ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 1(J), pp. 23588-23595, January, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A NOVEL TEXT ENCRYPTION ALGORITHM USING DNA ASCII TABLE WITH A SPIRAL APPROACH

Kiran Kumar R and Bharathi Devi P

Department of Computer Science, Krishna University, Machilipatnam

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0901.1495

ARTICLE INFO

Article History:
Received 17th October, 2017
Received in revised form 21st November, 2017
Accepted 05th December, 2017
Published online 28th January, 2018

Key Words:

DNA computing, DNA Cryptography, Codons, Encryption, Decryption, Spiral, DNA ASCII

ABSTRACT

There is a need of introducing new encryption techniques to protect the data which is transmitted in a network or which is stored in a cloud as many cryptography algorithms are broken. In this scenario, DNA Cryptography has emerged to provide security to the information in the form of DNA sequences. Various bio molecular techniques used to implement DNA cryptography algorithms. Due to random nature of DNA many cryptographic approaches have become unbreakable. The capability of storing huge information nearly petabytes in few grams of DNA made the researchers introduce more cryptographic algorithms.

In the present paper, the authors proposed a novel cryptography algorithm which divides the given message into two parts and performs XOR operation with randomly generated Key. Here, the key also splits into two parts. The XOR is applied on the Left part of Plaintext and Right Part of Key and the Right part of Plaintext with Left part of Key. In this model the authors proposed DNA ASCII table which maps the DNA sequences to numerical data which in turn converts into binary and then turns into DNA bases. These DNA bases are arranged in spiral fashion and it is transmitted through secure media.

INTRODUCTION

Every Organization thinks about how to secure the information. With the increase of technology, threats also increase. Providing security to the data while transmission is a very essential aspect for any organization. The key aspect of information is it must only be viewed by both the sender and receiver. In view of this, the researchers showed interest to invent number of security algorithms. Providing security to the data can be done using cryptographic techniques. By using these techniques, the data is transferred securely through the internet. In cryptography, the information which is transmitted in an unreadable format, called encryption process, and at the receiver end the unreadable format can be converted into readable format, called as decryption process[1]. The unreadable format is called as cipher text. Traditionally, we use cryptography approaches like DES, AES, RSA etc., A technique like Elliptic Curve Cryptography has the drawback of more time complexity and it is difficult to take the random points on a curve[2]. Physics and Computer Scientists introduced quantum cryptography, which has the drawback of implementing digital signatures. Based on the work done by the Leonard Adleman using DNA bases to solve the mathematical complex problems, which is known as DNA computing[3], Gehani implemented DNA based Cryptography, which hides the information in the form of DNA bases[4]. With the help of DNA Computing, complex problems can be solved by parallel search known as massive parallelism. The field of bioinformatics is a branch of biology, computer science and mathematics which analyses the DNA sequences and also implements algorithms which provides security to the data.

What is DNA?

DNA is abbreviated as Deoxyribo Nucleic Acid is the basic storage medium of genetic information of every living organism. It contains large number of molecules, nucleotides. Each nucleotide contains a Sugar group, a Phosphate group and a Nitrogen bases. There are four Nitrogen bases in the DNA structure named as Adenine(A), Thymine(T), Guanine(G) and Cytocine(C)[5-8].These bases determines the structure of DNA. The bases in a DNA sequence forms genes, which in turns converts into Proteins in human body. In nature, the DNA existed in the form of double helix, discovered by James Watson in 1953,which contains two long strands of DNA structure[9]. One strand is complementary to other strand. This structure is also called as Complementary structure because A

Corresponding author:* **Kiran Kumar R
Department of Computer Science, Krishna University, Machilipatnam

&T, C&G are complementary bases each other. The nature of DNA spreads into the field of computer science tremendously.

