IJCAT - International Journal of Computing and Technology, Volume 3, Issue 7, July 2016
ISSN : 2348 - 6090
www.IJCAT.org

An Improved Private Key Cryptography Based Algorithm Securing Text Data

[1] Sonawane Yogesh Kailas, [2] Vijay Kumar Verma

[1] M.Tech (CSE) IV Sem. Lord Krishna College of Technology
Indore M.P. India 453331

[2] Asst. Professor Computer Science & Engineering Department
Lord Krishna College of Technology
Indore M.P. India 453331

Abstract - Today communication and information sharing is very fast because of internet and smart phone. People are using mail massage, transaction information without paper works. Several important information like banking transactions, credit information, confidential data is transferred using internet. We need to prevent our data from unauthorized access. We need to convert our data in a non-readable format. Sender converts that data in non-readable form and again at receiver end receiver convert the non-readable data into readable form. The art and science of creating no readable data or cipher so that only intended person is only able to read the data is called Cryptography. In this paper we propose an improved private key based encryption techniques which convert data in no readable form. Decryption is reverse of encryption proposed approach. Plaintext is the intended original message.

Keywords **- Cryptography, Plaintext, Cipher Text, Private Key, Public Key.**

1. Introduction

There are several different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. The main purposes of Cryptography are

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non- repudiation: Non-repudiation does not allow theSender of a message to refute the claim of not sending the message.

Access Control: Access Control specifies and controls who can access what.

Availability: The principle of availability states that resources should be available to authorized parties all the times.

2. Literature Review

In 2011 Vinod Shokeen, Niranjan Yadav proposed "Encryption and Decryption Technique for Message Communication". They Proposed a fast and secure encryption algorithm using substitution mapping, translation and transposing operations. The proposed symmetric encryption technique has two advantages over traditional schemes. First, the encryption and decryption procedures are much simpler, and consequently, much faster. Second, the security level is higher due to the inherent poly-alphabetic nature of the substitution mapping method used here, together with the translation and transposition operations performed in the algorithm.

In 2011 B. Ravi Kumar, Dr. P.R.K. Murti proposed "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS)"Bit Shifting and Stuffing (BSS) represent only seven bits per its ASCII value. In computer system to represent a printable character it requires one byte, i.e. 8 bits. So a printable character occupies 7 bits and the last

bit value is 0 which is not useful for the character. In BSS method we are stuffing a new bit in the place of unused bit which is shifting from another printable character. So in this BSS methodology after encryption, for every eight bytes of plain text it will generate seven bytes cipher text and in decryption, for every seven bytes of cipher text it will reproduce eight bytes of plaintext.

In 2012 Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveena, proposed" Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers". They discussed types of cryptography and different keys in cryptography. They give brief description about symmetric key algorithms and we are proposing new algorithm in symmetric key cryptography. They proposed algorithm which contains two levels of Exclusive OR (XOR) operation. Proposed algorithm is useful in transmission of messages and data between one user and another.

In 2012 Monika Agrawal & Pradeep Mishra proposed "Comparative Survey on Symmetric Key Encryption Techniques". They present a detailed study of most of the symmetric encryption techniques with their advantages and limitations over each other.

In 2013 Krishna Kumar Pandey & Vikas Rangari proposed "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security "Proposed work used enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. The proposed algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. This algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender

In 2013 Obaida Mohammad & Awad Al-Hazaimeh proposed "A New Approach for Complex Encrypting and Decrypting Data". They enhanced security goals by using maintains of the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

In2014 Ezeofor C. J.& Ulasi A. G proposed "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" They presents analysis of network data encryption and decryption techniques used in communication systems. Visual Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block sizes were captured and plotted against total time response taken during data encryption using Microsoft Excel.

In 2014 Satyajeet R. Shinge& Rahul Patil proposed "An Encryption Algorithm Based on ASCII Value of Data". They presented a symmetric cryptographic algorithm for data encryption and decryption based on ASCIIvalues of characters in the plaintext. The proposed algorithm encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data.

In 2014 Mitali & Vijay Kumar proposed "A Survey on Various Cryptography Techniques" This represented a fair performance comparison between the various cryptography algorithms on different settings of data packets. They analyze the encryption and decryption time of various algorithms on different settings of data.

In 2015SuchitaTayde&SeemaSiledar proposed "File Encryption, Decryption Using AES Algorithm in Android". They used Advanced Encryption Standard and implemented on various platforms especially in small devices like mobile phone. Proposed application allows user to run application on android platform to encrypt the file before it is transmitted over the network. It is used for all type of file encryption such as text, docx, pdf and image encryption.

3. Proposed Method

3.1. Encryption Process

We assign a code to alphabets A=1, B=2, C=3D=4,……...Z=26.
Consider a same text NETWORKS. Now the length of original string ETWORK is counted, which is 8. Now the length of original string NETWORKS is counted, which is 8.

Since 8 is even number, the Key is generated using (n/2) i.e. 8/2=4 or else the key generated should be (n+1)/2).
Now the key i.e. letter at position 4 isW and key chosen will be wordcorresponding numeric value i.e. k=23 (consider A=1, B=2… Z=26)

Table 1 First step of encryption process

Original text	***Add key in numeric value and abstract from 26***	***Corresponding text***
N	11	K
E	2	B
T	17	Q
W	20	T
O	12	L
R	15	O
K	8	H
S	16	P

After round 1 of encryption, we get KBQTLOHP. Apply transposition i.e. Rail Fence Cipher Text = KQLHBTOP

Table 2 Second step of encryption process

Original text	*Use ASCII value convert into Binary and reverse it and replace with decimal*	*ASCII Equivalent in Character*
K	180	-|
Q	174	«
L	179	|
H	183	Π
B	189	¥
T	171	½
O	168	¿
P	175	»

