International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 01 (January- February, 2018)

Design a Robust and Secure System for Encryption Using Mathematical Function for Wireless Network

Prashant Kumar Shukla
Department of Information Technology, SIRT, Bhopal
prashantshukla2005@gmail.com

Dr. Pradeep Chouksey
Technocrats Institute of Technology, Bhopal
dr.pradeep.chouksey@gmail.com

Dr. Harsh Kumar
Dr. K. N. Modi University, Nawai
drharshkumar@hotmail.com

Abstract: - *Encryption is the concept spread all over in today's scenario. In the smart computing and intelligence scenario information must be kept secret and only be shared with the trusted parties. Encryption techniques add delays increased the overhead of the smart computing devices. Concept of digital logic in computer system works faster than available different other schemes so it is made as better choice used for faster encryption minimizing the delay in network. Mathematical equations are the complex equations which makes encryption secure and complex than any other techniques. One attribute called aavalanche effect is used in encryption in which different cipher values are obtained using 2 different keys for the same plain text values. In this paper, an encryption scheme is proposed called robust and secure system for encryption (RSSE). In this technique a complex and secure mechanism of encryption is defined by mathematical equation using variant compliments with Gray code has been proposed, which uses the mathematical functions to generate a pseudo number which helps in generation of variants keys with which random and independent cipher text is obtained. By analysing the performance of this proposed scheme, it is found that the scheme provides more security of our data than other available methods and also key as well as algorithm is very strong for preventing different kinds of attack possibility.*

Keywords: - delay, cryptology, encryption technique, chaos function, cipher text.

1. INTRODUCTION

In the field of information technology, every second give rise to technological enhancements but on contrary it also hit alarm of ensuring threats for information security. The effective and best way to reduce the threat is to encrypt the information. Generally, the encryption techniques practiced traditionally includes substitution and transposition. In Substitution, the information is being exchanged with the symbols or information while on the other hand transposition provides the replacing of actual place of information into new designed position. But these mechanisms are not far enough to compete to current intruders attacks. Thus, Mathematical equations are the complex equations which makes encryption secure and complex than any other techniques. Mathematical equations are defined as the equation which uses the mathematical function which can be implemented as random number generator. Its solution is little complex but its produces highly range of random number which can be used in the proposed technique for the keys generation which then been applied for encryption and decryption. A novel crypto-numerical condition cryptography strategy using advanced legitimate implanted scheme is presented in this work for secure &quick encryption useful for data decoding for real-world applications. This proposed instrument gives a high-level of intervention and involution to oppose the direct and differential-assaults and furthermore improves security of system by giving befuddlement and dissemination to framework. These front systems have comprehended numerous scrapes of cryptography and upgraded security and execution; however these procedures have some real disadvantages. The subsisting calculations and strategies are not easily justifiable for clients since they utilize numerous numerical capacities. Encryption as well as decryption process have to do using a single-key in symmetric-key crypto-system. Only a single-key is used on both ends at sender side as well as receiver side. If once the key is trapped by anyone, the decoding can be easily done. The solution for the problem is asymmetric-key cryptosystem in which two different keys are used for coding and decoding. These keys are indistinguishably commensurate for coding and unscrambling at one-time however extraordinary-keys have to use for particular plain-text. More secure technique can be developed using numerous-keys also irregularity of these keys is upgraded the system using computerized ideas like 2's & 3's supplement. It is withal upgrades using Gray code. Regardless of the possibility that an interloper kens the keys utilized one time, at that point the keys are transmuted whenever for a similar plain-text. Complexity of the system can be enhanced using advanced ideas like xor-technique as opposed to strenuous scientific capacities.

