iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: VIII Month of publication: August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8089

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Enhanced Key Protection in Private Key Cryptography

Ashish Agarwal[1], Amit Kumar Gupta[2]

Abstract: The adventurous ventures of technology have proved to be the reason(s) to consistently work in the orientation that lands you in the new domain acquiring its foundation in the existing frameworks. Scientists have always been proposing modifications or working on new proposals, thus creating possibilities to endeavour in thinking out of the box in order to gain the essence of ground breaking technologies. The critique by the scholars available on the information giants accessible via internet displays the zeal around the globe, which unifies the nations. The emergence of social networking sites such as social networking websites and the ease of engagements by accepting the digital means though connect above boundaries, at the same time demands infallible safety assurance to maintain the foundational motto of such medium. We, here propose a way of safeguarding the key that wraps the information communicated using symmetric key.

Index Terms: Cryptography, Key, Private Key, Public key, Asymmetric cryptography, Symmetric Cryptography, Linked list

I. INTRODUCTION

It has been one of the undisputed requirements that user(s) do expect the transmission of information with no change in its order of reference[1]. This prompted us to make our effort by considering a data structure called doubly linked list. After going through the research paper(s) on this domain, we would consider 2^n factor by securing the key. As can be referred, 2^n, a proposed modification in the asymmetric algorithm i.e., R.S.A. algorithm can render the enhanced security measures.

We can describe our attempt to strengthen the security of the key chronologically as follows[2][3]:-

A. Suppose information say, D is to be transferred to the other end.
B. Now, a private key say, K which is nothing but a variable that will encrypt the information, D i.e., K->D
C. As already in practice, we can use asymmetric algorithm (we have considered R.S.A. algorithm)
D. In this manuscript, we apply the 2^n factor to the key.
E. We can display it as: 2^n|D|K
F. Here, n is the median length of the information, D calculated using a mathematical function called ceil function.

Thus, we can assemble number of node in this manner each encrypted with 2^n factor. This, on the receiver's end will be unfolded in the reverse manner.

II. PICTORIAL REPRESENTATION

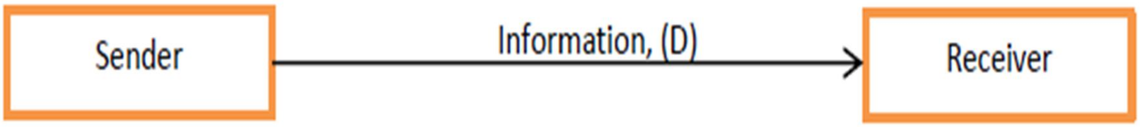


Fig:1- Scenario: Sender wants to send some data to the receiver.

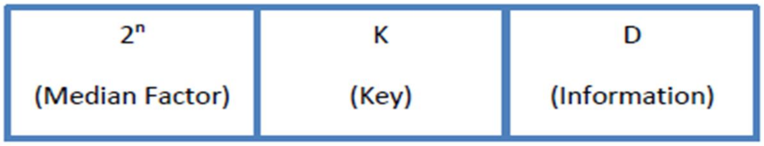


Fig:2- Key: Linked list key

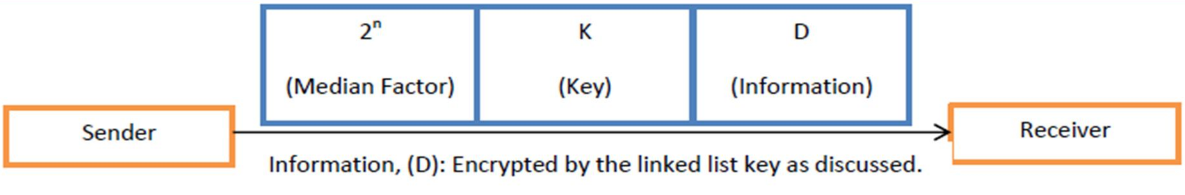

2^n
(Median Factor)
K
(Key)
D
(Information)
Sender
Receiver
Information, (D): Encrypted by the linked list key as discussed.

Fig:3- Proposed Scenario

III. CONCLUSION

Communication via digital means is one the easiest ways to carry out profitable jobs provided underlying framework is robust enough to nullify the unethical attempts of suspected and unauthorised accesses[4]. It is beyond doubt that merger of the pillars of cryptography into one generates the system with double enhancements in its characteristics. We have already displayed in our previous works, the feasibility of 2^n, in the asymmetric cryptosystem, which in turn guards the key in private cryptosystem[2][5]. It is this journey of our efforts, which instigated us to look for the compatibility of such modification(s) in the data structures used in the underlying frameworks. We could easily maintain the flow of information in the secure communication channel. Despite preventive steps and inclusive nature of conceptual background, flaws may creep in which lays the path for maintenance in disguise of challenge(s).

IV. FUTURE WORK

As already mentioned, any new technology, proposal, idea or modification does carry with itself a room for enhancements. It is very much applicable with our proposal too, in which we tend to increment its degree of inclusiveness with the magnitude of data that is expected to be exchanged. We, anyhow tend to look out ways that would overcome the expected compatibility issue(s) or suspected complexity related challenge(s). Our aim is to focus in widening the working domain of our proposed usage of a data structure that in no way violates the features of doubly linked lists. With our consistent efforts towards creating a balance between communication channels and underlying framework, we also look for possibility(s) for the merger of other data structure(s)[6]. Thus attempting to maintain the essence of authenticated communication and authorised reciprocation, technology(s) always have an open upper end.

