



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cryptographic Technique Involving Genetic Algorithm And Chemical Periodic Table

Abhishek Karole, Dr. S. S. Shrivastava,

Research Scholar, Professor

Department of Mathematics

Institute for Excellence in Higher Education, Bhopal, India

Abstract: The aim of this paper is to establish an algorithm for encryption and decryption of a message based on symmetric key cryptosystem involving Genetic Algorithm and Chemical Periodic Table. In the planned algorithm we use genetic crossover, mutation technique, ASCII 7-bit table and chemical periodic table.

Index Terms - Encryption, Decryption, Genetic Algorithm, Crossover, Mutation and Chemical Periodic Table.

I. INTRODUCTION

Cryptography is the art and science of achieving security by encoding messages to make them non-readable [3, 4, 15]. Cryptography is the art of writing any information in such a manner that it cannot be understood by anybody else but the authorized person. It is the art of protecting information by transforming into indecipherable. The real act of converting readable information which is 'plaintext' into the form that cannot be understood is referred to as encryption. And the reverse act is referred as decryption, hence this cryptosystem is known as Symmetric key encryption and decryption, while if using different keys for encryption and decryption then system is known as asymmetric key encryption and decryption. Encryption and decryption algorithm involves Genetic algorithm for intermediate cipher and using of Chemical Periodic table for final Cipher.

Genetic Algorithm [2, 6, 11, 14, 16, 18] is a heuristic search method based on the theory of natural selection. Generally, genetic algorithms have five steps which contain three basic operators: population generation, crossover, and mutation. For intermediate cipher we used two operators i.e., Crossover and mutation. On taking more than one parent chromosomes, the child chromosome is produced in crossover function. Single point crossover, two-point crossover, Uniform crossover and three parent crossovers [3] are various crossover techniques. There are various types of mutation techniques such as Gaussian mutation flipping of bits, uniform mutation, non-uniform mutation, boundary mutation and inversion mutation. For final cipher we used traditional chemical periodic table and combine it with ASCII Characters to establish a new Table i.e., ASCII-Character Periodic Table. The periodic table [5, 13] of the chemical elements is a table that displays all known chemical elements in a systematic way. The elements in the periodic table are ordered by their atomic number (Z) and are arranged in periods (horizontal rows) and groups (vertical columns). The layout of the periodic table is designed to illustrate periodic trends, similarities and differences in the properties of the elements.

II. RELATED WORK

The proposed symmetric algorithm for encryption and decryption is based on Genetic Algorithm and Chemical Periodic Table. Genetic Algorithm and Chemical Periodic Table is considered and featured by Mittal [9, 10], Mandle [7, 8], Sindhuja [12], Sinha [13] and others. Information and vital knowledge about the topic are taking considered by the cited Researcher using their respective articles. We introduced a newfound symmetric cryptosystem for encryption and decryption to provide the confidentiality to the data/message by utilizing Genetic Algorithm (Crossover and Mutation operators) and Chemical Periodic Table.

III. METHODOLOGY

By taking Consideration of Following Mittal [9, 10], Mandle [7, 8], Sindhuja [12], Sinha [13] and other researchers, in this paper we develop an algorithm for encryption and decryption of a message using genetic algorithm and chemical periodic table, the new established algorithms is created by using following steps which are:

(i) Initial Conversion:

(a) Plain text is converted into individual numeric values by using the ASCII 7-Bit Table.

(b) Convert each numeric Value into a corresponding 7-bit binary form.

(c) Combining the binary string and divide into two segments.

(ii) Genetic Algorithm (Crossover and Mutation operators):

Genetic algorithms are vital step to produce the intermediate cipher text, the idea is to be applying two-point crossover technique on bits, then applying swap mutation in each 7-bit binary code subsequently convert 7-bits them into numeric value then convert numeric value to corresponding character by using ASCII 7-bit code. Hence, we achieved the intermediate cipher text.

(iii) Chemical Periodic Table:

To achieve the final cipher text, the chemical periodic table are used on the intermediate cipher, convert the intermediate cipher into their symbol of periodic element then those symbols is converted to atomic numbers this stage is responsible for final cipher text. Here is the following ASCII-Character Periodic Table:

Table I

Alphabet Number	Chemical Element Symbol	Atomic Number	Alphabet Number	Chemical Element Symbol	Atomic Number
'A'	'H '	01	'u'	'Cd'	48
'B'	'He'	02	'v'	'In'	49
'C'	'Li'	03	'w'	'Sn'	50
'D'	'Be'	04	'x'	'Sb'	51
'E'	'B '	05	'y'	'Te'	52
'F'	'C '	06	'z'	'I '	53
'G'	'N '	07	'0'	'Xe'	54
'H'	'O '	08	'1'	'Cs'	55
'I'	'F '	09	'2'	'Ba'	56
'J'	'Ne'	10	'3'	'La'	57
'K'	'Na'	11	'4'	'Ce'	58
'L'	'Mg'	12	'5'	'Pr'	59
'M'	'Al'	13	'6'	'Nd'	60
'N'	'Si'	14	'7'	'Pm'	61
'O'	'P '	15	'8'	'Sm'	62
'P'	'S '	16	'9'	'Eu'	63
'Q'	'Cl'	17	'.'	'Gd'	64
'R'	'Ar'	18	'!'	'Tb'	65
'S'	'K '	19	'@'	'Dy'	66
'T'	'Ca'	20	'#'	'Ho'	67
'U'	'Sc'	21	'\$'	'Er'	68
'V'	'Ti'	22	'%'	'Tm'	69
'W'	'V '	23	'^'	'Yb'	70
'X'	'Cr'	24	'&'	'Lu'	71
'Y'	'Mn'	25	'*'	'Hf'	72
'Z'	'Fe'	26	'('	'Ta'	73

' ' (Space)	'Co'	27	)'	'W '	74
'a'	'Ni'	28	'-'	'Re'	75
'b'	'Cu'	29	'='	'Os'	76
'c'	'Zn'	30	'_'	'Ir'	77
'd'	'Ga'	31	'+'	'Pt'	78
'e'	'Ge'	32	':'	'Au'	79
'f'	'As'	33	'\'	'Hg'	80
'g'	'Se'	34	' '	'Tl'	81
'h'	'Br'	35	'"'	'Pb'	82
'i'	'Kr'	36	'<'	'Bi'	83
'j'	'Rb'	37	'>'	'Po'	84
'k'	'Sr'	38	','	'At'	85
'l'	'Y '	39	':'	'Rn'	86
'm'	'Zr'	40	'?'	'Fr'	87
'n'	'Nb'	41	'/'	'Ra'	88
'o'	'Mo'	42	'['	'Ac'	89
'p'	'Tc'	43	'{'	'Th'	90
'q'	'Ru'	44	']'	'Pa'	91
'r'	'Rh'	45	']}'	'U '	92
's'	'Pd'	46	';'	'Np'	93
't'	'Ag'	47	'"'	'Pu'	94
			'"'	'Am'	95

IV. ALGORITHM

4.1 Encryption Algorithm:

1. Consider plain text.
2. Convert that plain text into individual numeric values by using the ASCII 7-Bit Code.
3. After obtaining the numeric values, convert each numeric Value into a corresponding 7-bit binary form.
4. Combining the binary string and divide into two segments.
5. Applying two-point crossover technique on desired bits, e.g., 29 and 42, which is mutually reciprocated between encryptor and decryptor.
6. The two crossover segment bits, applying swap mutation e.g., swapping of 3rd bit to 5th bit in each 7-bit binary code.
7. Following separate each 7-bit binary segment convert them into numeric value by using ASCII 7-bit code.
8. Subsequent convert the numeric value into corresponding character.
9. Resultant of the conversion, we obtained the intermediate cipher text.
10. Consequently, each character of the intermediate cipher text is converted into their corresponding symbol of periodic element.
11. These pair of two-character symbols of the periodic element then transformed into their atomic number.
12. Succeeding by converting, we obtained the cipher text.

4.2 Decryption Algorithm:

1. Start with the cipher text obtained from the encryption process.
2. From the cipher text, each pair of two-numerical character of atomic number is converted into their symbol of periodic element.
3. Following conversion, afterwards each pair of two-character symbol of periodic element is transformed into their respective ASCII character using Periodic table. we get
4. Follow up, convert each character of the cipher text into its corresponding numeric value using the ASCII 7-bit code.
5. Transform each numeric value into its corresponding 7-bit binary form.
6. Combine the binary strings into a single binary sequence.
7. Execute Reverse Bits Swap Mutation by separate the combined binary string back into individual 7-bit binary codes.
8. For each 7-bit binary code, perform a bits swap mutation by swapping the 5th bit back to the 3rd bit.
9. Recombine the individual 7-bit binary codes into the complete binary sequence.

10. Applying reverse, the two-point crossover technique that was applied during encryption at the Desired positions e.g., 29 and 42. after reversing the crossover, divide the binary string back into individual 7-bit segments.
11. Convert each 7-bit binary segment back into its corresponding numeric value using the ASCII 7-bit code.
12. Finally, convert the numeric values back into their corresponding characters to retrieve the original plain text.