2. RELATED WORK

For communication, most of the industries and companies depend upon different types of crypto-systems which utilize less memory as well as provide high security. Many methods are proposed to fulfill the needs of present demand. Mathematical methods are also used for encryption getting fast and secure transmission which is more secure as well as efficient with minimum memory utilization [11]. An electronic device is used for getting electrocardiogram (ECG) signals to develop ECG encryption system [15]. There is also a concept used for switching encryption keys among many keys to enhance the security using chaotic systems [8]. For multimedia applications, complex algorithms and key in large size is used to improve security and privacy [13]. For block encryption, a chaotic maps system is presented using pseudo-dynamic sequences generating uniform and independent time efficient and faster encryption [10]. Getting set of linear equations to reduce attack possibility in running time a new encryption is introduced [9]. Chaos theory based encryption technique is also suggested using constant value and some initial varying condition for ad-hoc network [6]. These different encryption systems provide better encryption with fast, secure and less memory utilized encryption.

3. PROPOSED METHODOLOGY

Mathematical equations are the complex equations which makes encryption secure and complex than any other techniques. A complex and secure mechanism of encryption is defined by mathematical equation using variant compliments with Gray code has been proposed, which uses the mathematical functions to generate a pseudo number with helps in generation of variants keys with which random and independent cipher text is obtained. Performing cryptanalysis test over proposed method depicts the security and strength of the algorithm as well as of keys. The defined technique is fast and secure which implies the generation of multiples keys for encryption or decryption process. But for a particular it is made clear that keys are similar for the encryption and decryption. Thus it conveys that various keys being generated for multiple encryptions for a single character which make it secure and complex for known cryptanalysis attacks. There is no proper condition for key generation so that all the characters of information with the multiple keys are encrypted with the variation in their key generation. Multiple keys make it complex but follow randomness which ensure security and also enhance that no similar character of information uses the similar key in encryption and decryption process.

Thus the generations of these keys are complex but random keys provide the fast and efficient encryption in the communication of information and no idea to intruder about its generation. The symbols used for key-generation technique, encryption and decryption are as follows:

Pi = Plaintext
Ci = Ciphertext
E (Pi) = Encryption of plaintext
D (Ci) = Decryption of ciphertext
Ki = key generation

For the generation of the key, and obtain this, a random generation number mathematical equation is been used:

For n = 0 to j:

$X_{n+1} = \{P\ (X_{n-1}) + A\ \{5 \sin (2X_n - 1) + 3 \tan^2 (X_n - 2)\} – Q\ (X_{n-2}) + B\ \{6 \cos (X_n)\}\}\ \text{MOD}\ 256$

Where A,P,B, Q are any integer (1,2,3,4,5,……), X_n = initial value where n = 0,1,2,…. j = number of keys to be generated.

3.1 Procedure of key generation

1. Generate the pseudo number by the random generator equation using on the both ends:
   For n = 0 to j
   $X_{n+1} = \{P\ (X_{n-1}) + A\ \{5 \sin (2X_n - 1) + 3 \tan^2 (X_n - 2)\} – Q\ (X_{n-2}) + B\ \{6 \cos (X_n)\}\}\ \text{MOD}\ 256$
2. The generated multiple keys obtained by firstly applied 2's complement and then 3's complement on various values of X_{n+1} and the keys is counted by giving the fixed number to variable j.
3. Security and complexity is increased by applying 2's and 3's complement on the X_{n+1} values generated so they obtained values are random and independent.
4. For more security enhancement the values is again put for Gray code process then obtain values are the keys generated and these keys are variant and random.
5. These keys changed into 8-bit bi-nary format.

3.2 Encryption Process

Firstly, convert each character into 8-bit binary form using their ASCII code with the decimal number. These are encrypted by using digital concept bit-wise XOR gate-logical function. The XOR is done over each letter by using the key generated. This process is encrypted for every character and keys are used for encryption of the whole information.

$$\text{Plaintext} \longrightarrow \text{ASCII} \longrightarrow \text{Binary code}$$

$$E(P).\ K = \text{Ciphertext}$$

And this process continues till all the characters are encrypted.

3.3 Decryption process

The decryption process is reversal of encryption process. In this, the ciphertext is XOR using the key same used during encryption and the plaintext is obtained

D(C). K = Plaintext

This process is repeated until we decrypt all the character of whole information.

