ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure Symmetric Key Algorithm [SSKA] For Information Exchange Using Modulo 67

Mr.H.Mohamed Ashik[*1], Mrs.S.Vydehi[2]

[*1]M.Phil Scholar, Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, India

[2]Professor, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, India

hmdashik@gmail.com

Abstract

The e-data usage is increasing day by day. Nowadays exchange of data over the internet is increased higher than before. Security is the main issue in communication over a network. Protection must be given against attackers. Solutions for network security comes with concepts like cryptography in which distribution of keys have been done. Cryptography plays a vital role in providing security. There are two types of cryptography mechanism: Symmetric and Asymmetric Key. Symmetric Key use single key for encryption and decryption whereas Asymmetric Key uses two keys one for encryption another for decryption. The most commonly used algorithm is Symmetric Key algorithms. The power or strength of these algorithms is based on the difficulty to break the original messages. In this paper, new modulo 67 Symmetric Key algorithm method is proposed Three keys are used in which one is a user entered key which is converted into ASCII and binary then first key is produced and second natural number is entered by user which is used to find the inverse of modulo 67. Third key is generated just like second key generation method. The proposed algorithm is used for Encryption and Decryption.

Keywords: Cryptography, Plain Text (PT), Cipher Text (CT), Key generation, Symmetric Key, Encryption & Decryption.

Introduction

Symmetric or secret key cryptography, a single or only one key is used for both encryption and decryption. Sender uses the key using some set of rules to encrypt the plaintext and sends the cipher text to the receiver. The receiver uses the same key or rule set to decrypt the message and recover the plaintext. secret key cryptography is also called symmetric key algorithm. The distribution of the key is biggest difficulty in this approach. Stream cipher or block cipher is the general category of Secret key cryptography algorithm. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

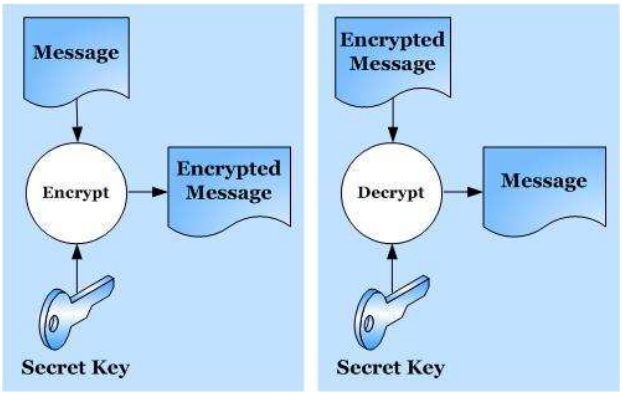

Figure 1. Encryption and Decryption

Encryption is the process of encoding plain text and converts it to non-readable format called cipher text. Decryption is the process of decoding cipher text converting it to plain text. There are two types of cryptography namely: Symmetric Key Cryptography and Asymmetric Key Cryptography. Same key is used both for encryption as well as decryption process in symmetric key cryptography. Whereas in asymmetric key cryptography separate keys are

ISSN: 2277-9655
Impact Factor: 1.852

used, one for encryption process and the other for decryption process.

Cryptography different goals:

- **Authentication:** The process of proving one's identity. It identify whether the person is authorized one to access the data.
- **Privacy/confidentiality:** Ensuring that authorized person only can read the message.
- **Integrity:** Received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message.

A. Types of cryptography

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again (known as decryption). The common types are Secret Key Cryptography which is also known as Symmetric Key Cryptography and Public Key Cryptography which is also known as Asymmetric Key Cryptography.

Secret Key Cryptography

In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver uses the same key to decrypt the message and recover the plaintext. Secret key cryptography schemes are generally categorized as being either *stream ciphers* or *block ciphers*. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher uses one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

Public Key Cryptography

Public or asymmetric key cryptography consist of two keys or of key pairs: one private key and one public key. One is used for encryption and the other for decryption.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Related Works

Encryption/Decryption has become a key component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based security. But now a day's hacking has become a common practice in society which made such cryptographic algorithms no longer safe. In this paper we have studied number of such symmetric key algorithms and selected one of them for reference in the proposed algorithm.

Dr.Saeed Q Y Al-Khalidi, Prakash Kuppuswamy, , proposed an algorithm based on Modulo37 in the year 2012.

- It Uses two keys: k1 and K2. K1 for positive number and k2 for negative number, find the inverse of selective number using modulo 37.
- The value is assigned for message A=1,B=2,….,Z=26,0=27,…,9=36,Space=37.
- For Encryption: Calculate the assigned value with modulo37 CT=(integer value*k1)mod37 , CT1=(CT*k2)mod37=Cipher Text.
- For Decryption: (CT1*k1'*k2')mod37,
- Alphabets and numbers have been used in this algorithm.

Dr.E.George Dharma PrakashRaj, JanailinWarjri proposed an algorithm based on Modulo69 in the year 2013.