4.3 Illustration:

A. Encryption:

1. Consider a message:

"Advanced mathematics is a field of study that has many applications in various fields, including engineering".

Pick up a part of this message as given below:

AdVaNcEd MaThEmAtIcS

2. Convert plain text into corresponding numeric values using ASCII 7-Bit Code.

A	d	V	a	N	c	E	d
65	100	86	97	78	99	69	100 32
M	a	T	h	E	m	A	t I c S
77	97	84	104	69	109	65	116 73 99 83

3. After taking the numeric values, convert each numeric value into corresponding 7-bit binary form as follows:

A	65	100 0001	a	97	110 0001
d	100	110 0100	T	84	101 0100
V	86	101 0110	h	104	110 1000
a	97	110 0001	E	69	100 0101
N	78	100 1110	m	109	110 1101
c	99	110 0011	A	65	100 0001
E	69	100 0101	t	116	111 0100
d	100	110 0100	I	73	100 1001
SPACE	32	010 0000	c	99	110 0011
M	77	100 1101	S	83	101 0011

4. Combining the binary string and divide into two segments:

1000001110010010101101100001100111011000111000101110010001000001001101110000110101001
101000100010111011011000001110100100100111000111010011

Segment 1: 1000001110010010101101100001100111011000111000101110010001000001001101

Segment 2: 1100001101010011010001000101110110110000011110100100100111000111010011

5. Applying two-point crossover technique on desired bits e.g. 29 and 42 which is mutually reciprocated between encryptor and decryptor, we get:

Segment 1:

1000001110010010101101100001110110110000011000101110010001000001001101

Segment 2: 1100001101010011010001000101100111011000111110100100100111000111010011

6. Applying swap mutation on both segments as agreed by sender and receiver e.g. swapping of 3rd bit and 5th bit in each 7-bit binary code, we arrive at:

Segment 1: 1000001111000010101101100001111100110000011010001111000001000001011001

Segment 2: 1100001101010011010001010001101101011000111110100100100111000111000111

7. Convert each 7-bit into corresponding numeric value by using ASCII 7-Bit code, we get as follows:

100 0001	65	110 0001	97
111 0000	112	101 0100	84
101 0110	86	110 1000	104
110 0001	97	101 0001	81
111 1001	121	101 1010	90
100 0001	65	110 0011	99
101 0001	81	111 0100	116
111 0000	112	100 1001	73
010 0000	32	110 0011	99
101 1001	89	100 0111	71

8. Subsequent convert the numeric value into corresponding character:

65 112 86 97 121 65 81 112 32
A p V a y A Q p

89 97 84 104 81 90 99 116 73 99 71
Y a T h Q Z c t I c G

9. Resultant of the conversion, we obtained the intermediate cipher text:

ApVayAQp YaThQZctIcG

10. Consequently, each character of the intermediate cipher text is converted into their corresponding symbol of periodic element, which give us:

A	'H'	A	'H'	a	'Ni'	c	'Zn'
p	'Tc'	Q	'Cl'	T	'Ca'	t	'Ag'
V	'Ti'	p	'Tc'	h	'Br'	I	'F'
a	'Ni'	SPACE	'Co'	Q	'Cl'	c	'Zn'
y	'Te'	Y	'Mn'	Z	'Fe'	G	'N'

On combining we get:

H TcTiNiTeH ClTcCoMnNiCaBrClFeZnAgF ZnN

11. Now transformed these symbols (pair of two-character) into their atomic number.

'H'	01	'H'	01	'Ni'	28	'Zn'	30
'Tc'	43	'Cl'	17	'Ca'	20	'Ag'	47
'Ti'	22	'Tc'	43	'Br'	35	'F'	09
'Ni'	28	'Co'	27	'Cl'	17	'Zn'	30
'Te'	52	'Mn'	25	'Fe'	26	'N'	07

12. Write these atomic numbers in sequence, we obtained the final ciphertext as follows:

0143222852011743272528203517263047093007

Via public channel this cipher text is send to the receiver.