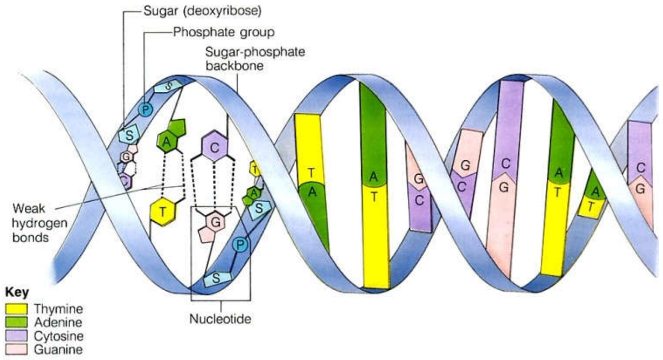


Figure 1 Structure of DNA

Related Works

The Massive Parallelism and the capability of storing huge information in DNA create an interest to the researcher in the field of DNA Cryptography. Not only that, it also gives high security to the data by applying various cryptographic algorithms [10]. The DNA Cryptography makes the information unbreakable and also DNA based algorithms implemented to break the traditional cryptography algorithms[11].The key technologies of DNA - Polymerase Chain Reaction(PCR), DNA digital coding and DNA synthesis are mostly used now-a-days to develop DNA Cryptography algorithms[12]. Utilizing short-DNA strands which contains an encoded information by using Polymerase Chain Reaction give better results in the field of DNA steganography [13]. The various works by [14-16] made a major breakthrough in the field of DNA Cryptography.

Proposed Algorithm

In this paper, DNA based Cryptography algorithm is proposed to increase the security of data and also increase the reliability of transmission of data in network channel. In this scheme both biological and mathematical concepts are used to encrypt the plaintext message. One more key aspect is that it used randomly generated key which lies between the set $\{0, 1\}^*$. The length of key depends upon the number of characters in the plaintext. If the length of plaintext is n, then the key length is n*8. In this paper, the authors proposed DNA ASCII Table which contains 0 to 255 values for each unique numeric value mapped into four DNA sequences. Actually, three DNA nucleotides which can be mapped to 64 codons can be used in protein synthesization[17]. Similarly, the four bases where each base when replaced with any one the four DNA bases 4*4*4*4=256 unique DNA sequences each of length 4 are generated increasing the key domain up to 256. This DNA ASCII table is mapped with original ASCII table[Table1]. In the mapping process the DNA sequences can be shuffled in 256! ways which the makes the data more secured.

The proposed methods perform the encryption process in level based. In the first level the message which was sent by the sender is transmitted is converted into ASCII which in turns converted into Binary. Later the key was randomly generated from the set {0,1}* which is of length as plaintext length*8. Now, Divide the Plaintext message into two equivalent parts named M_R and M_L and the key also divided into two equal parts and named as KR and KL. In general, the right part of text performs XOR operation with right part of key and then interchanges the left and right parts of plaintext which makes the attacker to guess the half part of the text easily. To avoid such problem, perform the XOR(M_L,K_R) and XOR(M_R,K_L). Now, the binary values are converted into DNA bases (00-A, 11-T, 01-C, 10-G). Divide the DNA bases into four bases each. Find the DNA ASCII Value for the DNA bases from the DNA ASCII Table. Again, convert the DNA ASCII Value into its equivalent binary value and these binary in turn converts into DNA bases. The DNA Sequences are now arranged into spiral matrix (Figure 2). The length of the text is divided by four and it is arranged accordingly. For example, if length of text is 36, it is arranged as 9 rows and 4 columns(9X4). The data is concatenated row wise (Figure 3) to obtain the final Cipher text which is sent to the receiver. The reverse process gives the original plaintext.

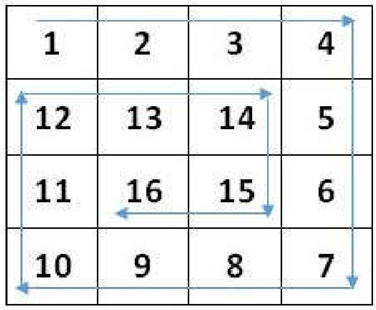


Figure 2 Spiral pattern

For Example if the DNA Sequence of some plaintext is ACGTAAAAGCTTACGT then it is arranged in a spiral pattern as in figure 3. But it is sent as a row wise sequence which is ACGTTTCATTGACGAA.