- It Uses two keys : K2 is generated through user entered key length calculation using Modulo 69.
- K1 is natural number, inverse of natural number is calculated using modulo 69.
- Assigning synthetic value for message including special characters.
- A=1,B=2,….,Z=26,0=27,…,9=36,Space=37,!=38,…,~=69.
- For Encryption: Calculate with modulo69.
- C1=V1*K1 , C2=C1+K2, C2mod69=Cipher Text.
- For Decryption : P1= V2-K2, P2=P1*N1, P2mod69=Plaintext.
- In this algorithm alphabets and special characters used.

Vishwa gupta,Gajendra Singh ,Ravindra Gupta proposed Advance cryptography algorithm for improving data security in the year 2012.

ISSN: 2277-9655
Impact Factor: 1.852

- In this algorithm random number is used for generating initial key.
- Block based substitution is method is used.
- Use 512 bit key size to encrypt which is 64 bytes and divide it into 4 blocks of 16-bytes.
- For secure purpose XOR operation is applied between the blocks.
- Resultant key block applied XOR operation with plain text 16 bytes, Apply circular shift with 3 values and then perform XOR operation again.
- Consumes large amount of memory space .

Ayushi Proposed A Symmetric Key Cryptographic Algorithm in the year 2010.

- ASCII value is generated for the letter and generated corresponding binary value and reversing the binary.
- Takes 4 digit divisor which is less than 1000 and proposed two reverse operation for increasing security.
- No standard key generation method
- This method is suitable for small amount of data.
- Key size is small.

K.Govinda,E.Sathiyamoorth Proposed a Multilevel Cryptography Technique Using Graceful Codes in the year 2011.

- In this algorithm, White spaces are removed from the original string.
- Each character is mapped into ASCII value.
- The ASCII value is then encrypted into a set of random numbers using graceful code algorithm.
- The random numbers are then permuted.
- Decryption process is converting the permuted numbers to graceful code and then from graceful code to original numbers.

Jamal N. Bani Salameh Proposed A New Symmetric-Key Block Ciphering Algorithm in the year 2012.

- It encrypts a 64-bit (8 * 8) plaintext to a 64-bit(8 * 8) cipher text in eight rounds under the control of the key.
- The user key length and the number of rounds are variable.
- key mixing, S-boxes, Linear Transformation are applied in this algorithm.

Proposed Work

In this paper, we propose a new algorithm which follows the symmetric key mechanism. Symmetric key cryptography is an encryption system in which the sender and receiver of a message share a single, common key to encrypt and decrypt the message.

Here we proposed a new symmetric key algorithm and new key generation method. The proposed method is used for encryption and decryption process, using modulo67 and inverse modulo67. This algorithm is used for encryption and decryption, in which the same key is used both for encryption as well as decryption.

As we know that a message may consist of alphabets from A-Z, numbers from 0-9 and special characters such as +,-,%,< and so on. In this algorithm, firstly we assign integer values for each letters, digits and special characters. Alphabet 'A' is assign with integer value '1', B=2, C=3,…..so on till Z=26. Next we assign the integer value 1=27, 2=28,…so on till 9=36. Space=37, !=38, "=39,…so on as shown below. The second part is the key generation process. By using the proposed key generation method we generate the keys. K1 is generated by user entered key is converted into ascii value and then ascii value is converted into binary value then this original binary value is shifted 1 bit and produced new binary value then original binary value and new binary value is XOR ed, so we can get new shifted binary value then value is calculated and find key value using modulo67. K2 is an integer value taken from the user. The inverse of modulo67 of K2 is generated, K3 is generated like K2.

1. Integer Assigning

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
1	2	3	4	5	6	7	8	9
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
10	11	12	13	14	15	16	17	18
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**0**
19	20	21	22	23	24	25	26	27
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
28	29	30	31	32	33	34	35	36
space	**!**	**"**	**#**	**$**	**%**	**&**	**'**	**(**
37	38	39	40	41	42	43	44	45
)	*****	**+**	**,**	**-**	**.**	**/**	**:**	**;**
46	47	48	49	50	51	52	53	54
<	**=**	**>**	**?**	**@**	**[**	****	**]**	**^**
55	56	57	58	59	60	61	62	63
_	**`**	**{**	**|**	**}**	**~**			
64	65	66	67	68	69			

ISSN: 2277-9655
Impact Factor: 1.852

2. Key Generation

Here Three keys will be used K1,K2 and K3.Initially K1 is generated. The first key i.e. K1 is generated by user entered key is converted into ascii value and then ascii value is converted into binary value then this original binary value is shifted 1 bit and produced new binary value then original binary value and new binary value is XOR ed, so we can get new shifted binary value then the value is calculated with modulo67. Secondly select a natural number say, n1. Find the Inverse of the number using modulo67.say k1. Thirdly select a natural number say, n2. Find the Inverse of the number using modulo67.say k2.

