Volume 3, Issue 6, June 2018

ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

Data Encryption and Decryption Process Using Private Key Cryptography

Amarkant Goud
M Tech(CSE) 4th Sem.
Lord Krishna College of Technology
Indore M. P. India

Vijay Kumar Verma
Assistant Professor Dept. C.S.E.
Lord Krishna College of Technology
Indore M. P. India

***Abstract*: Internet & smart phone makes easy to access and share data from any here in the world. Every day terabytes of data are being generated and used. Several important real life applications like banking transactions, credit information, and confidential data is transferred using internet. Security mechanism like password or encoding data is common tools. Cryptography is best solution for security .Cryptography means encoding message in non-readable format it is called encryption and convert message in to non-readable to readable format called decryption. In this paper we proposed an new and efficient approach which generate the key form the text itself .We use ACSII code with binary conversion and logical not. Proposed approach provides stronger encryption as compared to previous approaches.**

Keywords: redundant, attribute, discovery, dependency, Integrity, constraints, normalization

I. INTRODUCTION

Symmetric cryptography is usually implemented by the use of one-way functions. In mathematic terms, these are functions that are easy to compute in one direction but very difficult to compute in reverse. This is what allows you to publish your public key, which is derived from your private key. It is very difficult to work backwards and determine the private key. A common one-way function used today is factoring large prime numbers. It is easy to multiply two prime numbers together and get a product. However, to determine which of the many possibilities are the two factors of the product is one of the great mathematical problems. If anyone were to invent a method for easily deducing factors of large prime numbers, it could make obsolete much of the public key encryption used today. Fortunately, other one-way functions work for this application, such as calculations on elliptical curves or computation of inverse logarithms over a finite field. Cryptography plays an integral part in data security. Cryptography provides confidentiality and maintains integrity between genuine users. Cryptography used mathematical techniques for security aspects such as confidentiality, data integrity, entity authentication, and data authentication. A cryptographic algorithm works using combination of key to encrypts the plaintext. The security of encrypted data is entirely dependent on the strength of the cryptographic algorithm and the secrecy of the key

TERMINOLOGY

• Plain Text: The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.
• Cipher Text : The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced.
Encryption : A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
• Decryption: A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non- readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
• Key : A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

II. LITERATURE REVIEW

There are a lot of algorithms have been proposed by various researcher to enhance cryptography techniques. There are always some factors that have been considered for future improvement of the existing algorithm. In our literature review we study some of recently developed methods

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 2014 Ezeofor C. J. & Ulasi A. G proposed "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" They present 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 2015 Zaeniah, Bambang Eka Purnama proposed "An Analysis of Encryption and encryption Application by using One Time Pad Algorithm ".Security of data in a computer is needed to protect critical data and information from other parties. One way to protect data is to apply the science of cryptography to perform data encryption. There is wide variety of algorithms used for encryption of data; this study used a one-time pad algorithm for encrypting data. Algorithm One Time Pad uses the same key in the encryption process and a decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. Therefore, analysis will be done for an application that implements a one-time pad algorithm for encrypting data. The application that implements the one time pad algorithm can help users to store data securely.

In 2016 A. Joseph Amalraj1 et al proposed " A Survey Paper On Cryptography Techniques"
They show that to improve security and efficiency, most email system adopt Public Key Infrastructure (PKI) as the mechanism to implement security, but public key infrastructure based systems suffer from expensive certificate management and problems in scalability. The main objective of this approach is awareness of email security and its requirements to the common computer users. A number of cryptographic techniques are developed for achieving secure communication. They proposed mailing system which provides standard security model.

In 2017 Rafael Alvarez et al proposed "Algorithms for Lightweight Key Exchange ". They show that some secure protocols, especially those that enable forward secrecy; make a much heavier use of public-key cryptography, increasing the demand for lightweight cryptosystems that can be implemented in low powered or mobile devices. These performance requirements are even more significant in critical infrastructure and emergency scenarios where peer-to-peer networks are deployed for increased availability and resiliency. They showed that several public-key key-exchange algorithms, determining those that are better for the requirements of critical infrastructure and emergency applications and propose a security framework based on these algorithms and study its application to decentralized node or sensor networks.

