Enciphering using Bit-Wise Logical Operators and Pairing Function with Text Generated Hidden Key

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

R. Pradeep Kumar Reddy
Assistant Professor
YSR Engineering College of
YOGI VEMANA UNIVERSITY
Proddatur, A.P, India

S. Hari Krishna
YSR Engineering College of
YOGI VEMANA UNIVERSITY
Proddatur, A.P, India

ABSTRACT
In present days electronic communication is a fundamental method of exchanging information. Secure communication is a major concern by which people can share information with varying degrees of certainty that third parties cannot capture the information that is transmitted over network. With the introduction of internet and distributed systems security issues are more challenging and complex. Hence information security is an important consideration in these days. Cryptography and information security is helping to develop more number of practical approaches to enforce security for networks. In this paper the proposed algorithm which uses basic encryption techniques like substitution, transposition, bitwise logical operations along with pairing function to encrypt the data. The algorithm itself generates the key from plain text and hides within plaintext.

Keywords
Encryption, Decryption, Pairing function, NOT, XOR

1. INTRODUCTION
From the past decade internet is considered as primary and important tool that provides communication to each and every corner of the world. With this e-commerce is the field that is significantly gaining its importance, because of which security becomes massively essential to handle. Electronic business field is increasing at a greater pace for which a wide range of secured applications are required. Historical and scientific approach of providing security is Cryptography. Cryptography has a long and fascinating history [7] and has become an essential component of modem operating systems [9]. This cryptographic science that provides security is purely based on mathematical operations. Historically for years passed by this technique is being used. Cryptography, the science of encrypting and decrypting message was used way back in around 1900 BC when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate [2]. In past Julius Caesar also created one of the earliest cryptographic systems to send military messages to his generals [1].

Cryptography is the science that hides information from disclosing to unauthorized people. It is defined as a technique of converting ordinary information into meaningless information to keep the message safe [8]. This is made possible by developing a procedure that hides message called as encryption. Once this procedure is applied on message it is very difficult to get back the original form of message without using decryption procedure [5]. This encryption and decryption is possible with the help of key. Security of information depends on the encryption-decryption algorithm and the strength of secret key used [3]. Key is one of the main ingredients for cryptographic algorithms that define the overall processing. As key plays a vital role in providing security, so that has to be protected. Unless the key is not known to other security mechanisms are difficult to break.

Based on key cryptographic algorithms are divided into two categories. The first category is symmetric key also called secret-key where a single key is used for both encryption and decryption and the second one is asymmetric key also called as public key in which one key is used for encryption and another key is used for decryption. In this paper a new type of symmetric algorithm is proposed that deals with a hidden key in the text with its own advantages.

2. PRINCIPLES OF CRYPTOGRAPHY
Secure mechanisms are used as a part of cryptographic techniques when sender (S) and receiver (R) are communicating over an unsecured channel. Cryptographic techniques are used to accomplish the subsequent targets.

Confidentiality is the primary task of security systems. It nothing but protecting the data transmitted from passive attacks. To remain data private and confidential security mechanisms are applied. Confidentiality is usually achieved by processing the plain text with encryption algorithm and encryption key that gives cipher text which is not in readable form. For reversing the action of security to get the original text at receiving end equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric cryptographic algorithms use the symmetric or same key for encryption and decryption, while asymmetric cryptographic algorithms use an asymmetric or public/private key pair [4].

Data integrity is the next that assurance on data received, whether it is accurately as sent by the sender without any modification, insertion, deletion, or replay in the network. Integrity is usually achieved by generating message authentication codes or hashes values at the sending end and compared at the receiving end to determine if the data was altered [4]. At the receiving end receiver conforms that data is not change in the middle of the network when the values are same and if the values are different they believes that some change has been occurred.

Authentication is the most important task. It is the procedure to ensure that the data is received from the authorized person or not. Receiver must be protected from unauthorized users sending data as if it is from the genuine users. So there should be a checking mechanism about the sender at the receiving

end. This is possible by digital certification which has digital signature of authorized users.