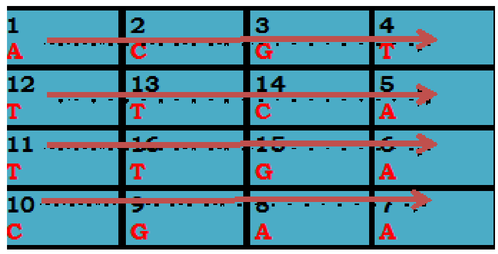


Figure 3 Row wise Concatenation

Algorithm DNAASCIIEncrypt(M)

This algorithm is used to encrypt the plaintext Message M into cipher text C which is transmitted to the receiver.
Begin

1. Convert the Plaintext M into its equivalent Binary values.
2. Split the Binary data into two equal length parts say M_L& M_R.
3. Generate the key randomly in the set {0,1}* which is of the same length of binary data.
4. Divide the key also into two equal length parts say K_L& K_R.
5. M_L=$M_L \oplus K_R$
6. M_R=$M_R \oplus K_L$
7. M=M_L+M_R('+' act as concatenation operator).
8. Convert M into its equivalent DNA bases(00-A,01-C,10-G,11-T).

Table 1 DNA ASCII Table

Dec	Hex	Binary	Char-acter	Description	DNA Codon
0	00	00000000	NUL	Null	AAAA
1	01	00000001	SOH	start of header	AAAC
2	02	00000010	STX	start of text	AAAG
3	03	00000011	ETX	end of text	AAAT
4	04	00000100	EOT	end of transmission	AACA
5	05	00000101	ENQ	enquiry	AACC
6	06	00000110	ACK	acknowledge	AACG
7	07	00000111	BEL	Bell	AACT
8	08	00001000	BS	backspace	AAGA
9	09	00001001	HT	horizontal tab	AAGC
10	0A	00001010	LF	line feed	AAGG
11	0B	00001011	VT	vertical tab	AAGT
12	0C	00001100	FF	form feed	AATA
13	0D	00001101	CR	enter / carriage return	AATC
14	0E	00001110	SO	shift out	AATG
15	0F	00001111	SI	shift in	AATT
16	10	00010000	DLE	data link escape	ACAA
17	11	00010001	DC1	device control 1	ACAC
18	12	00010010	DC2	device control 2	ACAG
19	13	00010011	DC3	device control 3	ACAT
20	14	00010100	DC4	device control 4	ACCA
21	15	00010101	NAK	negative acknowledge	ACCC
22	16	00010110	SYN	synchronize	ACCG
23	17	00010111	ETB	end of trans. Block	ACCT
24	18	00011000	CAN	cancel	ACGA
25	19	00011001	EM	end of medium	ACGC
26	1A	00011010	SUB	substitute	ACGG
27	1B	00011011	ESC	escape	ACGT
28	1C	00011100	FS	file separator	ACTA
29	1D	00011101	GS	group separator	ACTC
30	1E	00011110	RS	record separator	ACTG
31	1F	00011111	US	unit separator	ACTT
32	20	00100000	Space	space	AGAA
33	21	00100001	!	exclamation mark	AGAC
34	22	00100010	"	double quote	AGAG
35	23	00100011	#	number	AGAT
36	24	00100100	$	dollar	AGCA
37	25	00100101	%	percent	AGCC
38	26	00100110	&	ampersand	AGCG
39	27	00100111	'	single quote	AGCT
40	28	00101000	(	left parenthesis	AGGA
41	29	00101001	)	right parenthesis	AGGC
42	2A	00101010	*	asterisk	AGGG
43	2B	00101011	+	Plus	AGGT
44	2C	00101100	,	comma	AGTA
45	2D	00101101	-	minus	AGTC
46	2E	00101110	.	period	AGTG
47	2F	00101111	/	Slash	AGTT
48	30	00110000	0	Zero	ATAA
49	31	00110001	1	One	ATAC
50	32	00110010	2	two	ATAG
51	33	00110011	3	three	ATAT
52	34	00110100	4	four	ATCA
53	35	00110101	5	five	ATCC
54	36	00110110	6	six	ATCG
55	37	00110111	7	seven	ATCT
56	38	00111000	8	eight	ATGA
57	39	00111001	9	nine	ATGC
58	3A	00111010	:	colon	ATGG
59	3B	00111011	;	semicolon	ATGT
60	3C	00111100	<	less than	ATTA
61	3D	00111101	=	equality sign	ATTC
62	3E	00111110	>	greater than	ATTG
63	3F	00111111	?	question mark	ATTT
64	40	01000000	@	at sign	CAAA
65	41	01000001	A		CAAC
66	42	01000010	B		CAAG
67	43	01000011	C		CAAT
68	44	01000100	D		CACA
69	45	01000101	E		CACC
70	46	01000110	F		CACG
71	47	01000111	G		CACT
72	48	01001000	H		CAGA