III. PROBLEM STATEMENT

The main problem of the cryptography algorithms are
1. Key size: - Key size is a major problem for encryption and decryption of text data. There are no criteria to decide the size of the key. Strong key make encryption strong. If the size of the key is large than the encryption and decryption process makes slow.
2. Number of Key: - Some of the algorithm used more than one key for encryption. There are no criteria to use any number of key. More number of keys create complexity and difficult to share because single key can be easily share.
3. Selection of key:-Generally key is a numeric value which is decided by the user .Key is shared between sender and receiver. How to decide a key for encryption is also a problem. Selection of key is mostly based on algorithm are techniques used for encryption and decryption.
4. Arithmetic complexity:- Arithmetic complexity is measure in term of calculation or mathematical operation used for encryption and decryption . Complex calculation takes more time to encrypt the text. So reduce complex calculation is also a difficult problem.
6. Execution time:-Any algorithm which takes time to encrypt the text into cipher text is known as execution time. The execution time is depends on the operation used in the algorithm. Reducing execution time is also a difficult problem.

OBJECTIVES

1. **Reducing Key Size**: - Key size is a major problem for in encrypting and decrypting. Each and every algorithm objective is to reduce key length but key should be effective and work efficiently for text data.
2. **Automatic Generation of Key: -** Symmetric key based algorithm used common key shared by sender and receiver. These key are decided by the sender and same key is used by receiver in our proposed work shared key is generated automatically based on the length of the text.
3. **Reducing Arithmetic Complexity: -** our objective is to reduce avoid or minimize arithmetic calculation by replacing with simple calculations. In our proposed method we use simple ASCCI code and binary number form for encrypting and simple one division.

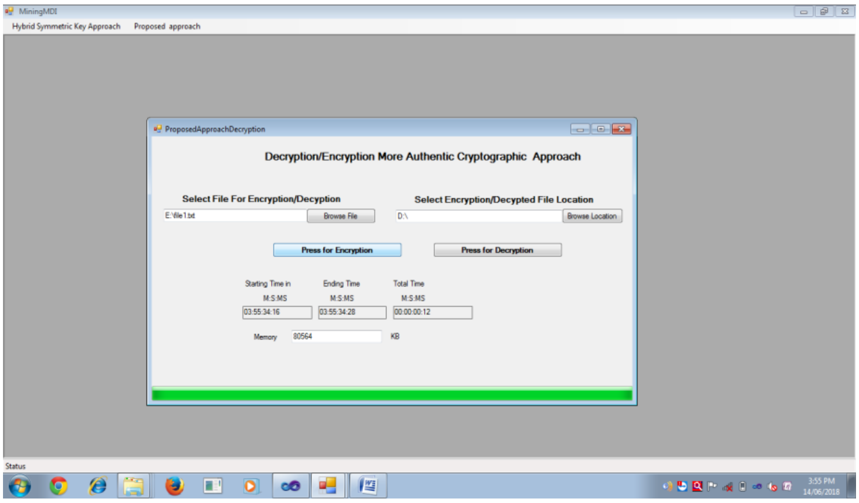
4. **Reducing Memory and Execution Time: -** Each algorithm needs memory to perform calculation and storing temporary data, algorithm need time to perform calculation complex calculation needs more CPU time .Our objective to reduce memory and execution time.
5. **Minimizing Number of keys: -** Each algorithm needs key to encrypt text into non readable form. Number of key is also a critical issue because more number of keys create complexity during encryption and decryption process. Some algorithm used more number of key some required less number of key. Our objective is to use minimum number of key and make strong encryption.

IV. PROPOSOSED APPROACH

Step1: Read the input text.
Step2: Now add the key in front of the text.
Step3: Find ASCII code of each text and convert into binary data.
Step5: Find out One's complement of the previous binary data.
Step6: Convert binary data and obtain the Decimal value from it.
Step7: Decimal value is now divided by 4 and finds equivalent ASCII code of the result divide and put it as one character with reminder.
Step9: Now merge the result with the remainder to got cipher text.
Step10: Finally got the cipher Return encrypted text.