3. CRYPTOGRAPHY AS BACKDROP

The process of converting plaintext to cipher text is known as enciphering or encryption and the reverse process of converting plain text from cipher text is called deciphering or decryption. The overall process of providing security depending on how text is processed in encryption and decryption algorithms is termed differently.

Enciphering is the process of translating letters or symbols individually. Encoding is the process of translating entire words or phrases into other works or phrases. Encryption is the group term that covers encoding and enciphering.

Decryption is the reverse process of encryption algorithm with reverse operations for operations that are used in encryption algorithm.

As it is discussed in cryptographic algorithm, or cipher, mathematical functions are used for encryption/decryption. If the security of an algorithm is based on keeping it secret, it is nothing but a restricted cipher. Restricted ciphers are historically attractive but not sufficient today as the attackers are increasing in many dimensions. If they find the cipher text then everything is lost according to restricted cipher. Along with this problem in handling cipher text there is no capability to have quality control on the algorithm since it must be kept hidden..

Every proposed algorithm for encryption and decryption constitute mathematical operations that are used to transform the text from plain text to cipher text. As a part of transforming text from one form to other along with mathematical operations two basic general principles of cryptography are commonly used. They are called substitution and transposition which are usually used in every encryption and decryption algorithms.

Substitution is the process in which each element of plain text like bit or letter or group of bits or letters are mapped into another element(s) of unreadable text that cannot be easy to read by others.

Transposition is the process in which each element of plain text like bit or letter or group of bits or letters are rearranged in different order than plain text which is also not easy to read by others.

When these two techniques are applied on the plain the fundamental requirement is that no information of the original text is to be lost and all operations are to be reversible.

3.1 Types of Cryptography

Cryptography is a practice by which plaintext that is to be sent to receiver is scrambled which is referred as cipher text. This process is called as encryption. The reverse process of bringing back the pain text from scrambled form is called as decryption. This is performed at the receiving end. Many algorithms have been developed to provide security and they are classified in different ways. The most familiar type of classification is dividing the algorithms based on the type of key used. The first one is secret key cryptographic algorithms also known as symmetric key algorithms and the second type is public key cryptographic algorithms also known as asymmetric key algorithms.

3.1.1 Secret key Cryptography

In secret key algorithms a single key is used for both encryption as well as decryption. Sender uses encryption algorithm to process plain text along with key to get cipher text. Receiver uses decryption algorithm and same key used by sender to get back plain text from cipher text. As a single key is used for both encryption and decryption this cryptography is called secret key cryptography or symmetric key cryptography.

With this cryptography both sender and receiver should know secret key and the biggest threat lies from generating the key to distributing key between them.

3.1.2 *Secret key Cryptography*

In public key algorithms a pair of keys is used, one is called private key and other is public key. Private key is not shared with any one and the public key is sharable to all users. Security for private key is in the hands of owner of key. Any authorized user can get public key from directory service and can communicate securely.

With this cryptography third party certification problems on reliability of public key may arise and this key requires complicated mathematical operations that lead slow processing.

4. OUR SCHEME

The proposed algorithm uses the keys for encryption which are generated from the message itself and is not required to be defined by the user separately. According to Kirchhoff, the security of encryption system should depend on the secrecy of the encryption /decryption key rather than encryption algorithm [6]. In general for symmetric and asymmetric cryptographic algorithms key must be recomputed before any data encryption or decryption [10]. This relates to security issues for key management, time factor and economical issues to define the key for every session. In this proposed algorithm keys generation is totally dynamic based on various factors like length of text and remainders of plaint text, ASCII values divided by length of text. The output of the encryption is totally in the format of numbers and is in the double of the size of plain text. The pairing function is used in encryption. It is a process to uniquely encode two natural numbers into a single natural number. For encryption paring function is used and de-paring function is used in decryption algorithm.