3.4 Algorithms

(i) Key generation Algorithm

1. *Set the constant and parameters of the equation*
2. *Generate the pseudo number using the equation:*
   X_{n+1} = {P (X_{n-1}) + A {5 sin (2X_n - 1) + 3 tan^2 (X_n - 2)} – Q (X_{n-2}) + B {6 cos (X_n)}} MOD 256 for n = 0 to j
3. *Apply 2's and 3's complement.*
4. *Apply Gray's code process over the pseudo random number generated from X_{n+1} to generated key k_1, $k_{2\ldots}$ k_n.*
5. *Keys are converted into binary 8-bit form.*

(ii) Encryption process Algorithm:

1. *Convert each character of information using ASCII code and convert into binary form.*
2. *Encrypt the character using random key and then using XOR digital logic.*
3. *Then the process continues using random key with each character which is independent and does not relay on any other.*

(iii) Decryption process Algorithm:

1. *Obtain the cipher text and the key.*
2. *Decrypt the character using the random key used during encryption with the XOR digital logic.*
3. *Then the process continues, using this process each character is decrypted and plaintext is obtained.*
4. *Then the plaintext is given their ASCII code using the decimal value obtained.*

3.5 Example

Suppose the plaintext is: prashant

3.5.1 Key Generation

X_{n+1} = {P (X_{n-1}) + A {5 sin (2X_n - 1) + 3 tan^2 (X_n - 2)} – Q (X_{n-2}) + B {6 cos (X_n)}} MOD 256

Where

P = 92, Q = 37, X_0 = 23, X_{-1} = 47, X_{-2} = 35, A = 19, B = 21, j = 2

For j = 1

X_{0+1} = {92 (47) + 19 {5 sin (2 x 23 -1) + 3 tan^2 (23) - 2)} – 37 (35) + 21 {6 cos (23)}} MOD 256
X_{0+1} = {(4324) + 19 {5 sin (45) + 3 (0.424)^2 - 2)} – (1295) + 21 {6 x 0.92}}
X_{0+1} = {(4324) + 19 {(5 x 0.707) + (3 x 0.18- 2)} – (1295) + (21x 5.52)}
X_{0+1} = {(4324) + 19 {(3.53) + (- 1.45} – (1295) + (115.98)}
X_{0+1} = {(4324) + 19 {(2.08)} – (1295) + (115.98)}
X_{0+1} = {4324 + 39.52 – 1295 + 115.98}
X_{0+1} = {3184.5}
X_{0+1} = {Round of (3184.5)}
X_{0+1} = 3185 mod 256
X_1 = 113

For j = 2

X_{1+1} = {92 (23) + 19 {5 sin (2 x 113 -1) + 3 tan^2 (113) - 2)} – 37 (47) + 21 {6 cos (113)}} MOD 256
X_{1+1} = {(2116) + 19 {5 sin (225) + 3 (-2.35)^2 - 2)} – (1457) + 21 {6 x - 0.39}}
X_{1+1} = {(2116) + 19 {(-3.53) + (16.65 - 2)} – (1457) + 21 {- 2.34}}
X_{1+1} = {(2116) + (19x 11.12) – (1457) + (- 49.23)}
X_{1+1} = {(2116) + (211.28) – (1457) + (- 49.23)}
X_{1+1} = (822.44)
X_{1+1} = {Round of (822.44)}
X_{1+1} = {Round of (822.44)}
X_{1+1} = 822 MOD 256
X_2 = 54

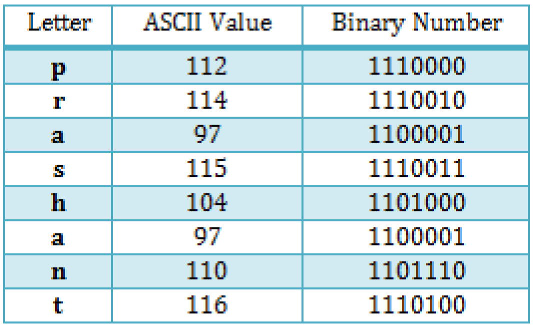
Now, we get the values of $X_1$and X_2that are 113 and 54 respectively. The keys can be generated by applying the 2's and 3's complement then also applying Gray's code process to generate keys k_1, k_2 ,….. k_n.