Table 1 DNA ASCII Table

Dec	Hex	Binary	Char-acter	Description	DNA Codon
73	49	01001001	I		CAGC
74	4A	01001010	J		CAGG
75	4B	01001011	K		CAGT
76	4C	01001100	L		CATA
77	4D	01001101	M		CATC
78	4E	01001110	N		CATG
79	4F	01001111	O		CATT
80	50	01010000	P		CCAA
81	51	01010001	Q		CCAC
82	52	01010010	R		CCAG
83	53	01010011	S		CCAT
84	54	01010100	T		CCCA
85	55	01010101	U		CCCC
86	56	01010110	V		CCCG
87	57	01010111	W		CCCT
88	58	01011000	X		CCGA
89	59	01011001	Y		CCGC
90	5A	01011010	Z		CCGG
91	5B	01011011	[	left square bracket	CCGT
92	5C	01011100	\	backslash	CCTA
93	5D	01011101	]	right square bracket	CCTC
94	5E	01011110	^	caret / circumflex	CCTG
95	5F	01011111	_	underscore	CCTT
96	60	01100000	`	grave / accent	CGAA
97	61	01100001	a		CGAC
98	62	01100010	b		CGAG
99	63	01100011	c		CGAT
100	64	01100100	d		CGCA
101	65	01100101	e		CGCC
102	66	01100110	f		CGCG
103	67	01100111	g		CGCT
104	68	01101000	h		CGGA
105	69	01101001	i		CGGC
106	6A	01101010	j		CGGG
107	6B	01101011	k		CGGT
108	6C	01101100	l		CGTA
109	6D	01101101	m		CGTC
110	6E	01101110	n		CGTG
111	6F	01101111	o		CGTT
112	70	01110000	p		CTAA
113	71	01110001	q		CTAC
114	72	01110010	r		CTAG
115	73	01110011	s		CTAT
116	74	01110100	t		CTCA
117	75	01110101	U		CTCC
118	76	01110110	V		CTCG
119	77	01110111	W		CTCT
120	78	01111000	X		CTGA
121	79	01111001	Y		CTGC
122	7A	01111010	Z		CTGG
123	7B	01111011	{	left curly bracket	CTGT
124	7C	01111100	|	vertical bar	CTTA
125	7D	01111101	}	right curly bracket	CTTC
126	7E	01111110	~	tilde	CTTG
127	7F	01111111	DEL	delete	CTTT
128	80	10000000			GAAA
129	81	10000001			GAAC
130	82	10000010	‚		GAAG
131	83	10000011	Ƒ		GAAT
132	84	10000100	„		GACA
133	85	10000101	…		GACC
134	86	10000110	†		GACG
135	87	10000111	‡		GACT
136	88	10001000	ˆ		GAGA
137	89	10001001	‰		GAGC
138	8A	10001010	Š		GAGG
139	8B	10001011	‹		GAGT
140	8C	10001100	Œ		GATA
141	8D	10001101			GATC
142	8E	10001110			GATG
143	8F	10001111			GATT
144	90	10010000			GCAA