The pairing function is

$$P(a,b)= ((a+b)^2+3a+b)/2 = N$$

The De-pairing function is

$$R = (\sqrt{8N + 1} - 1)/2;$$

where a - Text, b - Key, N - Integer value

$$a = N - (R*(R+1)/2);$$

$$b = ((R*(R+3))/2)-N;$$

As a part of Mathematical and Logical operations NOT and XOR bitwise Logical operations are used in this algorithm to create diffusion and confusion. Along with these binary conversions and decimal conversions are also used. In addition to these pairing function is used in encryption algorithm and de-pairing function is used in decryption algorithm.

5. PROPOSED ALGORITHM

5.1 Encryption Algorithm

The process of converting plaintext to cipher text is known as encryption.

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 : Take the first remainder value and compare with other values to find out repeated remainder values and note the second remainder position if any repeated.
STEP5: Left rotate plaintext characters with the distance of second repeated remainder position from the first remainder.
STEP6: Covert the previous values to binary form and perform NOT operation.
STEP7: Convert the NOT operation result to decimal values.
STEP8: By dividing with length of plaintext obtain the remainders and quotient values.
STEP9: Take the quotient value and perform XOR operation with the remainder value.
STEP10: Pair the XOR result with remainder value by using pairing function to obtain integer value.
STEP11: Again by dividing with length of plaintext obtain the remainders and quotient values.
STEP12: Append these two values in the way of Quotient values followed by Remainder values.
STEP13: Stop

5.2 General Schema of Encryption

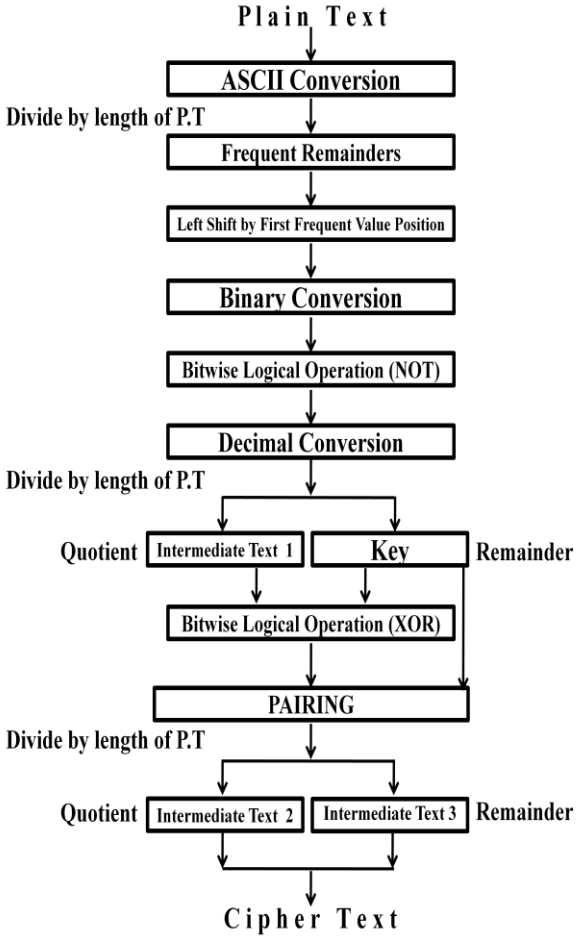

Fig 1: Block Diagram of Encryption Algorithm

5.3 Decryption Algorithm

Restoring the plaintext from the cipher text is known as decryption.

STEP1: Start
STEP2: Read the cipher text.
STEP3: Take the length of cipher text and divide into two halves.
STEP4: Read the first half values as quotients and other half values as remainders.
STEP5: Multiply the quotient with half of cipher text length and add remainder value to obtain a single integer value.
STEP6: De-pair the previous result using De-Pairing function to obtain two integer values which are considered as again quotients and remainders.
STEP7: Perform XOR operation between quotient values and remainder values.
STEP8: Again multiply XOR result with half length of cipher and add remainder value to obtain a single integer value.
STEP9: Convert the Step8 result binary form and perform NOT operation.
STEP10: Convert the NOT resultant to decimal value.
STEP11: Obtain the Remainders of the step10 result to find out the frequent remainders and note the positions of frequent remainders last position.
STEP12: Left rotate the array up to the last position times.
STEP13: Convert ASCII values to characters to get Plain text.
STEP14: Stop