To obtained 2's and 3's complement of $X_1$and X_2,

X_1 = 113 = 01110001

1 -compliment 10001110
+ 1
2- compliment 10001111
+ 1
3- compliment 10010000

After getting 3's compliment of number, then applying Gray's code process to generate keys k_1, k_2 ,….. k_n.



Letter	ASCII Value	Binary Number
p	112	1110000
r	114	1110010
a	97	1100001
s	115	1110011
h	104	1101000
a	97	1100001
n	110	1101110
t	116	1110100

The keys are fixed by using gray code on random numbers $X_{n.}$ The gray code is generated by applying steps given below on X_n values. One example given below can make your conception clear on this type of conversion.3's compliment of X_1 = 10010000

$(10010000)_2$

(11011000) Gray Code

(11011000) Gray Code = $(216)_{10}$ in decimal number. This decimal number is our key for encryption and decryption of plain text to cipher text. Accordingly, we obtained 2's and 3's complement then gray code and their decimal number of all X_n values.

X_1= 113 = 01110001 gray code = 11011000 = 216

X_2 = 54 = 00110110 gray code = 10101110 = 174

Keys (K_1 = 216, K_2 = 174).

3.5.2 Encryption Process

Encryption process transforms the normal data which is easily readable by anyone into un-readable form with the help of multiple-keys. Here plain text is ***"prashant"***

Plain text metrics

p	r	a	s
h	a	n	t

ASCII value metrics

112	114	97	115
104	97	110	116

Key metrics

216	174	216	174
216	174	216	174

(i) p is part of plain text (ASCII - 112 it's Binary - 01110000)

Key (k1) = 216

Binary – 11011000

Plaintext	XOR	key	Ciphertext
p (112)		(k1)	
0	XOR	1	1
1	XOR	1	0
1	XOR	0	1
1	XOR	1	0
0	XOR	1	1
0	XOR	0	0
0	XOR	0	0
0	XOR	0	0

Cipher text = 10101000 = 168 = ¿

(ii) r is (114) *k2 = 174*
01110010 ***10101110 = 11011100 = 220 = Ü***

(iii) a (97) *k1 = 216*
01100001 ***11011000 = 10111001 = 185 = ¹***

(iv) s (115) *k2 (174)*
01110011 ***10101110 = 11011101 = 221 = ¦***

(v) h (104) *k1 (216)*
01101000 ***11011000 = 10110000 = 176 = °***

(vi) a (97) *k2 (174)*
01100001 ***10101110 = 11001111 = 207 = ¤***

(vii) n (110) *k1 (216)*
01101110 ***11011000 = 10110110 = 182 = Â***

(viii) t (116) *k2 (174)*
01110100 ***10101110 = 11011010 = 218 = Ú***

3.5.3 Decryption Algorithm

Decryption scheme converts the un-readable data in read-able data with the help of same keys.
Cipher text = {¿, Ü, ¹, ¦, °, ¤, Â, Ú}

