International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-5, Issue-2, March 2017
DOI: 10.21276/ijircst.2017.5.2.5

Methods for Protection of Key in Private Key Cryptography

NehaTyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav

Abstract - **The susceptible nature of information against forthcoming threats has become a ponderous affair for the professionals of this field. It is a result of the rational and steady struggle by the carrying people that has produced multiple approaches which shields vital information from speculated security attacks. For the everyday users who are unfamiliar of these potential incursion(s) to their intimate information, feel helpless when they encounter persecutor(s) who wish to exploit the confidentiality of this elemental information. Here we have discussed about a distinctive approach which deal with these upcoming attacks. We have tried to produce an algorithm which will safeguard users against objectionable invasion of reserved information. We have incorporated a set of diverse techniques to produce an algorithm which is immune to these incursions. These methods interpolate perceptions like Hybrid cryptography [3], R.S.A. algorithm [1], Key management, Hash functions or Encrypted key exchange.**

Index Terms— **Hybrid cryptography, Security threats, Private Key cryptography, Public key cryptography, Cryptography, Encryption, Key, R.S.A. algorithm.**

I. Introduction

Private key encryption also known as symmetric key encryption is by far the more elementary encryption and hence regarded and known to be uncomplicated in implementation . However, this uncomplicated nature of private key encryption makes it sensitive against these potential incursions made to sabotage the confidentiality of this intimate information.

In our paper “Protection of key in Private Key Cryptography” [1] we deal with the Importance of cryptography and goes with all security issues as well as to improve the pillars i.e. Encryption of plain text and Decryption of cipher text by introducing a new tool that may be called as Hybrid Key Cryptography [3].

Other than this we find out why security is required and how it is widening day by day and why protection of information is required as well as how a secure channel for communication is a vital requirement for cryptography in order to achieve safe and secure communication [2].

Therefore, wehave tried to improve the communication channel in which we have introduced two methods for securing the private key which is send by sender to receiver.

II. Methods

A. Secure Channel

In this method we provide security to the communication channel (provided the key that is used to encrypt the data remains same) and safeguard the communication channel from any invasions that may occur on the channel.

Our main motive in this method is to safeguard the communication channel rather than the key present for the encryption and decryption process. This method is determined to prevent the communication channel from any outside attacks which could compromise the encrypted information being transferred from sender to receiver.

To implement these security measures we may use various methods or algorithms. The most popularly known method is to introduce some identity code which will ensure the sender that the person who is on receiver end is an authorized person. This method can be successful and may ensure the legitimacy of intimate conversation being carried on between the two communicating parties .This code is available to both the communicating parties and allow each of them to generate a reliable means of authentication.

B. Secure Key

In this method we provide security to the key that is used to encrypt the data (provided the channel that is used to transfer the key remains same) and safeguard the communication channel from any invasions that may occur on the channel.

This method focuses on safeguarding the key which is the most important element in the cryptography process. We may try to use ‘Hybrid Encryption’ and ‘Double Encryption’ concept to ensure that the key is secure from persecutors who try to invade private information by retrieving the key. It is a renowned fact that a weak key bogs down even the strongest of the algorithms so here we may try to secure the most important element in the process of cryptography i.e. - The Key.

To perform this method there are many number of prevailing algorithms available. Each of these algorithms

Manuscript received March 10, 2017

NehaTyagi, Assistant Professor, Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

AshishAgarwal, Student (B.Tech.), Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

AnuragKatiyar, Student (B.Tech.), Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

ShubhamGarg, Student (B.Tech.), Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

ShudhanshuYadav, Student (B.Tech.), Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

allows us to provide wide range of security to the key in play. Every algorithm has its own benefits as well as drawbacks and provides a certain value to the key.

The main focus of these methods lies on the perception that with the increase in the complexity of the key it becomes a challenge for the invaders to crack the key. These methods also provide a unique platform for future works that would be done on this perception.

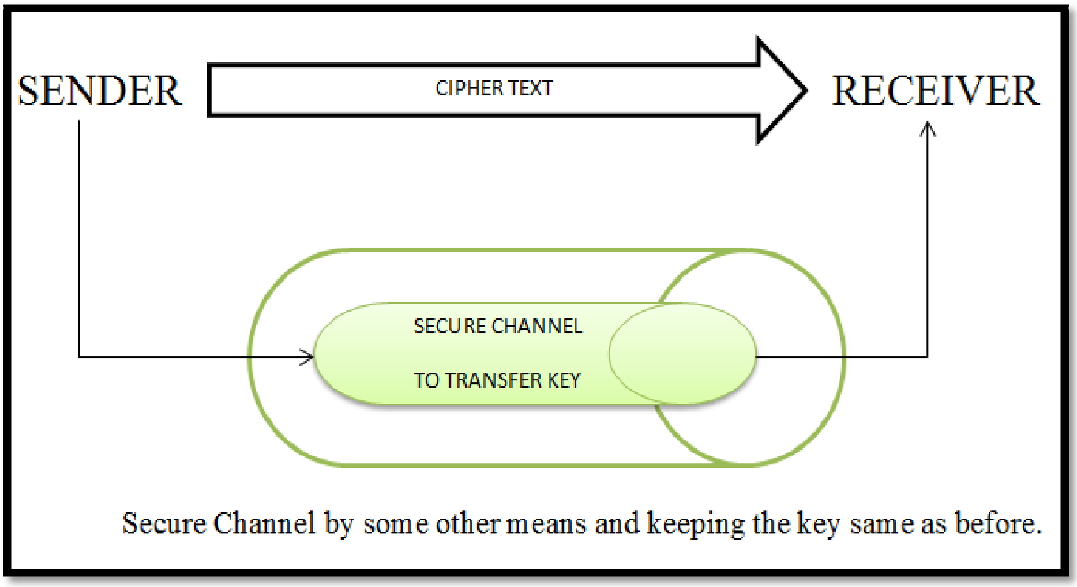
SENDER
CIPHER TEXT
RECEIVER
SECURE CHANNEL
TO TRANSFER KEY
Secure Channel by some other means and keeping the key same as before.