REFERENCES

[1] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Protection of Key in Private Key Cryptography” paper published in “International Journal of Advanced Research”, Volume 5, Issue 2, Feb 2017.

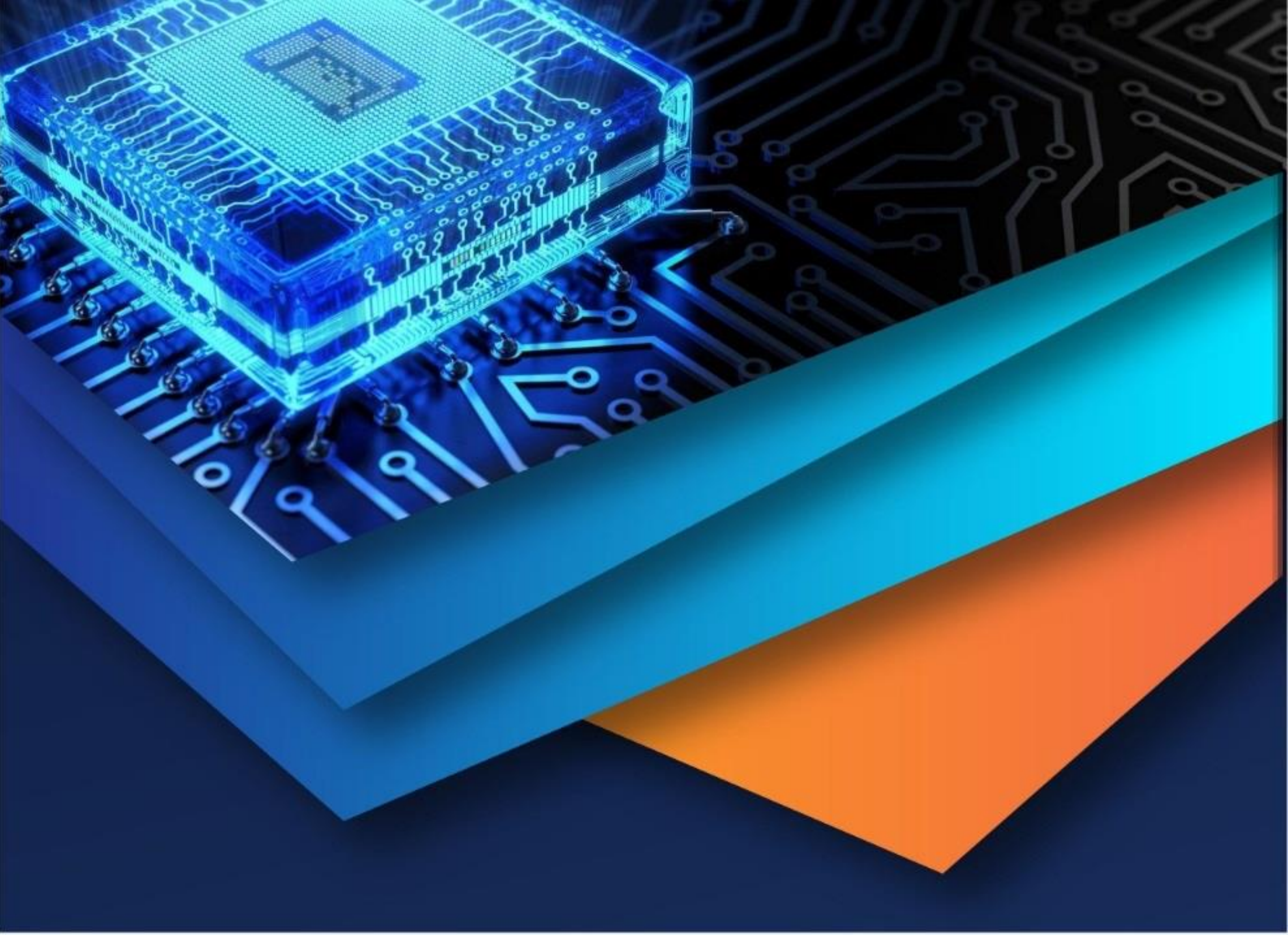
[2] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Algorithm for Protection of Key in Private Key Cryptography” paper published in “International Journal of Engineering Research in Computer Science and Engineering”, Volume 4, Issue 3, Mar 2017.

[3] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Function Codes for Protection of Key in Private Key Cryptography” paper published in “Journal of Emerging Trends and Innovative Research”, Volume 6, Issue 3, Jun 2017.

[4] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Hybrid Key Cryptography: A Tool for Security” paper published in “International Journal of Innovative Research in Science, Engineering and Technology”, Volume 6, Issue 3, Mar 2017.

[5] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Methods for Protection of Key in Private Key Cryptography” paper published in “International Journal of Innovative Research in Computer Science & Technology”, Volume 5, Issue 2, Mar 2017.

[6] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, “Information Security: A Saga of Security Measures” paper published in “International Journal Of Engineering And Computer Science”, Volume 6, Issue 3, Mar 2017.



doi crossref
10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY