International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.040

Design and Implementation of Cryptographic Algorithm Based on Reactive Elements and RNA Codons for Secured Transmission

Saswata Dasgupta
Department of Computer Sc. & Engineering
JIS College of Engineering, Kalyani,West Bengal, India

Kumar Gaurav Verma
Department of Computer Sc. & Engineering
JIS College of Engineering, Kalyani,West Bengal, India

Sudipta Sahana
Assistant Professor, Department of Computer Sc. & Engineering
JIS College of Engineering, Kalyani,West Bengal, India

Rajdeep Chowdhury
Assistant Professor, Department of Computer Application
JIS College of Engineering, Kalyani,West Bengal, India

Abstract – Network Security has become imperative in the contemporary scenario and subsequently an assortment of modus operandi is espoused to evade it. Network administrators need to adhere with latest advancement in both hardware and software field to prevent user data from malicious intrusions. The formulated paper outlines a cryptographic algorithm based on elements of Reactive Series and RNA Codons employing the identical concept amid its functionality. An amalgamation would endow with a proficient and prearranged approach of amassing data with stringent security modus operandi, with effective deployment of all obtainable space. The incorporation of the novel cryptographic algorithm would ensure performance enhancement in course of action. The pertinent employment of the formulated work is ensured in a variety of organizations where accrual of cosseted data is of extreme enormity.

Keywords – Encryption; Decryption; ASCII Table; Reactivity Series; Codon Table; RNA

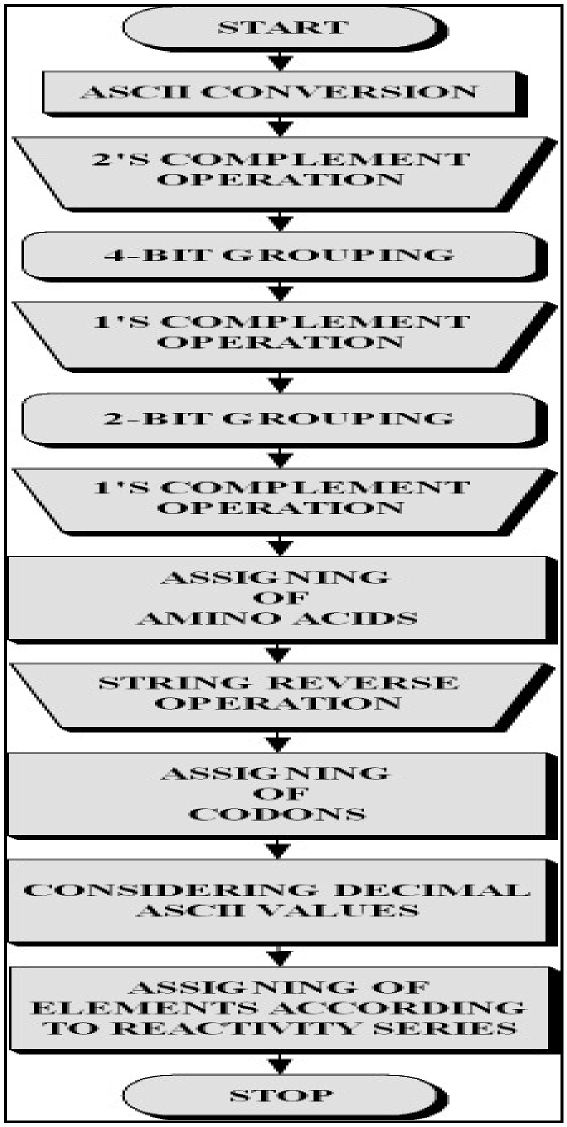
I. INTRODUCTION

The concept of ideal confidentiality has been prevalent since the 1950s and the modus operandi of encrypting data is quite highly accepted, when the notion of security implementation comes at its premier standards. Nevertheless, over the years, the modus operandi to engender the Seed employed in such encryption techniques has only diversified with the endeavour of making a move towards a much more robust technique, to say the least. The proposed cryptographic algorithm is classified as a Stream Cipher algorithm, as the Seed is applied to apiece character at a time. The concept of Reactive Elements according to the Reactivity Series is applied in the proposed algorithm. Furthermore, the paper guides with the mechanism in which the appliance have been ensured in a part by part basis, for utmost ease in understanding. It is imperative to employ a dynamic Seed to ascertain ideal confidentiality. It would be effectual to say that the entire paper covers the prime aspect established in conceptual juncture and meets economic feasibility, viability as well as scalability.

http://dx.doi.org/10.21172/ijiet.82.040

II. Proposed Algorithm

For utmost ease of understanding, the entire flowchart of the proposed work is stated below:



Figure–1: Flowchart of Entire Work

A. Encryption –

At the very first inception, considering the plain text to be **"Test@1234"**

http://dx.doi.org/10.21172/ijiet.82.040

Character	ASCII Value
T	01010100
e	01100101
s	01110011
t	01110100
@	01000000
1	00000001
2	00000010
3	00000011
4	00000100

Step 1: Apiece character of the plain text is converted to its corresponding 8-bit ASCII Value.

ASCII Value	2's Complement
01010100	10101100
01100101	10011011
01110011	10001101
01110100	10001100
01000000	11000000
00000001	11111111
00000010	11111110
00000011	11111101
00000100	11010110

Step 2: Apiece 8-bit ASCII Value is operated with 2's Complement.

8-bit ASCII	4-bit Grouping
10101100	1010 1100
10011011	1001 1011
10001101	1000 1100
10001100	1000 1100
11000000	1100 0000
11111111	1111 1111
11111110	1111 1110
11111101	1111 1101
11010110	1101 0110

Step 3: Grouping of 4 bits of segments is ensured.

4-bit Groups	1's Complement
1010 1100	0101 0011
1001 1011	0110 0100
1000 1100	0111 0010
1000 1100	0111 0011
1100 0000	0011 1111
1111 1111	0000 0000
1111 1110	0000 0001
1111 1101	0000 0010
1101 0110	0010 1001

Step 4: 1's Complement operation is performed.

4-bit Groups	2-bit Grouping
0101 0011	01 01 00 11
0110 0100	01 10 01 00
0111 0010	01 11 00 10
0111 0011	01 11 00 11
0011 1111	00 11 11 11
0000 0000	00 00 00 00
0000 0001	00 00 00 01
0000 0010	00 00 00 10
0010 1001	00 10 10 01

Step 5: Segments of 2 bit Grouping is ensured.

2-bit Groups	1's Complement
01 01 00 11	10 10 11 00
01 10 01 00	10 01 10 11
01 11 00 10	10 00 11 01
01 11 00 11	10 00 11 00
00 11 11 11	11 00 00 00
00 00 00 00	11 11 11 11
00 00 00 0 1	11 11 11 10
00 00 00 10	11 11 11 01
00 10 10 01	11 01 01 10

Step 6: Operation of 1's Complement is ensured

2-bit Groups	Amino Acids
10 10 11 00	C C A U
10 01 10 11	C G C A
10 00 11 01	C U A G
10 00 11 00	C U A U
11 00 00 00	A U U U
11 11 11 11	A A A A
11 11 11 10	A A A C
11 11 11 01	A A A G
11 01 01 10	A G G C

Step 7: Apiece 2-bit segments are assigned to Amino Acids U G C A, as stated below:
00 – U 01 – G 10 – C 11 – A

Original Value	Reversed Value
C C A U	U A C C
C G C A	A C G C
C U A G	G A U C
C U A U	U A U C
A U U U	U U U A
A A A A	A A A A
A A A C	C A A A
A A A G	G A A A
A G G C	C G G A

Step 8: Reverse String operation is performed.

Hence, ignoring the last and the first bit simultaneously and considering the rest 3 bits for referring to the Codon Table until all segments are employed, is ensured.

		Second Position								
		U		C		A		G		
		code	Amio Acid	code	Amio Acid	code	Amio Acid	code	Amio Acid	
First Position	U	UUU	phe	UCU	ser	UAU	tyr	UGU	cys	U
		UUC		UCC		UAC		UGC		C
		UUA	leu	UCA		UAA	STOP	UGA	STOP	A
		UUG		UCG		UAG	STOP	UGG	trp	G
	C	CUU	leu	CCU	pro	CAU	his	CGU	arg	U
		CUC		CCC		CAC		CGC		C
		CUA		CCA		CAA	gln	CGA		A
		CUG		CCG		CAG		CGG		G
	A	AUU	ile	ACU	thr	AAU	asn	AGU	ser	U
		AUC		ACC		AAC		AGC		C
		AUA		ACA		AAA	lys	AGA	arg	A
		AUG	met	ACG		AAG		AGG		G
	G	GUU	val	GCU	ala	GAU	asp	GGU	gly	U
		GUC		GCC		GAC		GGC		C
		GUA		GCA		GAA	glu	GGA		A
		GUG		GCG		GAG		GGG		G
										Third Position

Figure–2: Codon Table

Amino Acids	Codons
U A C C	t y r C
A C G C	A a r g
G A U C	a s p C
U A U C	U i l e
U U U A	p h e A
A A A A	A l y s
C A A A	g l n A
G A A A	G l y s
C G G A	a r g A

Codons	Decimal ASCII
t y r C	11612111467
A a r g	6597114103
a s p C	9711511299
U i l e	85105108101
p h e A	11210410165
A l y s	65108121115
g l n A	10310811065
G l y s	71108121115
a r g A	9711410365

Step 9: For apiece character, the decimal ASCII Value is considered

Step 10: Replacing apiece decimal number with its corresponding elements, in accordance to the Reactivity Series.
(Considering only those 10 elements which are more reactive than Hydrogen, inclusive)

Numeric Value	Corresponding Element
0	K
1	Na
2	Ca
3	Mg
4	Al
5	Zn
6	Fe
7	Sn
8	Pb
9	H

Decimal ASCII	Element Segments
11612111467	NaNaFeNaCaNaNaNaAlFeSn
6597114103	FeZnHSnNaNaAlNaKMg
9711511299	HSnNaNaZnNaNaCaHH
85105108101	PbZnNaKZnNaKPbNaKNa
11210410165	NaNaCaNaKAlNaKNaFeZn
65108121115	FeZnNaKPbNaCaNaNaNaZn
10310811065	NaKMgNaKPbNaNaKFeZn
71108121115	SnNaNaKPbNaCaNaNaNaZn
9711410365	HSnNaNaAlNaKMgFeZn

Hence, the cipher would be –

NaNaFeNaCaNaNaNaAlFeSnFeZnHSnNaNaAlNaKMgHSnNaNaZnNaNaCaHHPbZnNaKZnNaKPbNaKNaNaNaCaNaKAlNaKNaFeZnFeZnNaKPbNaCaNaNaNaZnNaKMgNaKPbNaNaKFeZnSnNaNaKPbNaCaNaNaNaZnHSnNaNaAlNaKMgFeZn

As the length of the cipher is too long, the repeated elements are added, as stated below:

2NaFeCa3NaAlFeSnFeZnHSn2NaAlNaKMgHSn2NaZn2NaCa2HPbZnNaKZnNaKPbNaK3NaCaNaKAlNaKNaFeZnFeNaKPbNaCa3NaZnNaKMgNaKPb2NaKFeZnSn2NaKPbNaCa3NaZnHSn2NaAlNaKMgFeZn

B. Decryption –

For decryption purpose, the reverse order operations of the proposed algorithm is ensured and operated to fetch the plain text from the cipher text.

III. CONCLUSION

Whenever the term safety comes in intellect and initiative, security is synonymous, but from time to time implementing security mechanism(s) like cryptographic techniques, biometric methods, genetic algorithm, quick response code mechanisms, etc. has not only been sturdy but cost constrained as well. The design, implementation and incorporation of the cryptographic algorithm are the core of the conferred security amid predicament at bay like malicious intrusions. The proposed algorithm ensures the secured transmission modus operandi and thereby diminution in access time. The formulation of the paper ensures deliberations as well as elucidation on how the security methodology could be implemented and incorporated, employing an innovative cryptographic modus operandi.