(i) ¿ (168) *k1 (216)*
10101000 ***11011000 = 01110000 = 112 = p***

(ii) Ü (220) *k2 (174)*
11011100 ***10101110 = 01110010 = 114 = r***

(iii) ¹ (185) *k1 = 216*
10111001 ***11011000 = 01100001 = 97 = a***

(iv) ¦ (221) *k2 (174)*
11011101 ***10101110 = 01110011 = 115 = s***

(v) ° (176) *k1 (216)*
10110000 ***11011000 = 01101000 = 104 = h***

(vi) ¤ (207) *k2 (174)*
11001111 ***10101110 = 01100001 = 97 = a***

(Vii) Â (182) *k1 (216)*
10110110 ***11011000 = 01101110 = 110 = n***

(Viii) Ú (218) *k2 (174)*
11011010 ***10101110 = 01110100 = 116 = t***

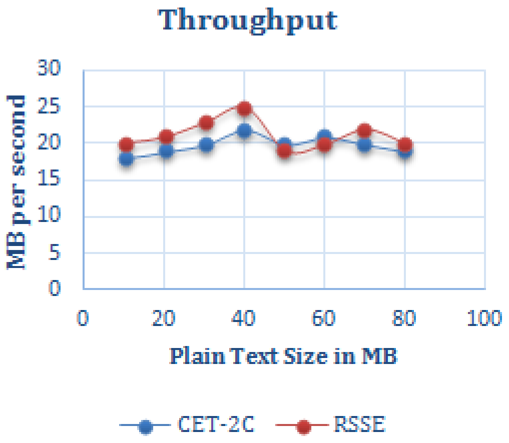
Plaintext = ***prashant***

4. RESULT COMPARISON OF RSSE WITH CET-2C

Result of RSSE technique has been observed and comparative analysis with CET-2C scheme is done using different parameters like throughput, encryption-time. These parameters are analyzed by varying plain text data-size ranging from 10mb to 80mb.

4.1 Throughput

Throughput is calculated as total no of plain-text data encrypted in particular time duration.



How much plain-text data is encrypted in 1 second is calculated in this work. Analysis has been done by giving different size of plain-text data ranging from 10mb to 80mb. Result shows as given in graph below that throughput is increases as the size of plain-text data is increases. Proposed RSSE algorithm is compared with one existing scheme CET-2C. Below given shows that how the performance is improved using RSSE scheme. Overall 6.97% average performance improvement is observed in throughput with comparison to CET-2C. The improvement of performance is indicated that throughput is increased in RSSE scheme than cet-2c. Performance improvement in proposed scheme is calculated using given below method.

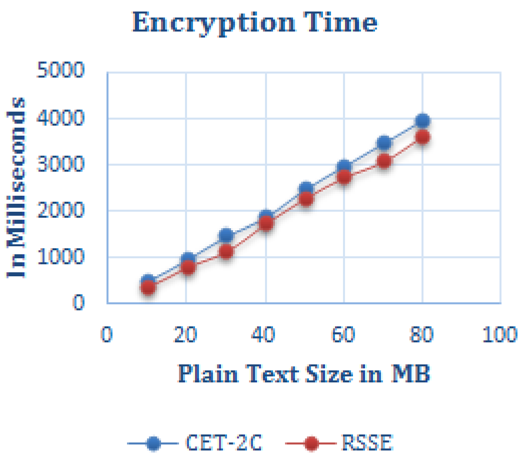
$$PI^{TP} = \frac{RSSE^{TP} - CET\text{-}2C^{TP}}{CET\text{-}2C^{TP}} \times 100$$

Here PI^{TP} is denoted performance improvement in throughput, CET-$2C^{TP}$ is referring to throughput of cet-2c, $RSSE^{TP}$ is referring to throughput of RSSE.

4.2 Encryption Time

Throughput			
Plain-text (in mb)	Time (in second)		Improve %
	CET-2C	RSSE	
10	18	20	11.11
20	19	21	10.53
30	20	23	15.00
40	22	25	13.64
50	20	19	-5.00
60	21	20	-4.76
70	20	22	10.00
80	19	20	5.26

Time complexity have to calculated using total time taken for encrypting plain-text data into cipher-text data. Encryption time is varying and depended on length of the key-size and size of the given plain-text data. Analysis has been done by giving different size of plain-text data ranging from 10mb to 80mb. Result shows as given in graph below that encryption time is increases as the size of plain-text data is increases. Proposed RSSE algorithm is compared with one existing scheme CET-2C. Below given table shows that how the performance is improved using RSSE scheme.



Overall 13.32% average performance improvement is observed in encryption time with comparison to CET-2C. The improvement of performance is indicated that encryption time taken by RSSE scheme is less than cet-2c. Performance improvement in proposed scheme is calculated using given below method.

$$PI^{TE} = \frac{CET\text{-}2C^{TE} - RSSE^{TE}}{CET\text{-}2C^{TE}} x\ 100$$

Here PI^{TE} is denoted performance improvement in encryption time, CET-$2C^{TE}$ is referring to encryption time of cet-2c, $RSSE^{TE}$ is referring to encryption time of RSSE.