5.4 General Scheme of Decryption

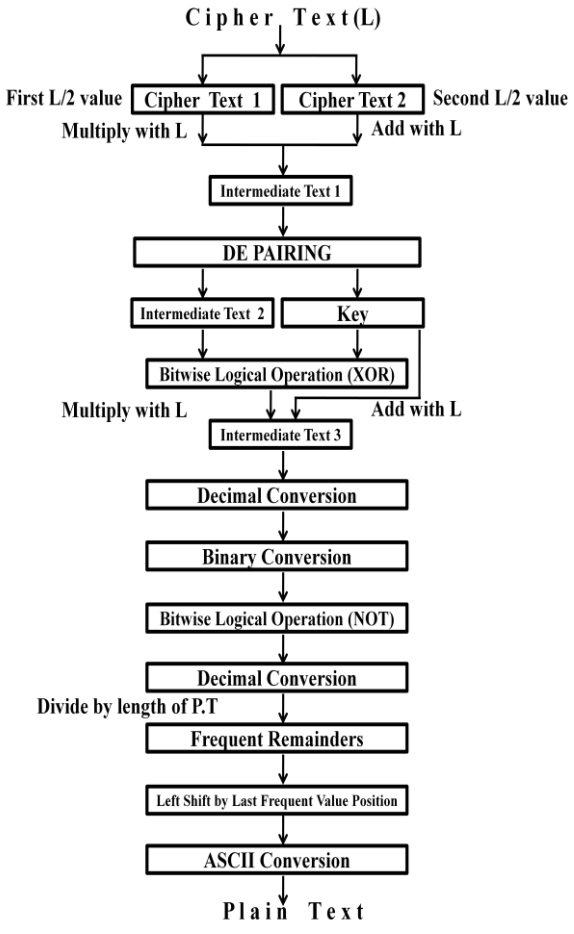

Fig 2: Block Diagram of Decryption Algorithm

6. RESULTS

Results of encryption and decryption algorithms are shown in the Table 1, Table 2, Table 3, Table 4.

6.1 Encryption

In this example the plaintext message considered for encryption algorithm is: - Security@15 and the processed results are tabulated in Table 1 and Table 2.

Table 1. Encryption Processed Results

Plain Text	ASCII values	Length of text (L)	Remainders (Text divide by L)	Frequent remainders compared with first remainder	Select the first repeated position (R)	Left rotate plain text by R times	Convert to Binary	Perform NOT operation
S	83	11	6	6		105	01101001	10010110
e	101		2			116	01110100	10001011
c	99		0			121	01111001	10000110
u	117		7			64	01000000	10111111
r	114		4			49	00110001	11001110
i	105		6	6	6	53	00110101	11001010
t	116		6	6		83	01010011	10101100
y	121		0			101	01100101	10011010
@	64		9			99	01100011	10011100
1	49		5			117	01110101	10001010
5	53		9			114	01110010	10001101

Table 2. Encryption Processed Results Continued

Convert to Decimal	Text 1 (Divide by L obtain quotients)	Key (Divide by L obtain remainders)	XOR (Text1, Key)	Pairing (XOR, Key)	Cipher text 1 (Divide by L obtain quotients)	Cipher text 2 (Divide by L obtain remainders)
150	13	7	10	160	14	6
139	12	7	11	178	16	2
134	12	2	14	138	12	6
191	17	4	21	329	29	10
206	18	8	26	603	54	9
202	18	4	22	355	32	3
172	15	7	8	127	11	6
154	14	0	14	105	9	6
156	14	2	12	107	9	8
138	12	6	10	142	12	10
141	12	9	5	114	10	4

A 11 character plain text (Security@15) is given to the encryption algorithm and cipher text obtained after combining first part of results named as cipher text 1 and second part of results named as cipher text 2 is 14 16 12 29 54 2 11 9 9 12 10 6 2 6 10 9 3 6 6 8 10 4. The values of cipher text 1 and cipher text 2 are shown in the last two columns of the table 2. Cipher text 1 is quotients obtained by dividing the output of paring function with L value and cipher text 2 is remainders obtained by dividing the output of pairing function with L value.

