ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 345-351

Enhanced Content Based Double Encryption Algorithm Using Symmetric Key Cryptography

MR. JUNESTARFIELD LYNGDOH KYNSHI* and DR. DEEPA V JOSE

Department of Computer Science, Christ University,Bangalore, India.
*Corresponding author E-mail: junestarfield.kynshi@cs.christuniversity.in

http://dx.doi.org/10.13005/ojcst/10.02.13

(Received: March 23, 2017; Accepted: March 29, 2017)

ABSTRACT

This paper aims to solve the problems of the existing technique of the content based double encryption algorithm using symmetric key cryptography. Simple binary addition, folding method and logical XOR operation are used to encrypt the content of a plaintext as well as the secret key. This algorithm helps to achieve the secure transfer of data through the network. It solved the problems of the existing algorithm and provides a better solution. The plaintext are encrypted using the above methods and produce a cipher text. The secret key is encrypted and shared through secure network and without knowing the secret key it is difficult to decipher the text. As per expected, enhanced encryption algorithm gives better result than the existing encryption algorithm.

Keywords: Cryptography, Symmetric key cryptography, Ciphered text, Public Key, Private Key, Circular bit Shifting, Encryption, Decryption.

INTRODUCTION

The term “Cryptography”, originated from the Greek word which means “Hidden Writing”. It plays an important role in data security. Every organization needs a secure transfer of confdential information over the network and cryptography provides a way to secure data communication with different cryptographic algorithms. Some algorithms which provide secure communication are like DES, AES SHA1 and MD5.

Cryptography is a technique to secure data from unauthorized access when they transmitted over the network[1]. Cryptography achieves the security goals—confidentiality, integrity, authenticity and non-repudiation through encryption and decryption[2]. Confidentiality means only authorized parties can understand the data. Integrity refers to the message that arrives is the same as the message that was originally sent. Authenticity means only authorized person can access the information. Non-repudiation means receiver actually received the message and sender actually sent it. Encryption is the process of changing the original text to a secret message using cryptographic algorithm [3]. Decryption is the process of converting cipher text back to the original plaintext[3].

The concept of cryptography is based on two terms- i.e. plaintext and cipher text[4]. The original message is called the plaintext and the encrypted version is called the cipher text[4]**.** Cryptography is broadly classified into two types- i.e. Symmetric key encryption and Asymmetric key encryption[4].

Symmetric key cryptography also known as secret key cryptography use a same private key for both encryption and decryption. The sender encrypted the message using the private key and receiver decrypted using the same key. Asymmetric key also known as public key cryptography uses two different key[5] i.e. public key and private key. The sender encrypted the message using a public key and receiver decrypt with a private key[5].

Problem Statement

- If two or more digits of random number are same, then after converted to binary number and left shift based on the number of 1 present, the two or more digits will always be same[6].
- If digit of a random number is 0, then after converted to a binary number and left shift based on the number of 1 present the digit will still be 0[6].
- Cipher text of space will always be same (like # is the cipher text for all spaces)[6].

PROPOSED WORK AND DISCUSSIONS

Encryption algorithm

1. Read the plain text from the user.
2. To encrypt the plaintext to 1st cipher text repeat the following procedure.

a. Count the length of each word.
b. Find the ASCII value of each letter.
c. Add each letter's ASCII value with the corresponding word length excluding spaces to generate the first encrypted text.

3. Take any random number from the user.
4. Repeat the following step to generate the cipher key.

a. Increment MSB by 1, next bit by 2 and so on
b. Take MSB of input number and generate its corresponding 8-bit binary number and count the number of 1 present in it.
c. Left circular shift the digit based on the number of 1 present in the binary number.
d. Store the shifted decimal value in an array.
e. Read the next bit and follow step 4 until LSB is being read.
f. Insert a negative number at the last of the array to identify the end of the array.