REFERENCES

[1] Chowdhury, R., Datta, S., Dasgupta, S., De, M., "Implementation of Central Dogma Based Cryptographic Algorithm in Data Warehouse for Performance Enhancement", International Journal of Advanced Computer Science and Applications, 6 (11), November, 2015, ISSN (Online)–2156 5570, ISSN (Print)–2158 107X, pp. 29–34
[2] Chowdhury, R., Dey, K., S., Datta, S., Shaw, S., "Design and Implementation of Proposed Drawer Model Based Data Warehouse Architecture Incorporating DNA Translation Cryptographic Algorithm for Security Enhancement", Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2014, Organized by Sri Jayachamarajendra College of Engineering, Mysore,

Proceedings in USB: CFP14AWQ-USB, ISBN–978-1-4799-6628-8, INSPEC Accession Number–14881472, Published and Archived in IEEE Digital Xplore, ISBN–978-1-4799-6629-5, pp. 55–60

[3] Chowdhury, R., Bose, R., Sengupta, N., De, M., "Logarithmic Formula Generated Seed Based Cryptographic Technique Using Proposed Alphanumeric Number System and Rubik Rotation Algorithm", Proceedings of IEEE 2012 International Conference on Communications, Devices and Intelligent Systems, CODIS 2012, Organized by Jadavpur University, Kolkata, Proceedings in CD: IEEE Catalog Number–CFP1207U-CDR, ISBN–978-1-4673-4698-6, Proceedings in Print: IEEE Catalog Number–CFP1207U-PRT, ISBN–978-1-4673-4697-9, INSPEC Accession Number–13285714, Published and Archived in IEEE Digital Xplore, ISBN–978-1-4673-4700-6, pp. 564–567

[4] Chowdhury, R., Ghosh, S., De, M., "String Graphixification Based Asymmetric Key Cryptographic Algorithm Using Proposed Concepts of GDC and S-Loop Matrix", Proceedings of IEEE/OSA/IAPR International Conference on Informatics, Electronics & Vision 2012, ICIEV 2012, Organized by University of Dhaka, Dhaka, Bangladesh, Proceedings in CD: IEEE Catalog Number–CFP1244S-CDR, ISBN–978-1-4673-1152-6, Proceedings in Print: IEEE Catalog Number–CFP1244S-PRT, ISBN–978-1-4673-1151-9, Conference Proceedings: ISSN–2226 2105, INSPEC Accession Number–13058551, Published and Archived in IEEE Digital Xplore, ISBN–978-1-4673-1153-3, pp. 1152–1157

[5] Chowdhury, R., Gupta, S., S., Saha, A., "Stochastic Seed Based Cryptographic Technique [SSCT] Using Dual Formula Key [DFK]", Proceedings of International Conference on Communication and Industrial Applications, ICCIA 2011, Science City, Kolkata, Proceedings in CD: IEEE Catalog Number–CFP1135R-CDR, ISBN–978-1-4577-1916-5, Proceedings in Print: IEEE Catalog Number–CFP1135R-PRT, ISBN–978-1-4577-1915-8, Published and Archived in IEEE Digital Xplore, ISBN–978-1-4577-1915-8, pp. 1–5

[6] Chowdhury, R., De, N., Ghosh, S., "Design and Implementation of RNS Model Based Steganographic Technique for Secured Transmission", International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2 (3), ISSN–22776451(P), ISSN–2277128X (O), pp. 132–136

[7] Chowdhury, R., Saha, A., Dutta, A., "Logarithmic Function Based Cryptosystem [LFC]", International Journal of Computer Information Systems, 2011, 2 (4), ISSN–22295208, pp. 70–76

[8] Chowdhury, R., Saha, A., Biswas, P., K., Dutta, A., "Matrix and Mutation Based Cryptosystem [MMC]", International Journal of Computer Science and Network Security, 2011, 11 (3), ISSN–17387906, pp. 7–14

[9] Kahate, A., "Cryptography and Network Security", Tata McGraw–Hill Education Pvt. Ltd., 2007, ISBN (10)–0-0706-4823-9, ISBN (13)–978-0-0706-4823-4

[10] Stallings, W., "Cryptography and Network Security Principles and Practices", Prentice Hall, 2005, ISBN (10)–0-1318-7316-4, ISBN (13)–978-0-1318-7316-2