Enciphering using Elegant Pairing Functions and Logical Operators

B. Reddaiah, PhD
Assistant Professor
YSR Engineering College of
YOGI VEMANA UNIVERSITY
Proddatur, A.P, India

ABSTRACT

As technology started growing verbal exchange became a principal method of exchanging data. With the introduction of web and pay out programs protection problems are more difficult and elaborate. Secure correspondence is a remarkable worry by which individuals can communicate data to changing degrees of assurance that outsiders can't catch the data that is transmitted over system. Consequently data security is an essential thought in nowadays. Cryptography and data security is growing more to deal with authorized security for systems. In this work the proposed algorithm makes use of basic encryption methods like substitution, transposition, bitwise logical operations together with pairing operate to encrypt the information. The algorithm itself generates the important key from simple text and hides inside plaintext.

Keywords

Encryption, Decryption, Elegant pairing function, Symmetric Key

1. INTRODUCTION

For the last 20 years web is considered as essential and critical mechanism that presents communication to every single corner of the world. With this kind of facility provided by internet e-commerce is the field that is essentially picking up its significance. Due to this security turns-out to be very much important to handle. Electronic business field is expanding at a more noteworthy pace for which an extensive variety of secured applications are required. Recorded and investigative methodology of providing security is Cryptography. Cryptography has a long and attractive history [8] and has turned into a key segment of modem systems [10]. This cryptographic science that gives security is absolutely taking into account scientific and mathematical operations. This technique is being used from the past. Cryptography, the scientific approach of encoding and unscrambling message was utilized way back in around 1900 BC when a scribe in Egypt initially utilized a deduction of the standard hieroglyphics of the day to impart [3]. In past Julius Caesar additionally made and used cryptographic system to send military messages to his officers [2]. Cryptography is the science that conceals data from revealing to unofficial individuals. It is characterized as a strategy of changing over plain text into good for nothing data to keep the message safe [9]. This is made conceivable by building up a system that covers up message called as encryption. When this system is used on message it is extremely hard to get back the first type of message without utilizing decryption methodology [6]. This enciphering and deciphering is made possible with the support of key. Security of data relies on the enciphering and deciphering calculation and the value of mystery key utilized [4]. Key is one of the primary elements for cryptographic calculations that characterize the overall activity. As key acts as a main ingredient in giving security, there is every need to provide security for it. If the key is not known to unauthorized people it is hard to break security. In view of key cryptosystems are separated into two classes. The primary class is symmetric key also referred as secret key cryptography. Here same key is make use for both encryption and decryption and the secondary one is asymmetric key also referred as public key cryptography in which one key is used for encryption and another key is used for decryption.

In this work a new kind of symmetric cryptosystem is developed that uses Elegant paring function and common mathematical and logical operators to process and get the cipher text from plain text along with text hidden symmetric key.

2. FACTS IN DEVELOPING A SYSTEM

Using cryptography and developing crypto systems is very hard. The largest parts of crypto systems in the marketplace are lacking confidence. Among these a few are evidently imperfect. The others are more cleverly managed from its flaws. Every now and then people find out the flaws immediately, while in some cases it takes years together. At times it takes a decade prior to someone formulates new mathematics to crack the method. Defects that are hidden cannot be brought out all the way through by customary beta testing. It is evident that security has nothing to do with the functionalities. A cryptosystem can be functionally ordinary and from top to bottom lacking security. Defects stay behind as undiscovered until someone intentionally observes for the defects. Most significantly, a single defect cracks the security of the complete cryptosystem. If cryptography is seen as a sequence then the method is simply as secure as it’s weakest. With this it is compulsory to secure everything. While developing cryptosystems it is not sufficient to develop the algorithms and protocols work well but the performance also must be perfect. A good product with a weak algorithm is ineffective and a good standard algorithm, protocol and implementation can be removed by a damaged random generator. Under these situations the majority of balanced design choices are used as few relations as likely and as high a percentage of tough relations as likely. Since it is not practical for a system designer to develop a absolutely new system, an intelligent designer reuses the existing components that are normally understood to be secure and develops a new crypto system.

As described above every organization that tries to protect data has to develop strong and error free system. In this work new type of symmetric key and extraction of key is used. By keeping aside traditions function Elegant pairing function is used.