5. Repeat the following steps to generate the 2nd cipher text.

a. Add all digits of the input number.
b. If produced result is not a single digit, then repeat until a single digit formed.
i. Add all the digits of produced result.
c. Add the single digit value with each letter of the first encrypted text including spaces to generate the 2nd cipher text.

6. Do the following to generate a 3rd cipher text.

a. Form a group of four letters each from the 2nd cipher text.
b. Take an ASCII value of the first letter in each group and add all the digits.
c. If produced result is not a single digit, then repeat until a single digit formed.
i. Add all the digits of produced result
d. The produced result from each group are applied logical XOR operation with the corresponding ASCII value from each group except the first ASCII value from each group.

7. Send the cipher text, the cipher key and the negative number to the receiver.

Decryption algorithm

1. Read the shared negative number and cipher key
2. Do the following steps to generate a decryption key.

a. Repeat until a negative number is found.
i. Consider the first digit from cipher key and generate its corresponding 8bit binary number and count number of 1 present in the binary number.
ii. Right circular shift the digit based on the number of 1 present in the binary number.
iii. Decrement the first digit by 1, next digit by 2 and so on.
iv. Add the shifted decimal value with a key and store the result in a key.

b. If generated key is not a single digit, then repeat until a single digit formed.
i. Add all the digits of the key and store it in a key.

3. Do the following to generate the first decrypted text from cipher text.
a. Form a group of four letters each from the cipher text.
b. Take an ASCII value of the first letter in each group and add all the digits.
c. If produced result is not a single digit, then repeat until a single digit formed.
i. Add all the digits of produced result.
d. The produced result from each group are applied logical XOR operation with the corresponding ASCII value from each group except the first ASCII value from each group.
4. Do the following steps to generate the plaintext from the first cipher text.
a. Read the first decrypted text and generate the ASCII value of each letter.
b. Subtract the single digit key from the ASCII value of each letter including spaces to generate the second decrypted text.
c. Count the length of each word formed in the first decrypted text.
d. Generate the ASCII value of each letter of the first decrypted text and subtract the corresponding word length from it.
5. Plain text generated.

Illustration

The enhanced encryption and decryption algorithms are illustrated with an example below:

Encryption

Suppose "Hello! Bob encipher my file with ID: @303." is the input plain text from the sender. To obtain the secrecy between the sender and receiver, the plaintext is encrypted thrice. First, using a simple addition method, add each letter's ASCII value with the length of the corresponding word (excluding the spaces). Second, take a random number from the user and apply a folding method to produce the encryption key and add with corresponding ASCII value of first encrypted text. To obtain the encryption key, we do the following-

Let the random number 353 taken from the user.

- 1st round: 3+5+3=11
- 2nd round: 1+1=2

Encryption Key: 2

Third, form a group of four letters each and take an ASCII value of the first letter in each group and apply folding method. Each value of the folding method with the second encrypted ASCII value of the corresponding group are applied XOR operations excluding the first ASCII value from each group.

How the plain text is encoded using the encryption key is illustrated in Table 1.

Key Encryption

To generate the shared link, each digit of the random number is converted into a binary number. Increment the most significant bit by 1, next bit by 2 and so on. Rotate left each digit according to the number of 1 present in their corresponding binary number and stored the number in an array. The process of encrypting a random number into key is shown in Table 2.
Input No: 353

Resulting array is shown in Table 3 and 1st shared link in Table 4.
2nd shared link: -94

Sender sent the ciphered text "Pe||w+ Etj*gxnpyriz$qx'ioqh!}grf"IN8"A>197" and two shared link, one array that contains the digits of the taken input number which contains the key and another one is a negative number to specify the end of the array.*3.3.3 Decryption*

Receiver received the ciphertext "Pe||w+ Etj*gxnpyriz$qx'ioqh!}grf"IN8"A>197" with two shared link.

The receiver first fetches the negative number which indicates the end of the array and then fetch each digit from the array and decipher them to get the decryption key. The process of decrypt the ciphered number is shown in Table 5.

