Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/3207
DOI URL: http://dx.doi.org/10.21474/IJAR01/3207
ISSN NO. 2320-5407

RESEARCH ARTICLE

PROTECTION OF KEY IN PRIVATE KEY CRYPTOGRAPHY.

Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg and Shudhanshu Yadav
G.L. Bajaj Institute of Technology & Management, Plot 2, Knowledge Park 3, Greater Noida, Distt. Gautam Budh Nagar, Uttar Pradesh, India.

Manuscript Info

Manuscript History

Received: 18 December 2016
Final Accepted: 14 January 2017
Published: February 2017

Key words:-
Cryptography, Key, Private Key, Public key, Asymmetric cryptography, Symmetric Cryptography

Abstract

The ever increasing technologies with parallel advancements in the development of notorious attempts, to play with the integrity of the information, in the field of communication over the internet present the need for the equally enhancing security measures. We here, try to analyze the security steps and related phenomena which have been developed specific to the symmetric cryptosystems. With the application of different protocols and their related drawbacks, we try to introduce a few changes, if possible, without diminishing the essence of such protocols. Our attempt is to look for the possibility of introducing asymmetric cryptosystem security measures to meet our purpose. The works already being done are a source of reference to invoke something inquisitive towards our topic. Such works include techniques such as key management, magic rectangle, hash functions, encrypted key exchange, etc.

Introduction:-

Over the years, the topic of cryptosystems and their associated safety has been gathering the attention of the security related departments to safeguard such systems against the attacks; they undergo or may counter in future references. Before we move towards exploring the potential security protocols, we must remember that any cryptosystem primarily is composed of two main processes namely, encryption and decryption respectively. The main idea behind the application of encryption technique is to strengthen any communication system with the security feature of confidentiality and not integrity. The sole idea of confidentiality is to provide the information exchange between authorized parties and restrict the reach of unauthenticated party (ies) to the information.

The various issues concerned regarding the algorithms and protocols for implementing the same are as follows:-

- The process of authorization should be kept intact.
- The private key used by the sender to encrypt data should not be susceptible to a usual guess by the attacker.
- The communication channel being used to transfer the data from sender's end to the receiver's end should be made protected against any suspected cryptanalytic activity.
- There should be a mechanism to monitor the information flow.
- Not just passwords or any usual practice of securing data should be used but some mathematical application should also be looked into.
- The algorithm being used to carry out associated steps must be compatible to the system's configuration.

Corresponding Author:-AshishAgarwal.
Address:-G.L. Bajaj Institute of Technology & Management, Plot 2, Knowledge Park 3, Greater Noida, Distt. Gautam Budh Nagar, Uttar Pradesh, India.

- The techniques of making confidential communication should not be mistaken with the methodologies of keeping integrity of the information.
- Also, our protocols should not violate the rules and regulations as laid by standard organizations.
- The semantics should take care of proper speed and sequencing of data.
- The message should reach the intended receiver located at any part of the world.

There may be some other issues beside the above listed. In order to have glimpse at the utmost need to the safety in terms of security of the information of user, we can take aid of several statistical data being published by respective organizations timely. This will let us understand the need to upgrade the various available security measures with some new updates or design absolutely new methodology to meet the need. The WhatsApp vulnerability to spying of the messages even after the application of end to end encryption using signal protocol, points to the need of continuous and comprehensive enhancements in the technologies that are in use at present. That is the reason for increased interest in pursuing research in the field of network security.

Therefore, it is needed that the techniques available should be able to shield our data with optimum security features without allowing the attackers to play with the connection between sender and receiver. We can use a predictive analysis i.e. a form of advanced analysis that uses both new and historical data to forecast future activity, behavior and trends.

Cryptography:-

It is a technique, using suitable algorithm(s), which deals with the encryption and decryption of the secret information. The method of applying cryptographic techniques classifies it into two categories namely symmetric key cryptography and asymmetric key cryptography.