3. CRYPTOGRAPHY AS BACKDROP

Method of changing original text to unreadable form of text is known as encryption or enciphering and to get back the original text from scramble and unreadable from of text is called decryption or deciphering [1]. The output of each algorithm in providing security depends on how text is processed in encryption and decryption algorithms. There are two types of encryption techniques to process text. The first is the substitution technique by which each element of plain text like bit or letter or group of bits or letters are replaced with another letter(s) of unreadable text that will become difficult to read by others. The second is the transposition technique by which each element of plain text like bit or letter or group of bits or letters are reorganized in dissimilar way than plain text and it is also difficult to read and understand. Along with this a combined technique called product cipher can be used. It is by combining more than one technique. When these techniques are used on the original text the elementary constraint is that no information from the plain text is to be lost. The next constraint is that all the operations used should have reversible operations.

3.1 Classification of Cryptography

From the past many cryptographic algorithms are developed to provide security and they are separated in different ways. But the most common and widely followed classification is separating the algorithms on the type of key that is used for processing. The primary one is symmetric key algorithm where a single key is used for both encryption and decryption and the second one is asymmetric key algorithms that have two keys. One key is used for encryption and the other for decryption.

3.1.1 Symmetric key Cryptography

In this type of cryptography a single key is used. Sender and receiver share the similar secret key for both encryption and decryption [5].

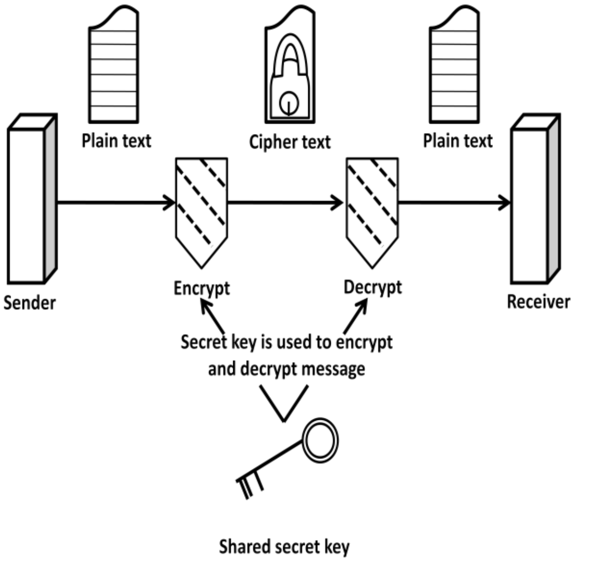

Fig 1: Symmetric key cryptography

3.1.2 Asymmetric key Cryptography

In asymmetric type of cryptography two keys are used for encryption and decryption. Here one key is called as public key and other is private key [5]. Among these keys public key the one that can be shared with everyone and the private key is non sharable key that will be present with only the owner of it.

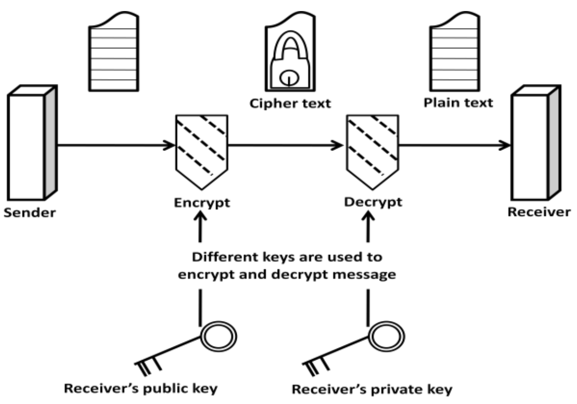

Fig 2: Asymmetric key cryptography

4. OUR SCHEME

According to Kirchhoff, the security of encryption system should depend on the secrecy of the key rather than encryption algorithm [7]. In general for symmetric and asymmetric cryptographic algorithms key must be recomputed before any data encryption or decryption [11]. Here in this method key is generated from message itself. As a part of operations bitwise Logical operation, shift operations binary conversions and decimal conversions are used. Elegant pairing function is used in encryption algorithm and un-pairing function is used in decryption algorithm.

The elegant pairing function for encryption is

$$\text{Elegant Pair[x, y]=}\begin{cases} y^2 + x & x \neq \max\ [x, y] \\ x^2 + x + y & x == \max\ [x, y] \end{cases}$$

Where x and y are non-negative integers, Elegant pair[x,y] outputs a single non-negative integer that is uniquely associated with that pair.