Table 1 DNA ASCII Table

Dec	Hex	Binary	Char-acter	Description	DNA Codon
145	91	10010001	‘		GCAC
146	92	10010010	’		GCAG
147	93	10010011	“		GCAT
148	94	10010100	”		GCCA
149	95	10010101	•		GCCC
150	96	10010110	–		GCCG
151	97	10010111	—		GCCT
152	98	10011000	˜		GCGA
153	99	10011001	™		GCGC
154	9A	10011010	š		GCGG
155	9B	10011011	›		GCGT
156	9C	10011100	Œ		GCTA
157	9D	10011101			GCTC
158	9E	10011110			GCTG
159	9F	10011111	Ÿ		GCTT
160	A0	10100000		space	GGAA
161	A1	10100001	¡		GGAC
162	A2	10100010	¢	cent	GGAG
163	A3	10100011	£	pound	GGAT
164	A4	10100100	¤	currency sign	GGCA
165	A5	10100101	¥	yen, yuan	GGCC
166	A6	10100110	¦	broken bar	GGCG
167	A7	10100111	§	section sign	GGCT
168	A8	10101000	¨		GGGA
169	A9	10101001	©	copyright	GGGC
170	AA	10101010	ª	ordinal indicator	GGGG
171	AB	10101011	«		GGGT
172	AC	10101100	¬		GGTA
173	AD	10101101			GGTC
174	AE	10101110	®	registered trademark	GGTG
175	AF	10101111	¯		GGTT
176	B0	10110000	°	degree	GTAA
177	B1	10110001	±	plus-minus	GTAC
178	B2	10110010	²		GTAG
179	B3	10110011	³		GTAT
180	B4	10110100	´		GTCA
181	B5	10110101	µ	mu	GTCC
182	B6	10110110	¶	pilcrow	GTCG
183	B7	10110111	·		GTCT
184	B8	10111000	¸		GTGA
185	B9	10111001	¹		GTGC
186	BA	10111010	º	ordinal indicator	GTGG
187	BB	10111011	»		GTGT
188	BC	10111100	¼		GTTA
189	BD	10111101	½		GTTC
190	BE	10111110	¾		GTTG
191	BF	10111111	¿	inverted question mark	GTTT
192	C0	11000000	À		TAAA
193	C1	11000001	Á		TAAC
194	C2	11000010	Â		TAAG
195	C3	11000011	Ã		TAAT
196	C4	11000100	Ä		TACA
197	C5	11000101	Å		TACC
198	C6	11000110	Æ		TACG
199	C7	11000111	Ç		TACT
200	C8	11001000	È		TAGA
201	C9	11001001	É		TAGC
202	CA	11001010	Ê		TAGG
203	CB	11001011	Ë		TAGT
204	CC	11001100	Ì		TATA
205	CD	11001101	Í		TATC
206	CE	11001110	Î		TATG
207	CF	11001111	Ï		TATT
208	D0	11010000	Ð		TCAA
209	D1	11010001	Ñ		TCAC
210	D2	11010010	Ò		TCAG
211	D3	11010011	Ó		TCAT
212	D4	11010100	Ô		TCCA
213	D5	11010101	Õ		TCCC
214	D6	11010110	Ö		TCCG
215	D7	11010111	×	multiplication sign	TCCT
216	D8	11011000	Ø		TCGA