6.2 Decryption

In this example the cipher text message considered for decryption algorithm is: - 14 16 12 29 54 2 11 9 9 12 10 6 2 6 10 9 3 6 6 8 10 4 and the processed results of decryption algorithm are tabulated in 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)	De-paring		XOR (Text 4, Key)	Intermediate text (L/2)* cipher text 3+key)
				Text 3	Key		
22	14	6	160	10	7	13	150
	16	2	178	11	7	12	139
	12	6	138	14	2	12	134
	29	10	329	21	4	17	191
	54	9	603	26	8	18	206
	32	3	355	22	4	18	202
	11	6	127	8	7	15	172
	9	6	105	14	0	14	154
	9	8	107	12	2	14	156
	12	10	142	10	6	12	138
	10	4	114	5	9	12	141

Table 4. Decryption Processed Results Continued

Binary	Perform NOT	Text 4 Convert to Decimal	Remainders of decimal (Divide by (L/2))	Frequent remainder positions compared with first	Select last remainder position	Left rotate text 4 by selected position times	Plain text
10010110	01101001	105	6	6		83	S
10001011	01110100	116	6	6		101	e
10000110	01111001	121	0			99	c
10111111	01000000	64	9			117	u
11001110	00110001	49	5			114	r
11001010	00110101	53	9			105	i
10101100	01010011	83	6	6	6	116	t
10011010	01100101	101	2			121	y
10011100	01100011	99	0			64	@
10001010	01110101	117	7			49	1
10001101	01110010	114	4			53	5

A 22 valued cipher text (14 16 12 29 54 2 11 9 9 12 10 6 2 6 10 9 3 6 6 8 10 4) is given to decryption algorithm to get the plain text message and the derived message is Security@15

7. ADVANTAGES OF ALGORITHM

In this proposed algorithm there is no need of separate key management. This act is required and is very critical issue in symmetric key cryptosystems. This algorithm also uses symmetric key for both encryption and decryption and key is derived from text of the user and transmitted along with text to the other end. That is key is included in the cipher text and transmitted to receiver where the receiver get backs key in the process of decryption. While using this algorithm separate key will be derived when at least a single bit of plain text is changed. As key is not separately developed and transmitted there is no need to provide security for key with this algorithm. So, extra time is not consumed in developing key for each and every session. When this type of key is used economic burden in developing key and managing key also will be decreased.

8. CONCLUSION

The key generate through this algorithm is also symmetric key. There is no need of separate key generation algorithm required as key is generated from the plain text or cipher text by encryption or decryption algorithm. Pairing function used here is a distinct function that cannot be seen in general algorithms which is one of the strength of this proposed algorithm.

8.1 Future Scope

As a part of future study this algorithm may be extended to image encryption also. The size of the cipher text generate by encryption algorithm can be limited to the size of plain text.

9. REFERENCES

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

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

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

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

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

[6] 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.

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

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

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

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

10. AUTHOR 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 and Digital Image Processing. He has published papers both in National & International Journals.

R. Pradeep Kumar Reddy is a Research Scholar in Yogi Vemana University doing his Ph.D under the esteemed guidance of Dr C. Nagaraju. He is working as Assistant Professor, Department of Computer Science and Engineering, YSR Engineering College of Yogi Vemana University, Proddatur, Andhra Pradesh. He has completed M.Tech from SRM University. His current research is focused on Digital Image Processing, Cryptography and Network Security and Software Engineering. He published many papers and attended conferences.

S. Hari Krishna completed B. Tech from YSR Engineering college of Yogi Vemana University, Proddatur, Andhra Pradesh. His research is focused on Cryptography and Network Security. He published papers and attended many conferences.