Example:

Case (i) - when x is maximum

Consider [x, y] = [18, 6,] we should take second function

$= x^2 + x + y$
$= (18)^2 + 18 + 6$
$= 343 = z$

Case (ii) - when x is minimum

Consider [x, y] = [8, 18], we should take first function

$= y^2 + x$
$= (18)^2 + 8$
$= 343 = z$

The Elegant un-pairing function for decryption is

$$\text{Z=}\begin{cases} \{z - [\sqrt{z}]^2,\ \left[\sqrt{z}\right]\} & z - [\sqrt{z}]^2 < [\sqrt{z}] \\ \{[\sqrt{z}],\ z - \left[\sqrt{z}\right]^2 - \left[\sqrt{z}\right]\} & z - [\sqrt{z}]^2 \geq \left[\sqrt{z}\right] \end{cases}$$

The inverse function elegant unpair [Z] outputs the pair associated with each non-negative integer Z
Example:
Consider z = 343; First we should find $\{z - [\sqrt{z}]^2$

$= 343 - (\sqrt{343})^2$
$= 343 - 324$
$= 19 > \sqrt{z}\ (18)$

So, we select second function $\{[\sqrt{z}],\ z - \left[\sqrt{z}\right]^2 - \left[\sqrt{z}\right]\}$

$= \{\sqrt{343}, 343 - (18)2 - (\sqrt{z})\}$
$= \{18, 343 - 342\}$
$= \{18, 1\}$

5. PROPOSED ALGORITHM

5.1 Encryption Algorithm

In this process plain text is converted to cipher text by using elegant pairing function and logical operators.

STEP1: Start
STEP2: Read the plain text.
STEP3: Divide the ASCII converted values of plain text with length of the plaintext to obtain remainders.
STEP4: Find the unique remainder values and select the highest value in it (R).
STEP5: Left shift plaintext characters by highest unique remainder.
STEP6: Covert the previous values to binary form.
STEP7: Convert the NOT operation result to decimal values.
STEP8: Perform left circular shift operation by R times.
STEP9: Convert the left circular shifted values to decimal values
STEP10: Divide the length of plain text to get the remainders and quotient values.
STEP11: Take the quotient value and perform XOR operation with the remainder value.
STEP12: Pair the XOR result with remainder value by using elegant pairing function to obtain integer value.
STEP13: Again divide length of plaintext to get the remainders and quotient values.
STEP14: Append these two values by taking Quotient values first followed by Remainder values.
STEP15: Stop

5.2 Representation of Encryption

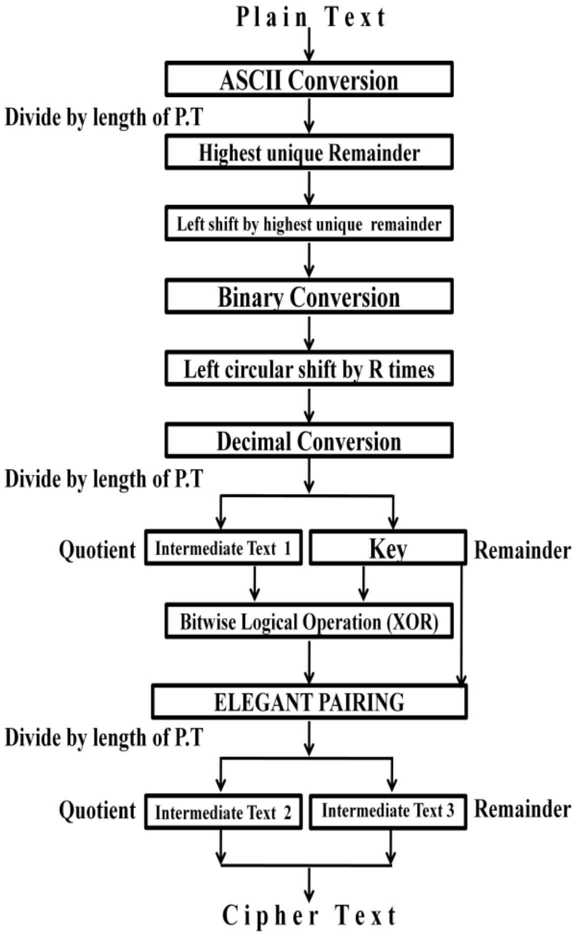

Fig 3: Block Diagram of Encryption Process

5.3 Decryption Algorithm

Plain text is retrieved from cipher text by using elegant un-pairing function and logical operators.
STEP1: Start
STEP2: Read the cipher text.
STEP3: Consider the length of cipher text and divide into two parts.
STEP4: Read the first part values as quotients and other part values as remainders.
STEP5: Multiply the quotient values with the length of first part and add second part with remainder value then combine to get a single integer value.
STEP6: De-pair the previous result using Un-Pairing function to get two integer values. The first part is taken as quotients and second as remainders.
STEP7: XOR the quotient values and remainder values.
STEP8: Multiply XOR result with length of first part and add remainders to length of second part to get a single integer value.
STEP9: Convert the output to decimal and then binary form.
STEP10: Perform right circular shift by R times
STEP11: convert the output to decimal values
STEP12: Get the unique remainders by dividing shifted values with length of plain text.
STEP13: Shift them by least unique remainders
STEP14: Convert them to ASCII values and then to characters to get Plain text.
STEP15: Stop