Table 1 DNA ASCII Table

Dec	Hex	Binary	Char-acter	Description	DNA Codon
217	D9	11011001	Ù		TCGC
218	DA	11011010	Ú		TCGG
219	DB	11011011	Û		TCGT
220	DC	11011100	Ü		TCTA
221	DD	11011101	Ý		TCTC
222	DE	11011110	Þ		TCTG
223	DF	11011111	ß		TCTT
224	E0	11100000	à		TGAA
225	E1	11100001	á		TGAC
226	E2	11100010	â		TGAG
227	E3	11100011	ã		TGAT
228	E4	11100100	ä		TGCA
229	E5	11100101	å		TGCC
230	E6	11100110	æ		TGCG
231	E7	11100111	ç		TGCT
232	E8	11101000	È		TGGA
233	E9	11101001	É		TGGC
234	EA	11101010	Ê		TGGG
235	EB	11101011	Ë		TGGT
236	EC	11101100	Ì		TGTA
237	ED	11101101	Í		TGTC
238	EE	11101110	Î		TGTG
239	EF	11101111	Ï		TGTT
240	F0	11110000	Đ		TTAA
241	F1	11110001	Ñ		TTAC
242	F2	11110010	Ò		TTAG
243	F3	11110011	Ó		TTAT
244	F4	11110100	ô		TTCA
245	F5	11110101	õ		TTCC
246	F6	11110110	ö		TTCG
247	F7	11110111	÷		TTCT
248	F8	11111000	ø		TTGA
249	F9	11111001	ù		TTGC
250	FA	11111010	ú		TTGG
251	FB	11111011	û		TTGT
252	FC	11111100	ü		TTTA
253	FD	11111101	ý		TTTC
254	FE	11111110	þ		TTTG
255	FF	11111111	ÿ		TTTT

9. Divide M into 4 bases each and mapped with decimal value of DNA ASCII Table(Table 1).
10. Convert the decimal values into binary values and store them in C.
11. Convert C into DNA bases(00-A,01-C,10-G,11-T).
12. Arrange the DNA bases in spiral approach(Figure 2) and then concatenate(Figure 3) row wise which is our cipher text.

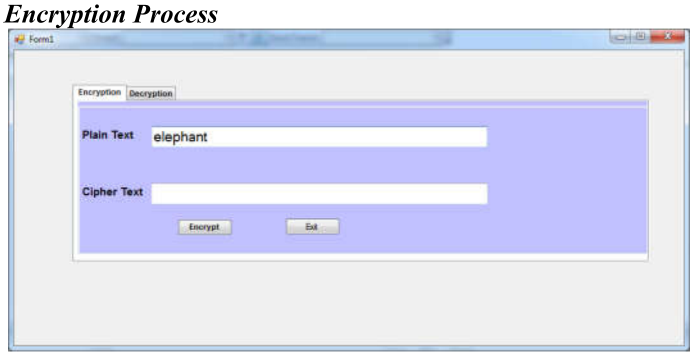
End.

Decryption Algorithm

The reverse process of the above algorithm is Decryption Algorithm.

Experimental Results

Encryption Process



Decryption Process

Result Analysis & Avalanche Effect

The related work, DNA Cryptosystem using DNA ASCII table with spiral approach algorithm is implemented in .NET framework and the time taken for encryption and decryption process of various plaintext in unit of bytes is noted in the tabular form.

The following table shows the performance of proposed algorithm in terms of milliseconds.

Table 2 Performance Analysis

No.of Bytes	Encryption time	Decryption time
20	0.0037492	0.0007790
100	0.0050861	0.0010924
200	0.0088962	0.0024560
2000	0.0110922	0.0561267
5000	0.0360928	0.0862258
10000	0.0861128	0.1296585