B. Decryption:

1. Start with the ciphertext, which is obtained from the encryption process.

0143222852011743272528203517263047093007

2. From the cipher text, each atomic number (pair of two-numerical character) is converted into their symbol from chosen periodic table as follows:

01	'H '	01	'H '	28	'Ni'	30	'Zn'
43	'Tc'	17	'Cl'	20	'Ca'	47	'Ag'
22	'Ti'	43	'Tc'	35	'Br'	09	'F '
28	'Ni'	27	'Co'	17	'Cl'	30	'Zn'
52	'Te'	25	'Mn'	26	'Fe'	07	'N '

3. After the conversion, each symbol of periodic element (which are given as above) is transformed into their respective ASCII character using chosen periodic table, we get:

'H '	A	'H '	A		'Ni'	a	'Zn'	c
'Tc'	p	'Cl'	Q		'Ca'	T	'Ag'	t
'Ti'	V	'Tc'	p		'Br'	h	'F '	I
'Ni'	a	'Co'	SPACE		'Cl'	Q	'Zn'	c
'Te'	y	'Mn'	Y		'Fe'	Z	'N '	G

Arrange the obtained alphabets in a sequence, we get:

ApVayAQp YaThQZctIcG

4. Convert each character of the intermediate ciphertext into their corresponding numeric values using the ASCII 7-bit code as follows:

65 112 86 97 121 65 81 112 32

A p V a y A Q p

89 97 84 104 81 90 99 116 73 99 71

Y a T h Q Z c t I c G

5. Transform each numeric values into its corresponding 7-bit binary form as follows:

100 0001	65	110 0001	97
111 0000	112	101 0100	84
101 0110	86	110 1000	104
110 0001	97	101 0001	81
111 1001	121	101 1010	90
100 0001	65	110 0011	99
101 0001	81	111 0100	116
111 0000	112	100 1001	73
010 0000	32	110 0011	99
101 1001	89	100 0111	71

6. Combine the binary strings into a single binary sequence:

1000001111000010101101100001111100110000011010001111000001000001011001110000110101001
1010001010001101101011000111110100100100111000111000111

7. Execute reverse bit swap mutation by separate the combined binary string back into individual 7-bit binary codes.

1000001 1110000 1010110 1100001 1111001 1000001 1010001 1110000 0100000 1011001 1100001
1010100 1101000 1010001 1011010 1100011 1110100 1001001 1100011 1000111

8. For each 7-bit binary code, perform a bit swap mutation by swapping the 5th bit back to the 3rd bit.

1000001 1100100 1010110 1100001 1101101 1000001 1000101 1100100 0100000 1001101 1100001
1010100 1101000 1000101 1001110 1100011 1110100 1001001 1100011 1010011

9. Recombine the individual 7-bit binary codes into the complete binary sequence.

1000001110010010101101100001110110110000011000101110010001000001001101110000110101001
1010001000101100111011000111110100100100111000111010011

10. Applying reverse the two-point crossover technique that was applied during encryption at the desired positions e.g. 29 and 42. After reversing the crossover, divide the binary string back into individual 7-bit segments.

Segment	1	before	crossover:
		1000001110010010101101100001110110110000011000101110010001000001001101	
Segment	2	before	crossover:
		1100001101010011010001000101100111011000111110100100100111000111010011	
Segment	1	after	crossover:
		1000001110010010101101100001100111011000111000101110010001000001001101	
Segment	2	after	crossover:
		1100001101010011010001000101110110110000011110100100100111000111010011	

11. Combining both segments after Crossover, we get:

1000001110010010101101100001100111011000111000101110010001000001001101110000110101001
1010001000101110110110000011110100100100111000111010011

12. Convert each 7-bit binary segment back into its corresponding numeric value using the ASCII 7-bit code, we arrive at:

A	65	100 0001	a	97	110 0001
d	100	110 0100	T	84	101 0100
V	86	101 0110	h	104	110 1000
a	97	110 0001	E	69	100 0101
N	78	100 1110	m	109	110 1101
c	99	110 0011	A	65	100 0001
E	69	100 0101	t	116	111 0100
d	100	110 0100	I	73	100 1001
SPACE	32	010 0000	c	99	110 0011
M	77	100 1101	S	83	101 0011

13. Finally, convert the numeric values back into their corresponding characters to retrieve the original plaintext.

The Plaintext - AdVaNcEd MaThEmAtIcS

Note: We can encrypt the whole message by considering a large segment.

V. RESULT AND DISCUSSION

The proposed algorithm makes use of an encryption system that combines the periodic table and Genetic Algorithm (GA). Plaintext is transformed into ASCII-7 bit binary values using a single encryption key. for intermediate ciphertext, genetic operators are used: crossover (combining parent genes to form offspring) and mutation (flipping bits for uniqueness). The final ciphertext is created by converting pairs of symbols to atomic numbers and replacing each character in this intermediate text with the symbol for the relevant periodic table element. High confidentiality and robustness are guaranteed by this two-layered strategy, which makes use of GA and periodic table components. The technique is very secure against attacks since it is very difficult to break the ciphertext without knowing the precise crossover, mutation sites, and periodic table layouts employed.