5.4 General Scheme of Decryption

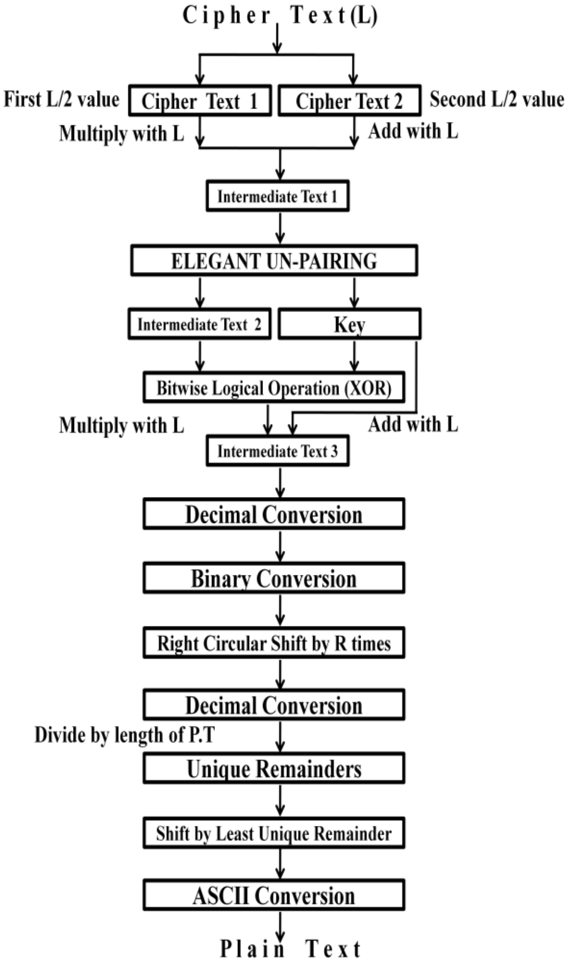

Fig 4: Block Diagram of Decryption Process

6. RESULTS

After processing encryption and decryption algorithms by using Elegant pairing and Un-pairing functions on word ‘LAKshmikanth’ the following are results shown in the Table 1, Table 2, Table 3 and Table 4.

6.1 Encryption

The encryption algorithm results for the above said example are tabulated in Table 1 and Table 2.

Table 1. Results of Encryption

Plain Text	ASCII values	Length of text (L)	Remainders (Text divide by L)	Unique remainders	Highest unique remainder (R)	Left rotate plain text by R times	Convert to Binary	Perform left circular shift by R times
L	76	12	4	4		65	01000001	00001010
A	65		5	5		75	01001011	01011010
K	75		3	3		115	01110011	10011011
s	115		7	7		104	01101000	01000011
h	104		8			109	01101101	01101011
m	109		1			105	01101001	01001011
i	105		9	9		107	01101011	01011011
k	107		11	11	11	97	01100001	00001011
a	97		1			110	01101110	01110011
n	110		2	2		116	01110100	10100011
t	116		8			104	01101000	01000011
h	104		8			76	01001100	01100010

Table 2. Results of Encryption carried on

Change to Decimal	Text 1 (Divide by L to get quotients)	Key (Divide by L to get remainders)	XOR (Text1, Key)	Elegant Pairing (XOR, Key)	Cipher text 1 (Divide by L to get quotients)	Cipher text 2 (Divide by L to get remainders)
10	1	0	1	2	1	0
90	7	6	1	37	3	1
155	12	11	7	128	10	8
67	5	7	2	51	4	3
107	8	11	3	124	10	4
139	11	7	12	163	13	7
155	12	11	7	128	10	8
11	1	0	1	2	1	0
115	9	7	14	217	18	1
163	13	7	10	117	9	7
67	5	7	2	51	4	3
98	8	2	10	112	9	4

Plain text ‘LAKshmikanth’ of size 12 characters is taken as input for encryption function and cipher text is generated as two parts namely cipher text 1 and cipher text 2. The final cipher text is 1 3 10 4 10 13 10 1 18 9 4 9 0 1 8 3 4 7 8 0 1 7 3 4 after combining cipher text 1 with cipher text 2.

