initially filled with the alphabets of the key. Once the key is occupied in the table, all the remaining alphabets occupy the remaining space in the table (the alphabets are inserted into the table in horizontal manner from left to right). Please note that 'I' and 'J' occupy the same space of the table.

B. Genetic Algorithm

Genetic algorithm [3] is a heuristic search method based on the theory of natural selection. The three basic operators of genetic algorithm are population generation, crossover, and mutation.

Population generation: Genetic Algorithms (GA), usually starts with the process of population generation. The chromosomes are represented either in binary or hexadecimal.

Crossover: Process of obtaining parent solution (new generation) by applying the crossover operator on individuals of the existing generation. It is noticed that the new generation is always more fit than the parent generation.

Mutation: It is the important process of genetic algorithm as it brings genetic diversity in the species. A mutation operator is used to perform the process of mutation.

II. RELATED WORK

In 2012, Ankita Agarwal proposed an encryption method, where genetic algorithm based secret key image encryption using genetic operator is discussed [4]. The paper introduces a approach of Genetic Algorithm in which, the operations of Genetic algorithm (Crossover and Mutation) are exploited and an encryption method is developed for candidate type of data.

Later, in 2014, Sindhuja K and Pramela Devi S, have proposed method to encrypt data using right shift, matrix addition, modulo operation and genetic operations [5]. Key generation process and intermediate cipher algorithm is used in this paper. Here symmetric key substitution algorithm is used to ensure confidentiality in networks. In 2015, Amritha Thekkumbadan Veetil (myself) have used the genetic operators for encryption and have developed an encryption method. The method is designed considering security of data will transmission.

III. PROPOSED WORK

In this section I have extended playfair encryption method using genetic operators. As an example in this paper I have used the key and plaintext as ‘COMPUTER’ and ‘SECRET”.

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

A. Encryption Steps [6]:

1. Follow the usual procedure of playfair and group the letters of plaintext into pairs. After applying playfair ‘SECRET’ will become ‘LBMTBR’. Now group them.

SE CR ET

LB MT BR

2. Now it's time to extend playfair. Convert the alphabets into decimal and then to binary. Start with LB.

L - 12 - 01100
B - 2 – 00010

3. To apply the genetic operators, here I have considered L ad B as the two parents.

4. Select a crossover point randomly and perform the crossover between the two parents L and B. I have selected the crossover point as 2 (CP is the crossover point).

L CP = 2

0	1	1	0	0

B

0	0	0	1	0

After crossover the child obtained is '01010' and the left over part of the chromosome is '00100' (used in decryption).

Child Chromosome

0	1	0	1	0

4. Randomly select a mutation point in-order to perform mutation in the child chromosome. I have selected the mutation point as 4. The bit gets inverted when mutation is performed.

0	1	0	1	0

After mutation, child chromosome will be represented as:

0	1	0	0	0

Decimal value of 01000 is 8 and alphabet corresponding to 8 is H. The left over value was 00100 with decimal value 4.

Note: If the child chromosome becomes 00000 after mutation then we can represent it with any special symbol (α, β, etc).

During encryption, for every word the crossover point and mutation point varies which increases the strength of the method. The cipher text corresponding to 'SECRET' is {H4,N21,α18}. For decryption the cipher text along with 24 is send to the receiver, 2 is the crossover point and 4 is the mutation point.

B. Decryption Steps [6]:

The receiver receives the cipher text {H4, N21, α18} along with 24.

1: Take the first pair H4. Convert only the alphabetic part (H) to binary.

H - 8 – 01000

2. From 24 it's clear that 4 is the mutation point and 2 is the crossover point.

3. Perform reverse mutation and invert the fourth bit.

0	1	0	0	0

0	1	0	1	0

4. Perform reverse crossover. For this the decimal part attached with the letter (4) is required.

4 – 00100

Chromosome after reverse mutation

4

CP = 2

0	1		0	1	0
0	0		1	0	0

5. The child chromosome will be 01100 and left out part is 00010

0	1	1	0	0

01100 is 12, which represent alphabet L.

00010 is 2, which represent alphabet B.

6. Now the alphabets available are LB. Use the decryption method of traditional playfair encryption to decode it correctly.

7. After applying playfair we get SE corresponding to LB and thus the plaintext as 'SECRET'.

IV. CONCLUSION

The method proposed in this paper as an extension for playfair encryption is simple and easy to implement. Crossover and mutation operators of genetic algorithm are used along with playfair which provides high security to the transmitted data. Frequent binary and decimal conversions and vice versa increases strength of the method. This method provides an extra layer of protection.

V. REFERENCES

[1] Behrouz A. Forouzan, "Cryptography & Network security", Tata McGraw – Hill, 2007.
[2] William Stallings, "Cryptography and Network Security", 3rd Edition.
[3] S., N. Sivanandan, S. N. Deepa, "Introduction to Genetic Algorithm", Springer Verlag Berlin Heidelberg, 2008.
[4] Ankita Agarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[5] Sindhuja K , Pramela Devi S, "A Symmetric Key Encryption Technique Using Genetic Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014.
[6] Amritha Thekkumbadan Veetil, "An Encryption Technique Using Genetic Operators", International Journal of Scientific & Technological Research, Volume 4, Issue 07, July 2015.