Symmetric key cryptography, as the name suggests, the key used to shield the information is same and shared between sender and the receiver. We can apply several asymmetric measures or algorithm(s) to enhance the security of this shared key. A key which is used to encrypt & decrypt the information is called *private key* or *secret key* or *shared key* as it is known only to the parties involved in direct communication using the communication channel. The main issue in secret key cryptography is the protection of this shared key. As available algorithm such as *Diffie-Hellman Key Exchange* is used to share a secret key but suffers a drawback as a result of man-in-the-middle attack. RSA algorithm is used to again encrypt this shared key so that it is delivered free of threat, but is still vulnerable to attacks. The main class of attacks being invoked by notorious people to steal away information includes brute force attack. In order to counter such threats, one can definitely look for applying logarithmic complex calculations to generate a factor that would be able to lock our keys. It can be represented as follows:-

Let us suppose shared key:- S
Encryption key by RSA: E

- E -> S i.e. E encrypts S

Now, in order to transmit the information packed in double shield, we may try to apply the binary logic in accordance with mathematical principles in order to guarantee its safe disposal at receiver's end.

The key in symmetric key cryptography can be protected by either of the two stated methods-

- Protecting the channel by applying public key encryption algorithm such as RSA algorithm.
- Applying modified version of RSA algorithm on key before transmission of key in channel.

Asymmetric key cryptography, as the name suggests, two keys are used namely *private key* and *public key*. The message may be encrypted using the public key of receiver and to be decrypted by his/her private key. The most popular asymmetric algorithm in use is RSA algorithm. Its importance can be understood from the fact that it is used even in symmetric key cryptographic systems to render the security to the secret or shared key. It can be represented simply as:-

- Message say, M
- Sender say, S
- Receiver say, R
- Encryption using public key of R say, R''

- Decryption using private key of R say, R' respectively.

Again, we may try to apply different protocols to give this communication a level of security such as image encrypted using PGP i.e. Pretty Good Privacy in somewhat modified manner.

Recently US based security agency i.e. NSA, USA (National Security Agency, United States of America) has identified a problem named 'Going Dark Problem', which they have suggested, could be controlled using split key encryption in which the service provider retains half of the master key and law enforcement would retain other half so that decryption process requires the participation of both the parties. To such problems, we may think to apply protocols already available such as Kerberos but for the receiver's end i.e. whenever information is read, a ticket confirming the retrieval and consisting of the shared piece of identity, is sent to sender.

Future Scope:-

As it can be predicted that the area of information transfer is the one that covers many possibilities to unfold the new methods and protocols for safe communication, meanwhile preserving the confidentiality. Many new techniques have so far been suggested based on research but their implementation relies on the possibilities to counter changing trends. Furthermore we can think to introduce some changes in the functioning of RSA algorithm in order to safeguard against threats in form of attacks. It is not just the protection of information which is necessary but it is equally necessary to identify the attacker. Though, there may be drawbacks to the protocols already in use, we should try out different possibilities in terms of network methodologies.

Conclusion:-

The research area in the field of cryptography and associated security is ever widening, so is equally important to look for modified algorithms and rules governing them. Protecting the information as well as communication channel are the major ways to make any cryptosystem secure and safe in terms of its application to information exchange. The concepts of double encryption or half encryption being talked about and former used also, suggests same that information may be secured at the cost of increasing complexities to the process of communication. Thus it is a challenge to establish a balance between the security measures and the overall cost of the system in terms of time, computation, space, etc.

References:-

1. Hardik Gandhi, Vinit Gupta, "Research on enhancing public key by the use of MRGA with RSA and N-Prime RSA" paper published by "International Journal for Innovative Research in Science & Technology", Volume 1, Issue 12, May 2015.
2. Jyotirmoy Das, "A Study on Modern Cryptography and their Security Issues" published by "International Journal of Emerging Technology and Advanced Engineering", Volume 4, Issue 10, October 2014.
3. Mitali, Vijay Kumar, Arvind Sharma, "A Survey on Various Cryptography Techniques" published by "International Journal of Emerging Trends & Technology in Computer Science" Volume 3, Issue 4, July-August 2014.
4. Swati Kashyap, Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm" published by "International Journal of Advanced Research in Computer Science and Software Engineering" Volume 5, Issue 4, April 2015