Fig 1: Secure Channel

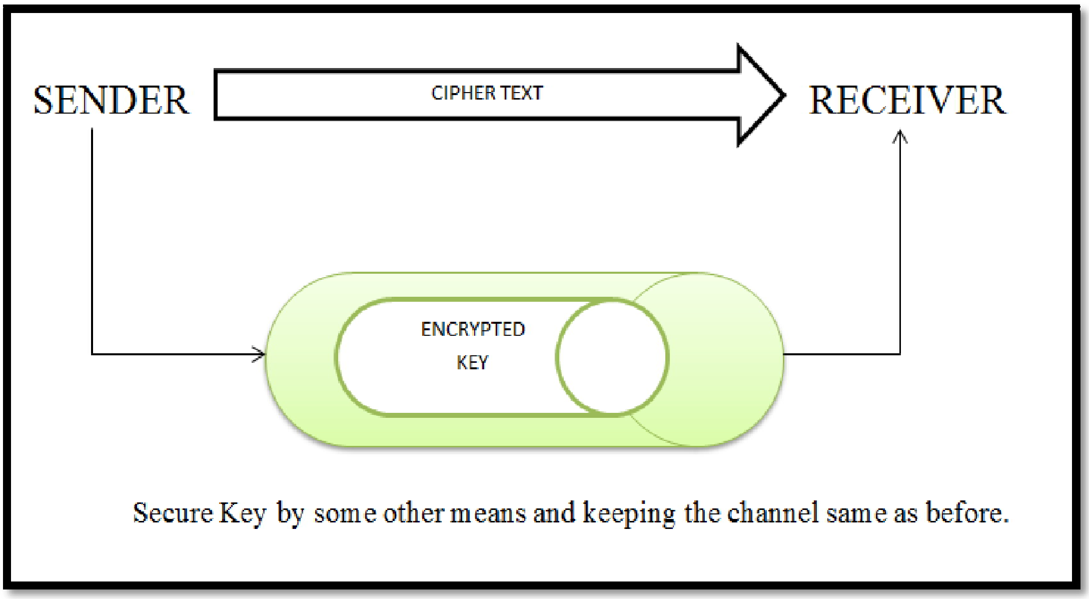
SENDER
CIPHER TEXT
RECEIVER
ENCRYPTED
KEY
Secure Key by some other means and keeping the channel same as before.

Fig 2: Secure Key

III. Further Discussion

The method used inculcates the contemporary concepts of Hybrid Cryptography with a popular encryption technique R.S.A. algorithm. The space and time complexities plays considerable role in success of any code. Increasing the complexity substantially increases the security of information but on the far side implementation of code massively depends on the cryptosystems in play. In order for the method to be popular, we also have to consider the capabilities of systems which are going to act out of the method. All things considered, these two methods have a potential to protect private details and most certainly create a platform on which further work can be implemented. The method in itself hands us an scope to work on as the current framework will face challenges with time and continuous efforts from our side will be made to make it one of the most substantial protection techniques and nearly invincible.

IV. Conclusion

Cryptography field is dealing with a constant surge of new and advance attacks which forces this field to be in a uniform state of evolution. Admitting to the discovery of these extensive attacks with tremendous magnitudes, introduction of techniques which can safeguard us against them becomes paramount especially when everything is travelling the digital road. Induction of new techniques is not obligatory as we can also adopt from the endeavors of professionals in this field. We have tried to remodel and modify the contemporary methods in devising the algorithm which will improve the communication and shield intimate information.

REFERENCES

[1] NehaTyagi, AshishAgarwal, AnuragKatiyar, ShubhamGarg, ShudhanshuYadav, “Protection of Key in Private Key Cryptography” published by “International Journal of Advanced Research”, Volume 5, Issue 2, Feb 2017.

[2] ArpitAgrawal, GunjanPatankar,”Design of Hybrid Cryptography Algorithm for Secure Communication” published by “International Research Journal of Engineering and Technology”, Volume 3 Issue 1, Jan 2016.

[3] Meenakshi Shankar, Akshay.P, “Hybrid Cryptographic Techniques Using RSA Algorithm and Scheduling Concepts” published by ”International Journal of Network Security & Its Application”, Volume 6, Issue 6, Nov 2014.