Encryption Time			
Plain-text (in mb)	Time (in ms)		Improve %
	CET-2C	RSSE	
10	500	380	24.00
20	1000	830	17.00
30	1500	1170	22.00
40	1900	1760	7.37
50	2500	2300	8.00
60	3000	2760	8.00
70	3500	3100	11.43
80	4000	3650	8.75

5. CONCLUSION

Encryption is the concept spread all over in today's scenario. In the perspicacious computing and perspicacity scenario information must be kept secret and only be shared with the trusted parties. Encryption techniques integrate delays incremented the overhead of the astute computing contrivances. Digital logic circuits works more expeditious than any other techniques so as it can be utilized for more expeditious encryption minimizing the delays. Mathematical equations are the intricate equations which makes encryption secure and intricate than any other techniques. Avalanche effect is the property of encryption in which various keys engenders unique cipher-text of the information. In this, an intricate mechanism of encryption is defined by mathematical equation utilizing variant compliments with Gray code has been proposed, which utilizes the mathematical functions to engender a pseudo number with avails in generation of variants keys with which desultory and independent cipher text is obtained. Performing crypt-analysis of the method gives the security and vigor of the algorithm and keys.

REFERENCES

[1]. Akhshani, samsudin, akhvan, a novel parallel hash-function based on 3d chaotic- map.eurasip j. adv. signal pro.2013, 1-12.

[2]. Bhavani, rani, symmetric encryption using logistic-map. 1st inter-national conf. on recent avd. In IT, dhanbad-India, March 15-17 2012, pp.1-5.

[3]. Fang, Chen, zhao, Block-cipher design generalize single-algorithm on chaos. Tsinghua-sci-technol-2011, pp194-206.

[4]. Qing, wx yuan, block-encryption algorithm based dynamic-sequence of multiple- chaotic-systems. Comm. non-linear science number simulation 2009, pp574-581.

[5]. Rizvi, shukla and khare "an intelligent- fast chaotic-encryption using digital-logic- circuits for ad-hoc and ubiquitous comp.", entropy2016, pp201.

[6]. Assad-SE. Chaos-based Information-hiding &security. Proc. of 7th Inter-national conf. for Internet-tech. &secure trans., London, DEC 10-12, 2012, pp67-72.

[7]. Yayuz, ozkay-nak, Designing chaotic-s-boxe on time-delay-chaotic-sys. Non-linear-dyn-2013, 74, pp551-557.

[8]. Agrawal h, Agrawal b, Implement. Of AES & RSA using chaos-sys. Int. J. sci.-eng.-res.-2013, 4, pp1413-1417.

[9]. Wang, zang, tong, liu, and An Image encryption scheme based hyper-chaotic-rabino & exponent chaos maps. Entropy-2015, 17, pp181-196.

[10]. Beltran-r.-h. Low-comp-chaotic encrypt-sys. Rev.-mex.-fis.-2007, pp58-65.

[11]. bai-x, niu, liu, zhang, Research of hard-ware-encryption card-based on-chaos. Proc. of International conference on sensor network security-technology & priv. com-system-Taiwan, 2013, pp116-119.

[12]. Zaher A Digital-com. using novel-comb of chaotic-shift-key &doffing-cscillat. Int. J. innov-comp. control-2013, 9, pp1865-1879.

[13]. Chen, Lin, Wong, Simul. Arithmetic cod & encryption using chaotic-maps. Ieee-trans.-circuit-sys.-2010, 57, pp146-150.

[14]. Faragallah, nigm, mousa, rabaie, proc. Perf. On encrypt-data-base using rea algo. Int. J. netw.-secur-2012, 14, pp280-288.

[15]. Stalin, khare, shukla, rizvi, App. crypt. Using chaos-func.for fast digital-log. Based sys. In ubiquitous comp. Entropy-2015, 17, pp1387-1410.

[16]. Zambreno, pande, A chaotic encryption Scheme for realtime-embed.sys design & implementation Telecom system 2013, 52, pp551-561.

[17]. Shi, Z.; Bi, S.; Zhang, H.; Lu, R.; Shen, X. Improved auxiliary particle filter-based synchronization of chaotic Colpitts circuit and its application to secure communication. Wireless Communication Mobile Computing 2013, 1–15.