Decoded number: 353

Apply folding method to generate the decryption key-

- 1st round: 3+5+3=11
- 2nd round: 1+1=2

Table 1: How the plaintext are encrypted using simple addition with word length, addition with the encryption key and logical XOR operation

Plain text	word length	ASCII value	ASCII value added with word length	1st decrypted text	Added with encryption key	2nd decrypted text	After folding method	Apply folding method and XOR operations	cipher text
H		72	78	N	80	P	8	80	P
e		101	107	K	109	m		101	e
l	6	108	114	k	116	t		124	|
l		108	114	r	116	t		124	|
o		111	117	u	119	w	2	119	w
!		33	39	‘	41	)		43	+
		32	32		34	“		32	
B		66	69	E	71	G		69	E
o	3	111	114	r	116	t	8	116	t
b				e		b		106	j
		32	32		34	“		42	*
e		101	109	m	111	o		103	g
n		110	118	v	120	x	3	120	x
c		99	107	k	109	m		110	n
i	8	105	113	q	115	s		112	p
p		112	120	x	122	z		121	y
h		104	112	p	114	r	6	114	r
e		101	109	m	111	o		105	i
r		114	122	z	124	|		122	z
		32	32		34	“		36	$
m	2	109	111	o	113	q	5	113	q
y		121	123	{	125	}		120	x
		32	32		34	“		39	‘
f		102	106	j	108	l		105	i
i	4	105	109	m	111	o	3	111	o
l		108	112	p	113	r		114	q
e		101	105	i	107	k		104	h
		32	32		34	“		33	!
w		119	123	{	125	}	8	125	}
i		105	109	m	111	o		103	g
t	4	116	110	x	112	z		114	r
h		104	108	l	110	n		102	f
		32	32		34	“	7	34	“
I		73	76	L	78	N		73	I
D	3	68	71	G	73	I		78	N
:		58	61	=	63	?		56	8
		32	32		34	“	7	34	“
@		64	69	E	71	G		65	A
3		51	56	8	58	:		62	>
0	5	48	53	5	55	7		49	1
3		51	56	8	58	:	3	57	9
.		46	51	3	53	5		55	7

Table 2: How the encryption key is encrypted

Digit	After incrementing	Binary number	Number of 1 in binary number	Binary value after n bit left rotation	Decimal value after n bit left rotation
3	4	00000100	1	00001000	8
5	7	00000111	3	00111000	56
3	6	00000101	2	00010100	20

Table 4: 1st Shared link

8	56	20	-34

Table 3: Resulting array

8	56	20

Table 5: How the decryption key is decrypted

Decimal value after n bit left rotation	Binary number	Number of 1 in binary number	Binary number after n bit right rotation	Decoded digits	After decrementing
8	00001000	1	00000100	4	3
56	00111000	3	00000111	7	6
20	00010100	2	00000101	6	3

Decryption key: 2

Receiver takes a group of four letters each and find an ASCII value of the first letter in each group and apply folding method. Each value of the folding method with the encrypted text ASCII value of the corresponding group are applied XOR operations excluding the first ASCII value from each group.

The process of decoding the fetched ciphered text using the XOR operation and decryption key is illustrated in Table 6.

RESULTS

```
Enter text you want to encrypt:
Hello! Bob encipher my file with ID: @303.

Enter the Random number:
353
```

Fig. 1: plaintext and random number from user

```
The first Cipher text is:
Nkrru' Ere mvkqxpmz o{ jmpi {mxl LG= E8583

The second Cipher text is:
Pmttw)"Gtg"oxmszro|"q}"lork"}ozn"NI?"G:7:5'

The third cipher text is:
Pe||wt Etj*gxnpyriz$qx'ioqh!}grf"A>197
```

Fig. 2: Encrypted text

```
Enter text you want to decrypt:
Pe||wt Etj*gxnpyriz$qx'ioqh!}grf"A>197
```