So finally the cipher text is -|«|Π¥½¿»

3.2 Decryption Process

Received cipher text is -|«|Π¥½¿»

Table 3 First step of decryption process

ASCII Equivalent in Character	*Replace ASCII value & logical not of binary and replace by ASCII*	*Equal character*
-|	75	K
«	81	Q
|	76	L
Π	72	H
¥	66	B
½	84	T
¿	79	O
»	80	P

Text Obtained – KQLHBTOP. Apply Reverse Transposition as Text Obtained: - KBQTLOHP
Key used in Encryption, k=23

Table 4 Second step of decryption process

Chipper text	*Subtract key with Numeric Value D & subtract from26*	*Corresponding Alphabet*
K	14	N
B	5	E
Q	20	T
T	23	W
L	15	O
O	18	R
H	11	K
P	19	S

4. Proposed Algorithm

Step 1: Find the length of the word by using number of character.
Step 2: Use n/2 for even length word, use a numeric value by considering A=1, B=2 …Z=26. Find key (K) according to the value of n2/ from neumeric value
Step 3: If the length is odd use (n+1)/2 andFind key (K) according to the value of (n+1)/2 from numeric value
Step 4: Add key into numeric value by using formula D= (NV+K). Now subtract with 26 from this value and replace with corresponding text.
Step 5: Convert this value into binary format and apply logical NOT.
Step 6: Generator Decimal number and replace with corresponding character.
Step 7: Final got chipper text.

5. Graphs and Analysis

We evaluate the performance of proposed algorithm and compare it with symmetric algorithm. The experiments were performed on i3 processor (2.5GHz Intel Processor with 4M cache memory), 2GB main memory and 400 GB secondary memory , and running on Windows 7. The algorithms are implemented in using C# Dot net frame work version 10.

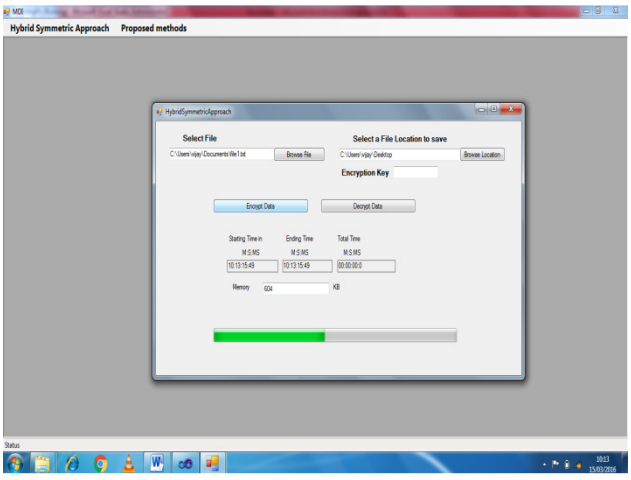

Figure 1 Execution time and file size

We compare the proposed algorithm with symmetric key algorithms by using file size and execution time for encryption table 5 shows file size and execution time for both algorithms for encryption.

Table 5 File size and execution time

File Size in KB	*Symmetric algorithm*	*Proposed method*
50	1438	1282
100	2426	1686
200	3242	2668

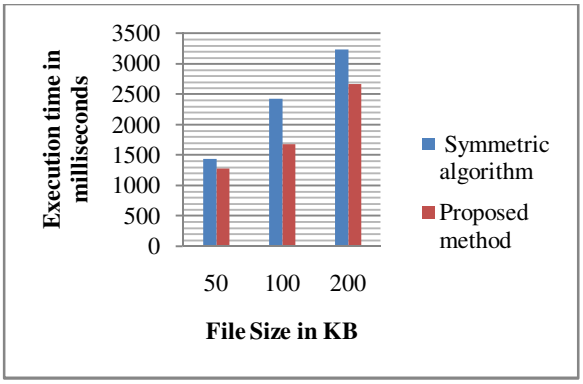

Figure 2 Comparison graphs with execution time and file size

6. Conclusion

We proposed an efficient encryption based approach for encryption of text data. In the proposed approach we automatically generate key form the text. By comparing with symmetric approach using different parameter like data base size execution time and the memory required for encryption and decryption it is clear that the proposed approach perform well as compared to the symmetric approach.

References

[1] Vinod Shokeen, Niranjan Yadav "Encryption and Decryption Technique for Message Communication" International Journal of Electronics & Communication Technology IJECT Vol. 2, Issue 2, June 2011 ISSN: 2230-7109

[2] B. Ravi Kumar & Dr.P.R.K.Murti "Data Encryption and Decryption processUsing Bit Shifting and Stuffing (BSS)Methodology"International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 7 July 2011

[3] Ch. Santhosh Reddy & Ch. Sowjanya, "Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153

[4] Monika Agrawal & Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques "International Journal on Computer Science and Engineering (IJCSE).ISSN: 0975-3397 Vol. 4 No. 05 May 2012

[5] Krishna Kumar Pandey & Vikas Rangari "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security" International Journal of Computer Applications (0975 – 8887) Volume 74– No. 20, July 2013

[6] Obaida Mohammad Awad Al-Hazaimeh "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013

[7] Ezeofor C. J. &Ulasi A. G. "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology Vol. 3, Issue 12, December 2014

[8] Satyajeet R. Shinge & Rahul Patil "An Encryption Algorithm Based on ASCII Value of Data" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234

[9] Mitali&Vijay Kumar "A Survey on Various Cryptography Techniques" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Volume 3, Issue 4, July-August 2014 ISSN 2278-6856

[10] Suchita Tayde & Seema Siledar "File Encryption, Decryption Using AES Algorithm in Android Phone" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 5, May 2015 ISSN: 2277 128X