Explanation of result is as follows:

SN	Name of attack	Opportunity of attack	Explanation
1	Ciphertext attack	Very Difficult	The chosen mutation and crossover techniques make decryption challenging, creating uncertainty about mutated bits and crossover types. The periodic table enhances ciphertext robustness, ensuring strong encryption
2	Chosen ciphertext attack	Very Difficult	The mutation and crossover techniques complicate decryption, creating uncertainty about which bits are mutated and the crossover type used, enhancing ciphertext security.
3	Known plaintext attack	Very Difficult	Since there are two types of cipher text, we obtain throughout, therefore there is no similarities can be seen, as final cipher text is obtained in numbers, and it's all possible because of the using the periodic table.
4	Chosen plaintext attack	Very Difficult	It's not that easy to decrypt since no sense of similarities can be found its very hard for the breaker to get the idea of the plaintext.

VI. CONCLUSION

The algorithm described in this paper is moderately complicated to implement in a cryptographic scheme. By using a dual layer cipher i.e., an intermediate cipher algorithm and a final cipher text and a key generation mechanism, they offer confidential security for data transfers. Here, we employ genetic algorithms (crossover and mutation operators). To provide additional security, we combine genetic algorithm with the chemical periodic table, which is responsible for the robust final cipher.

REFERENCES

- [1] Agarwal Ankita: Secret Key Encryption Algorithm Using Genetic Algorithm, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012, pp. 216-218.
- [2] Bhasin Harsha, Kumar Ramesh and Kathuria Neha: Cryptography using Cellular Automata, International Journal of Computer Science and Information Technology, Vol. 4(2), 355-357, 2013.
- [3] Forouzan Behrouz A.: Cryptography & Network Security, McGraw Hill Education, 2007.
- [4] Kahate Atul: Cryptography and Network Security, Tata McGraw Hill, New Delhi, 2008.
- [5] Kalubandi Venkata Krishna Pavan, and Yamuna M.: Chemical Formula Encryption Using 7 – bit Periodic Table, International Journal of Pharm Tech Research, Vol.6, No.3, pp 990-995, 2014.
- [6] Kumar Chandan, Dutta Sandip and Chakborty Soubhik: Musical Cryptography using Genetic Algorithm, ICCPCT, 2014, pp. 1742-1747.
- [7] Mandle Amit Kumar and Namdeo Varsha: Application of a Recurrence Matrix to Cryptography using Genetic Algorithm, International Journal of Recent Technology and Engineering, Volume-8 Issue-5, January 2020, pp. 2387-2389.
- [8] Mandle Amit Kumar and Namdeo Varsha: Cryptography Involving Musical Notes and Genetic Algorithm, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume 9, Issue 2, December 2019.

- [9] Mittal Ayush and Gupta Ravindra Kumar: Encryption and Decryption of a Message Involving Genetic Algorithm, International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249–8958, Volume 9, Issue 2, December 2019.
- [10] Mittal Ayush: A New Cryptographic Technique Involving Genetic Algorithm, International Journal of Scientific & Technology Research, Volume 9, Issue 3, March 2020.
- [11] Patil Shraddhali N. and Parab Dhanashree H., Nambly Akshay, John Linda Mary: Encryptic Message using Musical Notes by Genetic Algorithm, IJREM, Vol. 3, Issue 1, 2017, pp. 63-66.
- [12] 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, pp. 414-416.
- [13] Sinha Anurag and Bhadani Amrit Kumar: Double Layer Cryptography Using Multiplicative Cipher and Chemical Periodic Table, International Education & Research Journal, Vol. 7, pp. 33-41, 2021.
- [14] Sivanandan S., N. and Deepa S. N.: Introduction to Genetic Algorithm, Springer Verlag Berlin Heidelberg, 2008.
- [15] Stallings William: Cryptography and Network Security Principles and Practices, Prentice Hall, 2005.
- [16] Surya S., Muhammad Ilyas H.: Genetic Algorithm Based Cryptographic Approach using Karnatic Music, IRJET, Vol. 4, Issue 6, 2017, pp. 1995-2001.
- [17] Veetil Amritha Thekkumbadan: An Encryption Technique Using Genetic Operators, International Journal of Scientific & Technology Research, Volume 4, Issue 7, July 2015.
- [18] Zbigniew Kokosiński, Marcin Kołodziej, Krzysztof Kwarciany: Parallel Genetic Algorithm for Graph Coloring Problem, Computational Science - ICCS 2004, Vol. 3036, pp. 215-222, 2004.