6.2 Decryption

Cipher text 1 3 10 4 10 13 10 1 18 9 4 9 0 1 8 3 4 7 8 0 1 7 3 4 is given for the decryption function that uses Elegant un-paring function and logical operators to get back the original plain text. Cipher text is given as cipher text 1 and cipher text 2. The process is shown in the following Table 3 and Table 4.

Table 3. Decryption Processed Results

Length of cipher text (L)	First (L/2) values cipher text 1	Second (L/2) values cipher text 2	Intermediate text (L/2)* cipher text 1+cipher text 2)	Un-paring		XOR (Text 3, Key)	Intermediate text (L/2)* cipher text 3+key)
				Text 3	Key		
24	1	0	2	1	0	1	10
	3	1	37	1	6	7	90
	10	8	128	7	11	12	155
	4	3	51	2	7	5	67
	10	4	124	3	11	8	107
	13	7	163	12	7	11	139
	10	8	128	7	11	12	155
	1	0	2	1	0	1	11
	18	1	217	14	7	9	115
	9	7	117	10	7	13	163
	4	3	51	2	7	5	67
	9	4	112	10	2	8	98

Table 4. Decryption Processed Results Continued

Binary form	Right circular shift by R	Text 4 Convert to Decimal	Remainders of decimal (Divide by (L/2))	Unique remainders	Select least unique remainder	Rotate text 4 by least unique remainders	Plain text
00001010	01000001	65	5	5		76	L
01011010	01001011	75	3	3		65	A
10011011	01110011	115	7	7		75	K
01000011	01101000	104	8			115	s
01101011	01101101	109	1			104	h
01001011	01101001	105	9	9		109	m
01011011	01101011	107	11	11	2	105	i
00001011	01100001	97	1			107	k
01110011	01101110	110	2	2		97	a
10100011	01110100	116	8			110	n
01000011	01101000	104	8			116	t
01100010	01001100	76	4	4		104	h

Cipher text of length 24 (1 3 10 4 10 13 10 1 18 9 4 9 0 1 8 3 4 7 8 0 1 7 3 4) is given as input for decryption algorithm to get the plain text message and the derived plain text message is LAKshmikanth.

7. ADVANTAGES OF ALGORITHM

In this proposed work elegant pairing function is used which works like triple ordered function. This function can process large dimensional values. Along with this function simple logical operators are used. Here there is no need for separate key management technique as key is generated from the text itself. Because of this there are no transmission problems in key transmission.

8. CONCLUSION

The pairing function used in this work is elegant pairing function that is different from normal functions that are used in traditional algorithms. This provides more strength to the entire process. Symmetric key is used in this process that is generated from the text itself. So there is no need for separate key generation algorithm.

8.1 Future Scope

The strength of the pairing functions can be increased by improving the function to speed up the execution time. In this way the future study can be made.

9. REFERENCES

[1] B. Reddaiah, R Pradeep kumar Reddy, S. Hari Krishna "Enciphering using Bit–wise logical operators and paring function with text generated hidden key," IJCA (0975-8887), Vol. 121, No. 8, July 2015: pp. 30-35.

[2] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50

[3] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

[4] Behrouz A. Forouzan, Cryptography and Network Security, Special Indian Edition, TATA McGraw Hill.

[5] K. Gary, "An Overview of Cryptography", an article available at www.garykessler.net/library/crypto.html

[6] "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.html#Algorthms

[7] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better utilization" International Journal of Computer Trends and Technology-July to Aug Issue 2011.

[8] D. KHAN, "The Codebreakers", Macmillan Publishing Company, New York, 1967.

[9] P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[10] A. S. Tanenbaum, "Modern Operating Systems", Prentice Hall, 2003.

[11] Janan Ateya Mahdi, Design and Implementation of proposed B-R Encryption Algorithm, IJCCCE, VOL.9, NO.1, 2009.

10. AUTHOR'S PROFILE

Dr. B. Reddaiah received Ph.D. degree in Computer Science and Engineering in the faculty of Engineering in 2015 from Acharya Nagarjuna University, Andhra Pradesh. He is working as Assistant Professor, Department of computer Science and Engineering, YSR Engineering College of Yogi Vemana University, Proddatur, Andhra Pradesh. His current research is focused on Software Engineering, Cryptography and Network Security, Big-Data, Cloud Computing and Digital Image Processing. He has published papers both in National & International Journals.