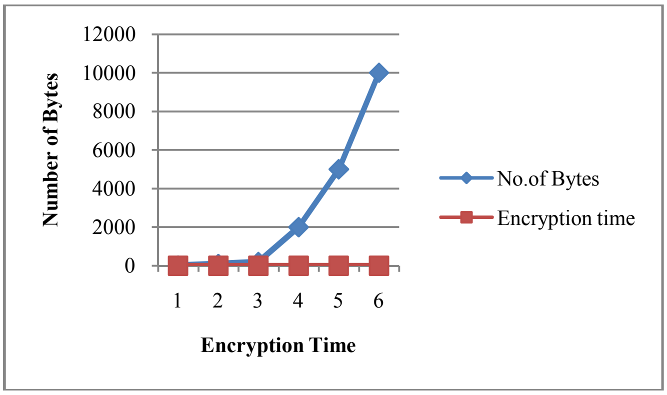


Figure 4 Encryption Time Analysis

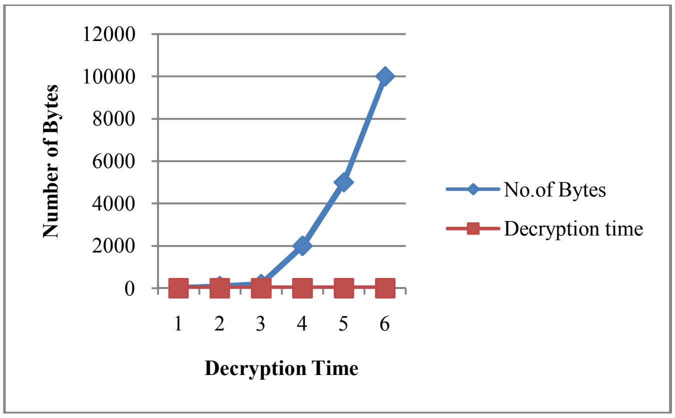


Figure 5 Encryption Time Analysis

Comparison of Avalanche Effect

The avalanche effect says, that a lot of the output must change, even when the input changes only a little [https://simple.wikipedia.org/wiki/Avalanche_effect]. In other words, a small change in the key or the plaintext should cause a strong change in the ciphertext.

The avalanche effect calculated by using the formula

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in cipher text}}{\text{Number of bits in the cipher text}} \times 100\%$$

Avalanche effect is calculated and a comparison study is done on various existing cryptographic techniques and the proposed work.

Let us take an example as

The first Plaintext as elephant
Later one of the character is modified as elxphant
Keyword: buzzword

Caesar Cipher

Ciphertext1:01101000011011110110100001110011011010110110010001110001011101111

Ciphertext2:01101000011011110110000101110011011010110110010001110001011101111

Playfair Technique

Ciphertext1:0111001001110001011000110111000101101110011010000110110011101101

Ciphertext2:0111001001110001011101110111100001101110011010000110110101110110

Vigenere Cipher

Ciphertext1:01100110011001100110001001101111011001000110111101100101011101111

Ciphertext2:01100110011001100111011101101111011001000110111101100101011101111

Blowfish

The number of bits flipped in the ciphertext in this algorithm is approximately 19 bits and the average percentage of avalanche effect is 29.68[17].

Data Security using DNA ASCII Table with a spiral approach

Ciphertext1:0110100110000001000101001100010100001011111011010110010001100011

Ciphertext2:1011000110111011111111111010011000100101010111110101111111001011 0

Table Avalanche effect of various existing cryptography techniques and the proposed work

Name of the Algorithm	Number of bits flipped	%
Ceaser Cipher	2	3.125
Playfair	4	4.69
Vigener Cipher	3	3.125
Blowfish	19	29.68
DNA Cryptosystem using DNA ASCII Table with spiral approach	40	53.12