3. Encryption Process

- First substitute or assign integer value for plain text.
- Multiply synthetic value with first random selected natural number.
- The first result value is multiplied with second random selected natural number.
- The second result value is Added with Key 1.
- Again third result value is calculate with modulo 67.

4. Decryption Process

- Subtract received cipher text value with key1.
- Secondly k3 value is multiplied with -1.
- First and second result is multiplied with k2.
- Multiplied result is calculate with modulo67.

Implementation

Symmetric encryption approach is used in our proposed encryption and decryption method. We already know symmetric key use single key for both encryption and decryption . here we have used there key values for higher security.

A. Key Generation Process

Let us suppose key enter by user is as follows

(I) Ex. Key = AG%2
A=65, G=71, %=37, 2=50
Original value =
01000001 01000111 00100101 00110010
After single bit shift =
10000010 10001110 01001010 01100100
After XOR operation =
11000011 11001001 01101111 01010110
Calculated value =593
Calculated value modulo67 = **57**
Key1 (or) K1 = 57.

(II) Select random integer no and find inverse of number.
Ex. Integer number = 4.So, N1=4.

Inverse of 4=17(verification 4*17 mod 67=1) so, **key2 (or) K2=17.**

(III) Select random integer no and find inverse of number.
Ex. Integer number = 9.So,N2=9.
Inverse of 9=15(verification 9*15 mod 67=1) so, **key3 (or) K3=15.**

B. Encryption Process

Let, Plain Text = NETWORKING. Each characters in the plain text is assign with integer values as discussed above. The encryption process is as shown in Table 2 using keys N1,N2 and K3.

Plain Text	PT value(PT1)	PT1* N1 (PT2)	PT2* N2 (PT3)	PT3+K 1 (PT4)	PT4 MO D 67 (CT)	**C T**
N	14	56	504	561	25	**Y**
E	5	20	180	237	36	**9**
T	20	80	720	777	40	**#**
W	23	92	828	885	14	**N**
O	15	60	540	597	61	****
R	18	72	648	705	35	**8**
K	11	44	396	453	51	**.**
I	9	36	324	381	46	**)**
N	14	56	504	561	25	**Y**
G	7	28	252	309	41	**$**
1	28	112	1008	1065	60	**[**
4	31	124	1116	1173	34	**7**

C. Decryption Process

After encrypted the plain text we received cipher text is " Y9#N\8.)Y$[` " and its equivalent synthetic value is "25,36,40,14,61,35,51,46,25,41,60,65" now we decrypt the cipher text using K1,K2 and K3. (ie, inverse of N1 & N2).

ISSN: 2277-9655
Impact Factor: 1.852

Cipher Text (CT)	CT Value(CT1)	K1-CT1 (CT 2)	K3*(-1) (CT 3)	K2*CT2*CT3 (CT4)	CT4MOD67 (PT)	P.T
Y	25	32	-15	-8160	14	N
9	36	21	-15	-5355	5	E
#	40	17	-15	-4335	20	T
N	14	43	-15	-10965	23	W
\	61	-4	-15	1020	15	O
8	35	22	-15	-5610	18	R
.	51	6	-15	-1530	11	K
)	46	11	-15	-2805	9	I
Y	25	32	-15	-8160	14	N
$	41	16	-15	-4080	7	G
[	60	-3	-15	765	28	1
7	34	23	-15	-5865	31	4

Conclusion

Secure Symmetric Key Algorithm is used to protect data from attackers. Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc., in this algorithm three keys are used to encrypt and decrypt the data. So, the data is more secure than other existing algorithm. Here we have used inverse modulo67 function and generated a key using the proposed key generation method. New symmetric algorithm is very authoritative and straight forward and more secure.

References

[1] *Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications, Volume1, 2010.*

[2] *Dinesh Goyal,Vishal Srivastava, "RDA Algorithm: Symmetric Key Algorithm" International Journal Of Information and Communication Technology Research , volume 2,April 2012.*

[3] *Dr.E.George Dharma Prakash Raj, Janailin Warjri,"KED- A Symmetric Key Algorithm for secured Information Exchange Using Modulo 69", I.J.Computer Network and Information Security, Volume 10 (37 - 43), August 2013.*

[4] *Majdi Al-qdah & Lin Yi Hui "Simple Encryption /Decryption Application", International Journal of Computer Science and Security, Volume-1, 2008.*

[5] *P. C. O. A.J Menezes, and S.A. Vanstone, "Handbook of Applied Cryptography": CRC Press, 1996.*

[6] *Prakash Kuppuswamy , Dr. Saeed Q Y Al-Khalidi, "Implementation Of Security Through Simple Symmetric Key Algorithm Based On Modulo 37", International Journal of Computers & Technology Volume 3, OCT 2012.*

[7] *S. William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999.*

[8] *Vishwagupta, Gajendra Singh,Ravindra Gupta, "Advance cryptography algorithm for improving data security", IJARCE Volume 2, Issue 1, January 2012.*

[9] *W. Stallings, Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009.*