Fig. 3: Ciphered text that need to encrypt

```
The first decrypted text is:
Pmttw)"Gtg"oxmszro|"q}"lork"}ozn"NI?"G:7:5

The second decrypted text is:
Nkkru' Ere mvkqxpmz o{ jmpi LG= E8583

The Plaintext is:
Hello! Bob encipher my file with ID: @303.
```

Fig. 4: Original plaintext

Table 6: How the cipher text are decrypted using logical XOR operation, subtraction with encryption key and subtraction with word length.

cipher text	ASCII value	After folding method	Apply folding method and XOR operations	1st decrypted text key	Subtract with encryption	2nd decrypted text	word length	Subtract with word length	Plain text
P	80	8	80	P	78	N		72	H
e	101		109	m	107	k		101	e
l	124		116	t	114	k	6	108	l
l	124		116	t	114	r		108	l
w	119	2	119	w	117	u		111	o
+	43		41	)	39	‘		33	!
	32		34	“	32			32	
E	69		71	G	69	E		66	B
t	116	8	116	t	114	r	3	111	o
j	106		98	b	96	`		93	b
*	42		34	“	32			32	
g	103		111	o	109	m		101	e
x	120	3	120	x	118	v		110	n
n	110		109	m	107	k		99	c
p	112		115	s	113	q	8	105	i
y	121		122	z	120	x		112	p
r	114	6	114	r	112	p		104	h
i	105		111	o	109	m		101	e
z	122		124	|	122	z		114	r
$	36		34	“	32			32	
q	113	5	113	q	111	o	2	109	m
x	120		125	}	123	{		121	y
‘	39		34	“	32			32	
i	105		108	l	106	j		102	f
o	111	3	111	o	109	m	4	105	i
q	114		113	r	112	p		108	l
h	104		107	k	105	i		101	e
!	33		34	“	32			32	
}	125	8	125	}	123	{		119	w
g	103		111	o	109	m		105	i
r	114		112	z	110	x	4	116	t
f	102		110	n	108	l		104	h
“	34	7	34	“	32			32	
I	73		78	N	76	L		73	I
N	78		73	I	71	G	3	68	D
8	56		63	?	61	=		58	:
“	34	7	34	“	32			32	
A	65		71	G	69	E		64	@
>	62		58	:	56	8		51	3
1	49		55	7	53	5	5	48	0
9	58	3	58	:	56	8		51	3
7	55		53	5	51	3		46	.

CONCLUSION

The enhanced algorithm provides the solution for the problems of the existing technique. It enhanced the existing algorithm by encrypting the plaintext thrice. It follows a simple technique to encrypt the plaintext, applying a binary addition operation and XOR operation on the content of the plain text. Incrementing each digit of random number, circular bit shifting operation and folding method are used to secure a shared link or a secret key. Without knowing the secret key, it is hard to decrypt the ciphered text.

REFERENCES

1. Stallings, W.: Cryptography and Network Security Principles and Practices, 4th edition, Prentice Hall, Pearson Education, 2009.
2. E Surya, C. Diviya. "A Survey on Symmetric Key Encryption Algorith". *International Journal of Computer Science & Communication Networks*, **2**(4), 475-477.
3. Behrouz A. Forouzan,. Cryptography & Network Security. Special Indian Edition, Tata McGraw-Hill,2007.
4. Chandra, S., Paira, S., Alam, Sk.S., Sanyal, G.: A comparative survey of symmetric and asymmetric key cryptography. In: IEEE International Conference on Electronics Communication and Computational Engineering (ICECCE 2014).
5. S.Chandra, S.Bhattacharyya, S.Paira, S.S.Alam, A study and analysis on symmetric cryptography. In: IEEE International Conference of Science Engineering and Management Research (ICSEMR), IEEE Xplore Digital Library, Print ISBN: 978-1-4799-7614-0 (2014).
6. Sourabh Chandra, Bidisha Mandal, Sk. Safikul Alam, Siddhartha Bhattacharyya, " Content based double encryption algorithm using Symmetric key cryptography", International Conference on Recent Trends in Computing, *Procedia Computer Science* **57**, 1228- 1234, (2015).