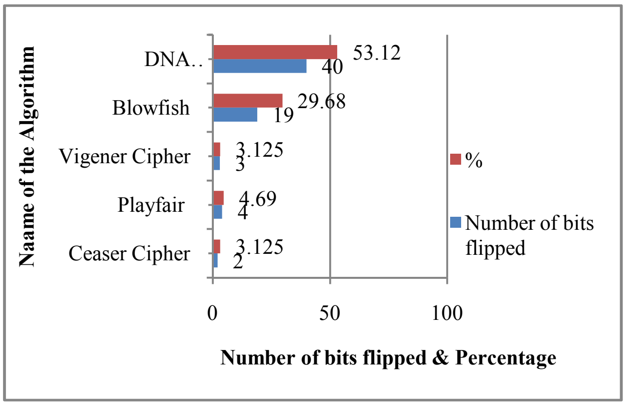


Figure 6 Analysis of Avalanche Effect

CONCLUSION

In this paper, the authors have recommended a new encryption technique for text. In the proposed algorithm as the key is generated randomly, it is an impossible task to the intruder to guess the plaintext. Initially, both sender and receiver approve the spiral pattern. The randomly generated key by the sender is transferred to the receiver through the secure medium. The proposed method has three level securities. In the first level, the cross join of XOR function with the plaintext and the key i.e., XOR (M_L,K_R) and XOR(M_R,K_L)is performed. In the next level the DNA Sequence which is of length four is mapped to DNA ASCII Value. A new DNA ASCII Table is designed so that the mapping can be identified in 256! possible ways making the job of intruder more complex. In the final level the DNA Sequences are arranged in a spiral fashion. The data is sent row wise to the receiver. The proposed algorithm increased the degree of confusion and diffusion to produce a better security system. In this paper, the authors made a comparative study of Avalanche Effect on various existing cryptographic techniques and the proposed method.

References

1. W. Stallings, Cryptography and Network Security(2003): Principles and Practices, 3rd edition, Prentice Hall, NJ.
2. E. Suresh Babu , C. Naga Raju and Munaga H.M Krishna Prasad(2016):Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks. *International Journal of Network Security*.,18(2):291-303.
3. Leonard M.Adleman(1994):Molecular Computation of solution to combinatorial problems Science. New Series., 266(5187):1021-1024.
4. Ashish Gehani, LaBean Thomas and John Reif(2004): DNA-based cryptography, In Aspects of Molecular Computing. Springer Berlin Heidelberg.,:167-188.
5. R.J.Lipton(1995):Using DNA to Solve NP-Complete Problems. Science., 268(542-545).
6. Chen Jie(2003): A DNA-based bio molecular cryptography design. Proceedings of IEEE International Symposium., 3:822-825.
7. G.Z.Cui, L.M.Qin and X.Zhang(2006): New Direction of data storage:DNA molecular storage technology. *Computer Engineering and Applications*., 42(26):29-32.
8. Mamta Rani and Sandeep Jain(2013):DNA Computing and Recent Developments. *International Journal of Computer Science and Engineering*., 3:607-610.
9. J.D.Watson, H.N.Hopkins, W.J.Roberts(1987), Molecular Biology of the Gene, 4th ed, Menlo Par, CA: The Benjamin/Cummings Publishing Co., Inc.,.
10. G.Z.Cui, L.M.Qin, Y.F.Wang and X.Zhang(2007): Infomration Secuirty Technology Based on DNA Computing, IEEE International Workshop on Anticounterfeiting Security., :288-291
11. K.Li, S.Zou and J.Xv(2008):Fast Parallel Molecular Algorithms for DNA based Computation:Solving the elliptic curve discrete logarithm problem over gf(2n). *Journal of Biomedicine and Biotechnology*, Hindwai.,:1-10.
12. X.Guozhen, L.Mingxin, Q.Liw and L.Xuejia(1999): New Field of Cryptography: DNA Cryptography. Chinese Science Bulletin, Springer Verlag, Germany.,51(12):1413-1420.
13. T.C.Catherinel, V.Risca, C.Bancroft(1999): Hiding Messages in DNA Microdots. *Nature Magazine*., 399:533-534.
14. T.Kazuo O.Akimitsu and S.Isao(2005): Public-Key System Using DNA as a one-way function for key distribution. *Biosystems*., 81:25-29.
15. Sherif T. Amin, Magdy Saeb and El-Gindi Salah(2006):A DNA-based implementation of YAEA encryption algorithm. In Computational Intelligence:120-125.
16. Pankaj Rakheja(2011): Integrating DNA Computing in International Data Encryption Algorithm(IDEA). *International Journal of Computer Applications*.,26(3):1-6.
17. Mona Sabry, Mohammed Hasheem, TaymoorNazmy and Mohamed EssamKhalifa(2010): A DNA and Amino Acids-Based Implementation of Playfair Cipher. *International Journal of Computer Science and Information Security*., Vol.8(3):129-136.

How to cite this article:

Kiran Kumar R and Bharathi Devi P.2018, A Novel Text Encryption Algorithm Using DNA ASCII Table With A Spiral Approach. *Int J Recent Sci Res.* 9(1), pp. 23588-23595. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0901.1495

****