IMPLEMENTATION ENVIRONMENT

we evaluate the performance of proposed algorithm and compare it with symmetric key cryptography. 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 . We take simple text file from a selected location. User a create text file anywhere in computer memory. When encryption process is completed a file with encrypted text is generated and saved at a location given by the user. For the decryption process user select an encrypted file from the location file and repeat the same process



Decryption/Encryption More Authentic Cryptographic Approach

Select File For Encryption/Decyption: E:\file1.txt

Select Encryption/Decypted File Location: D:\

Starting Time in M:S:MS: 03:55:34:16

Ending Time M:S:MS: 03:55:34:28

Total Time M:S:MS: 00:00:00:12

Memory: 80564 KB

Figure 1. Implementations

V. RESULT AND ANALYSIS

Comparison on the basis of key size

Table 1 Number of keys

Name of Algorithm	Key Size(bits)
Symmetric Approach	32
Proposed Approach	8

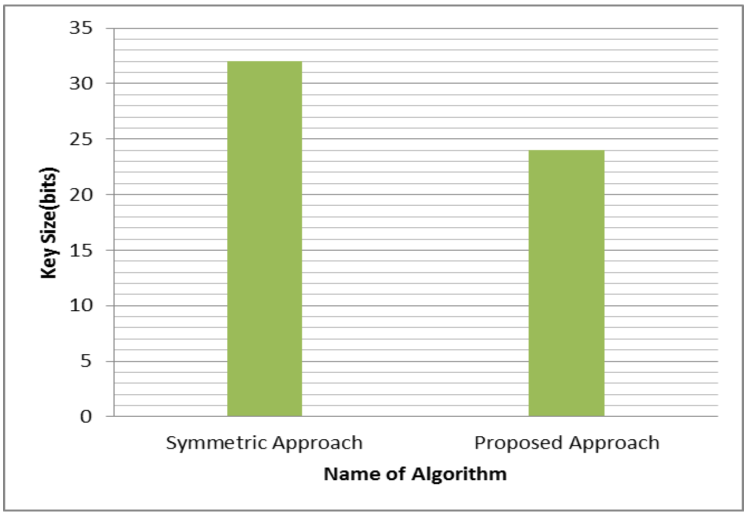


Figure 2. Comparison on the basis of key size

CONCUSION

All previous approach is used select to encrypt and decrypt the text data. We implemented proposed approach and symmetric approach and compare using different parameter like data base size execution time and the memory required for encryption and decryption. From the analysis it is clear that the proposed approach perform well as compared to the symmetric approach

REFERENCE

1. Mansoor Ebrahim & Shujaat Khan Symmetric Algorithm Survey: A Comparative Analysis International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.
2. Deepak Nagde, Raviraj Patel & Dharmendra Kelde "New Approach for Data Encryption using Two Way Crossover". International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 58 – 60.
3. 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 (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014.
4. 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.
5. Mitali, Vijay Kumar & Arvind Sharma "A Survey on Various Cryptography Techniques". International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 3, Issue 4, July-August 2014
6. Surabhi Shah & Megha Singh A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique Volume 4, Issue 9, September 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com.
7. Ashwini R. Tonde & , Akshay P. Dhande "Review Paper On FPGA Based Implementation Of Advanced Encryption Standard (AES) Algorithm "International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.
8. Prakash G L1 ,Dr. Manish Prateek2 and Dr. Inder Singh Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud SystemInternational Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014.
9. Suchita Tayde & Seema Siledar "File Encryption, Decryption Using AES Algorithm in Android Phone". Volume 5, Issue 5, May 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.
10. Kurapati Sundar Teja, Shanmukha Mallikarjuna Bandaru & Kurapati Pavan "Data Encryption and Decryption Algorithm Using Hamming Code and Arithmetic Operations". Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 5, Issue 8 August 2015.
11. Zaeniah & Bambang Eka Purnama An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, 2015.
12. A. Joseph Amalraj and Dr. J. John Raybin Jose " A Survey Paper On Cryptography Techniques" A. Joseph Amalraj et al, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016, pg. 55-59 © 2016, IJCSMC All Rights Reserved 55 Available Online at www.ijcsmc.com.
13. Rafael Alvarez and Cándido Caballero "Algorithms for Lightweight Key Exchange" 10th International Conference on Ubiquitous Computing and Ambient Intelligence, UCAmI 2017, San Bartolomé de Tirajana, Spain, 29 November–2 December 2017